Norton AntiSpam™ 2004

User's Guide

Norton AntiSpam™ User's Guide

Documentation version 1.0
PN: 10102586

Copyright Notice

Standard Template Library

Trademarks

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Symantec License and Warranty
Norton AntiSpam™

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

1. License:

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

You may:

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

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

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

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

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

You may not:

A. copy the printed documentation that accompanies the Software;

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

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

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

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

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

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

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

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided,

however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit Licensee to obtain and use Content Updates.

3. Product Installation and Required Activation:

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

4. Sixty (60) Day Money Back Guarantee:

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

5. Limited Warranty:

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

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

6. Disclaimer of Damages:

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

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

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

7. U.S. Government Restricted Rights:

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

8. Export Regulation:

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

9. General:

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

Contents

Feature summary

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

This section includes:

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

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

Activation protects you

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

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

When to activate your product

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

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

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

Locate the product key

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

Norton AntiSpam features

As email becomes more popular, many users are receiving an increasing amount of the unsolicited commercial email messages known as spam. Not only does spam make it difficult to identify valid email messages, some spam contains offensive messages and images.

Also, many Web sites are using more aggressive techniques to draw attention to the ads on their pages. Some have begun using larger, more prominent ads, while others rely on ad windows that appear when you enter or leave the site. Along with increasing the amount of time that it takes to display Web pages, some ads contain offensive content, cause software conflicts, or use *HTML* tricks to open additional browser windows.

Norton AntiSpam incorporates several powerful features to reduce your exposure to unwanted online content.

Automatic integration with email programs	Automatically creates a toolbar in supported email programs See "Use your email program toolbar" on page 26.
Allowed and Blocked lists	■ Uses user-defined address list to expedite scanning of email ■ Accepts all mail from Allowed list ■ Treats all mail from Blocked list as spam See "Manage how Norton AntiSpam detects spam" on page 28.
Simplified import of addresses	■ Imports lists of addresses from supported email programs ■ Allows all or selected addresses to be imported See "Identify authorized senders" on page 29.
Self-training	Uses outgoing mail to refine spam definition See "Teach Norton AntiSpam your email preferences" on page 32.

Custom spam rules	Lets you identify email addresses and text that should and should not be filtered See "Customize Norton AntiSpam" on page 56.
Ad blocking	Blocks ads based on user-defined criteria See "Blocking Internet advertisements" on page 61.
Popup blocking	Blocks pop-up windows based on user-defined criteria See "Enable or disable Popup Window Blocking" on page 35.
Live update of spam definitions	Updates copies of Symantec spam definition files automatically (subscription required) See "Keeping current with LiveUpdate" on page 49.

Installing Norton AntiSpam

2

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

System requirements

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

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

Installation of Norton AntiSpam is not supported on Windows 95/NT 4.0, Macintosh, Linux, or server versions of Windows 2000/XP computers.

Your computer must also meet the following minimum requirements.

Operating System	Requirements
Windows 98/98SE/Me	■ 155 MHz or higher processor ■ 32 MB of RAM ■ 70 MB of available hard disk space ■ CD-ROM or DVD-ROM drive ■ Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended)

Operating System	Requirements
Windows 2000 Professional Edition	■ 155 MHz or higher processor ■ 64 MB of RAM ■ 70 MB of available hard disk space ■ CD-ROM or DVD-ROM drive ■ Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended)
Windows XP Professional/Home Edition	■ 300 MHz or higher processor ■ 128 MB of RAM ■ 70 MB of available hard disk space ■ CD-ROM or DVD-ROM drive ■ Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended)

Supported email programs

Norton AntiSpam fully integrates with Microsoft Outlook 2000/XP/2003, Microsoft Outlook Express 5.5 and later, and Eudora 5.0 and later, providing a Norton AntiSpam toolbar for those programs. It is also compatible with most POP3-compatible email programs, including Netscape Messenger 4.X and Netscape Mail 6.0/P.

Scanning of Hotmail email is supported if you are using Hotmail with Microsoft Outlook XP/2003.

Email scanning does not support the following email clients and protocols:

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

About encrypted email connections

Norton AntiSpam does not support email connections using Secure Sockets Layer. Secure Sockets Layer (SSL) is a Netscape protocol designed to provide secure communications on the Internet. If you use an SSL connection to access your email, you are not protected by Norton AntiSpam.

Before installation

Before you install Norton AntiSpam, prepare your computer.

Prepare your computer

Close all other Windows programs before installing Norton AntiSpam. Other active programs may interfere with the installation and reduce your protection.

Install Norton AntiSpam

You can install Norton AntiSpam from a CD or from a file you downloaded.

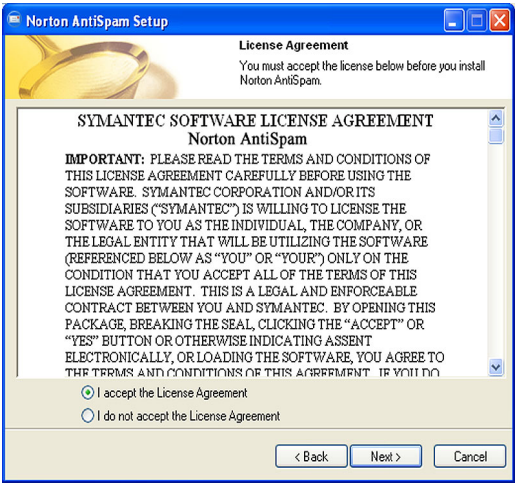
To install Norton AntiSpam

1 Do one of the following:
- If you are installing from a CD, insert the CD into the CD-ROM drive.
- If you downloaded your copy of Norton AntiSpam, double-click the file you downloaded, then click **Install**.

2 In the Norton AntiSpam window, click **Install Norton AntiSpam**.

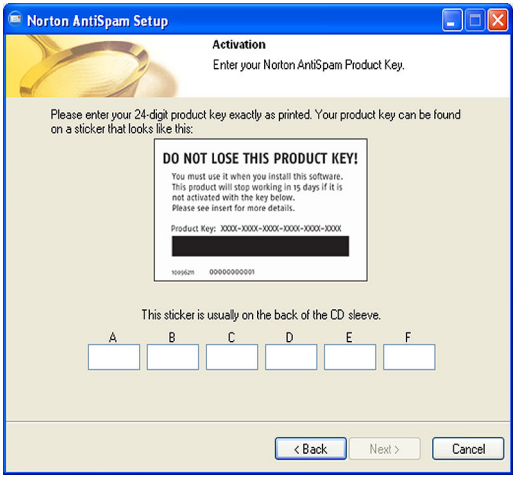
See "If the opening screen does not appear" on page 21.

3 Click **Next**.



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

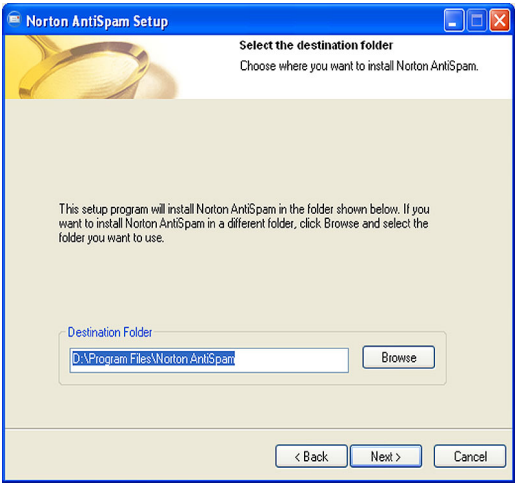
5 Click **Next**.



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

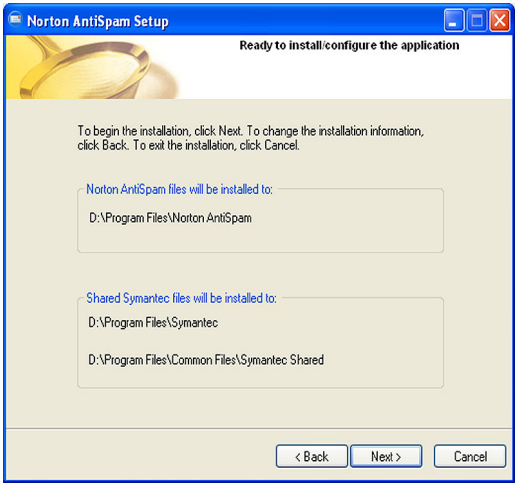
See "When to activate your product" on page 12.

7 Click **Next**.



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

9 Click **Next**.



10 Confirm the installation location, then click **Next** to install Norton AntiSpam.
Depending on your computer system speed, installation can take a few minutes.

11 After Norton AntiSpam is installed, read the readme text, then click **Next**.

12 Do one of the following:

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

13 Click **Finish**.

If the opening screen does not appear

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

To start the installation from the CD

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

After installation

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

Use the Information Wizard

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

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

To use the Information Wizard

1. In the welcome window, click **Next**.
2. If you purchased your computer with Norton AntiSpam already installed, you must accept the license agreement in order to use Norton AntiSpam. Click **I accept the license agreement**, then click **Next**.
3. In the Product Activation window, click **Activate and register your product now**.

See "When to activate your product" on page 12.

You must activate the software within 15 days.

4. Click **Next**.

See "Activate your product" on page 27.

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

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

7 Check if you would like to receive postal mail from Symantec and provide your name and address.

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

9 Select the post-installation tasks that you want Norton AntiSpam to perform automatically. Your options are:

Import Your Email Address Book	Add the people in your email address book to your Allowed List. See "Identify authorized senders" on page 29.
Run LiveUpdate	Ensure that you have the latest security updates. See "Keeping current with LiveUpdate" on page 49.

10 Click **Next**.

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

12 Click **Finish**.
If you selected any post-installation tasks, they start automatically.

If you need to uninstall Norton AntiSpam

If you need to remove Norton AntiSpam from your computer, you can use the Add/Remove Programs option in the Windows Control Panel, or the Uninstall Norton AntiSpam option on the Windows Start menu.

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

To uninstall Norton AntiSpam from the Windows Control Panel

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
   - On the Windows XP taskbar, click **Start** > **Control Panel**.
2. In the Control Panel, double-click **Add/Remove Programs**.
3. In the list of currently installed programs, click **Norton AntiSpam**.
4. Do one of the following:
   - In Windows 2000/Me, click **Remove**.
   - In Windows 98, click **Add/Remove**.
   - In Windows XP, click **Change**.
5. Click **Yes** to confirm that you want to uninstall the product.
6. Click **Finish**.
7. In the Installer Information dialog box, click **Yes** to restart your computer.
8. In the Application Maintenance window, click **Remove**.

Basics

3

Basics include general information about how to:

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

Check the version number

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

To check the version number

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

Start Norton AntiSpam

After installation, Norton AntiSpam automatically begins filtering your incoming email. You do not have to start the program to be protected. However, to update and customize your protection, you will want to do so.

To start Norton AntiSpam

❖ Do one of the following:

- On the Windows taskbar, click **Start** > **Programs** > **Norton AntiSpam** > **Norton AntiSpam**.
- On the Windows XP taskbar, click **Start** > **More Programs** > **Norton AntiSpam** > **Norton AntiSpam**.
- On the Windows desktop, double-click **Norton AntiSpam**.
- From within a supported email program, click **Open Norton AntiSpam**.

Use your email program toolbar

Norton AntiSpam adds a button or buttons to the toolbar of supported email programs. If a single Norton AntiSpam button is added, it drops down an abbreviated Norton AntiSpam menu. The buttons or menu options added are as follows:

This is Spam	Marks the selected email as spam
This is not Spam	Marks the selected email as allowed (not spam)
Empty The Spam Folder	Removes all email that has been placed in the Norton AntiSpam folder
Open Norton AntiSpam	Displays the Norton AntiSpam main window

Activate your product

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

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

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

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

To activate your product from the Activation Needed alert

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

To activate your product from the Help menu

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

Manage how Norton AntiSpam detects spam

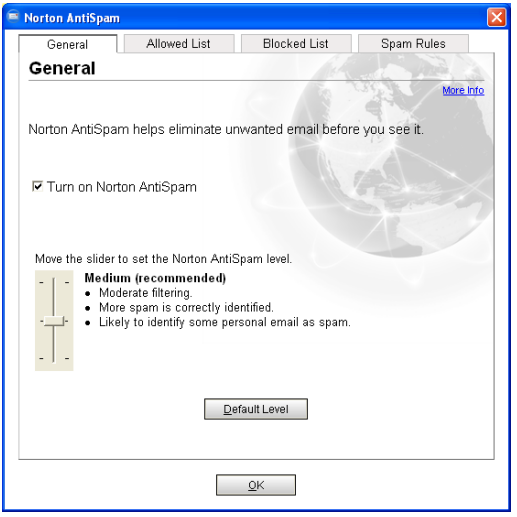
Norton AntiSpam begins filtering email as soon as it is installed. If you are using a supported email program, it will also be available from within that program after installation.

Adjust the email filter

You can determine how strictly Norton AntiSpam filters your email. Adjust the Norton AntiSpam parameters from the main window.

To adjust the email filter

1 In the main window, double-click **AntiSpam**.



2 In the General window, ensure that Turn on Norton AntiSpam is checked.

See "Turn off Norton AntiSpam" on page 36.

3 Use the Norton AntiSpam slider to control how Norton AntiSpam filters email. Your options are:

High	Maximum filtering. Most spam is correctly identified. More likely to identify personal email messages as spam.
Medium (recommended)	Moderate filtering. More spam is correctly identified. Likely to identify some personal email messages as spam.
Low	Light filtering. Some spam is correctly identified. Rarely identifies personal email messages as spam.

4 Click **OK**.

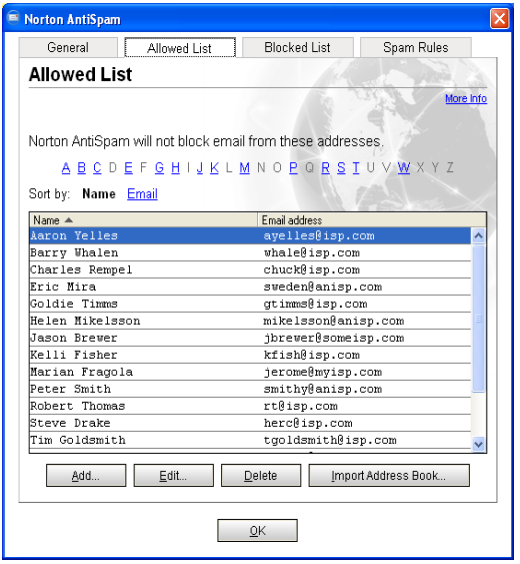
Identify authorized senders

To tell Norton AntiSpam that you want to receive email from a given address, add it to the Allowed list.

If you did not import your email address book to your Allowed list during installation, you can do so at any time after installation. You can import some or all of the addresses. You can also add names to the Allowed list individually.

To import your existing address book

1 In the main window, double-click **Allowed List**.



2 In the Allowed List window, click **Import Address Book**.

3 In the Import Address Book window, uncheck any addresses that you do not want to add to your Allowed list.

4 Click **OK**.

5 Click **OK** to close the Allowed List window.

To add names to your allowed list

1 In the main window, double-click **Allowed List**.

2 In the Allowed List window, click **Add**.

3 In the Add Address to Allowed List dialog box, type the email address you want to allow and, optionally, the first and last name of the sender.

4 Click **OK** to close the Add Address to Allowed List dialog box.

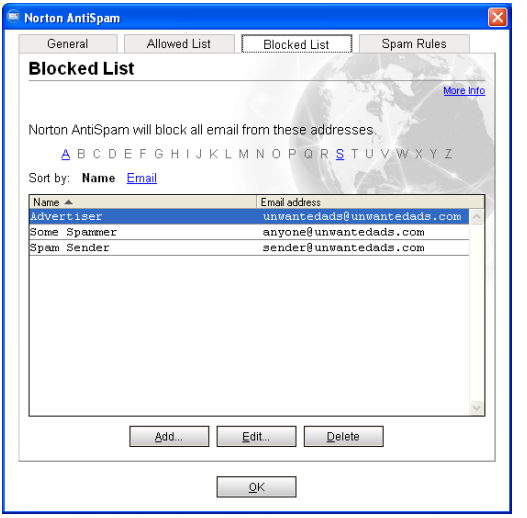
5 Click **OK** to close the Allowed List window.

Identify senders of spam email messages

When you know that you do not want to receive any email messages from a specific address, you can add it to the Blocked List. Norton AntiSpam will mark all email messages from this address as spam.

To add names to the Blocked List

1 In the main window, double-click **Blocked List**.



2 In the Blocked List window, click **Add**.

3 In the Add Address to Blocked List dialog box, type the email address you want to block and, optionally, the first and last name of the sender.

4 Click **OK** to close the Add Address to Blocked List dialog box.

5 Click **OK** to close the Blocked List window.

Teach Norton AntiSpam your email preferences

Norton AntiSpam's filtering engine attempts to identify spam automatically by using your outgoing email to determine your usual email correspondents. Over time, you can train Norton AntiSpam to reflect your personal preferences for receiving email more precisely.

To train the filtering engine

1. Start your email program.
2. Select each item that should have been marked as spam.
3. Using the buttons added to your email program by Norton AntiSpam, click **This is Spam**.
4. If you have set your options to ask before adding senders to the Blocked List, answer the prompt accordingly.

See "About Email options" on page 46.

5. Open the **Norton AntiSpam** folder.
6. Select each item that should not have been marked as spam.
7. Using the buttons added to your email program by Norton AntiSpam, click **This is not Spam**.
8. If you have set your options to ask before adding senders to the Allowed List, answer the prompt accordingly.
9. Close your email program.

Manage advertising filters

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

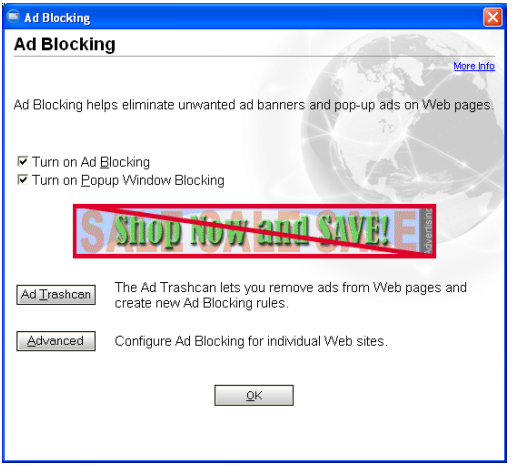
Enable or disable Ad Blocking

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

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

To enable or disable Ad Blocking

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



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

3 Click **OK**.

Enable or disable Popup Window Blocking

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

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

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

To enable or disable Popup Window Blocking

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

Turn off Norton AntiSpam

By default, Norton AntiSpam remains active once it is installed. If for any reason you want to temporarily disable it, you can turn it off from within the program itself.

To turn off Norton AntiSpam

1. In the main window, click **AntiSpam**.
2. On the right side of the main window, click **Turn Off**.

To turn on Norton AntiSpam

1. In the main window, click **AntiSpam**.
2. On the right side of the main window, click **Turn On**.

Monitor Norton AntiSpam

Norton AntiSpam maintains records of every action that the program takes. You should periodically review this information to spot potential problems.

There are three sources of Norton AntiSpam information:

Status & Settings window	Basic information about which protection features are active
Statistics window	Information about recent activity
Event Log	Internet activities and any actions Norton AntiSpam has taken

View the Statistics window

The Statistics window provides a quick way to check the number of email messages that Norton AntiSpam has blocked and the proportion of good email messages to spam.

To view the Statistics window

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

Reset information in the Statistics window

You can clear the statistics manually. This helps you see if a configuration change affects the statistics.

To reset information in the Statistics window

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

View Norton AntiSpam logs

Norton AntiSpam contains detailed information about the actions the program has taken to protect you from unwanted online content.

To view Norton AntiSpam logs

1. In the main window, click **Statistics**.
2. In the Statistics window, click **Log Viewer**.
3. In the left pane of the Log Viewer, click a log's title to view its contents.

For more information

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

Look up glossary terms

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

Use online Help

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

To use online Help

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

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

Window and dialog box Help

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

To access window or dialog box Help

❖ Do one of the following:
- In the window, click any available Help link.
- In the dialog box, click **Help**.

Readme file

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

To read the Readme file

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

Access the User's Guide PDF

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

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

To install Adobe Acrobat Reader

1. Insert the CD into the CD-ROM drive.
2. Click **Browse CD**.
3. In the CD window, double-click the **Manual** folder.
4. Double-click the program file.
5. Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

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

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

To read the User's Guide PDF from the CD

1. Insert the CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Manual** folder.
4. Double-click **NAS.pdf**.

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

To read a User's Guide from your hard disk

1. Open the location into which you copied the PDF.
2. Double-click the PDF.

Symantec products on the Web

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

To access the Web site from the Help menu

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

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

To access the Symantec Web site in your browser

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

Subscribe to the Symantec Security Response newsletter

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

To subscribe to the Symantec Security Response newsletter

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

Options

4

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

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

Set Norton AntiSpam options

The default settings for Norton AntiSpam provide a safe, automatic, and efficient way of protecting your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply.

To change settings for individual features

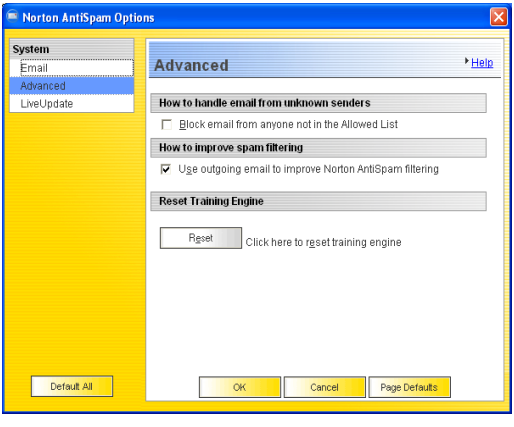
1. In the main window, do one of the following:
   - Double-click a feature you want to customize.
   - Select a feature, then in the lower-right corner of the window, click **Configure**.
2. Make the desired changes.
3. When you are done making changes, click **OK**.

To set global options

1. In the main window, click **Options**.
   If a menu appears, click **Norton AntiSpam**.
2. On the tab for the options you want to change, make the desired changes.
3. Click **OK**.

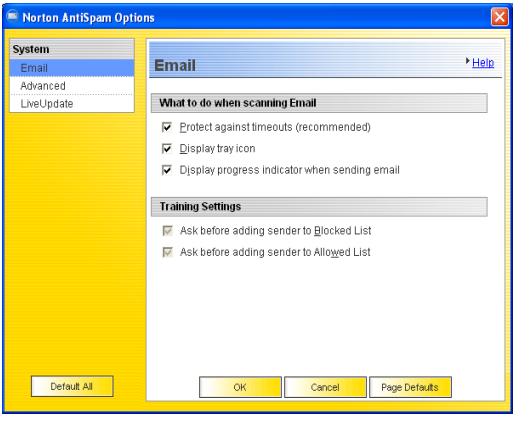
About Advanced options

Advanced options let you control whether Norton AntiSpam accepts email messages from unknown senders and whether it uses your outgoing email messages to improve its spam filtering.



About Email options

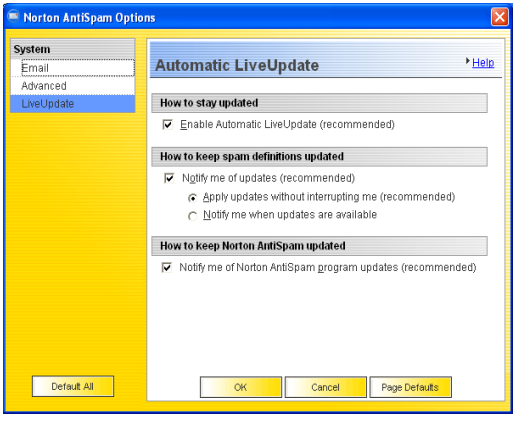
Email options let you control how Norton AntiSpam notifies you when it is scanning email messages for spam.



About LiveUpdate options

See "Keeping current with LiveUpdate" on page 49.

LiveUpdate options let you enable and disable Automatic LiveUpdate and specify how you want to be notified of updates. Automatic LiveUpdate automatically checks for Norton AntiSpam updates when you are connected to the Internet. For maximum security, you should leave Automatic LiveUpdate enabled.



Keeping current with LiveUpdate

5

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

Your normal Internet access fees apply when you use LiveUpdate.

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

About program updates

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

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

About protection updates

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

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

Obtain updates using LiveUpdate

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

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

To obtain updates using LiveUpdate

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

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

When you should update

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

If you can't use LiveUpdate

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

To obtain updates from the Symantec Web site

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

Set LiveUpdate to Interactive or Express mode

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

To set LiveUpdate to Interactive or Express mode

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

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

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

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

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

6 Click **OK**.

Turn off Express mode

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

To turn off Express mode

1 On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.

2 In the Control Panel window, double-click **Symantec LiveUpdate**.

3 In the LiveUpdate Configuration dialog box, on the General tab, click **Interactive Mode**.

4 Click **OK**.

About your subscription

See "About protection updates" on page 50.

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

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

Blocking unwanted email messages

6

Norton AntiSpam uses a pattern-matching engine that automatically compares the contents of incoming email messages to a list of spam characteristics. If the message contains many spam characteristics, it is more likely to be spam than a message that contains few spam characteristics. Based on this analysis, Norton AntiSpam estimates the likelihood that the message is spam.

See "Manage how Norton AntiSpam detects spam" on page 28.

Norton AntiSpam uses the settings you've chosen to determine which messages are marked as spam. If Norton AntiSpam is set to Low, messages must contain many spam characteristics before they are flagged as spam. If Norton AntiSpam is set to High, messages that contain only a few spam characteristics are flagged.

Some email servers use *SSL (Secure Sockets Layer)* connections to encrypt connections between your computer and the server. Norton AntiSpam cannot scan email messages received via SSL connections.

Create spam filters

When a message is identified as spam, Norton AntiSpam appends Norton AntiSpam: to the beginning of the message's subject. You can then use your email program to create filtering rules for all email messages containing this text if you so desire.

If you use Microsoft Outlook Express, Microsoft Outlook, or Eudora, you do not need to create spam filters.

To avoid losing legitimate email messages, use your email program to create a Norton AntiSpam folder. If your email program includes the ability to direct email messages to selected folders, set the program to sort all messages marked with Norton AntiSpam into this folder and periodically review the messages before deleting them. Consult your email program's documentation for more information about creating folders.

To create spam filters for unsupported email programs

1. Start the email program.
2. Create a new folder in which suspect email messages will be stored.
3. Select the rules function.
4. As the search criteria, type **Norton AntiSpam**.
5. Indicate the message's subject line as the part of the email message to search for this criteria.
6. Indicate that email messages that meet the search criteria should be moved to the suspect mail folder.
7. Click **OK**.

These steps describe the general process. The specific steps will vary in each email program.

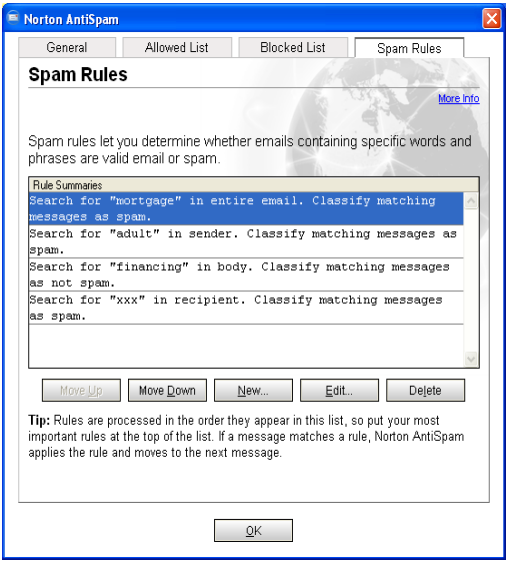
Customize Norton AntiSpam

Customize your protection by identifying email addresses and particular text strings that should and should not be filtered. When Norton AntiSpam encounters a message containing one of these addresses or text strings, it immediately categorizes the message based on your settings. This helps ensure that messages from trusted senders do not get marked as spam.

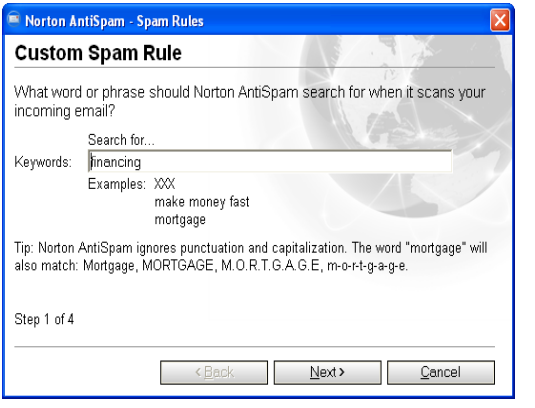
To add a new Norton AntiSpam entry

1 In the main window, double-click **AntiSpam**.

2 In the Norton AntiSpam window, click **Spam Rules**.

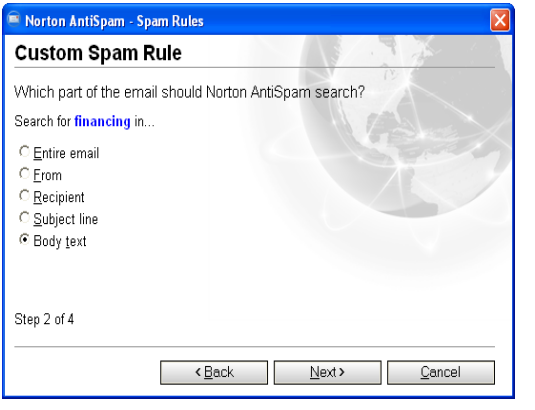


3 In the Spam Rules window, click **New**.

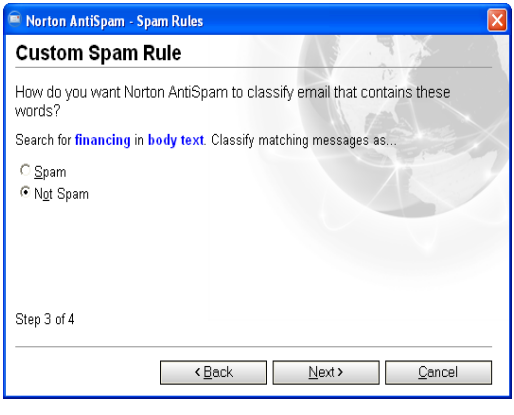


4 In the Search for text box, type an address or a text string.

5 Click **Next**.



6 Select where in incoming email messages Norton AntiSpam should search for the text. Your options are:
   - Entire email
   - From (sender's name)
   - Recipient
   - Subject line
   - Body text
7 Click **Next**.



8 Under Classify matching messages as, choose whether messages that include this text are spam or not spam.
9 Click **Next**.
10 Click **Finish**.
11 Click **OK** to close the Spam Rules window.

Modify or delete a Norton AntiSpam entry if it is causing messages to be incorrectly classified.

To modify or delete a Norton AntiSpam entry

1. In the main window, double-click **AntiSpam**.
2. In the Norton AntiSpam window, click **Spam Rules**.
3. In the Spam Rules window, select the Norton AntiSpam entry with which you want to work.
4. Do one of the following:
   - Click **Edit** to change the entry, and follow the same steps as adding an entry.
   - Click **Delete** to delete the entry.
5. Click **OK** to close the Spam Rules window.

Change the priority of a spam rule

When Norton AntiSpam compares an email message to the list of spam rules, it starts with the rule at the top of the list, then continues down the list until it finds a match. When a match is found, Norton AntiSpam categorizes the email message accordingly and moves to the next message. If you find that the spam email messages you receive tend to match one rule more than the others, you may want to move that rule to the top of the list.

To change the priority of a spam rule

1. In the main window, double-click **AntiSpam**.
2. In the Norton AntiSpam window, click **Spam Rules**.
3. Select the rule that you want to move.
4. Do one of the following:
   - Click **Move Up** to make the rule a higher priority.
   - Click **Move Down** to make the rule a lower priority.
5. Click **OK**.

Blocking Internet advertisements

7

When Ad Blocking is enabled, it transparently removes:

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

How Ad Blocking works

Ad Blocking detects and blocks ads based on two criteria: their dimensions and their locations.

Block by dimensions

Most online advertisers use one or more standard sizes for their ads. Ad Blocking includes the ability to block images and other *HTML* elements that have the same dimensions as these common ad sizes.

Block by location

Every file on the Internet has a unique address or URL (uniform resource locator). When you view a Web page, your computer connects to the address you request and displays the file that is stored there. If the page includes graphics, audio files, and other multimedia content, your browser displays the files as part of the page.

When you go to a Web page that includes an ad, the instructions used to display the page might include the following:

<p>Greetings from the Uninvited Ads company<img src="http://www.uninvitedads.com/nifty_images/image7.gif">

Your browser displays the text Greetings from the Uninvited Ads company on the screen. Then it connects to www.uninvitedads.com and requests a file called /nifty_images/image7.gif. (The suffix .gif indicates that this is a Graphics Interchange Format file, a common image file format.) The computer at www.uninvitedads.com sends the file to the browser, which displays the image.

When Ad Blocking is enabled and you connect to a Web site, it scans Web pages and compares their contents to two lists:

See "Keeping current with LiveUpdate" on page 49.

- A default list of ads that Ad Blocking blocks automatically. Use LiveUpdate to keep the list of blocked ads current.
- A list that you create as you block specific ads. You can add to and change this list.

See "Enable or disable Ad Blocking" on page 34.

If the page includes files from a blocked *domain*, Ad Blocking removes the link and downloads the rest of the page.

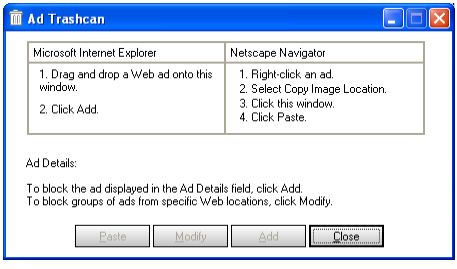
Use the Ad Trashcan

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

To use the Ad Trashcan

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

5 Click **Ad Trashcan**.
The Ad Trashcan window appears.



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

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

8 Click **Close**.

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

Use text strings to identify ads to block or permit

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

Ad Blocking provides a predefined (Defaults) Ad Blocking list that is used to determine which images should be blocked when displaying Web pages.

When Ad Blocking is enabled, all Web pages are scanned for the HTML strings specified in the (Defaults) list. Ad Blocking looks for the blocked strings within HTML tags that are used to present advertising. The HTML structures that contain matching strings are removed from the page by Ad Blocking before the page appears in the Web browser.

Make sure that what you place in the (Defaults) block list isn't too general. For example, www by itself is not a good string to block because almost every URL includes www. A string like www.uninvitedads is more effective because it only blocks graphics from the uninvitedads *domain* without affecting other sites.

How to identify Ad Blocking strings

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

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

Blocking all images on a particular site may make that site unusable. A good compromise is to block only the directories that contain ads. For example, if

www.uninvitedads.com stores its ads in /nifty_images/ and its navigational images in /useful_images/, you could block www.uninvited.com/nifty_images/ without seriously impeding your ability to use the site.

You can also create permit strings that allow Web sites to display images that match the string. This allows you to override the blocking effect of any string in the (Defaults) block list for individual sites. Permit rules take precedence over Block rules on any site.

Add an Ad Blocking string

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

To add an Ad Blocking string

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

Block	Block ads matching this string.
Permit	Allow ads matching this string.

6. Type an HTML string to block or permit.
7. Click **OK**.
8. When you are done, click **OK** to close the Advanced window.
9. Click **OK** to close the Ad Blocking window.

Modify or remove an Ad Blocking string

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

To modify or remove an Ad Blocking string

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

Troubleshooting

8

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

Explore the Symantec service and support Web site

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

To explore the Symantec service and support Web site

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

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

To search the Symantec service and support Web site

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

Troubleshoot Norton AntiSpam

This information will help you solve the most frequently encountered problems with Norton AntiSpam.

Why do I still receive spam?

Several factors make it difficult to completely eliminate spam. For example, different people will consider different classes of email messages to be unwelcome or intrusive. Some, for instance, do not want to receive anything they have not specifically requested. Others are glad to receive items regarding their interests or profession even if they have not specifically requested them.

Also, for every new method that is developed to control spam, there are numerous spammers trying to develop ways to circumvent it. This on-going contest of wills and skills is one reason Symantec maintains up-to-date spam definitions.

Finally, not all unwanted messages are unauthorized. Some companies require you to accept email messages in exchange for certain services. Many do not understand that in doing so they are agreeing to, in effect, accept spam.

How will email messages from addresses on my Blocked list be handled?

Norton AntiSpam moves email messages from these addresses to the Norton AntiSpam folder and marks them in the subject line as spam.

What if I mistakenly put an address on the Blocked list?

The only result will be that you will not see any email messages from this address in your main list. But if you periodically review the contents of your spam folder, you will be able to retrieve any email messages from that address and then correct the entry in your list.

Why did an email message someone sent me never arrive?

Some legitimate email messages may contain elements that are characteristic of spam messages. This may have caused Norton AntiSpam to incorrectly identify the message as spam. Depending upon the filters you have created in your email program, the message may be in your spam or trash folder.

See "Identify authorized senders" on page 29.

To avoid losing email messages from this person, add them to your Allowed list.

How do I keep my protection updated?

To some degree, Norton AntiSpam updates itself by learning from your outgoing email messages and other data. However, to receive up-to-date copies of Symantec spam definitions, you must subscribe to this service. You can then choose to have these definitions updated automatically.

Why do I need a subscription to spam definitions?

Though the product is self-training, local spam definitions are developed only by the criteria you input and from the sample of email messages you process. Symantec spam definitions are developed from a much larger set of information and can prevent you from seeing many of the more common types of spam.

Why does so much spam include clusters of meaningless characters?

These and other unusual elements in spam are intended to confuse spam filters that look for keywords.

Troubleshoot Ad Blocking

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

Does Ad Blocking block all advertising on the current page?

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

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

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

Are there security issues associated with advertisements?

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

Service and support solutions

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

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

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

Customer service

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

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

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

Technical support

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

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

Support for old and discontinued versions

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

Subscription policy

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

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web

content protection. Without these updates, you will be vulnerable to attacks.

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

Worldwide service and support

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

Service and support offices

North America

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

http://www.symantec.com/

Australia and New Zealand

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

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

Europe, Middle East, and Africa

Symantec Authorized Service Center
Postbus 1029
3600 BA Maarssen
The Netherlands

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

Latin America

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

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

June 3, 2003

Glossary

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

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

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

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

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

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

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

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

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

Index