Norton Personal Firewall™ for Macintosh® User's Guide

Norton™
Personal Firewall
For Macintosh®

Norton Personal Firewall™ for Macintosh® 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 1.0.2

PN: 07-30-00460

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 accompanying software to you only upon the condition that you accept all of the terms contained in this license agreement. Please read the terms carefully before continuing installation, as pressing the "Accept" button will indicate your assent to them. If you do not agree to these terms, please press the "Decline" button to exit install 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 licensers 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 one copy of the Software 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:

All Symantec products and documentation are commercial in nature. The Software and documentation are "Commercial Items", as that term is defined in 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. §252.227-7014(a)(5) and 48 C.F.R. §252.227-7014(a)(1), and used in 48 C.F.R. §12.212 and 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. §12.212, 48 C.F.R. §252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §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 Boulevard, 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 Boulevard, Cupertino, CA 95014.

C O N T E N T S

How to use a firewall

Chapter 1 About Norton Personal Firewall

Chapter 2 Installing Norton Personal Firewall

Chapter 3 Norton Personal Firewall basics

Chapter 4 Protecting disks, files, and data from intrusion

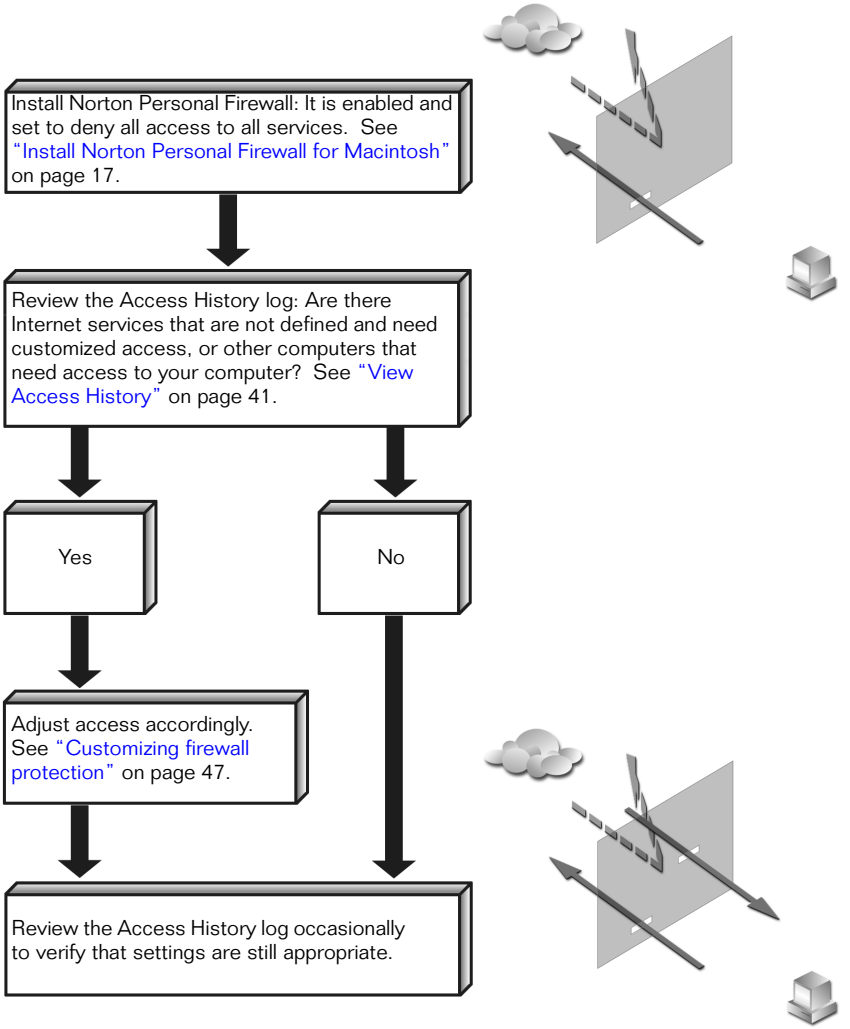
Chapter 5 Responding to access attempts

Chapter 6 Customizing firewall protection

Chapter 7 Troubleshooting in Norton Personal Firewall

Chapter 8 Keeping current with LiveUpdate

How to use a firewall



CHAPTER 1

About Norton Personal Firewall

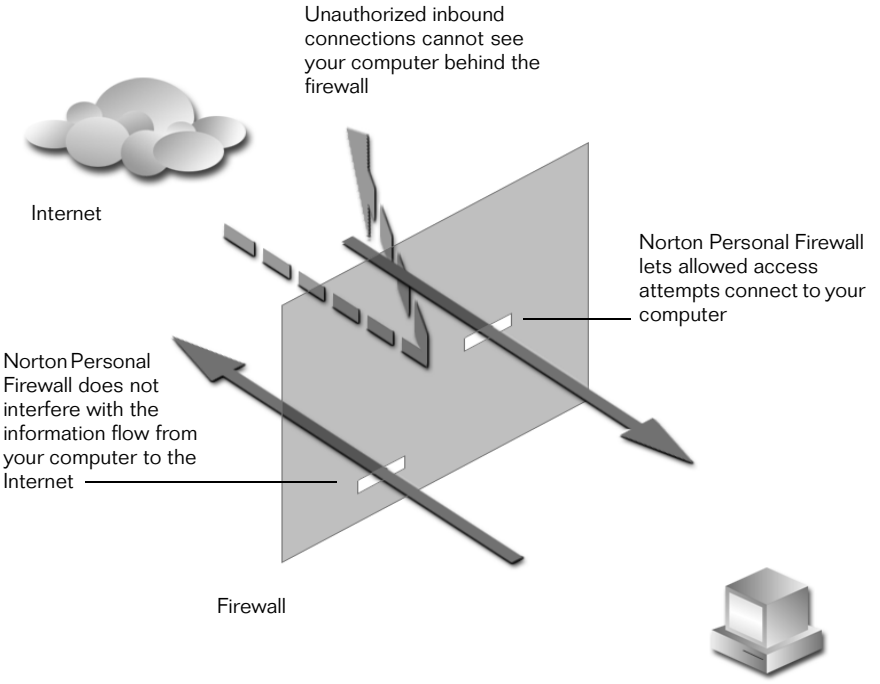
When you connect to the Internet, you can connect with millions of other computers. Those computers can also connect with your computer. Unprotected connections to the Internet leave your computer vulnerable to *hacker* attacks, *viruses*, *Trojan horses*, and many other Internet threats. (Hackers are people who break into computers without permission. Viruses and Trojan horses are programs that can corrupt the data on your computer.)

Norton Personal Firewall helps you monitor and control connections to your computer. It helps protect your security and privacy.

How Norton Personal Firewall works

Norton Personal Firewall provides a *firewall* between your computer and the Internet. Firewall programs are filters that block or allow connections over the Internet. By filtering connections, firewalls protect your computer from malicious Internet activity.

Norton Personal Firewall uses access settings to determine whether to permit or block connections. You can change these settings, permitting or blocking other computers from accessing your computer.



You specify the services that you want to protect (such as Web Sharing or File Sharing) and from which computers. You can allow or deny all access to a particular service, or allow or deny access to a service from certain computers. For example, you can block all access to File Sharing while allowing access to Web Sharing for computers belonging to people you know.

How to determine which computers get access

In most cases, you do not need to allow anyone access to your computer. However, there are certain computer configurations and Web and file sharing situations that require you to allow access.

- You have two or more computers networked, and at least one has Internet access. In this case, every computer with Internet access needs a copy of Norton Personal Firewall installed, with access allowed only to the other computers on the network.
- You have a Web site on your computer to which you want to restrict access. Using Norton Personal Firewall, specify Web sharing access to those whom you want to see your site, such as other family members.
- You are using a free Internet service provider that may require access to a port on your computer to maintain your connection. If the ISP is not granted that access, you lose the service.

When installed, Norton Personal Firewall is set to log all access attempts. You can always check the Access History window to see if someone isn't getting through who should.

For more information, see "Respond to access attempts" on page 40.

What can happen without a firewall

When you are connected to the Internet or another network, others connected to that network can access your computer. This situation can be dangerous if you have enabled file sharing or program linking. The danger comes from people commonly known as hackers.

About hackers

In the programming community, a hacker is someone who explores computers and their capabilities; the term carries no negative connotations. Programmers prefer to refer to malicious hackers as *crackers*. However, in the security community, the word cracker refers to someone who cracks code, not necessarily for malicious reasons. Because the word hacker is more commonly used outside of the programming community to indicate someone who breaks into computers to cause damage, that is the term used in this book.

Hackers access other people's computers for a variety of reasons:

- To obtain information that can be used for their profit or other advantage
- To destroy data or otherwise disrupt processing on the computer
- To prove that they can

There are as many motives for hacking as there are hackers. Assuming that you are safe because you are anonymous is misguided. Hackers don't necessarily care whose computer is attacked. They just look for one that's unprotected.

CHAPTER 2

Installing Norton Personal Firewall

Norton Personal Firewall provides complete intrusion protection for your Macintosh computer. It monitors all Internet connections to and from your computer, logging and alerting you to attempted connections.

Versions of Norton Personal Firewall for both Mac OS 8.1-9.x and Mac OS X are included on the CD. Features and procedures for both versions are nearly identical. Mac OS X-specific text is indicated by shaded text, as in this example.

System requirements

The system requirements are different, depending on whether you are installing Norton Personal Firewall for Mac OS 8.1-9.x or Norton Personal Firewall for Mac OS X.

For Mac OS 8.1-9.x systems

You need the following system configuration to run Norton Personal Firewall for Mac OS 8.1-9.x:

- Macintosh PowerPC processor
- CD-ROM drive
- 24 MB of memory
- 10 MB hard disk for installation

- 3 MB free disk space
- Internet connection
- Macintosh OS 8.1-9.x (8.5 or later for Control Strip functionality)

For Mac OS X systems

You need the following system configuration to run Norton Personal Firewall for Mac OS X:

- G3 or G4 processor
- CD-ROM drive
- 128 MB of memory
- 10 MB hard disk for installation
- Internet connection
- Macintosh OS X

About the CD

Use your Norton Personal Firewall for Macintosh CD to install your software.

The Installer for each version of Norton Personal Firewall is contained in its own folder on the CD, along with installation instructions and a Read Me file specific to that version. The Read Me file contains a summary of what's new and changed in Norton Personal Firewall, along with condensed versions of key procedures and technical tips.

In addition to the Norton Personal Firewall for Macintosh installer folders, there are two other items on the CD:

- SimpleText application: Lets you read the Read Me file in Mac OS 8.1-9.x.
- Documentation folder: Contains this User's Guide in PDF format and installation files for Adobe Acrobat Reader.

Install Norton Personal Firewall for Macintosh

Before installing, make sure you check the Read Me file.

Review Read Me

For late-breaking information and installation troubleshooting tips, see the Read Me file on the CD.

To read the file

1. Insert the CD into your CD-ROM drive.
2. Open the folder for the version of Norton Personal Firewall you are installing.
3. Double-click the Read Me file.

Once you have checked the Read Me file, install Norton Personal Firewall.

Install Norton Personal Firewall for Mac OS 8.1-9.x

If you are installing Norton Personal Firewall in the same location as a copy of Open Door's DoorStop firewall, the DoorStop files will be deleted, but your DoorStop settings will be maintained in Norton Personal Firewall.

To have both Classic and Mac OS X protected, install Norton Personal Firewall for both operating systems. Follow both sets of installation instructions to complete this task. You can install both versions while in Mac OS X. Starting the Norton Personal Firewall Mac OS 8.1-9.x installer in Mac OS X launches Classic.

To install Norton Personal Firewall for Macintosh OS 8.1-9.x

1. Insert the Norton Personal Firewall for Macintosh CD into the CD-ROM drive.

   If the CD window doesn't open automatically, double-click the **CD** icon to open it.
2. In the CD window, open the Install for OS 8.1-9.x folder.
3. Double-click **Personal Firewall Installer**.
4. In the Norton Personal Firewall window, click **Continue**.

5 Click **Accept** to accept the License and Warranty Agreement.

If you decline, the installation is cancelled.

6 Review the Read Me text and click **Continue**.

7 On the Install window, select one of the following:

- Easy Install: For a full installation.
- Custom Install: To select individual components.

8 Confirm the destination displayed or specify a different destination folder to which to install.

9 Click **Install**.

10 Follow the on-screen instructions to complete the installation.

11 Click **Restart**.

For information on what to do next, see "After installation" on page 19.

Install Norton Personal Firewall for Mac OS X

You must have started your computer in Mac OS X and be logged on as an Administrator in order to install the Mac OS X version of Norton Personal Firewall. If you do not know if your logon is an Admin logon, you can check it in System Preferences.

To check your logon type

1 Open System Preferences in Mac OS X.

2 Click **Users**.

Your logon name and type are listed.

Easy Install performs a full installation; there is no Custom Install.

To install Norton Personal Firewall for Macintosh OS X

1 Insert the Norton Personal Firewall for Macintosh CD into the CD-ROM drive.

If the CD window doesn't open automatically, double-click the **CD** icon to open it.

2 In the CD window, open the Install for OS X folder.

3 Double-click **Install Personal Firewall**.

4 In the Norton Personal Firewall window, click **Continue**.

5 Click **Accept** to accept the License and Warranty Agreement.

If you decline, the installation is cancelled.

6 Review the Read Me text and click **Continue**.

7 Confirm the destination displayed or specify a different destination folder to which to install.

If you have set up your computer for several users and want all users to have access to Norton Personal Firewall, you must install it in the Applications folder.

8 Click **Install**.

9 Follow the on-screen instructions to complete the installation.

10 Click **Restart**.

After installation

Now that you've installed Norton Personal Firewall:

- Restart your computer. For more information, see "Restart your computer" on page 20.
- Register your software. For more information, see "Register Norton Personal Firewall for Macintosh" on page 21.
- Check for late-breaking news about your new software by using the Internet link installed in the Norton Personal Firewall folder. For more information, see "Read Late Breaking News" on page 22.

Restart your computer

Clicking Restart at the end of installation restarts your computer in the operating system you were using to install the software. Clicking Quit quits installation without restarting the computer.

To restart your computer in a different operating system

- Click **Quit**.

Reset your computer's startup disk before restarting.

To reset the startup disk from Mac OS 9.1 to OS X

1. On the Apple menu, click **Control Panels > Startup Disk**.
2. Select the folder containing the OS X operating system.
3. Click **Restart**.

   Your computer restarts in Mac OS X.

Changing the startup disk in Mac OS X is done in System Preferences.

To reset the startup disk from Mac OS X to Mac OS 9.1

1. On the Apple menu, click **System Preferences**.
2. Click **Startup Disk**.
3. Click the **Mac OS 9.1** folder.
4. On the Apple menu, click **Restart**.

If you have trouble ejecting the CD after you restart your computer, try one of the following:

- Press the CD-ROM drive's eject button when your Macintosh restart chime sounds.
- On newer Macintosh computers with a slot-loading CD-ROM drive, press the mouse button while starting up to eject the CD.

After you install Norton Personal Firewall and restart your computer, it is protected from intrusion. The Norton Personal Firewall extension loads each time you start your computer and actively protects your computer unless you disable it.

Register Norton Personal Firewall for Macintosh

Using your existing Internet connection, you can register Norton Personal Firewall for Macintosh via the *Internet* (the global network of computers).

If you are running Macintosh OS 8.5 or higher, an icon in the Norton Personal Firewall for Macintosh folder lets you launch your browser and connect to the Symantec software registration page. If you are running an earlier version of Macintosh OS, point your browser to the Symantec Web page.

To register via the Internet

1. Connect to the Internet.

   If you use America Online (AOL) to connect to the Internet, you need to connect to it first. For more information, see "To connect to the Symantec Web site via AOL" on page 23.

2. Do one of the following:

   - If you are using Mac 8.5 or higher, in the Norton Personal Firewall for Macintosh folder, double-click **Register Your Software**.

     Your default Internet browser displays the Symantec Service & Support registration page.

   - If you are using Macintosh OS 8.1, start your browser and navigate to the Symantec Service & Support page:

     www.symantec.com/custserv/cs_register.html

3. On the Service & Support page, click **Norton Personal Firewall for Macintosh**.

4. Select the correct version of the product.

5 Click **Go**.

6 On the registration page for Norton Personal Firewall for Macintosh, type all of the required information.

7 Click **Submit Registration**.

Read Late Breaking News

Norton Personal Firewall for Macintosh installs a Late Breaking News link. Use this link to get the latest information available for your installed software.

To read Late Breaking News

1 Connect to the Internet.

If you use America Online (AOL) to connect to the Internet, you need to connect to it first. For more information, see "To connect to the Symantec Web site via AOL" on page 23.

2 Do one of the following:

- If you are using Mac 8.5 or higher, in the Norton Personal Firewall for Macintosh folder, double-click **Late Breaking News**.

  Your default Internet browser displays the Symantec Late Breaking News Web page for your product.

- If you are using Macintosh OS 8.1, start your browser and navigate to the Symantec Web page:

  http://www.symantec.com/product/home-mac.html

If you connect to the Internet through America Online

If you use America Online (AOL) as your Internet Service Provider (ISP), you must connect to AOL before you go to the Symantec software registration page or view the Late Breaking News.

To connect to the Symantec Web site via AOL

1. Log on to AOL.
2. On the AOL Welcome page, click the AOL Internet browser.
3. Move the AOL browser and any other open AOL windows out of the way.
4. In the Norton Personal Firewall window, do one of the following:
   - Double-click **Register Your Software**.

     Continue with the registration procedure. For more information, see "Register Norton Personal Firewall for Macintosh" on page 21.
   - Double-click **Late Breaking News**.

     Continue with the procedure for reading the news. For more information, see "Read Late Breaking News" on page 22.
5. Disconnect from AOL.

If you need to uninstall Norton Personal Firewall

Use the Norton Personal Firewall CD to remove Norton Personal Firewall from your system.

If you have installed Norton Personal Firewall in both Classic and Mac OS X and want to uninstall it, follow both sets of instructions to complete this task.

To uninstall Norton Personal Firewall from Mac OS 8.1-9.x

1. Insert the Norton Personal Firewall CD into the CD-ROM drive.

   If the CD window doesn't open automatically, double-click the **CD** icon to open it.
2. In the CD window, open the Install for OS 8.1-9.x folder.
3. Double-click **Personal Firewall Installer**.
4. Click **Continue** to progress through the information screens.

5 Click **Accept** to accept the License and Warranty Agreement.

If you decline, the installation is cancelled.

6 In the pop-up list, click **Uninstall**.

7 Select the location from which to uninstall Norton Personal Firewall.

8 Click **Uninstall**.

9 If you have other programs running, click **Continue** to quit the other programs.

10 Click **OK**.

To uninstall Norton Personal Firewall from Mac OS X

1 Insert the Norton Personal Firewall CD into the CD-ROM drive.

If the CD window doesn't open automatically, double-click the **CD** icon to open it.

2 In the CD window, open the Install for OS X folder.

3 Double-click **Install Personal Firewall**.

4 Click **Continue** to progress through the information screens.

5 Click **Accept** to accept the License and Warranty Agreement.

If you decline, the installation is cancelled.

6 In the pop-up list, click **Uninstall**.

7 Select the location from which to uninstall Norton Personal Firewall.

8 Click **Uninstall**.

9 If you have other programs running, click **Continue** to quit the other programs.

10 Click **OK**.

CHAPTER 3

Norton Personal Firewall basics

This chapter provides information about Norton Personal Firewall features and procedures.

How to start and exit Norton Personal Firewall

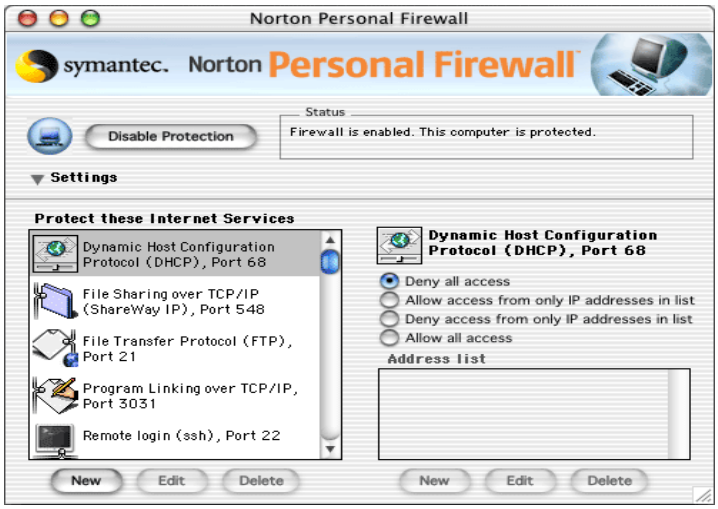
You do not need to start Norton Personal Firewall for your computer to be protected. Protection is enabled upon startup after you have installed Norton Personal Firewall.

To change or test your protection settings or review firewall activity, you need to start Norton Personal Firewall.

To start Norton Personal Firewall

1. Double-click the **Norton Personal Firewall** icon.
2. If the Setup window does not appear, on the Windows menu, click **Setup**.

3 If you cannot see the entire Setup window, click **Settings** to enlarge it.



The first time that you open the Setup window, the protection settings on the right side of the window do not appear. To see the settings for one of the services listed on the left side of the window, select it.

To exit Norton Personal Firewall in Mac OS 8.1-9.x

- On the File menu, click **Quit**.

To exit Norton Personal Firewall in Mac OS X

- On the Personal Firewall menu, click **Quit Personal Firewall**.

For more information

Norton Personal Firewall comes with built-in Help, a Read Me file, and this User's Guide in PDF format.

Access Help

Context-sensitive Help is built into the Norton Personal Firewall application for Mac OS 8.1-9.x.

To access Help

- Click **Help** in any window in Norton Personal Firewall.

  Help appears in a window on your Web browser.

Opening Help in Norton Personal Firewall for Mac OS X displays the Apple Help Viewer with a list of Help topics.

To access Help in Mac OS X

1. On the Help menu, click **Personal Firewall Help**.
2. On the list of Help topics, select a topic to read about it.

Open the Read Me file

The Read Me file on the Norton Personal Firewall for Macintosh CD contains information that was unavailable at the time this User's Guide was published.

To open the Read Me file

1. Insert the Norton Personal Firewall CD into your CD-ROM drive.
2. Open the folder for the version of Norton Personal Firewall that you are installing.
3. Double-click the **Read Me** file.

Access the User's Guide PDF

The *Norton Personal Firewall User's Guide* is available in printable Adobe Acrobat PDF format on the CD. An Adobe Acrobat Reader can be installed if it is not already on your computer.

You cannot view the PDF if you start your computer from the CD, because Acrobat Reader does not run when you start from a locked device.

If you are using Mac OS X, you do not need to install the Adobe Acrobat Reader. You can use Preview in Mac OS X to read the User's Guide PDF.

If you have the Adobe Acrobat Reader installed in Classic, double-clicking the PDF in Mac OS X launches Classic.

To install Adobe Acrobat Reader

1. In the Norton Personal Firewall for Macintosh CD window, open the Documentation folder.
2. Double-click the **Adobe Acrobat Reader installer** icon.
3. Follow the prompts to select a folder for Adobe Acrobat Reader and complete the installation.

To open the PDF

1. In the Norton Personal Firewall for Macintosh CD window, open the Documentation folder.
2. Double-click the User's Guide PDF.

   You can also drag the PDF to your hard disk. It needs approximately 8 MB of disk space.

Disable and enable firewall protection

When Norton Personal Firewall is installed, it is set to deny access to all TCP/IP services. For most users, these settings provide the protection they need without interfering with their work on the computer. You don't need to change any of the settings unless you have specific access rules that you want to define.

You can stop protection at any time by disabling Norton Personal Firewall. For example, you may want to disable Norton Personal Firewall temporarily if you are using *FTP* (File Transfer Protocol). You can disable it for a specified period or until you restart it.

You can disable (or enable) Norton Personal Firewall from two places: the Setup window or the Control Strip (if you have Macintosh OS 8.5-9.x).

To disable or enable Norton Personal Firewall from the Setup window

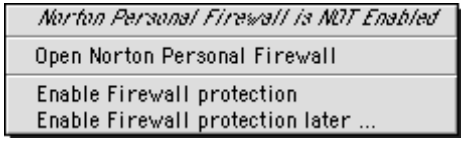
1. Double-click the **Norton Personal Firewall** icon to start Norton Personal Firewall.
2. Do one of the following:
   - Click **Disable Protection**.
   - Click **Enable Protection**.
3. If you chose Disable Protection, verify that you want to disable Norton Personal Firewall.
4. Close Norton Personal Firewall.

Control Strip instructions are not applicable in OS X.

To disable or enable Norton Personal Firewall from the Control Strip

1. Click the **Norton Personal Firewall** module to open the Control Strip menu.

   The current status of Norton Personal Firewall appears as the first line of the menu.
2. Do one of the following:
   - Click **Disable Firewall protection**.
   - Click **Enable Firewall protection**.
3. If you chose Disable Firewall protection, verify that you want to disable Norton Personal Firewall.



Disable Norton Personal Firewall temporarily

You can also use the Control Strip menu to launch Norton Personal Firewall and to disable protection for a specified time period or enable it after a specified time period.

To disable Norton Personal Firewall temporarily

1. Click the **Norton Personal Firewall** module to open the Control Strip menu.
2. Select one of the following:
   - Temporarily disable Firewall protection
   - Enable Firewall protection later
3. Type the number of minutes after which Norton Personal Firewall is to start.
4. Click **OK**.

About Basic and Advanced modes

Norton Personal Firewall has two modes of operation: Basic and Advanced. Basic mode is used to define access to the most commonly used services. Norton Personal Firewall is set to Basic mode by default.

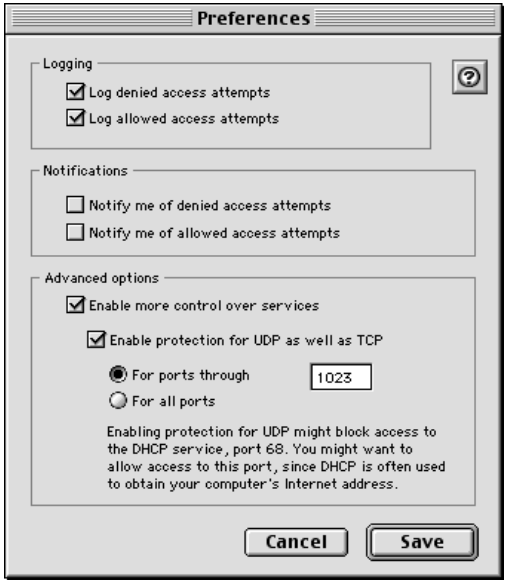
Advanced mode is used when you need to:

- Define access settings for a service not already listed in Norton Personal Firewall.
- Specify a subnet other than your own in a list of IP addresses.
- Extend protection to UDP ports.
- See more information about access attempts.

To change to Advanced mode

1 Do one of the following:

- In Mac OS 8.1-9.x: On the Edit menu, click **Preferences**.
- In Mac OS X: On the Personal Firewall menu, click **Preferences**.



2 Check **Enable more control over services**.

3 Click **Save**.

CHAPTER 4

Protecting disks, files, and data from intrusion

Norton Personal Firewall protects your computer from connections using the access settings you specify. You can allow access for certain computers, listing them by IP address, and you can define additional services to protect on your computer. Norton Personal Firewall tracks all access attempts and works together with AppleTalk to control access.

What Norton Personal Firewall protects

Norton Personal Firewall protects your computer from outside intrusion through *TCP/IP* (Transmission Control Protocol/Internet Protocol) and, optionally, *UDP* (User Datagram Protocol) connections. This means that, while you are connected to the Internet or another network, no computer can access the files, programs, or other information on your computer without your authorization. This authorization is granted to a computer, not to an individual user, so any user on that computer has access.

Norton Personal Firewall cannot be used to control outgoing information. For example, you cannot use it to block connections to objectionable Web sites, nor can you use it to encrypt personal information such as a credit card number that you are providing to a Web site. It also does not block direct *AppleTalk* connections. (AppleTalk is a communications protocol unique to the Macintosh.)

For more information, see "Norton Personal Firewall and AppleTalk" on page 35.

Specify access by IP address

When you allow or deny access for certain computers, you list those computers by their Internet *protocol* (IP) addresses (protocols are sets of rules that govern data transmission). *IP addresses* consist of four numbers from 0 to 255, connected by periods, such as 206.204.212.3. Every computer on the Internet has a unique IP address.

You may not know a computer's IP address, but you know its *host name*, the name that identifies a computer on a network. For example, www.symantec.com is the host name for the Symantec Web site. Host names are converted to IP addresses by the Domain Name System (DNS). You can enter a host name and search for the IP address using Norton Personal Firewall.

IP addresses can be specified individually, as a range beginning with a certain value, or as a range that corresponds to a *subnet*. A subnet is a local area network that is part of a larger intranet or the Internet.

Define protection for port numbers

You can list IP addresses to allow or deny access for each service on your computer. The most common services are already defined on the Setup window for you. For those not listed, you can create an entry in the services list by specifying its name and port number.

Internet services communicate by means of ports, with each service using a unique port number. For instance, Web sharing usually uses port 80, and file sharing over TCP/IP uses port 548. Sometimes services are run on alternate ports. If, for example, two *Web servers* (computers that deliver Web pages to your browser) were running on the same computer, they could not both use the same port number—one of them would be assigned an alternate port number. Specifying protection by port number is useful for creating protection for services not predefined by Norton Personal Firewall, and for creating protection for services that use alternate port numbers.

You can also specify protection for services that use UDP ports. However, this feature is intended for use only by those who understand Internet protocols well, as denying access to the wrong UDP ports can prevent your computer from functioning correctly on the Internet.

Track access attempts

Norton Personal Firewall records complete information about access attempts to your computer. It can log all denied accesses, allowed accesses, or both, and can provide you with immediate notification of allowed or denied accesses.

Norton Personal Firewall and AppleTalk

There are two principal network protocols used on Macintosh computers: AppleTalk and TCP/IP. AppleTalk provides local services that are not available over the Internet such as printing, sharing files with other computers on the same network, and company-specific applications. TCP/IP provides Internet services such as email and access to Web sites. With Mac OS 9, TCP/IP also provides services that have been traditionally available only over AppleTalk, including file sharing and program linking over the Internet or an intranet.

The discussion of Users and Groups and the security defined in Users and Groups does not apply in Mac OS X.

Users and Groups

The Users and Groups file is the major network security component built into the Macintosh operating system. The Users and Groups file (accessed through either the Users and Groups Control Panel or, in Mac OS 9, the File Sharing Control Panel) lets a computer's owner set up user accounts and passwords for access to the computer's built-in network services, and specify which accounts should have access to which services. User accounts are used to limit access to these services through either AppleTalk or TCP/IP. Access to Guests (users without passwords) can also be specified. Services that use Users and Groups security include Program Linking, File Sharing, Web Sharing, and Remote Access (which lets users dial into a particular computer). Access to these services is often configured through their respective Control Panels.

TCP/IP security on Norton Personal Firewall

Norton Personal Firewall adds a level of protection to any application that uses the TCP protocol by granting access only for limited sets of computers on the Internet, based on their IP addresses. This security is independent of the passwords required by Users and Groups. For example, if you have enabled file sharing over TCP/IP, the file sharing passwords created in Users and Groups are not enough for the users to gain access. You must also grant file sharing access for their computers in Norton Personal Firewall. You can either allow all access in Norton Personal Firewall and rely only on the Users and Groups security, or you can allow access only for certain IP addresses, providing two security checkpoints for file sharing access attempts.

AppleTalk and the Internet

When you start Norton Personal Firewall, it warns you if your AppleTalk is using the same port as your Internet connection. If both connections use the same port, it may result in allowing access to your computer over the Internet. If you receive this warning, you should do one of the following:

- Turn off Guest access in Users and Groups.
- Disable AppleTalk while you are connected to the Internet, as Norton Personal Firewall does not protect AppleTalk connections.
- If you are using a product, such as Timbuktu, that provides computer-to-computer access over AppleTalk or TCP/IP, consider disabling the AppleTalk features of the product, as they are not protected by Norton Personal Firewall.

CHAPTER 5

Responding to access attempts

Norton Personal Firewall logs all access attempts, whether they are allowed or denied. Use this log to verify that Norton Personal Firewall is working correctly.

Norton Personal Firewall for Mac OS 8.1-9.x and Norton Personal Firewall for Mac OS X each protect their respective operating systems. When Classic is launched, even if you are not actively working in it, Norton Personal Firewall is protecting it. (Until Classic is launched, it is not vulnerable to access attempts.)

Monitor firewall activity

When Norton Personal Firewall is installed, it is set to log both denied and allowed access attempts. These attempts appear in the Access History window, which you can view at any time.

Norton Personal Firewall for Mac OS 8.1-9.x and Norton Personal Firewall for Mac OS X each monitor and log accesses attempts for their respective operating systems. If you want to check for access attempts in both Classic and Mac OS X, you must check the Access History window in both versions of Norton Personal Firewall.

You may want immediate notification of access attempts under certain circumstances. For example, when you first install Norton Personal Firewall, you may want to evaluate every access attempt to ensure that Norton Personal Firewall is working. You may also want to receive immediate notification if you have changed some settings and want to make sure that they have produced the results you want.

To verify protection settings or changes to those settings before going online, use the Norton Personal Firewall self-test feature. Self-test simulates a TCP connection, logs an access attempt, and triggers a notification if you have enabled that feature. For more information, see "Test firewall settings" on page 38.

Enable or disable notification of access attempts

You can choose to be notified of all denied access attempts, all allowed access attempts, or both. If you have enabled notification, an alert appears every time an access attempt of the kind specified occurs.

For more information, see "Information about alert messages" on page 40.

Enabling or disabling notification has no effect on logging. Also, disabling logging has no effect on notification, although the notification alert will be your only record of the access attempt.

To enable or disable access notification

1. Start Norton Personal Firewall.

   For more information, see "How to start and exit Norton Personal Firewall" on page 25.
2. Do one of the following:
   - In Mac OS 8.1-9.x: On the Edit menu, click **Preferences**.
   - In Mac OS X: On the Personal Firewall menu, click **Preferences**.
3. Specify Notifications options.
4. Click **Save**.

Test firewall settings

Self-test checks firewall protection by simulating access to a service. You can run a self-test in either Basic or Advanced mode. Before beginning, make sure that logging is enabled.

In Basic mode, you can test the services listed in the Setup window, both predefined and custom. The test uses the IP address of your computer. If your computer uses a *PPP* (Point-to-Point protocol) connection and is not currently connected, or if your computer does not have an IP address, self-test uses the IP address 127.0.0.1.

In Advanced mode, you can test an expanded list of services and specify an IP address other than your computer's to use in the test. You may want to enter an IP address that you have listed to be denied access, for example. For more information, see "To change to Advanced mode" on page 31.

Testing with an IP address other than your own computer's is not available in the Mac OS X version of Norton Personal Firewall. The Self Test window in Mac OS X is the same in Basic and Advanced modes.

To see the results of the self-test, view the Access History window. If you have notification enabled for the type of access attempt being tested, the self-test results in an alert. If Norton Personal Firewall is not enabled, access is allowed to all services, which the self-test reflects.

In both Basic and Advanced mode, only TCP services are tested. Protection for a specific UDP service may or may not be the same as the corresponding TCP service, depending on how you have configured Norton Personal Firewall.

To use self-test in Basic mode

1. Start Norton Personal Firewall.

   For more information, see "How to start and exit Norton Personal Firewall" on page 25.
2. On the Windows menu, click **Self Test**.
3. Select a service port.

   The protection defined for the chosen service appears under the service name.
4. Click **Test**.

   The test results appear in Access History.

Advanced mode provides more options in Self Test.

To use self-test in Advanced mode

1 On the Windows menu, click **Self Test**.

2 Specify a service port number.

The protection defined for the chosen service appears under the service name.

3 Select one of the following:

- Test from this computer's IP address
- Test from IP address

If your computer does not have an IP address, Test from this computer's IP address is unavailable.

4 Type an IP address, if applicable.

5 Click **Test**.

Respond to access attempts

View the Access History window occasionally to check for any unusual activity or problem such as denied access for someone who should have access.

Information about alert messages

If you have enabled notification of access attempts, alert messages appear on your screen when access attempts occur.

Alerts contain details of access attempts. If an access attempt seems suspicious, view the Access History window.

To view information on an access attempt in the Access History window

- Double-click an access attempt.

Notification of further access attempts do not occur until the current notification alert is closed. Also, with operating systems earlier than Mac OS 9, processing in other applications may be suspended until the

alert is closed. Do not have notification on with those operating systems if other applications are active and you are away from your computer.

The type of alert you receive depends on which operating system the service being accessed is running. For example, if you have launched Classic, have Web sharing enabled in Classic, and an access attempt is made to Web sharing, you receive an alert from Norton Personal Firewall for Mac OS 8.1-9.x, no matter which operating system is currently active.

View Access History

All logged access attempts appear in the Access History window. Use this log of access attempts to spot potential security violations. When reading it, check for patterns such as:

- Many denied accesses, especially from a common client IP address
- Sequences of port numbers from the same client IP address, possibly indicating a port scan (someone trying many ports on your computer, looking for one that they can access)

It is normal to see some denied access attempts on a random basis (not all from the same IP address, and not to a sequence of port numbers). In some cases, access attempts are made due to activity on your own computer such as connecting to an FTP server and sending email.

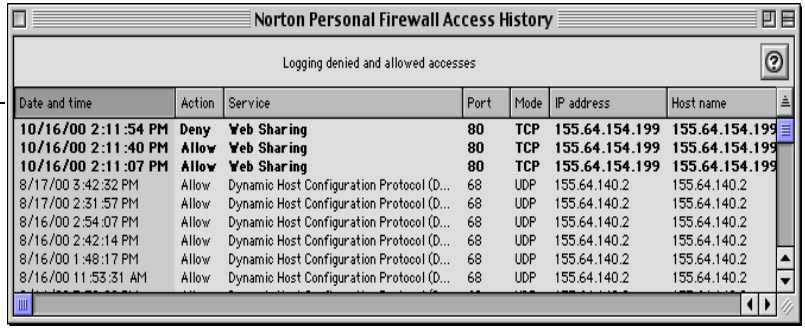
To view the Access History window

1 Start Norton Personal Firewall.

For more information, see "How to start and exit Norton Personal Firewall" on page 25.

2 On the Windows menu, click **Access History**.

Advanced mode format



You can view the Access History window in either Basic or Advanced mode. In Basic mode, the Port, Mode, and IP Address columns are not included.

For more information, see "To change to Advanced mode" on page 31.

Access History contents

The type of accesses being logged appears at the top of the window. The fields included in the window are as follows.

Date & Time	The date and time of the access attempt
Action	Whether the access attempt was allowed or denied
Service	The name, if any, of the Internet service to which access was attempted
Port	The port number to which access was attempted
Mode	The protocol used, either TCP or UDP
IP Address	The IP address of the computer from which access was attempted
Host Name	The host name of the computer from which access was attempted

Access attempts in bold type occurred within the previous 15 minutes.

Sorting columns

By default, lines are sorted by date, with the most recent lines on top.

To sort by column

- Select the column header.

  The header in dark gray is the one currently used for sorting.

Change the sort direction (ascending or descending) by selecting the sorting triangle to the right of the column headers.

Exporting Access History information

The contents of the Access History window can be exported to a tab-delimited text file. The Access History window must be open to export it.

To export the Access History information

1. In the Access History window, on the File menu, click **Export**.
2. In the Export dialog box, specify a location for the file.
3. Type a file name.
4. Click **Save**.

Clearing the Access History window

If the list in the Access History window gets too long, you can clear the window.

To clear the Access History window

1. In the Access History window, on the Edit menu, click **Clear Access History**.
2. Verify that you want to clear Access History.

   This has no effect on the log file; it still contains the access attempts logged to date.

Learn more about a specific access attempt

You can get more information on any entry in the Access History window.

To open the Access Information dialog box

1. In the Access History window, select a line.
2. On the Edit menu, click **Get Info**.

To copy Access History information to the Clipboard for use by another application

- In the Access Information dialog box, click **Copy**.

Accessing the Learn More Web site

The Norton Personal Firewall Learn More Web site displays more details about the access attempt and provides links to other sites that may provide details about the source (the Host Name field) of access attempts.

To open the Norton Personal Firewall Learn More Web site

- In the Access Information dialog box, click **Learn More**.

Change logging preferences

Logging of all access attempts is enabled by default. Keep this setting until you feel confident that your configuration of Norton Personal Firewall is working as you planned. Logging all accesses can create a large log file quickly, so you may eventually want to limit what is being logged.

To change logging preferences

1. Start Norton Personal Firewall.

   For more information, see "How to start and exit Norton Personal Firewall" on page 25.
2. Do one of the following:
   - In Mac OS 8.1-9.x: On the Edit menu, click **Preferences**.
   - In Mac OS X: On the Personal Firewall menu, click **Preferences**.
3. Specify Logging options.
4. Click **Save**.

Disable logging

Logging and service protection are independent of one another. For example, if you are logging allowed accesses and then make Norton Personal Firewall inactive, Norton Personal Firewall continues logging and logs all accesses, since all accesses are allowed. Under certain circumstances, such as when you want to create a new log file, you need to disable logging altogether. Disabling logging has no effect on Norton Personal Firewall protection.

To disable logging

1. Start Norton Personal Firewall.

   For more information, see "How to start and exit Norton Personal Firewall" on page 25.
2. Do one of the following:
   - In Mac OS 8.1-9.x: On the Edit menu, click **Preferences**.
   - In Mac OS X: On the Personal Firewall menu, click **Preferences**.
3. Uncheck the following:
   - Log denied access attempts
   - Log allowed access attempts
4. Click **Save**.

How the log file is structured

The log file is a tab-delimited text file named Norton Personal Firewall Log, located in the Preferences folder on your computer. It is written in an extended WebSTAR log format, which can be read by any word processor or spreadsheet application, or by some log-analyzer applications.

There are separate log files for each version of Norton Personal Firewall. They are stored in the Preferences folder that resides in its respective operating system's System folder.

Access attempts are logged using the following tokens (which are included in the !!LOG_FORMAT line whenever Norton Personal Firewall starts or a new log file is written):

DATE, TIME	Date and time of access in WebSTAR standard format
RESULT	OK for an allowed access; ERR! for a denied access
HOSTNAME	IP address of the client attempting access to the given port
SERVER_PORT	The port to which access is attempted by the given client
METHOD	The protocol used by the access attempt (TCP or UDP)

Exporting the log file to a spreadsheet and sorting the data may make it easier to spot patterns that could indicate a potential security violation. For example:

- Sort by the RESULT field and then by HOSTNAME. In the rows containing ERR! in the RESULT field, look for groupings of IP addresses in the HOSTNAME field. Large numbers of ERR! lines for a given IP address may indicate an attempted security breach.
- Sort by RESULT, then by HOSTNAME, and then SERVER_PORT. In the rows containing ERR! in the RESULT field, look for sequences of port numbers in the SERVER_PORT field that have the same IP address in the HOSTNAME field. Sequences of port numbers from a given IP address may indicate a port scan.

For information on an IP address in the log file (or in a notification alert), refer to the Access History window. For more information, see "To view the Access History window" on page 41.

CHAPTER 6

Customizing firewall protection

As you work with Norton Personal Firewall, you may need to adjust your access settings. For example, you may want to allow file sharing for a colleague working at another location. You may also find a service on your computer that is not listed separately on the Setup window and requires customized protection. You can add that service to the list. You can also extend protection to your computer's UDP ports.

Changes to access settings do not affect computers that are connected to your computer when you make the changes. When the connection is broken, the changes will take effect. For example, if a computer is connected to file sharing on your computer and you deny file sharing access, the computer remains connected until either the user logs off or you explicitly break the connection.

Access settings made in Classic apply only to Classic services. Settings made in Mac OS X apply only to Mac OS X. You must adjust the settings in each version of Norton Personal Firewall as appropriate for the services you have enabled in each operating system.

Set protection for standard Internet services

The Internet services built into the Macintosh OS are defined on the Setup window of Norton Personal Firewall. Services that are not listed are protected using the settings for the All Others service entry. They are all set to deny all access by default. You can change protection settings for any of the services listed.

To get started, open the Setup window. For more information, see "How to start and exit Norton Personal Firewall" on page 25.

For every service listed in the Setup window, you can:

- Deny all access.
- Allow access to addresses in the list.
- Deny access to addresses in the list.
- Allow all access.

These settings are listed in order from most to least restrictive.

To deny or allow all access to a service

1. Select the service to which you want to deny or allow all access.
2. Select the option that you want.

If you deny access to a service that someone is connected to, that change will not take effect until the connection is broken.

To allow or deny access to a list of IP addresses

1. Select the service to which you want to deny or allow access.
2. Select the option that you want.
3. Define the IP addresses to go in the list.

If you deny access to an IP address that is currently connected, that change will not take effect until the connection is broken.

To define a list of addresses to which to allow or deny access

1. Select the Internet service for which you want to define access.
2. Select whether you want to allow or deny access for a list of IP addresses.
3. Click **New** to add an address or range of addresses to the list.

Add IP addresses

Use the first two options in the New Address dialog box to add a single address or range of addresses to the allow or deny access list.

To add a single address

1. In the New Address dialog box, click **Single IP address**.
2. In the IP address field, type the address.
3. Click **OK**.

   The address appears in the list on the Setup window.

When you add a range of addresses, you enter only the beginning of the range. Norton Personal Firewall determines the end of the range based on how much of the beginning IP address you enter.

To add a range of addresses

1. In the New Address dialog box, click **IP Addresses starting with**.
2. In the Base IP address field, type enough of an address to get the range of addresses that you want.

   As you enter each digit of a Base IP address, Norton Personal Firewall determines the end of the range and displays it in the area of the New Address dialog box marked IP address range.
3. Click **OK**.

Search for IP addresses

If you are entering either a single address or a range of addresses, you can search for an address if you know the host name.

To search for an IP address

1. In the New Address dialog box, click **Find**.
2. In the Find IP Address dialog box, type the host name.
3. Click **Find**.
4. Click **OK** to enter the IP address found into the address field of the New Address dialog box.

Add subnet addresses

You can add subnets to your deny or allow access list. In Basic mode, you can specify only your own subnet. The *subnet mask* is filled in automatically. (A subnet mask defines how much of an IP address identifies the subnet.) In Advanced mode, you can specify either your own subnet or a different subnet. If you specify a different subnet, you must also provide its subnet mask.

For more information, see "To change to Advanced mode" on page 31.

To add addresses for your own subnet

1. In the New Address dialog box, click **Subnet**.
2. Click **Use My Subnet**.

   The base IP address and subnet mask for your subnet are filled in automatically.
3. Click **OK**.

When specifying a different subnet, you must enter the entire subnet mask.

To add addresses for a subnet other than your own

1. In the New Address dialog box, click **Subnet**.
2. Type the base IP address and the subnet mask for the subnet into the appropriate fields.
3. Click **OK**.

Define a custom service to protect

To specify access for a service that is not listed on the Setup window, you must define that service in Norton Personal Firewall. You must be in Advanced mode to perform this task.

For more information, see "To change to Advanced mode" on page 31.

To define a custom service

1. On the services list, click **New**.
2. Specify a service port number.
3. Type the name of the service.

   If you have selected a port number from the list, the name of the service appears automatically.

   An icon for the service appears automatically.
4. You can change the icon by copying and pasting the desired icon over the icon in the New Service dialog box.
5. Click **OK**.

   The new service appears in the list on the Setup window. You can now specify access for that service.

For more information, see "Set protection for standard Internet services" on page 47.

Edit or delete a custom service

You cannot edit or delete a predefined service, but you can edit or delete a custom service that you added to the list.

You cannot change the port number by editing the custom service. To change the port number, delete the service and add a new one with the correct port number.

To edit a custom service

1. In the Setup window, select the service that you want to edit.
2. Click **Edit**.
3. In the Edit Service dialog box, change the name of the service or change its icon (by cutting and pasting a new one).
4. Click **OK**.

To delete a custom service

1. In the Setup window, select the service that you want to delete.
2. Click **Delete**.
3. In the Warning box that appears, click **Delete** to verify that you want to delete the service.

Change protection settings

You can make changes to the protection settings for a service at two levels. You can change the level of restriction (for example, from Deny all access to Allow access from only addresses in list) or you can change the list of addresses associated with a restriction level. You make these changes in the Setup window.

If you make a change to a service's protection settings that denies access to someone who is currently connected to that service, the change will not take effect until that person is disconnected from that service, either by logging off or by you explicitly breaking the connection.

Change the level of restriction

You can change the level of restriction for a service at any time.

To change the level of restriction

1 In the Setup window, select the service that you want to change.

2 Select the new restriction option:

- If you are changing to a restriction option that refers to a list of IP addresses, you must create that list.

  For more information, see "Set protection for standard Internet services" on page 47.

- If you are changing to either Deny all access or Allow all access from an option for which you have specified a list of IP addresses, you do not need to delete those addresses. They remain visible but unavailable in the Setup window.

Change an IP address list

For either restriction option requiring an address list, you can add to the list, edit the addresses on the list, or delete addresses from the list on the Setup window.

Before changing a list, make sure that the list you want to change is displayed by clicking the appropriate service.

To add an IP address to a list

1. In the Setup window, click **New**.
2. Add IP addresses as necessary.
3. Click **OK**.

For more information, see "Add IP addresses" on page 49 and "Add subnet addresses" on page 50.

To edit an IP address or range of addresses in a list

1. In the Setup window, select the address or range of addresses.
2. Click **Edit**.
3. In the Edit Address dialog box, make the changes that you want.
4. Click **OK**.

Delete any addresses in a list that no longer apply.

To delete an IP address or range of addresses from a list

1. In the Setup window, select the address or range of addresses.
2. Click **Delete**.
3. In the Warning box that appears, click **Delete** to verify your request.

Ping protection

Ping protection is available only in the Mac OS X version of Norton Personal Firewall.

About Pings

A *Ping* is a request sent to a computer connected to a network for that computer to echo the data back to the computer that sent the request. Pings can be used to determine if a computer exists on a network, how long it takes to get a message to the computer, and the quality of the connection.

Pings can also be used to interfere with your computer's performance. In some cases, if a Ping has more than 64K of data, it can cause a computer to crash. Also, sending many Pings faster than the receiving computer can respond to them can slow the computer and potentially cause it to crash. These deliberate attempts to interfere with your computer's performance are called *denial-of-service attacks*.

Enable Ping protection

You can add Ping protection to the list of services Norton Personal Firewall protects. However, be careful about enabling Ping protection. Unless you have experienced denial-of-service attacks, you may want to leave it disabled, as Pings have legitimate uses on networks and for file sharing.

Norton Personal Firewall protects against ICMP type 8 Ping requests only.

To enable Ping protection

1. Start Norton Personal Firewall.

   For more information, see "How to start and exit Norton Personal Firewall" on page 25.
2. On the Norton Personal Firewall menu, click **Preferences**.
3. Check **Enable Ping Protection**.
4. Click **Save**.

   Ping Protection now appears in the Internet Services list in the Setup window.

Define the level of Ping protection you want. For more information, see "Set protection for standard Internet services" on page 47.

About UDP

User Datagram Protocol (UDP) is a relatively simple protocol used for Internet operations. For example, the Domain Name System (DNS), which translates host names into IP addresses, uses UDP.

There is little reason to protect UDP ports. However, if you have a specific reason for protecting a UDP port, protect it with caution. Denying access to UDP services can cause problems when accessing the Internet.

Enable UDP protection

In most cases, you will want to protect only UDP ports up through 1023. These low-numbered UDP ports are used for standard services such as *DHCP* (Dynamic Host Configuration Protocol, commonly used to obtain a computer's IP address) and NTP (Network Time Protocol, which can be used by the Date & Time Control Panel). Higher-numbered ports are used dynamically by certain UDP services such as DNS. Denying access to

high-numbered ports disables such services, since there is no way to know which port will be used by a given service.

To enable UDP protection

1. Start Norton Personal Firewall.

   For more information, see "How to start and exit Norton Personal Firewall" on page 25.

2. Do one of the following:
   - In Mac OS 8.1-9.x: On the Edit menu, click **Preferences**.
   - In Mac OS X: On the Personal Firewall menu, click **Preferences**.
3. Check the following:
   - Enable more controls over services
   - Enable protection for UDP as well as TCP
4. Specify the range of ports to protect.
5. Click **Save**.

How UDP protection works

Once you enable UDP protection, it works much like TCP protection. Norton Personal Firewall uses the same service list for UDP as it does for TCP. Normally, a service uses either a TCP or a UDP port, but Norton Personal Firewall protects both types of ports for a given service (if UDP protection for that port is active).

One way that UDP protection differs from TCP protection is that UDP is a *connectionless protocol* (does not require a connection to send a message), while TCP is a *connection-based protocol* (requires a connection before sending messages). With TCP, Norton Personal Firewall can allow or deny only the connection attempt, and not the information following the attempt. With UDP, Norton Personal Firewall must allow or deny every piece of information destined for a particular service. Therefore, it cannot block only incoming connection attempts; it must block all communications associated with the service.

Additional differences with UDP relate to logging and notification. With TCP, even if no service is active on a particular port, Norton Personal Firewall is notified of access attempts to that port and can log those access attempts. In general, Norton Personal Firewall is not notified of access attempts to UDP ports that are not active. It will not log or notify on these attempts, nor will the attempts be included in the Access History window.

If you enable UDP protection in Norton Personal Firewall for Mac OS X, it will log the UDP access attempts even if the UDP ports are not active.

Since UDP is connectionless, Norton Personal Firewall logs and notifies on every UDP packet for active ports that it is protecting (if the appropriate options have been configured). You may not want to log allowed accesses if you have enabled UDP protection, due to the number of log entries that could be generated. For example, since DNS uses a UDP port, the log would contain an entry for every time you connected to a Web site.

Even if you only protect lower-numbered UDP ports, you should create specific entries for certain services. For example, if your computer uses DHCP to get its IP address, you may want to specify Allow all (or Allow from addresses in list and enter the DHCP server's IP address) for the DHCP service, port 68. An entry for this service is automatically created by Norton Personal Firewall when you enable UDP protection. For maximum security, access to this service is initially set to Deny all.

CHAPTER 7

Troubleshooting in Norton Personal Firewall

Frequently asked questions

Scan this section for common firewall problems.

How do I turn off firewall protection?

You can turn off firewall protection in two places: the Setup window and the Control Strip menu (on Macintosh OS 8.5 or later).

Norton Personal Firewall works independently in Classic and Mac OS X. To turn it off completely, you must turn off both versions.

To turn off firewall protection in the Setup window

1. Double-click the **Norton Personal Firewall** icon.
2. If the Setup window does not appear, on the Windows menu, click **Setup**.
3. Click **Disable Protection**.

The following Control Strip procedures do not apply to the Mac OS X version of Norton Personal Firewall.

To turn off firewall protection on the Control Strip menu

1. On the Control Strip, click the **Norton Personal Firewall** module to open the menu.
2. Click **Disable Firewall protection**.

You can also use the Control Strip menu to disable Norton Personal Firewall protection for a specified amount of time.

To disable Norton Personal Firewall for a specified amount of time

1. On the Control Strip, click the **Norton Personal Firewall** module to open the menu.
2. Click **Temporarily disable Firewall protection**.
3. Type the number of minutes after which Norton Personal Firewall protection should restart.
4. Click **OK**.

Why can't I download files from a Web site?

You may be using FTP to transfer your files. Many features of the FTP protocol work by having the FTP server open a TCP connection back to your computer and then use that connection as a data port to get data from your computer. The problem is that the port number used for the data port is usually picked at random, which makes it difficult to allow access to the FTP server ahead of time.

To resolve FTP problems, do one of the following

- On the Control Strip menu, click **Temporarily disable Firewall protection**.

  Norton Personal Firewall needs to be off only when a file transfer begins. If you are transferring several files at once, make sure that Norton Personal Firewall stays off until the last file starts downloading. If you are using a computer with Mac OS 8.1 or Mac OS X, use the Setup window to disable and enable Norton Personal Firewall.
- In the All others service entry, allow access from the FTP server (use the IP address from the Access History window).

- If your FTP client application lets you specify a data port, create a service entry for the port that you want to use and allow access for the FTP server.
- If your FTP client application allows the use of passive mode FTP, which does not require a data port, use it. On Mac OS 8.5 and later, on the Advanced tab, set the Internet control panel for passive mode. On Mac OS X, set passive mode in the Network pane in System Preferences.

Why can't I access any Web site?

You have probably enabled UDP protection and have affected a low-level service that your computer needs to perform day-to-day Internet activities. Possibilities include:

- DHCP: Check the TCP/IP control panel to see if your computer is configured to get its IP address using DHCP. If it is, Norton Personal Firewall has created a service entry for DHCP. Edit that service entry to allow the DHCP server access to your computer. Use the DHCP server's IP address from the Access History window.
- DNS: Almost all outgoing Internet operations require DNS, which converts host names to IP addresses. Make sure that you are not blocking the dynamic ports used by DNS (usually ports 32768 or higher).

For more information, see "View Access History" on page 41 and "Add IP addresses" on page 49.

Why doesn't my FTP server work?

If you are running an FTP server on your computer, some clients may have trouble connecting to the server, even though you have allowed access to port 21. If a client is using FTP passive mode, the client may dynamically open a second connection to the server for a data port. Either have the client not use passive mode, or give the client access to the new port being opened by the server.

For more information, see "Define a custom service to protect" on page 50.

Why doesn't my printer work?

You may have turned off AppleTalk in response to the warning that it was using the same port as your Internet connection. To print, turn AppleTalk back on.

What service does this port number represent?

Following are TCP and UDP port numbers commonly used by Macintosh services.

TCP port numbers

Port	Usage	Notes
20	FTP data	Used only as a source port
21	FTP control	
23	Telnet	Common port for attacks
25	SMTP (email)	
53	DNS	Mainly uses UDP, not TCP
70	Gopher	
79	Finger	
80	HTTP (Web)	
88	Kerberos	
105	PH (directory)	
106	Poppass (change password)	
110	POP3 (email)	
111	Remote procedure call (RPC)	Used for many Unix programs
113	AUTH	
119	NNTP (news)	
139	NETBIOS session	Windows access (ASIP 6)
143	IMAP (new email)	
311	AppleShare Web Admin	ASIP 6.1 and later

Port	Usage	Notes
384	ARNS (tunneling)	
387	AURP (tunneling)	
389	LDAP (directory)	
407	Timbuktu 5.2 or later	Previous versions use other ports
427	SLP (service location)	Only uses TCP for large responses
443	SSL (HTTPS)	
497	Retrospect	UDP for finding clients
510	FirstClass server	
515	LPR (printing)	
548	AFP (AppleShare)	
554	RTSP (QuickTime server)	Also uses UDP 6970+
591	FileMaker Pro Web	Recommended alternate to 80
626	IMAP Admin	Apple extension in ASIP 6
660	ASIP Remote Admin	ASIP 6.3 and later
666	Now contact server	Violates actual port assignment
687	ASIP shared U&G port	ASIP 6.2 and later
1080	WebSTAR Admin	WebSTAR port number plus 1000
1417	Timbuktu Control (pre-5.2)	Logon is through UDP Port 407
1418	Timbuktu Observe (pre-5.2)	Logon is through UDP Port 407
1419	Timbuktu Send Files (pre-5.2)	Logon is through UDP Port 407
1420	Timbuktu Exchange (pre-5.2)	Logon is through UDP Port 407
1443	WebSTAR/SSL Admin	WebSTAR port number plus 1000
3031	Program linking (Apple events)	Mac OS 9 and later
4000	Now public event server	
4199	EIMS Admin	
4347	LANsurveyor responders	Uses UDP also

Port	Usage	Notes
5003	FileMaker Pro	Direct access, not through Web; UDP for host list
5190	AOL Instant Messenger	
5498	Hotline tracker	UDP port 5499 for finding servers
5500	Hotline server	
5501	Hotline server	
6699	Napster/Macster client	Used when server is in firewall mode
7070	Real Player	Also UDP ports 6970-7170
7648	CuSeeMe (video)	Client connections; UDP for audio/video
7649	CuSeeMe (video)	Connection establishment
8080	Common HTTP alternate	
19813	4D server	Previously 14566 (6.0 and earlier)

UDP port numbers

Port	Usage	Notes
53	DNS	Sometimes uses TCP
68	Dynamic Host Configuration Protocol (DHCP)	Commonly used to obtain a computer's IP address
69	Trivial File Transfer Protocol (TFTP)	
123	Network Time Protocol	
137	Windows Name Service	
138	Windows Datagram Service	
161	Simple Network Management Protocol (SNMP)	
407	Timbuktu	Handshaking only, prior to version 5.2

Port	Usage	Notes
458	QuickTime TV	
497	Retrospect	Finding clients on the network
514	Syslog	
554	Real Time Streaming Protocol (QuickTime)	
2049	Network File System (NFS)	
3283	Apple Network Assistant	
5003	FileMaker Pro	For obtaining host list
6970 +	QuickTime and RealPlayer	
7070	RTSP alternate (RealPlayer)	

How do I create a new log file?

If your log file is becoming unwieldy due to its size, you may want to start over with a new log file. You do not have to delete the old log file, and can save it for record keeping.

If you do not disable logging before renaming or moving the log file, Norton Personal Firewall continues logging to that file until logging is disabled or the computer is restarted, after which the new file is created.

To create a new log file

1. Start Norton Personal Firewall.

   For more information, see "How to start and exit Norton Personal Firewall" on page 25.
2. Do one of the following:
   - In Mac OS 8.1-9.x: On the Edit menu, click **Preferences**.
   - In Mac OS X: On the Personal Firewall menu, click **Preferences**.
3. Disable logging.

   For more information, see "Disable logging" on page 44.

4 Do one of the following:

- Rename the log file (called Norton Personal Firewall Log).
- Move the log file out of the Preferences folder.

5 Enable logging.

For more information, see "Change logging preferences" on page 44.

Norton Personal Firewall creates a new log file in the Preferences folder.

Why doesn't Norton Personal Firewall load?

There may be an extension conflict if you have many extensions and virtual memory is turned off. Try enabling virtual memory or deleting unneeded extensions.

Why doesn't file sharing work?

You may have enabled file sharing over TCP/IP. By default, all TCP/IP services are initially protected from any access. You must specify access to file sharing before it will be accessible.

Why can't I install Norton Personal Firewall for Mac OS X?

You must be booted in Mac OS X to run the Norton Personal Firewall for Mac OS X installer. You must also be logged on to Mac OS X as an Administrator.

Why can't I create an alias to Norton Personal Firewall?

If Norton Personal Firewall was installed under a different Mac OS X logon than the one you are currently using, you cannot create an alias to it because of the access permissions established in Mac OS X. Have the person who installed the software create an alias and place the alias in an area to which you have access. You can then drag the alias to the desired location.

My entries in IPFW keep disappearing

Norton Personal Firewall writes to IPFW with its own settings. Any entries you make independently in IPFW are overwritten.

Questions about home networking

Scan this section if you have a home network.

How do I protect all of the computers on my home network?

Install a copy of Norton Personal Firewall only on those computers with access to the Internet. If other computers are networked, but do not have Internet access, they do not need Norton Personal Firewall.

All computers connected to an AirPort should have a copy of Norton Personal Firewall installed.

How do I specify access for a computer with a dynamically generated IP address?

Computers that get their IP address from DHCP (Dynamic Host Configuration Protocol) usually don't have the same IP address every time they connect to a network. However, their IP addresses usually fall within a given range. Determine that range by checking the Access History window for denied accesses to that computer and noting the IP addresses used. You can then specify that range in the IP address list for the service for which you need to define access.

For more information, see "To view the Access History window" on page 41 and "To add a range of addresses" on page 49.

How does the firewall affect file and printer sharing?

Norton Personal Firewall provides security for TCP/IP connections. It does not affect AppleTalk connections. If you require that other computers have access to file sharing on your computer through TCP/IP, include their IP addresses in the allow access list for file sharing.

For more information, see "Add IP addresses" on page 49.

CHAPTER 8

Keeping current with LiveUpdate

LiveUpdate updates all Symantec products installed on your computer, as well as its own program files. If you have Norton AntiVirus installed, LiveUpdate also updates the files used by Norton AntiVirus to keep your virus protection current.

Using your existing Internet connection, LiveUpdate connects to the Symantec LiveUpdate server, checks for available updates, then downloads and installs them.

If you have installed Norton AntiVirus in Mac OS X and Classic and want to update features in both versions, you must run LiveUpdate separately in Classic and in Mac OS X to completely update virus protection.

About product updates

Product updates are minor improvements to your installed product, usually available for download from a Web site. These differ from product upgrades, which are newer versions of entire products. Product 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 downloading and installing product updates. It saves you the trouble of locating and downloading files from an Internet site, then installing them, and deleting the leftover files from your hard disk.

About virus definitions

One of the most common reasons for computer virus infections is that you have not updated your protection files regularly. Symantec provides online access to updated virus protection files, called *virus definitions*, by subscription.

Virus definition files contain the latest virus signatures and other technology from the Symantec AntiVirus Research Center (SARC). Updated virus definition files let Norton AntiVirus Auto-Protect and the Norton AntiVirus scanner detect the newest viruses.

The initial subscription is included with the purchase of the product. For more information, see "Subscription policy" on page 80.

About LiveUpdate and Mac OS X

LiveUpdate updates virus definitions and Norton AntiVirus program files for Mac OS X components only. If you have Symantec products installed in Mac OS 9.1 or lower, you must run LiveUpdate in the Classic environment.

In Mac OS X, Norton AntiVirus has a setting that lets OS X remind you to update your virus definitions if the current virus definitions are over one month (30 days) old, or are dated the previous year.

The following alert appears when it's time to update virus definitions:

When should you update?

You should run LiveUpdate as soon as you have installed your product. Once you know your files are up-to-date, run LiveUpdate at least once a month.

If you have Norton AntiVirus, Norton Personal Firewall, Norton Internet Security, or Norton SystemWorks installed, update at least once a month to ensure you have the latest virus definitions and/or firewall protection.

If you are running LiveUpdate in Mac OS 8.x through 9.1, you can set LiveUpdate to run at a scheduled time. For more information, see "Schedule future updates" on page 74.

Before updating

In some cases there are preparations you must make before running LiveUpdate. For example, if you use America Online (AOL) as your Internet Service Provider (ISP), you must log on to AOL before you use LiveUpdate.

If you use America Online to connect

If you use America Online (AOL) as your Internet Service Provider (ISP), you need to log on to AOL before you use LiveUpdate.

To use LiveUpdate with AOL

1. Log on to AOL.
2. On the AOL Welcome page, click the AOL Internet browser.
3. Start LiveUpdate.
4. Follow the procedure from "Update everything now" on page 71.
5. When the LiveUpdate session is complete, close your AOL browser.

   If your LiveUpdate session requires that you restart your computer, disconnect from AOL before restarting.

If you update on an internal network

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

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

If you can't use LiveUpdate

When new virus definitions become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can download new virus definition files from the Symantec Web site.

To download files from the Symantec Web site

1. Start your Internet browser and go to the following site:

   http://www.sarc.com/avcenter/defs.download.html

   If this page doesn't load, go to http://www.sarc.com and click the **Definition Updates** link, then click the **Download Virus Definition Updates** link.
2. On the Download Virus Definitions page, click **Norton Personal Firewall for Macintosh**.
3. Click **Download Updates**.
4. On the Download Updates page, select the file to download.

   Be sure to select files for the appropriate version of your product.

   Information about the update is included with the download.

If you can't access the primary download site

If the page doesn't load, you might have to go to a more general location on the Symantec Web site.

To go to the Symantec AntiVirus Research Center Web site

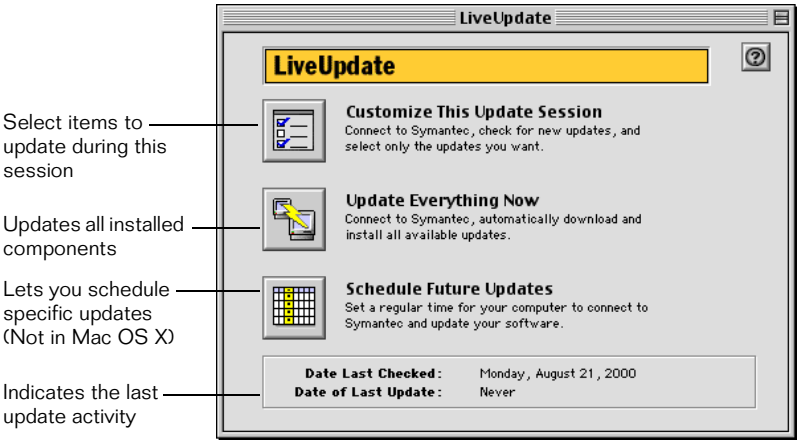
1. Point your browser to the following site:

   http://www.sarc.com
2. Click **Definition Updates**.
3. Click **Download Virus Definition Updates**.

Update procedures

You can have LiveUpdate look for updates to all files at once, or select individual items to update.

In Classic or previous versions of Mac OS, you can schedule a future LiveUpdate session. For more information, see "Schedule future updates" on page 74.



Update everything now

Updating all available files is the fastest method to ensure the latest protection for all your Symantec products.

To update everything now

1. On the SystemWorks main window, click **LiveUpdate**.
2. Click **Update Everything Now**.

   A status dialog box keeps you informed of the file transfer process.
3. If you want to skip a file download, click **Skip File**.

   The file transfer takes a few minutes. When it is complete, LiveUpdate notifies you. For more information, see "View the LiveUpdate Summary" on page 72.

Customize a LiveUpdate session

If you want to update only one or two items, you can select them and omit items you don't want to update.

To customize a LiveUpdate session

1. In the LiveUpdate window, click **Customize This Update Session**.

   LiveUpdate presents a list of available updates. By default, all are checked for inclusion in this update session. If your files are already up-to-date, no items are available for selection.
2. Uncheck the items you don't want to update.
3. Click **Update**.

   The file transfer takes a few minutes. When it is complete, LiveUpdate notifies you. For more information, see "View the LiveUpdate Summary" on page 72.

After updating

When a LiveUpdate session is complete, the LiveUpdate Summary window displays a list of what was updated, along with brief notes. LiveUpdate also downloads a What's New file, which is placed on the Desktop.

View the LiveUpdate Summary

The LiveUpdate Summary dialog box displays a summary of the activity, and a list of products updated in this session.

Some updates require that you restart your computer. When this recommendation appears in the summary description, the Restart button is active.

To restart after a LiveUpdate session

- On the LiveUpdate Summary window, click **Restart**.

Read the LiveUpdate What's New file

LiveUpdate places a What's New file on the Desktop. This contains details of what files were updated by LiveUpdate.

To do this	Follow these steps
Read the What's New file	Double-click the file.
Close the What's New file	Press Command-Q to quit SimpleText.
Delete the What's New file	Drag it to the Trash.

Empty the Trash after a LiveUpdate session

After you update program files with LiveUpdate, there are items in the Trash. LiveUpdate moves the older discarded files to the Trash. If you haven't already restarted after updating, you might get a message that these files are in use. After you restart your computer, you can empty the Trash.

Check product version numbers and dates

LiveUpdate's window displays the version numbers and dates of the most recent updates.

You can also check the version numbers and dates in the product's About box, accessible from the Apple menu.

To view an application's About box

1. Start your product.
2. On the Apple menu, click **About <product name>**.

   The About box lists version number and copyright dates.
3. When you've finished viewing the About box, click **OK**.

Schedule future updates

Scheduling is not available in Mac OS X. If you have Mac OS X and create a scheduled event in the Classic environment, Classic must be running for the scheduled event to occur. If Classic is not running when the event is due to occur, it will occur the next time Classic is launched.

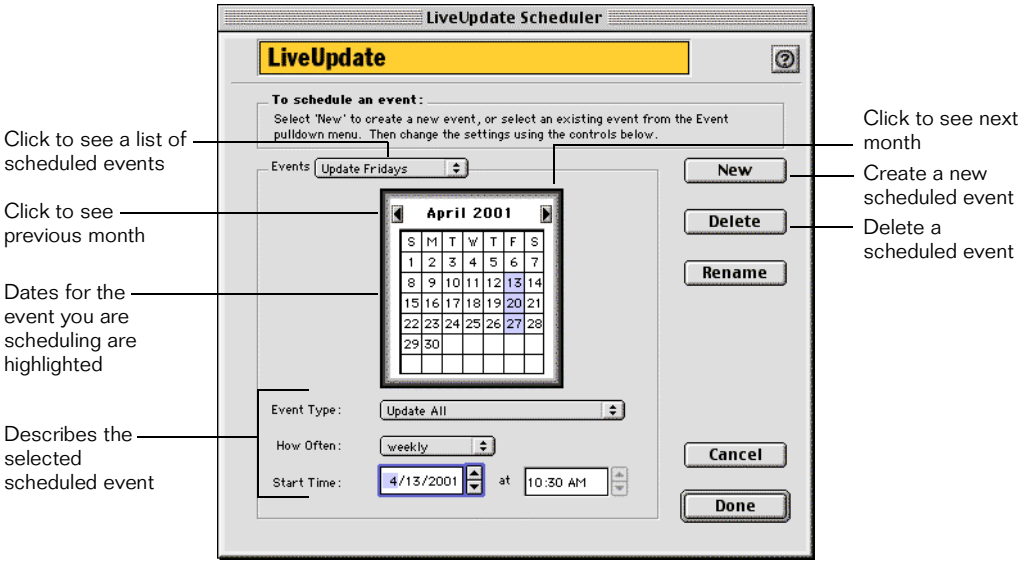
Using the LiveUpdate Scheduler, you can set up events to run at a schedule time, without your participation.

If your Macintosh is turned off during the time an event should take place, the event occurs the next time you start your Macintosh.

Before scheduling an update, test it once manually. For more information, see "Update everything now" on page 71, and "Customize a LiveUpdate session" on page 72.

To schedule future updates

1 In the LiveUpdate main window, click **Schedule Future Updates**.



2 Click **New**.

3 In the Scheduled Event name text box, type a descriptive name (for example, "Update Fridays").

4 Click **OK**.

5 In the Event Type list, specify the item to scan.

Your choices are:

Event Type	Description
Update All	Updates all installed products.
Update <Product Name>	Updates the product you select. The names of installed Symantec products appear on the list.

6 In the How Often list, specify when the update should occur.

Your choices are:

When	Description
once	Runs the event one time only at the indicated time.
daily	Runs the event daily on the indicated day.
weekdays	Runs the event every weekday, Mondays through Fridays, at the indicated time.
weekly	Updates once a week on the specified day and at the specified time.
monthly	Runs the event monthly at the indicated time.
disabled	Never runs the event.

The days on which the updates will occur appear highlighted in the calendar.

7 Finish scheduling the update by typing the time and date:

- Click the Hour text box and use the arrow keys to set the start hour.
- Click the Minute text box to set the start minute.

  This option is not available if the scan occurs at startup or shutdown.

8 Click **Done**.

Edit scheduled events

You can easily make changes to the events you schedule.

To edit a scheduled event

1. On the Tools menu, click **Scheduler**.
2. In the Event list, click the scheduled event you want to change.
3. Make your changes.

   For a description of the scheduling options, see "Schedule future updates" on page 74.
4. To change the event name, click **Rename** and type a new name.
5. Click **Done**.

Delete scheduled events

You can delete events you no longer want.

To delete a scheduled event

1. On the Tools menu, click **Scheduler**.
2. In the Event list, click the scheduled event to delete.
3. Click **Delete**.
4. Click **Done**.

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. Macintosh users can click the About... command on the Apple menu, and then click Info to view Technical Support and Customer Service contact information.

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 (FAQ), 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 then click Go! On the Service & Support page for your product, click Contact Options.

- 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://service.symantec.com 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
U.S.A.

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

Automated Fax Retrieval

(800) 554-4403
(541) 984-2490

Argentina and Uruguay

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

http://www.service.symantec.com/mx
+54 (11) 5382-3802
Fax: +54 (11) 5382-3888

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

http://www.service.symantec.com/br
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032
Fax: +353 (1) 811 8033

Automated Fax Retrieval

+31 (71) 408-3782

Mexico

Symantec Mexico
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

http://www.service.symantec.com/mx
+52 (5) 481-2600
Fax: + 52 (5) 481-2626

Other Latin America

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

http://www.service.symantec.com/mx

Subscription policy

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

When you near the end of your subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your initial subscription ends, you must renew your subscription before you can update your virus, firewall, or web content protection. Without these updates, your vulnerability to attack increases. Renewal subscriptions are available for a nominal charge.

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.

April 20, 2001

Norton Personal Firewall™ for Macintosh®

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	$ 4.95
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

S

T

U

V

W