Introducing Norton Internet Security

Norton Internet Security provides your PC with comprehensive protection from Internet-based threats and lets you create a safe, supervised environment for family members who use the web.

Using Norton Internet Security, you can:

- Set up a personal firewall that protects your PC and data from curious intruders, malicious hackers, and attacks by rogue Web sites.
- Block objectionable Web sites and specify which types of Internet programs (newsgroups, chat programs, email and so on) can be used by family members.
- Prevent family members from giving out confidential information to Web sites they visit.
- Reduce the risks to your privacy by blocking cookies and referer fields when you visit Web sites.
- Block banner ads and reduce other visual distractions on web pages.

Click here {button ,AL("About the Accounts window;About the Parental Control window;About the Privacy window;About the Security window;About the Status window;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

Product Support Online

These options give you access to product support online, as well as additional information about Norton Internet Security and security in general.

- Technical Support is available online at http://www.symantec.com/techsupp/. Use this link to open the site in your default web browser. Then select Norton Internet Security in the product list.
- The Norton Internet Security User’s Guide and the complete Norton AntiVirus User’s Guide are included on the product CD in Adobe Acrobat format. The Adobe Acrobat Reader is also located on the CD. The guides and the reader are located in the \Manuals folder on the CD. Adobe Acrobat Reader is also available at http://www.adobe.com/.
- The Norton Internet Security website includes general security information not covered in the User’s Guide or online help. To open the site, select Norton Internet Security website from the Help menu.

Click here {button ,AL("About the Accounts window;About the Parental Control window;About the Privacy window;About the Security window;About the Status window;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

Updating Norton Internet Security with LiveUpdate

Symantec’s LiveUpdate feature lets you obtain software updates and subscription content, including updates to the list of categorized Web sites and new firewall rules that protect your PC from the latest Internet security threats.

Note: To obtain subscription content, your Norton Internet Security subscription must be current. Check the Status window if you are unsure about the status of your subscription. If your subscription has expired, you can renew your subscription using LiveUpdate.

Click here {button ,AL("About the Accounts window;About the Parental Control window;About the Privacy window;About the Security window;About the Status window;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

About user accounts

Norton Internet Security makes it easy for you to create user accounts on your PC that provide a safer, more child-friendly Internet environment for young family members.

For example, you could create a Norton Internet Security account that blocked objectionable Web sites and prevented your children from using chat programs. This account could be set up as the Startup Account so that your PC would start up each time with these restrictions in effect. When adults in the household required full access to the Internet, they could log on to Norton Internet Security using the supervisor account created when the product was installed.

Click here {button ,AL("About the Accounts window;About the Parental Control window;About the Privacy window;About the Security window;About the Status window;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

To set up user accounts for family members

Norton Internet Security makes it easy for you to create user accounts on your PC that provide a safer, more child-friendly Internet environment for young family members. To create a user account, you must be logged in with supervisor rights.

1. Click **Accounts** on the left side of the window.
2. Click **Create Account**.

Click here {button ,AL("About the Accounts window;About the Parental Control window;About the Privacy window;About the Security window;About the Status window;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

Understanding Internet-based risks and threats

Although the vast majority of the Internet is safe to visit, there are some areas of cyberspace that pose potential security and privacy risks. If you have children who use a PC to access the Internet, an additional concern is filtering out inappropriate content.

Using Norton Internet Security, you can protect yourself and your family from the following Internet-based threats:

- Viruses: The threat of receiving infected files over the Internet is very real. Infected files can be downloaded from Web sites, instant messaging programs, email attachments, or by other means.
- Malicious active content: Web pages can run ActiveX controls on your PC without your knowledge or permission. If used maliciously, ActiveX controls can allow a hacker to ransack the contents of your hard disk, delete files, or steal passwords.
- Trojan horses: These programs are typically copied to your PC through email attachments, pushed content, or browser plug-ins. Once on your machine, a Trojan horse can take control of your PC for the purpose of stealing passwords or making your files available to the outside world.
- Privacy threats: Chat rooms, email, instant messaging software, and Web sites are all possible avenues in which private information can be revealed. For example, in filling out an innocent looking contest form, a child can reveal address and phone number information to an unscrupulous individual.
- Objectionable content: The Internet is littered with Web sites and newsgroups that purvey hatred, racial bigotry, graphic sexual content, and various criminal activities.
- Personal contact: Although rare, instances in which strangers initiate contact with teens and youngsters do happen. This can occur through unsupervised access to chat areas, newsgroups, or instant messaging software.

Click here {button ,AL("About the Accounts window;About the Ad Blocking window;About the Parental Control window;About the Privacy window;About the Security window;About the Status window;Norton Internet Security overview;technical support",0,`',`')} for more information.

The current settings for this user are shown in the Security, Privacy, Parental Control, and Ad Blocking windows. If the user is not logged on the name appears in red; if the user is logged on the name is shown in blue.

If you have logged on to Norton Internet Security and have supervisor rights, you can select any user account from the list and then make changes to the user’s Security, Privacy, Parental Control and Ad Blocking settings. Any changes you make are automatically saved but don’t go into effect until the user logs on to Norton Internet Security.

Click to suspend or resume the Security protection features.

Click to suspend or resume the Privacy protection features.

Click to suspend or resume the Parental Control features.

Click to suspend or resume the Ad Blocking features.

Click to specify any confidential data that you want protected from going out over the web (HTTP).

The Personal Firewall has four basic settings:

- None: Disables the firewall blocking and alerting.
- Low: Enables firewall protection but with a minimal number of firewall rules. This level of protection is designed to keep out commonly used attacks.
- Medium: Enables firewall protection using a set of rules that blocks all ports except those used by common Internet applications. This setting assures good security without intrusiveness or performance overhead.
- High: Enables comprehensive firewall protection. No access to the Internet is allowed unless there is an explicit firewall rule for that type of access. Although this setting provides the highest level of protection, it may affect network performance or block some legitimate Internet services.

Using the following settings, you can control how Java applets work on your system:

- None: Allows all Java applets to run on your PC.
- Medium: Prompts you each time a Java applet attempts to run on your PC.
- High: Prevents all Java applets from running.

Using the following settings, you can control how ActiveX controls work on your system:

- None: Allows all ActiveX controls to run on your PC.
- Medium: Prompts you each time an ActiveX control attempts to run on your PC.
- High: Prevents all ActiveX controls from running.

About the Status window

From the Status window you can:

- See who is currently logged on to Norton Internet Security.
- Click **Disable** to temporarily suspend all forms of Norton Internet Security protection.
- Click individual protection services (Security, Privacy, Parental Control, or Ad Blocking) to temporarily suspend protection features.
- View real-time statistics that indicate how Norton Internet Security is protecting your system. For a detailed account of protection activity, click the individual statistics associated with each service. To reset the statistics, right-click an empty area in the Status window.
- Check the expiration period of Norton Internet Security’s subscription content.

Click here {button ,AL("About the Accounts window;About the Parental Control window;About the Privacy window;About the Security window;About the Status window;Norton Internet Security overview;technical support",0,`',`')} for more information.

About the Security window

In the Security window you can view, modify, and enable Internet security settings for the selected user. If the selected user is not currently logged on, the user's name is shown in red and the settings will not go into effect until the user logs on to Norton Internet Security.

The slider control provides three Security settings:

- High: Configures the Personal Firewall so that all the applications on your PC are prevented from connecting to the network unless they have been approved to do so. The user will also be given the option to run or cancel Java Applets and ActiveX controls whenever they are run.
- Medium: Configures the Personal Firewall so that all the applications on your PC are allowed to access the network unless the application appears to behave like a known malicious program. (The Medium setting compares the application to a large list of malicious programs.) Java Applets and ActiveX controls are run normally.
- Minimal: Configures the Personal Firewall so that all the applications on your PC can access the network unless the application appears to be malicious. (The Minimal setting compares the application to a small list of programs known to be malicious.) Java Applets and ActiveX controls are run normally.

The default setting is Medium. It provides a good balance between security benefits and issues of convenience and performance.

To control specific Security settings for the selected user, click **Custom Level**. If you change the Security settings and want to revert to the original settings, click **Default Level**.

Click here {button ,AL("About the Accounts window;Changing the Startup Account;Norton Internet Security overview;Safeguarding the privacy of family members;Setting up user accounts;technical support;To view the Norton Internet Security log file;Understanding Internet-based risks and threats",0,`',`')} for more information.

To safeguard the privacy of family members

Norton Internet Security lets you block family members from sending confidential data over the web. For example, you could prevent a child from entering her address and phone number in web registration forms.

Note: This feature only blocks unsecured web data (HTTP). It does not block data sent through secured web pages (HTTPS), chat, email, or other types of Internet services.

To block a family member from sending information over the web:

1 Click **Privacy** on the left side of the window.

2 Select the user you want to restrict from the Settings For menu.

3 Click **Enable Privacy**.

4 Click **Custom Level**.

5 Select **High** as the setting for Confidential Information and then close the Custom Privacy Settings dialog box.

6 Click **Confidential Info**. (Only supervisors and normal users can specify or edit confidential data. This button is disabled for all other users.)

7 Click **Add** and then enter the data you want to block.
Because Norton Internet Security blocks only the exact character sequence you enter (including spaces, dashes, and other special characters), you may need to enter the confidential data in several forms.

Click here {button ,AL("About the Parental Control window;About the Privacy window;Norton Internet Security overview;Restricting Access to Internet Applications;Setting up user accounts;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

About the Privacy window

In the Privacy window you can view, modify, and enable Internet security settings for the selected user. If the selected user is not currently logged on, the user’s name is shown in red and the settings will not go into effect until the user logs on to Norton Internet Security.

The slider provides three Privacy settings:

- High: Prompts the user each time confidential information is sent from the computer to a non-secured Web site (HTTP). Likewise, the user is prompted each time a cookie is sent to a Web site. Browser privacy is also enabled to prevent Web sites from retrieving the address of the last Web site visited or the email address used with the browser.
- Medium: Prompts the user each time confidential information is sent from the computer to a non-secured Web site (HTTP). Cookies, however, are sent to Web sites without requiring permission from the user. Browser privacy is also enabled to prevent Web sites from retrieving the address of the last Web site visited or the email address used with the browser.
- Minimal: Disables the monitoring of confidential information sent to Web sites. Cookies are not blocked but browser privacy is enabled so that Web sites cannot retrieve the last Web site that was visited or the email address used with the browser.

The default setting is Medium. It provides a good balance between security benefits and possible issues of convenience and performance.

To protect credit card information and other sensitive data from being sent out over the web, click **Confidential Information**.

To control specific Security settings for the selected user, click **Custom Level**. If you change the Security settings and want to revert to the original settings, click **Default Level**.

Click here {button ,AL("About the Accounts window;Changing the Startup Account;Cookies;Norton Internet Security overview;Safeguarding the privacy of family members;Setting up user accounts;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

About the Parental Control window

Norton Internet Security lets you create a safer, more child-friendly Internet environment for your family members. Using the Parental Control features, you can:

- Block objectionable Web sites

The basis of Norton Internet Security’s web filtering feature is an extensive categorized list of Web sites created and maintained by Symantec. Using this list as a starting point, you can customize the web access settings for each individual in your household.

To restrict the types of Web sites the user can access, click **Sites**.

- Block access to specific Internet applications

Using this option you can configure a child’s account to let them browse the web but not play specific Internet games or use chat programs.

To restrict the user from using selected Internet-based programs, click **Applications**.

By default, children’s accounts do not block any Internet applications but they do restrict access to certain categories of Web sites. Click **Sites** to see which types of Web sites are blocked by default. If you make changes and want to revert to the account’s original settings, click **Defaults.**

Any changes you make to the Parental Control settings of the selected user are automatically saved. The settings go into effect when Norton Internet Security starts up (if the child’s account has been configured as the startup) or if the child logs on to Norton Internet Security.

Click here {button ,AL("About the Accounts window;About the Privacy window;Changing the Startup Account;Norton Internet Security overview;Restricting Access to Internet Applications;Safeguarding the privacy of family members;technical support",0,`',`')} for more information.

To restrict access to Internet-based applications

Norton Internet Security lets you restrict individuals from using specific types of Internet-based applications. For example, you could configure a child’s account to let her browse the web but not use email, instant messaging software, or a particular Internet-based game.

Note: This feature is only available when the Personal Firewall is set to high.

To block a user’s access to specific Internet programs:

1. Choose the user account you want to restrict from the drop-down list. The account should be for a restricted user.
2. Click **Enable Parental Control**.
3. Click **Applications**, then click the types of Internet applications to permit. (If you want to permit a type of Internet application that is not in the list, click General.)
4. As a final step, start the application on your PC. If Norton Internet Security issues an alert, click **Configure a Rule for the Future**.

Click here {button ,AL("About the Accounts window;About the Parental Control window;Changing the Startup Account;Safeguarding the privacy of family members;Setting up user accounts;Understanding Internet-based risks and threats",0,`',`')} for more information.

About the Ad Blocking window

Many sites use banner ads in their web pages that often employing animated graphics to get the attention of visitors. If you find banner ads to be distracting, you can block them using Norton Internet Security. In addition, you can also use the ad blocking feature to block specific ads that are featured on a web page.

Choose an item for more information:

Blocking specific ads from Internet Explorer

Blocking specific ads from Netscape Navigator

Click here {button ,AL("About the Status window;Norton Internet Security overview;technical support",0,`',`')} for more information.

To block banner ads and other forms of web advertising:

1 Click **Ad Blocking** on the left side of the screen. This option blocks banner ads from displaying on your browser.

2 Click **Enable**.

You can also use the ad blocking feature to block specific ads that are featured on a web page.

Choose an item for more information:

Blocking specific ads from Internet Explorer

Blocking specific ads from Netscape Navigator

Click here {button ,AL("About the Ad Blocking window;To block banner ads and other forms of web advertising",0,`',`')} for more information.

To block specific ads from appearing in Internet Explorer:

1 Click **Ad Blocking** on the left side of the screen.

2 Click **Trashcan** in the Ad Blocking window.

3 Drag the ad from Internet Explorer to the trash can shown in the dialog box.

4 Click **Add**.

Click here {button ,AL("About the Ad Blocking window;technical support;To block banner ads and other forms of web advertising",0,`',`')} for more information.

To block specific ads from appearing in Netscape Navigator:

1 Click **Ad Blocking** on the left side of the screen.

2 Click **Trashcan** in the Ad Blocking window.

3 Right-click the ad in Netscape Navigator and click **Copy Image Location**.

4 Click **Paste**.

Click here {button ,AL("About the Ad Blocking window;technical support;To block banner ads and other forms of web advertising",0,`',`')} for more information.

To block access to inappropriate Web sites:

1 Click **Parental Control** on the left side of the screen.

2 Choose the user account you want to restrict from the drop-down list. The account should be for a restricted user.

3 Click **Enable Parental Control**.

4 Click **Sites**, then click the types of Web site categories you want to block.

Click here {button ,AL("About the Ad Blocking window;technical support;To block banner ads and other forms of web advertising",0,`',`')} for more information.

About the Accounts window

Users with supervisor rights can create Norton Internet Security user accounts to provide a safer, more child-friendly Internet environment for family members.   Accounts are created using options in the Accounts window; Internet rights and privileges are set in the Security, Privacy, and Parental Control windows.

- Log off/Log in

Click Log Off to change users. Whenever the current user logs off, a built-in account named Not Logged In becomes active. When this account is activated, Norton Internet Security shuts down all network connections.

- Change passwords

Click Change Password to modify the logged in user’s password.

If you have supervisor rights, these additional options are available:

- Create new accounts

Click Create Account to set up new Norton Internet Security accounts for family members.

- Delete accounts

Click Delete Account to remove a Norton Internet Security account.

- Change account properties

Click Properties to change the basic account settings for any user.

Click here {button ,AL("Changing the Startup Account;Norton Internet Security overview;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

To change the Startup account

Each time Norton Internet Security starts, one of the user accounts is automatically logged in. This account, known as the Startup account, provides the initial configuration settings for Norton Internet Security.

The supervisor account you set up during installation is the default Startup Account. If you prefer to have a different account provide the startup settings for Norton Internet Security, you can change the Startup account.

To change the Startup account:

1 In the Accounts window, select one of the user accounts.

2 Click **Properties**.

3 Click **Make This The Startup Account**.

Click here {button ,AL("About the Accounts window;Norton Internet Security overview;Restricting Access to Internet Applications;Safeguarding the privacy of family members;Setting up user accounts;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

Customize Security Settings dialog box

This dialog box lets you create a customized level of security for the user. The changes you make are saved automatically and go into effect when the user logs on.

- Personal Firewall: Specifies how Norton Internet Security firewall rules are applied.
- Java Applet Security: Lets you to control how the browser handles Java applets when they are downloaded from Web sites. (Blocking Java applets may prevent some web pages from working properly.)
- ActiveX Control Security: Lets you control how the browser handles ActiveX controls when they are encountered on the Internet. (Blocking ActiveX controls may prevent some web pages from working properly.)
- Silently Block Unused Ports: Lets you disable alert messages that are otherwise issued when an inbound connection attempt is made to a port on your PC and a corresponding listening service is not available on your PC. Checking this option does not compromise security since attempts to connect will always fail when there is no corresponding listening service. For example, this situation would occur if someone tried to connect to your system with Symantec's pcAnywhere and you didn’t have a pcAnywhere host running on your local system.

Choose an item for more information:

Personal Firewall settings

Java Applet Security settings

ActiveX Control Security settings

Click here {button ,AL("About the Security window;Norton Internet Security overview;Restricting Access to Internet Applications;Setting up user accounts",0,`',`')} for more information.

Personal Firewall settings

The Personal Firewall has four basic settings:

- None: Disables firewall blocking and alerting.
- Low: Enables firewall protection but with a minimal number of firewall rules. This level of protection keeps out commonly used network-based attacks.
- Medium: Enables firewall protection that blocks all ports except those used by common Internet applications. This setting assures good security without undo intrusiveness or performance penalties.
- High: Enables comprehensive firewall protection. No access to the Internet is allowed unless there is an explicit firewall rule for that type of access. Although this setting provides the highest level of protection, it may affect network performance and block some legitimate Internet services.

Click here {button ,AL("firewall faq;firewall general;technical support;To view or modify firewall rules;Understanding Internet-based risks and threats",0,`',`')} for more information.

Java Applet Security settings

The Java Applet Security control has three settings:

- None: Allows Java applets to run.
- Medium: Prompts each time a Java applet attempts to run.
- High: Blocks Java applets. (Blocking Java applets may prevent some web pages from working properly.)

Note: This feature is only available when the Personal Firewall is set to high.

Click here {button ,AL("Norton Internet Security overview;technical support;To view the Norton Internet Security log file;Understanding Internet-based risks and threats",0,`',`')} for more information.

ActiveX Control Security settings

The ActiveX Control Security control has three settings:

- None: Allows ActiveX controls to run.
- Medium: Prompts each time an ActiveX control attempts to run.
- High: Blocks ActiveX controls. (Blocking ActiveX controls may prevent some web pages from working properly.)

Click here {button ,AL("Norton Internet Security overview;technical support;To view the Norton Internet Security log file;Understanding Internet-based risks and threats",0,`',`')} for more information.

Customize Privacy Settings dialog box

This dialog box lets you create a customized level of privacy for the user. The changes you make are saved automatically and go into effect when the user logs on.

- Confidential Information: Specifies how confidential information is handled when the user enters it on a Web site.
- Cookie Blocking: Specifies how cookies are handled when a Web site requests them.
- Enable Browser Privacy: Prevents a Web site from retrieving your email address from the browser and finding out which Web site was last visited.
- Enable Secure Connections (HTTPS): Lets the user access Web sites using HTTPS, a secure protocol that is often required for credit card purchases.

Click here {button ,AL("About the Privacy window;Safeguarding the privacy of family members;Understanding Internet-based risks and threats",0,`',`')} for more information.

To view or modify firewall rules:

1 On the toolbar, click **Options**.

2 Click **Internet Security**.

3 Click **Advanced Options**.

4 Click **Firewall**.

Click here {button ,AL("About the Security window;Norton Internet Security overview;Restricting Access to Internet Applications;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

To view the Norton Internet Security log file:

1 On the toolbar, click **Options**.

2 Click **Internet Security**.

3 Click **Advanced Options**.

4 Click **View Event Log**.

Click here {button ,AL("About the Security window;Norton Internet Security overview;Restricting Access to Internet Applications;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

Confidential Information dialog box

Norton Internet Security’s Confidential Information feature lets you block specific information from going out to Web sites. For example, you could enter your family’s home address if you did not want your children divulging it when they filled out registration and contest forms on the web.

Norton Internet Security blocks only confidential data sent to Web sites by means of HTTP. It does not block data sent out by secure protocol (HTTPS) or through applications that use other protocols (email, chat programs, news readers, and so on).

Click here {button ,AL("About the Parental Control window;About the Privacy window;Restricting Access to Internet Applications;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

Add Confidential Information dialog box

Use the dialog box to place confidential information in the database for protection by Norton Internet Security.

The confidential data entered by Norton Internet Security users is located in a single database. Any confidential information you enter can be seen and accessed by Norton Internet Security users with normal or supervisor rights.

Note: Norton Internet Security will block only the exact character sequence you enter in the database. For this reason, you may need to create several separate entries to protect your data. For example, if you entered a phone number as 555-444-4444, the sequence (555) 444-4444 would be permitted. Inserting spaces in the character sequence also affects how your data is blocked.

Click here {button ,AL("About the Privacy window;Changing the Startup Account;Norton Internet Security overview;technical support",0,`',`')} for more information.

Click to enable or disable all of the Security features. If you disable the Security features, the Personal Firewall is turned off and no blocking of Java applets or ActiveX controls will occur.

Click to enable or disable Privacy protection for the user.

This button enables or disables all of the Parental Control features.

This button enables or disables all of the Ad Blocking protection features.

Click to create a new Norton Internet Security account.

Click to remove the selected Norton Internet Security account.

Account Properties dialog box

The Account Properties dialog box lets you change basic account settings:

- Password: To change the account's password, enter a new password in the Password and Confirm Password text boxes.
- Account Type: Change the type of user account—normal, restricted, or supervisor.
- Enable Personal Firewall Alerts (unavailable to restricted users):

  Click this option to give the user some discretionary control when an application tries to connect to the network but no firewall rule exists for it. If the option is enabled, the user will be able to temporarily permit or block the application from accessing the network. If the user has supervisor rights, Norton Internet Security will provide the option of creating firewall rules for the application.

  Disable this option if you want to block applications from accessing the network when there are no specific firewall rules in place for them.
- Make this the startup account: Check this option if you want Norton Internet Security to start up with the account automatically logged in.

Click here {button ,AL("About the Accounts window;Changing the Startup Account;Norton Internet Security overview;Restricting Access to Internet Applications;Setting up user accounts;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

Create Accounts dialog box

User accounts provide an easy means of restricting the Internet access of household members. To set up user accounts, you need supervisor rights.

- Account Name: Enter a name for the user account.
- Password/Confirm Password: Enter a password for the user and then re-enter it as confirmation.
- Base Account On: Click the user profile that best fits the individual for whom you are creating an account. The different profiles—Child, Teenager, Adult, and Supervisor—each have their own Internet rights and privileges. If you need to adjust these settings afterwards, you can change any of the user's settings in the Security, Privacy, Parental Control, and Ad Blocking windows.
- Make this the startup account; Check this option if you want Norton Internet Security to start up with this account automatically logged in.

Click here {button ,AL("About the Accounts window;Changing the Startup Account;Norton Internet Security overview;Setting up user accounts;technical support;Understanding Internet-based risks and threats",0,`',`')} for more information.

Number of network accesses blocked by the Security controls. Click anywhere on this display area to see more information.

Number of network accesses allowed by the Security controls. Click anywhere on this display area to see more information.

Number of network accesses blocked by the Privacy controls. Click anywhere on this display area to see more information.

Number of network accesses allowed by the Privacy controls. Click anywhere on this display area to see more information.

Number of network accesses blocked by the Parental Controls. Click anywhere on this display area to see more information.

Number of network accesses allowed by the Parental Controls. Click anywhere on this display area to see more information.

Number of network accesses blocked by the Ad Block controls. Click anywhere on this display area to see more information.

Drag the slider to change the user’s Security settings. Higher settings provide more security but may impact system performance and convenience.

Drag the slider to change the user’s Privacy settings. Higher settings provide more privacy but may impact system performance and convenience.

Click to set up customized Security settings for the user.

Click this button if you have customized the user’s Security settings and want to revert back to the original default setting of Medium.

Check this option to disable alert messages that are otherwise issued when an inbound connection attempt is made with no corresponding listening service. Checking this option does not compromise security since attempts to connect will always fail when there is no corresponding listening service.

Click to set up customized Privacy settings for the user.

Click this button if you have customized the user’s Privacy settings and want to revert back to the original default setting of Medium.

Choose the type of information you want to block from going out over the web (HTTP).

Enter a meaningful name for the information you want to block.

Enter the exact sequence of characters, including spacing, that you want to block.

Specify Sites dialog box

Norton Internet Security lets you prevent family members from visiting Web sites with inappropriate or undesirable content.

Norton Internet Security provides two basic blocking options:

- Click **Specify permitted sites** to block all sites except those you specify as acceptable. Use this option if you want to let family members visit only a few handpicked sites.

  You can specify only a single list of acceptable sites. If you choose this blocking method for more than one child they will all be able to visit the same list of sites.

- Click **Specify blocked sites** to let the child visit any Web site except for those you decide to block out. The basis of this feature is an extensive categorized list of Web sites created and maintained by Symantec. Using this option, you can let the child visit the majority of sites on the web but block out those that fall into certain categories.

  If a site you want to block is not handled by the category list, you can block it by adding it to the Additional Sites to Block list.

Click here {button ,AL("About the Accounts window;About the Parental Control window;Norton Internet Security overview",0,`',`')} for more information.

Adding a site to a Block or Permit list

You can add sites to either a block list or a permit list, depending on the site blocking option you clicked.

Choose an item for more information:

Adding a Web site to a block list

Adding a Web site to a permit list

Click here {button ,AL("About the Parental Control window;Restricting Access to Internet Applications;Setting up user accounts;Understanding Internet-based risks and threats",0,`',`')} for more information.

Add Website to Blocked List dialog box

Enter the address of the Web site to block. Depending on how you enter the site’s URL, you can block the entire site or only parts of it:

www.symantec.com	(blocks all of the site)
www.symantec.com/techsupp/	(blocks only the technical support area)

Click here {button ,AL("About the Parental Control window;Restricting Access to Internet Applications;Setting up user accounts;Understanding Internet-based risks and threats",0,`',`')} for more information.

Add Website to Permitted List dialog box

Enter the address of the Web site you want to permit. Depending on how you enter the site’s URL, you can let the user visit the entire site or only parts of it:

www.symantec.com	(permits access to all of the site)
www.symantec.com/techsupp/	(permits access to only the technical support area)

- You can specify only one list of acceptable sites. If you choose this blocking method for more than one child, they will all be able to visit the same list of sites.
- Web sites often provide content that is located outside the site’s main URL. To give a child full access to a site, you may need to specify several different URLs.

Click here {button ,AL("About the Parental Control window;Restricting Access to Internet Applications;Setting up user accounts;Understanding Internet-based risks and threats",0,`',`')} for more information.

Click to block all sites except those you specify as acceptable. Use this option if you want to let the child visit only a few handpicked sites.

Click to let the user visit any Web site unless it is blocked by the category list or it appears in an additional block list.

Click if you need to enter any exceptions to the category list.

Click all the categories in the list to block. If a category in the list is unchecked, the user can visit sites of that type.

Sites in this list are blocked in addition to those Web sites in checked categories. Click **Add** to enter a site to this list.

Click to add a site to the list. Sites in this list are blocked in addition to those sites checked in the categories list.

Click to remove a site from the list of additional sites to block.

Sites in this list are not blocked, even if they fall under Symantec's blocked category list.

Click to add a site to the exceptions list. Sites in this list are not blocked, even if they fall under Symantec’s blocked category list.

Click to remove a site from the exceptions list.

Enter the address of the Web site.

The user will be allowed to visit only the sites that appear in this list—access to all other sites is blocked. Click Add or Remove to modify the list.

Click to add a site to the list of permitted sites.

Click to remove a site from the list of permitted sites.

Click to use the site blocking controls to manage your child’s access to the web.

Click to use the application blocking controls to manage your child’s access to Internet programs (chat, email, games, and so on).

Click to discard any changes you made to your child’s site and application settings. The default settings for a child’s account allow access to all Internet applications but block access to some types of Web sites.

Applications dialog box

Norton Internet Security maintains a list of categorized applications (newsreaders, web browsers, email programs, and so on) that covers hundreds of popular Internet-based programs. Using this list, you can choose which types of Internet programs—if any—you want your child to be able to use.

- To block access to a certain type of Internet program, uncheck its category in the list.

Click here {button ,AL("About the Parental Control window;Restricting Access to Internet Applications;Setting up user accounts;Understanding Internet-based risks and threats",0,`',`')} for more information.

Check the categories of Internet-based applications that you want your child to be able to use.

Click to enable or disable all of the Norton Internet Security features.

Description, type, and content associated with the confidential information blocked by Norton Internet Security.

Click to add a new piece of information to be blocked from going out to Web sites (HTTP).

Specifies how confidential information is treated when the user attempts to enter it at a Web site.

Specifies how cookies are treated when a Web site attempts to access them.

Check to prevent Web sites from obtaining the email address from the browser and the last site visited.

Check to allow the user to use the secure connections protocol when visiting a Web site. If this option is not checked, the user will be prevented from conducting credit card transactions at many sites.

Click to block specific advertising graphics displayed in either Internet Explorer or Netscape Navigator.

Security Alert Details

A security alert indicates that some form of network communication has been attempted between your PC and another computer. This event was detected and logged by Norton Internet Security’s Personal Firewall.

The event triggered an alert because it matched the criteria set by one of the firewall rules. The name of the firewall rule is shown in the Security Alert Details dialog box. For more information, you can view the event log maintained by Norton Internet Security and examine the firewall rule that was enforced.

Click here {button ,AL("About the Security window;Norton Internet Security overview;Restricting Access to Internet Applications;Understanding Internet-based risks and threats",0,`',`')} for more information.

Log In dialog box

Norton Internet Security grants users specific Internet access rights and other privileges. Before these rights and privileges go into effect, the user must log into Norton Internet Security.

To have Norton Internet Security automatically log in the user each time it starts up, make the account the Startup Account.

Click here {button ,AL("About the Accounts window;Changing the Startup Account;Setting up user accounts;Understanding Internet-based risks and threats",0,`',`')} for more information.

Click to log in or log off of Norton Internet Security.

Click the Norton Internet Security user account from the drop-down list.

Enter the password for the Norton Internet Security user account.

Click to change the password of the logged-in user.

Enter the current password.

Enter the new password.

Enter the new password to confirm your change.

Change Password dialog box

To change the password of the current logged in user, enter the old password, the new password, and then re-enter the new password to confirm your change.

Click here {button ,AL("About the Accounts window;Changing the Startup Account;Setting up user accounts;Understanding Internet-based risks and threats",0,`',`')} for more information.

The list shows the names and types of user accounts:

- Users with Supervisor rights can change the settings of any account.
- Users with Normal rights can only change their own account.
- Users with Restricted rights cannot make changes to any accounts.
- The Not Logged In account is a built-in account that prevents any network access. This account becomes active when a user logs off of Norton Internet Security.
- The Startup account is automatically logged in each time Norton Internet Security starts up. To change Startup accounts, click **Properties**.

Click to change the basic properties of the selected account.

Enter the name of the account you want to create.

Password for the account.

Confirmation password for the account.

Select the profile that best fits the individual for whom you are creating the account. Each profile has its own specific Internet access rights and privileges.

Check to have Norton Internet Security automatically log the user in each time the program starts.

Name of the Norton Internet Security user account.

Choose the type of account for the user:

- Supervisors can change the settings of any user’s account.
- Normal users can change only their own account settings.
- Restricted user cannot change the settings of any account.

Check this option to give the user some discretionary control when an application tries to connect to the network but no firewall rule exists for it. If this alerting option is enabled, the user can allow or block the connection. If the user has supervisor rights, they can create firewall rules that control how the application connects to the network.

If you disable the option, applications that are not covered by specific firewall rules will be blocked from accessing the network.

This option is unavailable to Restricted users.

Check to have the account log in automatically each time Norton Internet Security is started.

Click to remove the confidential information entry in the list.

Click to edit the confidential information entry selected in the list.

Norton Internet Security Options

Use these options to control general configuration settings for Norton Internet Security.

- Show Taskbar Icon: Check this option to display the Norton Internet Security icon in the system tray. You can then click the icon to log in and out of Norton Internet Security, exit the program, or perform other tasks.
- Startup: Click the startup option you prefer:
- Click **Manual** if you don't want Norton Internet Security to start automatically.
- Click **Run at System Startup** to have the program start automatically when you start your PC.
- View Event Log: Click to view a log containing information on content blocking, connections, firewall activity, and other Norton Internet Security events.
- View Statistics: Click to view real-time, detailed statistics that indicate how Norton Internet Security is protecting your system.
- Clear Statistics: Click to reset the statistics shown in both the Status window and the Statistics window.
- Advanced Options: Click this option to change advanced settings for the Personal Firewall and other Norton Internet Security features.

Click here {button ,AL("About the Security window;Changing the Startup Account;Norton Internet Security overview;To view the Norton Internet Security log file;Understanding Internet-based risks and threats",0,`',`')} for more information.

The HTTP Port List shows all of the HTTP ports monitored by Norton Internet Security. The default list contains all the standard HTTP ports, but you can add ports if you use applications that perform HTTP communication through nonstandard ports.

Click to add a new HTTP port to the list.

Click to remove an HTTP port from the list.

Click to block all forms of IGMP (Internet Group Management Protocol) communications, a protocol sometimes exploited by attackers to hang a victim’s system.

Click to block IP packets that are severely fragmented. IP packets of this type are typically used for purposes of attack rather than legitimate network communications.

Click to have Norton Internet Security automatically create firewall rules for you when an attempts to connect to the network and there are no firewall rules in place for that application.

If you want more control over the creation of firewall rules, you can disable this option so that you are prompted to create new firewall rules yourself using the Rule Assistant wizard. (This occurs only if Security is set to High and you are a Supervisor with the Enable Firewall Alerts account property enabled. If any of these conditions are not true, Norton Internet Security will allow the connection to occur.)

Time remaining before your content subscription expires. Content updates include new Web site profiles you can use create a child-friendly Internet environment, as well as new rules for the Personal Firewall that protect your PC from the latest hacker attacks.

Click for specific information about the alert.

Notice

Norton Internet Security has notified you that you are attempting to run a Parental Control or Privacy feature that requires Security to be enabled. To ensure that Norton Internet Security is correctly configured to safeguard your PC, click **Security** in the Status window or disable the Parental Control/Privacy features described in the notice.

Sets script-blocking options for individual sites or for (Defaults):

- Use default script behavior: Lets (Defaults) control the Script setting. Select (Defaults) to view the Script setting that will be used.
- Block all scripts: Blocks JavaScript and VBScript from running.
- Block script popups only: Blocks only scripts that open popup windows in your browser.
- Allow all scripts to execute: Allows VBScript and JavaScript to run.

Controls how Java applets and ActiveX controls are blocked by individual sites in the list.

To change the Binary Executable settings for (Defaults), use Security window options.

Sets Java applet options for individual sites:

- Use default Java applet behavior: Lets (Defaults) control the Java applet setting. Select (Defaults) to view the Java applet setting that will be used.
- Block Java applets: Blocks Java applets from running on your PC.
- Allow Java applets to execute: Allows Java applets to run on your PC.

Note: The Java applet setting for (Defaults) is controlled by Security window options and cannot be overridden with this control.

Sets ActiveX blocking options for individual sites:

- Use default ActiveX behavior. Lets (Defaults) control the ActiveX setting. Select (Defaults) to view the ActiveX setting that will be used.
- Block ActiveX controls: Blocks ActiveX controls from running on your PC.
- Allow ActiveX controls to execute: Allows ActiveX controls to run on your PC.

Note: The ActiveX setting for (Defaults) is configured in the Security window and cannot be overridden with this control.

Sets animated GIF options for individual sites or for (Defaults).

Set the GIF option for the selected site or for (Defaults):

- Use default animation behavior: Lets (Defaults) control the Animated GIF setting. Select (Defaults) to view the animated GIF setting that will be used.
- Allow animations to repeat: Allows animated GIF files to run on your PC.
- Block animations repeating: Blocks animated GIF files from running on your PC. Only the first frame of the GIF will be displayed.

Click to edit the selected firewall rule.

Overview of the Event Log

Norton Internet Security maintains individual logs for Content Blocking, Connections, Firewall, Privacy, Restrictions, System, and Web History.

Access reporting and analysis

The event logs provide a record of connections, URLs accessed, and the cookies, objects, and site referrals that have been blocked. In the Event Log viewer, each event log is displayed on a tab:

Window tab	Displays
Content Blocking	Information about ads and images that have been blocked. Lists the HTML code removed from pages in order to block ads and images.
Connections	Information about TCP/IP network connections made to and from this PC.
Firewall	Information about network communication intercepted by the firewall and rules that were processed. Lists the status of the Rule Assistant (interactive learning mode), shows the alerts displayed to the user by the Rule Assistant, provides summaries of TCP and UDP packet traffic, and itemizes the rules that have been enforced and created.
Privacy	Information about cookies that were blocked or permitted by the firewall. Lists the action taken for each cookie, the name of the cookie, and the site or domain that requested the cookie. Also shows information about referer fields that were blocked, including the address of the site from which you linked and the name of the site to which you linked.
Restrictions	Information about the Internet applications that were blocked or permitted by the firewall.
System	Information about what Norton Internet Security services are running.
Web History	An audit trail of the URLs visited from this PC.

Click here □ for more information.

Content Blocking Log

Messages in the Content Blocking log provide information about ads and images that have been blocked by Norton Internet Security. The messages indicate the HTML code that was removed in order to block ads and images, the web page it was removed from, and the URL string that triggered the blocking activity.

Click Refresh to update the Content Blocking log and the tab with current information.

For general information about the Event Log viewer, click here.

Click here ● for more information.

Connections Log

The Connections log shows a history of all TCP/IP network connections made with this PC.

Click Refresh to update the Connections log and the tab with current information. In addition to the date and time columns for the events on the tabs, the following information is available:

Remote The address or host name of the remote site and the service or port number.

Local The local address or machine name and the service or port number being used by the application.

Sent Bytes Number of bytes sent since the connection started.

Recv Bytes Number of bytes received since the connection started.

Elapsed Time The amount of time that the connection has been active.

Click here {button ,JI(`>maintwo',`overview_event_log')} for more information.

Firewall Log

The Firewall log provides information about network communication intercepted by the firewall and rules that were processed. It lists the status of the Rule Assistant (interactive learning mode) and shows the alerts displayed to the user by the Rule Assistant. It also provides summaries of TCP and UDP packet traffic, and itemizes the rules that have been enforced.

Click Refresh to update the Firewall log and the tab with current information.

For general information about the Event Log viewer, click here.

Click here for more information.

Privacy Log

This Privacy log displays the contents of the Privacy event log, which provides information about cookies that were blocked by Norton Internet Security. It shows the action taken for each cookie, the name of the cookie, and the Web site that requested the cookie. It also shows information about referer fields that were blocked, including the address of the site from which you linked and the name of the site to which you linked.

Click Refresh to update the Privacy log and the tab with current information.

For general information about the Event Log viewer, click here.

Click here ● for more information.

Restrictions Log

The Restrictions log provides information about the Internet applications and Web sites blocked by Norton Internet Security. These blocked applications and Web sites are specified in the Parental Control screen.

Click here {button ,AL("Privacy tab",0,`',`')} for more information.

System log

The System log provides information about Norton Internet Security activity as a Windows service and IP filtering activity. Details of filtering activity provide a record of inbound and outbound network connection attempts and the user action taken in response to these attempts.

Click Refresh to update the System log and the tab with current information.

For general information about the Event Log viewer, click here.

Choose an item for more information:

Refresh

Error

Warning

Information

Alert

System

System events are identified by type. Options on the System tab let you specify which types of events display: error, warning, information, alert, and system.

Click here ● for more information.

Refresh button (Event Log viewer)

Click Refresh to update the log and the current tab display with any new events that have been logged since the Event Log viewer was opened.

Error check box (Event Log viewer)

To display error messages on the System tab, the **Error** check box should be checked.

Warning check box (Event Log viewer)

To display warning messages on the System tab, the **Warning** check box should be checked.

Information check box (Event Log viewer)

To display information messages on the System tab, the **Information** check box should be checked.

Alert check box (Event Log viewer)

To display alert messages on the System tab, the **Alert** check box should be checked.

System check box (Event Log viewer)

To display system messages on the System tab, the **System** check box should be checked.

Web History Log

The Web History event log lists the URLs visited by your PC, providing a history of web activity.

On this tab you can to update the history list or go to a URL selected in the list.

Choose an item for more information:

Refresh

Go to

For general information about the Event Log viewer, click here.

Click here ● for more information.

Go to button (Event Log viewer)

On the Web History tab, to revisit a URL shown in the history list, click the URL and click the Go to button.

Log Menu

Commands on the Log menu let you clear the current tab or all tabs, set the maximum size for an event log file, print the events displayed on the current tab, or save the event information on the current tab to a text file.

Clear Tab
Clears the events displayed on the current tab. This clears the event log file maintained for the event category shown on the tab. After the log is cleared, new events are recorded at the beginning of the log.

Clear All Tabs
Clears the events displayed on every tab in the Event Log viewer. Effectively, this clears the individual event log file maintained for each tab's event category. After the log is cleared, new events are recorded at the beginning of the log.

Clear All Tabs Upon Logoff
Clears the events displayed on every tab in the Event Log viewer when you exit Norton Internet Security. This ensures that the event log is empty when you restart your machine. After the log is cleared, new events are recorded at the beginning of the log.

Save Tab As
Click Save Tab As to save the event log information shown on the current tab to a text file.

Print Tab
Prints the contents of the event log shown on the current tab.

Change Tab File Size
Opens the Log File Size dialog box where you can set the maximum size for the event log file that is maintained for the current tab category.

In the Size box, select the file size you want. When the log file reaches its maximum, new events wrap to the beginning of the file.

Note: Changing the size of the log file does not take effect until you restart your PC.   The current log file will be cleared. To save information in the current event log to a text file, on the Log menu, click Save Tab As.

Click here ● for more information.

Edit Menu

Commands on the Edit menu let you copy selected event information to the Clipboard and to select all information on the current tab.

Copy Click Copy to copy the currently selected event information to the Clipboard.

Select All Click Select All to select all the event information shown in the event list on the current tab.

Click here ● for more information.

Configuring and using the Event Log

Each tab in the Event Log viewer displays the contents of an event log file that is maintained for that category of information.

Some event log messages are longer than the message area displayed in the upper portion of the log. To see the complete message, click it. The full text is appears in the lower portion of the window.

Below is the list of data that is available for most events.

Date The date of the event.

Time The time of the event. The most recent event is listed first.

Message This is the event message. This appears on the Content Blocking tab, the Firewall tab, the Privacy tab, and the System tab.

Type Indicates what type of message this is. Available only on the System tab. Message types include: Error, Warning, Information, Alert, and System.

Source The component that produced the event. Available only on the System tab.

URL Visited The URL for a Web site visited from this PC. Available only on the Web History tab.

Click here ● for more information.

Error

These messages include the highest severity system errors.

Information

These messages include information about the current status of IP filtering.

Alert

These messages notify the user of network interactions detected by Norton Internet Security. For example, if the Rule Assistant is enabled, Norton Internet Security displays a user alert any time a new type of inbound or outbound network communication is attempted. An alert message is recorded in the Norton Internet Security event log. Alert messages provide details about the type of communication that was attempted and what action the user chose in response to the alert.

System Log

These messages indicate whether Norton Internet Security started as a Windows service on the PC.

Warning

These messages cover cases when software is operating in less than optimum conditions—for example, when resource usage is too high.

Using the Rule Assistant

Create Permit Rule: Introduction

The Rule Assistant indicates the type of rule you are creating and the properties of the rule that are currently defined. By default, the rule only permits this type of communication when using the application, service or ICMP message type, and address indicated. The Rule Assistant will present a series of choices that let you to modify the rule properties, making the rule more permissive.

You'll be asked to make these decisions:

- Does the rule permit this type of communication only for the application shown or does it apply to all applications? (not applicable for ICMP messages)
- If this is TCP or UDP network communication**,** does the rule permit communication only when using the remote service shown or does it apply to all types of services?
- If this is ICMP network communication**,** does the rule permit communication only when using the ICMP message type shown or does it apply to all types of ICMP messages?
- Does the rule permit communication only with the remote address shown or does it apply to communication with any address?

Click here {button ,JI(`>maintwo',`HELPID_RULEWIZARD_APP_PERMIT')} to continue defining a permit rule.

Create Permit Rule: Permit Communication by One or by All Applications

The Rule Assistant indicates the type of communication that the rule will permit. You must choose whether the rule should permit this type of communication only when using the application shown or permit this type of communication when using any application.

Click here {button ,JI(`>maintwo',`HELPID_RULEWIZARD_SERVICE_PERMIT')} to continue defining a permit rule.

Create Permit Rule: Permit Communication by One or by All Services

The Rule Assistant indicates the type of communication that the rule will permit and whether the rule applies to a specific application or applies to any application.

Now choose whether the rule should permit this type of communication only when using the remote service shown or permit this type of communication when using any service.

Click here {button ,JI(`>maintwo',`HELPID_RULEWIZARD_TYPE_PERMIT')} to continue defining a permit rule.

Create Permit Rule: Permit Communication by One or by All ICMP Message Types

The Rule Assistant indicates the type of ICMP message that the rule will permit.

You must choose whether the rule should permit ICMP network communication only when using the ICMP message type shown or permit ICMP communication when using any ICMP message type.

Click here {button ,JI(`>maintwo',`HELPID_RULEWIZARD_ADDR_PERMIT')} to continue defining a permit rule.

Create Permit Rule: Permit Communication with One or with All Addresses

- For TCP or UDP network communication, the Rule Assistant indicates the type of communication that the rule will permit and what application(s) and services it applies to.
- For ICMP network communication, the Rule Assistant indicates the type of type of communcation that the rule will permit and what ICMP message type(s) it applies to.

Now choose whether the rule should permit this type of communication only when using the address shown or permit this type of communication when using any address.

Click here {button ,JI(`>maintwo',`HELPID_RULEWIZARD_FINISH_PERMIT')} to continue defining a permit rule.

Create Permit Rule: Rule Summary

The Rule Assistant proposes a name for the rule you are creating. If you want to enter a different name for the rule, type it in the edit box. The rule name will be added to the Firewall Rule list on the Firewall tab in the Settings dialog box. Specify a name that lets you identify what the rule does.

The rule summary indicates the properties you've defined for the rule. If you want to change a rule property, click the Back button to reach the panel that determines the property you want to change.

If you want an entry to be written to the Firewall event log when any network communication matches this rule, select the Write check box.

Click Finish to create the permit rule.

- The rule is applied for the current communication event and for all future events of this type.
- The rule is added to the list of rules maintained on the Firewall tab in the Settings dialog box.

Click here ● for more information.

Create Block Rule: Introduction

The Rule Assistant indicates the type of rule you are creating and the properties of the rule that are currently defined. By default, the rule only blocks this type of communication when using the application, service or ICMP message type, and address indicated. The Rule Assistant will present a series of choices that allow you to modify the rule properties, making the rule more restrictive.

You'll be asked to make these decisions:

- Does the rule block this type of communication only for the application shown or does it apply to all applications?
- If this is TCP or UDP network communication, does the rule block communication only when using the remote service shown or does it apply to all types of services?
- If this is ICMP network communication, does the rule b;pcl communication only when using the ICMP message type shown or does it apply to all types of ICMP messages?
- Does the rule block communication only with the remote address shown or does it apply to communication with any address?

Click here {button ,JI(`>maintwo',`HELPID_RULEWIZARD_APP_BLOCK')} to continue defining a permit rule.

Create Block Rule: Block Communication by One or by All Applications

The Rule Assistant indicates the type of communication that the rule will block. You must choose whether the rule should block this type of communication only when using the application shown or block this type of communication when using any application.

Click here {button ,JI(`>maintwo',`HELPID_RULEWIZARD_SERVICE_BLOCK')} to continue defining a permit rule.

Create Block Rule: Block Communication by One or by All Services

The Rule Assistant indicates the type of communication that the rule will block and whether the rule applies to a specific application or applies to any application.

Now choose whether the rule should block this type of communication only when using the remote service shown or block this type of communication when using any service.

Click here {button ,JI(`>maintwo',`HELPID_RULEWIZARD_TYPE_BLOCK')} to continue defining a permit rule.

Create Block Rule: Block Communication by One or by All ICMP Message Types

The Rule Assistant indicates the type of ICMP message that the rule will block.

You must choose whether the rule should block ICMP network communication only when using the ICMP message type shown or block ICMP communication when using any ICMP message type.

Click here {button ,JI(`>maintwo',`HELPID_RULEWIZARD_ADDR_BLOCK')} to continue defining a permit rule.

Create Block Rule: Block Communication with One or with All Addresses

- For TCP or UDP network communication, the Rule Assistant indicates the type of communication that the rule will block and what application(s) and service(s) it applies to.
- For ICMP network communication, the Rule Assistant indicates the type of communcation that the rule will block and what ICMP message type(s) it applies to.

Now choose whether the rule should block this type of communication only when communicating with the address shown or block this type of communication when communicating with any address.

Click here {button ,JI(`>maintwo',`HELPID_RULEWIZARD_FINISH_BLOCK')} to continue defining a permit rule.

Create Block Rule: Rule Summary

The Rule Assistant proposes a name for the rule you are creating. If you want to enter a different name for the rule, type it in the box. The rule name will be added to the Firewall Rule list on the Firewall tab in the Settings dialog box. Specify a name that allows you to identify what the rule does.

The rule summary indicates the properties you've defined for the rule. If you want to change any of the rule properties, select the alternative setting from one of the drop-down lists or click Back to reach the panel that determines the property you want to change.

If you want an entry to be written to the Firewall event log when any network communication matches this rule, select the Write check box.

Click Finish to create the block rule.

- The rule is applied for the current communication event and for all future events of this type.
- The rule is added to the list of rules maintained on the Firewall tab in the Advanced Settings dialog box.

Click here ● for more information

Norton Internet Security Alert

This alert indicates that your PC is attempting some form of network communication, but there are no firewall rules in place to deal with it. In this situation, Norton Internet Security provides three options:

- Configure a rule for the future: Creates a firewall rule using the Rule Assistant, a wizard that guides you through the rule-creation process. Once you create a new rule for the program, Norton Internet Security will not need to alert you in the future.
- Block this network communication this time: Blocks the network connection one time. No firewall rule is created.
- Permit this network communication this time: Permits the network connection one time. No firewall rule is created.

Click here ● for more information.

Create Rule: Specifying Network Communication Settings

The Rule Assistant indicates the type of communication that the rule will permit. You must choose whether the rule should permit this type of communication only when using the application shown or permit this type of communication when using any application.

Click here ● for more information.

Create Permit or Block Rule: Choosing a Category

The Rule Assistant prompts you to select a category for the application. Once the application has been categorized, you can then block or give it access to the network using Norton Internet Security's Parental Control feature.

Click here ● for more information.

Inbound Communication Attempt from an Unknown Application

If Norton Internet Security notifies you that an “unknown application” is attempting to connect to your system, it may mean that an intruder is trying to gain access to your PC. Although an attack of this type does not pose a security threat (no corresponding service is running on your PC to allow the connection), you may prefer to create a firewall rule to prevent the warning from appearing in the future.

● To create a firewall rule using the Rule Assistant, click **Configure a rule for the future** in the Alert dialog box.

Click here ● for more information.

Create Block Rule: Rule Summary

The Rule Assistant proposes a name and properties for the rule you are creating. Click **Finish** to create the rule.

Click here ● for more information.

Norton Internet Security Advanced Settings dialog box

Web

Use options on this tab to specify on a per site basis how ad blocking, privacy, and active content are handled when using your browser to connect to various Web sites.

Ad blocking

The settings on this tab let you maintain global and site-specific ad blocking lists. An ad blocking list consists of HTML strings that are used by the Ad Blocking filter to prevent ads and images from being displayed on web pages.

Privacy

On this tab, you can define both global and site-specific settings to control what information your browser sends in the referer field, User-agent field and email field when getting pages from a Web site. You can also define how Norton Internet Security handles the return of cookies to a requesting Web site.

Active Content

The settings on this tab let you define global and site-specific settings to prevent web pages from running the following types of programs: JavaScript, Java applets, VBScript, and ActiveX controls. In addition, you can specify that animated images on web pages should not repeatedly display the animation sequence.

Firewall

On this tab, you can create and edit firewall rules to control which applications and services are permitted to make connections and what types of packets can go out or come into the PC over various protocols.

Other

On this tab, you can configure the taskbar icon to be visible on the desktop, as well as set other options.

Web Settings: Overview

The Web tab allows you to change ad blocking, privacy and active content settings for individual Web sites:

Ad blocking
The settings on this tab let you maintain global and site-specific ad blocking lists. An ad blocking list consists of HTML strings that are used by the Ad Blocking filter to prevent ads and images from being displayed on web pages.

Privacy
On this tab, you can define both global and site-specific settings to control what information your browser sends in the referer field, User-agent field and email field when getting pages from a Web site. You can also define how Norton Internet Security handles the return of cookies to requesting Web sites.

Active Content
The settings on this tab let you prevent web pages from running the following types of programs: JavaScript, Java applets, VBScript, and ActiveX controls. In addition, you can specify that animated images on web pages should not repeatedly display the animation sequence.

Choose an item for more information:

Add Site

Remove Site

Ad Blocking

Privacy

Active Content

Working with a proxy server

Your PC may connect to the Internet through a proxy server, which causes all HTTP communication to go through the port used by the proxy server. If HTTP communication is conducted through a non-standard port, you should add the port to the Port List.

Choose an item for more information:

How to determine whether Norton Internet Security is working with your proxy server

How to determine what port to monitor for HTTP communication

Add site

Click this button to open the New Site/Domain dialog box, which you can use to add a new site or domain to the hierarchical site list in the left pane. Then, type a Web site name or domain name and click OK to add it to the site list.

After adding a site, you can select it in the site list. Use settings on the Ad Blocking, Privacy, and Active Content tabs to specify rules and block list entries that Norton Internet Security uses only when you visit this Web site.

Click here ● for more information.

Remove site

To remove a site name or domain name from the site list on the Web tab, select it and then click Remove. Norton Internet Security prompts for confirmation before it removes the entry.

When a site or domain is removed, the site-specific or domain-specific ad blocking list and the privacy and active content settings are discarded.

If you remove a domain, all of the site entries beneath that domain are promoted within the Site list hierarchy to become second-level entries.

Click here ● for more information.

About the site list

On the Web tab in the Settings dialog box, a hierarchical site list shows each of the domains and sites for which web settings have been defined.

When you click a site in the list, the Ad Blocking, Privacy, and Active Content tabs show the settings defined for that site. Use options on the Ad Blocking, Privacy, and Active Content tabs to maintain site-specific settings for the currently selected site.

- To add a new site or domain to the site list, click Add Site.
- To remove a site or domain from the site list, click Remove Site.

Understanding the site list's tree structure

The site list uses a tree structure that can be up to three levels deep:

- At the root of the site list is (Defaults). Select (Defaults) to view the contents of the default blocking list that is applied to all sites.
- Each second-level entry in the site list may be either a domain name or a site name.
- Third-level entries in the site list are always site names for hosts within a domain.

When you add a domain name to the site list, any sites within the domain are organized as third-level entries beneath the domain name. For example, if you added the domain name ajax.com, then site entries for the web servers www.ajax.com and news.ajax.com would appear as third-level entries beneath ajax.com.

Removing a domain does not remove any site entries that are beneath that domain. If you remove a domain, all of the site entries beneath that domain are promoted within the site list hierarchy to become second-level entries.

Sites vs. domains in the site list

If you add a domain to the site list, you can create privacy and active content settings for the domain that will be used as defaults for all web servers within the domain. If you define a domain-specific ad blocking list, Norton Internet Security will use the domain list plus the (Defaults) list to perform ad blocking at any site within the domain that does not have its own site-specific block list.

If you add a site, you can create privacy and active content settings for the site that override the default settings defined for the (Defaults) site or for the domain that owns this site. If you define a site-specific ad blocking list, Norton Internet Security will use the site list plus the (Defaults) list to perform ad blocking.

Understanding the relationship between (Defaults) and the other entries in the site list

- Click (Defaults) to see or update the block strings that will be used at all sites to block ads. In addition:
- Sites will use the Privacy rules defined for (Defaults) if no site-specific Privacy rule exists and the Cookie Assistant is not enabled
- Sites will use the Active Content rules defined for (Defaults) if no site-specific Active Content rule exists and the Java/ActiveX Assistant is not enabled
- Click any site in the list to see the block strings that will be used only at that site to permit or block ads and images. In addition, you can see the current rules defined for privacy and active content at that site.
- To determine what active content and privacy rules are in effect at a site, select the site in the site list (left pane):
- Privacy tab: If the **Use these rules for <site>** check box is cleared, a message appears at the bottom of the tab indicating how Norton Internet Security is determining what privacy rules to use.
- Active Content tab: If the **Use these rules for <site>** check box is cleared, a message appears at the bottom of the tab indicating how Norton Internet Security is determining what active content rules to use.

Ad Blocking tab

The options on this tab let you maintain the (Defaults) ad blocking list and site-specific ad blocking lists, which are used to prevent ads and images from being displayed on web pages.

When ad blocking is enabled, all HTML pages are scanned for the HTML strings specified in the site-specific blocking list plus the (Defaults) blocking list. Any HTML statement that contains a matching HTML blocking string is removed from the page by Norton Internet Security before the page is interpreted and displayed by the web browser.

Choose an item for more information:

Overview: How Norton Internet Security Uses Ad Blocking Lists

Add

Modify

Remove

Click here ● for more information.

How Norton Internet Security uses the ad blocking lists

When you visit a Web site, Norton Internet Security performs ad blocking by consulting two ad blocking lists: the (Defaults) list and the site-specific list.

When ad blocking is enabled and you connect to a Web site, Norton Internet Security scans HTML pages at the site for the strings specified in the ad blocking list for that site. In addition, Norton Internet Security checks for matches to the strings specified in the ad blocking list for (Defaults). Norton Internet Security looks for matching strings within HTML tags that are used to present graphics and advertising. The HTML structures that contain a matching string are removed from the page by Norton Internet Security before the page is interpreted and displayed in the web browser.

About the (Defaults) ad blocking list

Norton Internet Security provides a pre-defined (Defaults) ad blocking list that is applied globally to the content of all Web sites. You can add, modify, and remove strings in the (Defaults) block list.

About the site-specific ad blocking list

You can create a site-specific ad blocking list that is applied only to web pages received from that site. Block strings on the site-specific list are used in addition to the block strings on the (Defaults) list.

Using Permit strings to override ad or image blocking at a specific site

Occasionally, you'll encounter a block string in the (Defaults) list that removes content you want to block at most sites, but that you need to permit in order to see content at a particular site. On a per site basis, you can override the blocking effect of any string in the (Defaults) block list. Simply add the same string to the site-specific ad blocking list and define it as a permit string. Then, when Norton Internet Security scans the HTML pages from that site, any HTML statement that contains a matching HTML string is allowed to remain on the page.

Considerations when adding block strings

The way that you define block strings will affect how restrictive or unrestrictive Norton Internet Security will be when filtering data.

For example, if you added the string ajax.com to the (Defaults) block list, you would end up blocking everything that comes from the ajax.com domain. If you were much more specific and added the string nifty_images/image7.gif to the site-specific block list maintained for www.ajax.com, you would probably end up blocking only that one particular image on one particular web page.

Add

The Add button opens the Add New HTML String dialog box where you can add a new HTML string to the selected blocking list.

To add a new HTML string:

1 In the left pane, select the site blocking list you want to work with:

- To add a string to the (Defaults) blocking list, click **(Defaults)** in the site list.
- To add a string to a site-specific blocking list, click the site or domain name in the site list.

2 On the Ad Blocking tab, click Add.

3 Type the HTML string you want to add and then specify whether you want to block or permit this string when it is found on web pages.

Note: HTML strings in the (Defaults) list are always used for blocking purposes. You cannot create a permit string in the (Defaults) list.

When ad blocking is enabled and you connect to a Web site, Norton Internet Security scans HTML pages at the site for the strings specified in the ad blocking list for that site. In addition, Norton Internet Security checks for matches to the strings specified in the ad blocking list for (Defaults). Norton Internet Security looks for matching strings within HTML tags that are used to present graphics and advertising. The HTML structures that contain a matching string are removed from the page by Norton Internet Security before the page is interpreted and displayed in the web browser.

Click here ● for more information.

Modify

To change an HTML string in a block list on the Ad Blocking tab, click the HTML string you want to update and then click Modify. In the Modify HTML String dialog box, you can type changes to replace the current string and you can specify whether this HTML string should be blocked or permitted.

Note: HTML strings in the (Defaults) list are always used for blocking purposes. You cannot create a permit string in the (Defaults) list.

When ad blocking is enabled and you connect to a Web site, Norton Internet Security scans HTML pages at the site for the strings specified in the ad blocking list for that site. In addition, Norton Internet Security checks for matches to the strings specified in the ad blocking list for (Defaults). Norton Internet Security looks for matching strings within HTML tags that are used to present graphics and advertising. The HTML structures that contain a matching string are removed from the page by Norton Internet Security before the page is interpreted and displayed in the web browser.

Click here ● for more information.

Remove

To remove an HTML string from a block list on the Ad Blocking tab, select it and then click Remove. Norton Internet Security will prompt for confirmation before removing the string.

Click here ● for more information.

Web Settings: Privacy Tab

The privacy settings allow you to define rules to control how your browser handles requests for various types of information made by the sites that you visit.

The **Cookies** setting allows you to specify how Norton Internet Security handles requests for cookies when you visit a site.

The **Referer** setting allows you to specify whether third-party sites are provided with information about what site triggered a request for data from their server.

The **Browser (User-agent)** setting allows you to specify whether sites are provided with information about what kind of browser you are using.

The **E-mail (From)** setting allows you to specify whether sites are given the email address that your browser uses to identify you as the sender of mail.

Choose an item for more information:

Cookies

Referer

Browser (User-agent)

E-mail (From)

Click here ● for more information.

Cookies

Some advertisers use cookies to track users on a variety of sites and send the information back to their corporate server. This setting specifies how Norton Internet Security handles requests for cookies for the current site.

There are three ways to handle a site's requests for cookies:

Permit When selected, Norton Internet Security permits your browser to return cookies

Block When selected, Norton Internet Security prevents your browser from returning cookies.

Reply When selected, Norton Internet Security returns the string specified in the **Cookie** box instead of the cookie.

If the **Use these rules for <site>** check box is cleared, the **Cookies** settings are not available. In this case, a message below the **Use these rules for <site>** check box indicates how Norton Internet Security is determining what privacy rules to use.

Troubleshooting Tip

In some cases, blocking a cookie or substituting a cookie reply may make it impossible to link to pages within a Web site.

Sites may use cookies to store your own Web site configuration, to remember items placed in your shopping cart at an online shopping site, or to store account and password information for subscription sites. For sites such as these, you can set up a site-specific rule to permit cookies.

Click here ● for more information.

Referer

Specifies whether third-party sites are provided with information about what site triggered a request for data from their server. By default, the **Referer** field is blocked.

For example, a web page may present an advertisement by including instructions for the browser to request the advertisement from a third-party site. As part of your browser's request for the advertisement, it provides information to the advertising site about the identity of the site you visited that triggered the request. This information is passed in a referer field in the HTTP GET header (which the browser uses to make the request).

There are three ways to handle requests for referral information:

Permit Allows your browser to reveal the URL of the page that triggered the request for data.

Block Prevents your browser from telling a site the URL of the page you were visiting that triggered the request for data.

Reply Directs your browser to insert a specific string in place of the referral data that is usually sent in the referer field.

Troubleshooting Tip

In rare cases, blocking a **Referer** field or substituting a **Referer Reply** may make it impossible to link to pages within a Web site. A Web site may use the **Referer** field to set criteria for whether pages can link to its server. For example, suppose the BeBop Concert Hall Web site provides concert reviews and sells tickets at its site. The BeBop site may not want to allow the web pages of rival ticket agencies to provide links to the concert review pages at the BeBop site. In this case, the BeBop site can check the **Referer** field to determine whether it contains a URL within the BeBop site. If it doesn't—meaning that the link came from a page outside the BeBop site—then the BeBop web server can be configured to refuse to respond to the server request.

Click here ● for more information.

Settings Dialog Box: Privacy Tab

Browser (User-agent)

Specifies whether sites are provided with information about what kind of browser and operating system you are using. If you enable the privacy filter, the **Browser (User-agent)** field is permitted by default.

There are three ways to handle requests for browser and operating system information:

Permit Allows your browser to reveal what kind of browser and operating system you are using.

Block Prevents your browser from revealing what kind of browser and operating system you are using.

Reply Directs your browser to insert a specific string in place of the browser and operating system information that is usually sent in the User-agent field.

Notes

Most sites that check the **User-agent** field are attempting to provide customized page content that is compatible with your browser and operating system. However, malicious sites may want browser and operating system information in order to proceed with some type of attack. Misidentification helps to resist this type of attack.

E-mail (From)

Specifies whether sites are given the email address that your browser uses to identify you as the sender of mail. If the privacy filter is enabled, the **E-mail (From)** field is blocked by default.

There are three ways to handle requests for email identity information:

Permit Allows your browser to provide the email address that you've defined for use as the senders address in messages that you send.

Block Prevents your browser from providing the email address that you've defined for use as the sender's address in messages that you send.

Reply Directs your browser to insert a specific string in place of the email address that may be sent in the From field.

Active Content tab

The settings on this tab let you prevent web pages from running the following types of active content: JavaScript, VBScript, Java applets, and ActiveX controls. In addition, you can specify that animated images on web pages should not repeatedly display the animation sequence.

Choose an item for more information:

Script Blocking

Binary Executable Blocking

Miscellaneous Blocking

Click here ● for more information.

Script Blocking

Some web pages use JavaScript or VBScript to display advertising, open secondary (popup) windows, or perform other actions when you load the web page. Using the Script control, you can configure the script-blocking behavior of individual sites or of (Defaults).

- Select **Block all script** to prevent JavaScript and VBScript from running. When this option is selected, Norton Internet Security comments out all of the HTML code within <script> </script> tags to block execution of these scripts.
- Select **Block script popups only** to prevent scripts from displaying secondary or popup windows but allow them to perform other actions. When this option is selected, Norton Internet Security examines the strings within HTML <script> </script> tags, and removes any open method JavaScript calls.
- Select the **Allow all script to execute** to let JavaScripts and VBScripts work normally.
- Select the **Use default script behavior** to let (Defaults) control the blocking behavior of an individual site. Click (Defaults) to view the script blocking setting.

Note

- Some web pages may fail to work correctly if JavaScript or VBScript is blocked.
- When **Block all script** is enabled, your browser may display a JavaScript error when it attempts to open a web page. In most cases, you can click OK to dismiss the error and continue viewing the web page.

Binary Executable Blocking

Some web pages use Java applets or ActiveX controls to display advertising, open windows, or perform other actions when you load the web page. Using the Binary Executable controls, you can configure the Java/ActiveX blocking behavior of individual sites.

Note: The Binary Executable settings for (Defaults) is configured in the Security window and cannot be overridden using the Active Content controls.

- Select **Block Java applets** and **Block ActiveX controls** to prevent these forms of active content from running.
- Select **Allow Java applets to execute** and **Allow ActiveX controls to execute** to let these programs work normally.
- Select **Use default Java applet behavior** and **Use default ActiveX behavior** to let (Defaults) control the blocking behavior of the individual site. Click (Defaults) to view the Java applet and ActiveX settings.

Tip: If either **Block Java applets** or **Block ActiveX controls** is enabled, your browser may display an error when it attempts to open a web page. In most cases, you can click OK to dismiss the error and continue viewing the web page.

Make Animated Images Non-repeating

To display an animated image (.GIF) on a web page, a series of graphic images are shown. The series of images are displayed repeatedly to create the animation effect.

- Select **Block animation repeating** to prevent web pages from repeatedly displaying a series of graphic images that create an animation. When selected, an animated graphic series is displayed only once when a page is accessed.
- Select **Allow animations to repeat** to let the animated GIF file run normally.
- Select **Use default animation behavior** to let (Defaults) control the animated GIF file. Click (Defaults) to view the animated GIF setting.

Click here ● for more information.

Firewall Settings

Firewall rules specify what forms of network communication your PC is permitted and what services and applications can communicate with it. You can add, modify, remove, and temporarily disable firewall rules.

Choose an item for more information:

Firewall Rules

Add

Modify

Remove

Test

Click here ● for more information.

Firewall Rules

Lists the rules that are in effect when the firewall is enabled.

Tips

- Rules are processed in the order in which they are listed.
- Once a Block or Permit rule is matched, all remaining rules are ignored. In other words, additional rules that match this type of communication are ignored if they appear below the first rule that matches.
- If an Ignore rule is matched, the type of communication that was attempted is logged to the firewall event log and then the rule processing continues until another match occurs. If there is no match, the communication is either blocked by default or the Rule Assistant is invoked.

To move a rule in the list order, click it and then use the up arrow or down arrow button to change its location in the order.

- Any TCP/IP communication that is not covered by existing firewall rules is blocked by default.
- To add a rule, click Add, and then use options in the Add Firewall Rule dialog box to define the new rule.
- To modify a rule, select it and then click Modify.
- To remove a rule from the list, select it and then click Remove.
- To temporarily disable a rule for test purposes, clear the rule’s checkbox. The rule remains disabled until you reboot the PC or another user logs in.

Click here ● for more information.

Firewall Tab

Add Click Add to open the Add Firewall Rule dialog box, where you can define a rule to permit, block, or ignore a specific type of network communication.

Modify To change a firewall rule, click the rule and then click Modify to open the Change Firewall Rule dialog box, where you can change the characteristics of the rule.

Remove To remove a firewall rule, click the rule and then click Remove.

Test Opens the Test Firewall dialog box, where you can test whether a specified type of network communication would be permitted or would be blocked by existing firewall rules.

Note: You don't have to enable the firewall in order to test the firewall rules.

Add Firewall Rule

Use settings in the Add Firewall Rule dialog box to define network communication rules for an application, a service, or an address.

Choose an item for more information:

Name

Action

Direction

- Protocol
- Category
- Application tab (TCP and UDP only)
- Service tab (TCP and UDP only)
- Address tab
- Logging tab

Add Firewall Rule: Name

Enter a descriptive name that identifies the rule you want to add. This rule name will appear in the **Firewall Rule** column in the rules list on the Firewall tab. The rule name will also appear in the Firewall Event Log if you choose to log events for the rule.

Add Firewall Rule: Action

Specifies whether the rule permits, blocks, or ignores the type of network communication defined within the rule.

Permit Allows communication of this type to take place.

Block Prevents communication of this type from taking place.

Ignore Updates the firewall event log each time communication of this type takes place. Rule processing then continues until a match is found. If there is no match, the communication is either blocked by default or the Rule Assistant is invoked.

How To Use Ignore Rules

When an Ignore rule is matched, logging occurs and then firewall processing continues in an attempt to match the communication to a subsequent Permit or Block firewall rule.

Note: For an Ignore rule to work effectively, it must appear in the firewall rule list above any related Permit or Block rule for that type of communication. It's a good idea to move all Ignore rules to the top of the firewall rule list.

The **Ignore** setting is intended to allow you to log some type of communication activity prior to enforcing a Permit rule or Block rule that applies to that type of communication. For example, suppose you have a Permit firewall rule that allows your FTP server to communicate with any network address. You could track how often users at a particular network address were connecting to your FTP server by setting up an Ignore rule to log instances of FTP server communication to and from that network address. The FTP server Ignore rule must precede the FTP server Permit rule.

How the Firewall Processes Rules

The rules in the firewall rules list are processed in the order in which they are listed.

- Once a Block or Permit rule is matched, all remaining rules are ignored. In other words, additional rules that match this type of communication are ignored if they appear below the first rule that matches.
- If an Ignore rule is matched, the type of communication that was attempted is logged to the firewall event log and then the rule processing continues until another match occurs. If there is no match, the communication is either blocked by default or the Rule Assistant is invoked.

To move a rule in the list order, click it and then use the up arrow or down arrow button to change its location in the order.

Add Firewall Rule: Direction

Specifies whether the rule applies to inbound network communication, outbound network communication, or network communication in either direction:

- Inbound communication involves packets sent to your PC.
- Outbound communication involves packets sent from your PC.

Add Firewall Rule: Protocol

Specifies what communications protocol the rule applies to: TCP only, UDP only, either TCP or UDP, ICMP only.

Add Firewall Rule: Category

Specifies the category of Internet application the rule applies to. Categorizing the application enables you to include or exclude the program using Norton Internet Security’s Parental Controls.

Add Firewall Rule: Application Tab

Settings on this tab allow you to define whether the rule applies to a single specified application or to any application that attempts the type of network communication covered by the rule.

Application If you want the rule to apply to a specific application, select **Application shown above**. Then enter the location and name of the application executable file.

- To search the file system for the application's location, click Browse.
- This setting is not available if **Any application** is selected.

Application Shown Above
When selected, specifies that the rule applies to the application identified in the **Application** box.

Any Application When selected, specifies that the rule applies to all applications on the local PC.

Browse Opens the Add Application From File System dialog box, where you can select the application that will be affected by the rule.

Add Firewall Rule: Service Tab

Settings on this tab allow you to define whether the rule applies to local or remote services, and whether it applies to a single specified service or to any service that attempts the type of network communication covered by the rule.

Choose an item for more information:

Remote Service

Local Service

Add Firewall Rule: Service Tab

Remote Service

In general, use the settings in this box if you are creating a rule that applies to outbound communication. This type of rule allows you to control communications to remote services from clients on your local machine.

Single service

Select this option if you want the rule to apply to a single type of remote service.

Any service

Select this option if you want the rule to apply to any remote service.

Service name or port

If you want the rule to apply to a single service, select **Single service**. Then enter the service name (for example, HTTP or FTP) or enter the port number used by that service.

Add Firewall Rule: Service Tab

Local Service

In general, use the settings in this box if you are creating a rule that applies to inbound communication. This type of rule allows you to control access to the servers running on your local machine.

Single service

Select this option if you want the rule to apply to a single type of local service.

Any service

Select this option if you want the rule to apply to any local service.

Service name or port

If you want the rule to apply to a single service, select **Single service**. Then enter the service name or enter the port number used by that service. For example, if you are running an FTP server on your PC, you might create rules that permit inbound communication to ports 20 and 21.

Add Firewall Rule: Address Tab

Settings on this tab allow you to define whether the rule applies to local or remote addresses, and whether it applies to a single specified address or to any address that attempts the type of network communication covered by the rule.

Choose an item for more information:

Remote Address

Local Address

Add Firewall Rule: Address Tab

Remote Address

In general, use the settings in this box if you are creating a rule that applies to communication to or from a remote computer.

Host address

Select this option if you want the rule to apply to a single remote IP address. Then specify the IP address or the name of the host in the **Address or host name** box.

Network address

Select this option if you want the rule to apply to a set of addresses (for example, all the PCs on a particular subnet). In the **Address** and **Subnet mask** boxes, enter the IP address and subnet mask that defines the network address.

Address range

Select this option if you want the rule to apply to a range of IP addresses. In the **First Address** box, enter the first (lowest) IP address in the range. In the **Last Address** box, enter the last (highest) IP address in the range.

Any address

Select this option if you want the rule to apply to communication to or from any remote address.

Add Firewall Rule: Address Tab

Local Address

In general, use the settings in this box if you are creating a rule that applies to communication to or from your PC.

Host address

Select this option if you want the rule to apply to a specific IP address for your PC. Then specify the IP address or the name of the host PC in the **Address or host name** box.

If your PC has network cards supporting multiple IP addresses or interfaces, this setting allows you to apply the rule to communication via a specific IP address or interface name. For example, if your PC is connected to a home network and also connects to the Internet, you might want to set up one rule that permits file sharing when you are connected to the home network, while setting up another rule that blocks file sharing when you are connected to the Internet.

If you want to set up a rule on a per-interface basis, you will need to determine the name or IP address of the interface. To do so:

1. Create a connection using the interface you are interested in.
2. Open the Norton Internet Security event log and click the Connection tab. Find the connection you opened and check the value in the **Local** column. The **Local** column shows the name of the currently active interface. Enter that name in the **Address or host name** box when creating a firewall rule for that interface.

Any address

Select this option if you want the rule to apply to communication to or from any IP address used by your local PC.

If your PC has network cards supporting multiple IP addresses, this setting allows you to apply the rule to communication via all the IP addresses used to connect to your machine.

Add Firewall Rule: Logging Tab

Settings on this tab allow you to specify whether Norton Internet Security should notify you when the current rule is matched and whether an event log entry should be logged.

Choose an item for more information:

Write an event log entry when this rule is matched

Log event after <n> matches

Show Security Alert when this rule is logged

Add Firewall Rule: Logging Tab

Write An Event Log Entry When This Rule Is Matched

Specifies that an entry is logged to the Firewall event log when network communication of the type described by the rule occurs.

Suppose that the rule you are creating permits your mail client application to perform outbound TCP communication to any remote service and any remote address. If you select this check box, then each time your mail client connects to the POP3 server via outbound TCP communication, an event is logged in the Firewall event log.

Tips

- Use the **Log event after <n> matches** setting to control how often an event is logged for this rule.
- Firewall events can be viewed on the Firewall tab in the Norton Internet Security Event Log viewer. Click the Norton Internet Security icon, which is in the notification area at the right side of the Windows taskbar. On the popup menu, click Event Log.

Add Firewall Rule: Logging Tab

Log Event After <n> Matches

Allows you to limit the frequency with which a rule match triggers a log event.

Specify the number of times a network communication event should match this firewall rule before a firewall event is logged or Status window notification occurs. Norton Internet Security counts how many times the rule is matched and writes a log event when the count reaches the number that you enter here.

For example, suppose that the rule you are creating permits inbound TCP communication to the FTP server running on your PC. If you specify a notification number of 20, then a single log event for this rule is written to the Firewall event log after 20 connections to your FTP server occur.

Tips

- This setting is unavailable if event logging for this rule is disabled. To enable event logging, select the **Write an event log entry when this rule is matched** check box.
- Norton Internet Security restarts the counter for rule matches whenever you restart your PC and whenever you add a new Firewall rule.

Add Firewall Rule: Logging Tab

Show Security Alert when this rule is logged

When selected, a Security Alert message is displayed at the bottom of the Status window when a network communication event matches this rule.

If you want to limit the frequency with which a rule match triggers notification in the Status window, use the **Log event after <n> matches** setting.

Tip: This setting is unavailable if event logging for this rule is disabled. To enable event logging, select the **Write an event log entry when this rule is matched** check box.

Test Firewall

You don't have to enable the firewall in order to test the firewall rules. Use settings in the Test Firewall dialog box to find out whether a specified type of network communication would be permitted or would be blocked by existing firewall rules.

To test the firewall:

1 Open the Norton Internet Security Advanced Settings dialog box and click the Firewall tab.

2 Click the Test button to open the Test Firewall dialog box.

3 In the Test Firewall dialog box, specify the properties of the type of communication you want to test.

To get help on a setting in the Test Firewall dialog box, click ? at the top of the dialog box, and then click the item.

4 Click Test to see how the firewall works with the type of communication you've specified.

Test result

- The **Test result** indicates whether the type of communication you are testing would be blocked or permitted. It also shows the name of the rule that matches the type of communication you are testing.
- If no rule matches the test condition, the **Test result** reports that the communication is blocked by the implicit block rule: when the firewall is enabled, any communication for which there is no rule defined is blocked by default.
- When you perform a firewall test and a rule matches the test condition, that rule is highlighted in the rules list on the Firewall tab in the Settings dialog box.

Other Settings

HTTP Port List. The HTTP Port List shows all of the HTTP port numbers monitored by Norton Internet Security. The default list contains all the standard HTTP ports, but you can add ports if you use applications that perform HTTP communication through nonstandard ports. For example, your PC may connect to the Internet through a proxy server which causes all HTTP communication to go through the port used by the proxy server. Web applications which use ports not covered in this list will not be filtered for ad blocking and active content blocking.

Block IGMP Protocol. Click to block the use of the Internet Group Management Protocol, a standard for IP multicasting on the Internet. Attackers sometimes exploit this protocol to hang a victim's machine once they obtain its IP address.

Block Fragmented IP Packet Headers. Click to block IP packets that have severely fragmented headers and contain data areas that are too small to be useful for legitimate network communications. IP packets of this type are used in system attacks.

Enable Automatic Firewall Rule Creation. Click to have Norton Internet Security automatically create firewall rules if an application attempts to connect to the network and there are no firewall rules already in place for that application. If this option is enabled, Norton Internet Security will create firewall rules for you that allow the application to connect to the network during the current session and in the future. You can review and edit these rules at a later time to adjust the way the firewall deals with the application.

If you want more control over the creation of firewall rules, you can disable this option so that you are prompted to create new firewall rules yourself using the Rule Assistant wizard.

Show Taskbar Icon

When selected, the Norton Internet Security program icon displays in the notification area on the taskbar (by default, in the right corner at the bottom of the screen). You can click the Norton Internet Security icon to open the program, log in to Norton Internet Security, or access other features.

Startup Options

Select one of these options to specify how and when the Norton Internet Security software starts on your PC:

Manual startup The Norton Internet Security software never starts automatically—you must start it manually. To start the software, click Start, point to Programs, then point to Norton Internet Security and click Start Norton Internet Security.

Run at system startup
The Norton Internet Security software is started automatically when you start your PC.

To filter the types of events displayed on the Event Log System tab:

● On the right side of the System tab, click the check box next to each event type you want to include in the Event Log viewer display. If an event type is not selected, its events will not be displayed.

Click here {button ,AL("Configure",0,`',`')} for more information.

To adjust the width of a column:

1 In the Event Log viewer, point to the boundary line on the right side of the column heading. The cursor changes from a pointer to a cross-hair.

2 Drag the boundary line to the desired width.

Click here {button ,AL("Display;Window",0,`',`')} for more information.

To refresh the displayed events:

- Click **Refresh** to update the current tab display with any new events that have been logged.

  By default, the data displayed in a tab refreshes automatically when you switch to that tab in the Norton Internet Security Event Log viewer.

Click here {button ,AL("Events",0,`',`')} for more information.

To clear the events from all event logs:

● On the Log menu, click **Clear All Tabs** to clear the events displayed on every tab in the Event Log viewer.

This clears the individual event log file maintained for each tab's event category. After a log is cleared, new events are recorded at the beginning of the log.

Click here {button ,AL("Events",0,`',`')} for more information.

To clear the events on the current tab:

● On the Log menu, click **Clear Tab** to clear the events displayed on the current tab.

This clears the event log file maintained for the event category shown on the tab. After the log is cleared, new events are recorded at the beginning of the log.

Click here {button ,AL("Events",0,`',`')} for more information.

To automatically clear the events on all tabs when you stop Norton Internet Security:

● On the Log menu, click **Clear All Tabs Upon Logoff** to automatically clear the contents of every event log file each time the Norton Internet Security software is stopped.

Click here {button ,AL("Events",0,`',`')} for more information.

To print log information:

1 Click the tab containing the information you want to print.

2 On the Log menu, click **Print Tab**.

Click here {button ,AL("Log File",0,`',`')} for more information.

To save log information as a text file:

1 Click the tab containing the information you want to save.

2 On the Log menu, click **Save Tab As**.

3 Specify a location and name for the text file.

Click here {button ,AL("Log File",0,`',`')} for more information.

To copy text from the Event Log viewer:

1 Select the text you want to copy.

2 On the Edit menu, click **Copy**. This copies the selected text to the Clipboard.

3 Use the Paste command of another application to add this text to a file.

Click here {button ,AL("Log File",0,`',`')} for more information.

To configure the size of an event log file:

1. Click the tab containing the log you want to configure.
2. On the Log menu, click **Change Tab Size**.
3. In the Size box, select the file size you want.

   This sets the maximum size for the event log file. When the event log file reaches its maximum, new events wrap to the beginning of the file.

You must restart your PC in order for the new log file size to be enforced. Changing the size of the log file causes the log to be cleared.

Click here {button ,AL("Log File",0,`',`')} for more information.

To keep the Statistics window visible at all times:

- On the View menu in the Statistics window, click **Always On Top**.

  This ensures that the Statistics window is always visible, even when you run a program in a full screen.

To open the Statistics Options dialog box:

- On the View menu in the Statistics window, click **Options**.

To configure the statistics categories for the Statistics window:

1 On the View menu, click **Options**.

2 The Statistics Options dialog box lists all of the category counters that you can display in the Statistics window.

3 You can do one of the following from here:

- To include a category of counters in the Statistics window, click the check box next to that category.
- To exclude a category of counters in the Statistics window, uncheck the check box next to that category.

Click here {button ,AL("Display in stats",0,`',`')} for more information.

To configure the column display in the Statistics window:

- On the View menu, point to columns and click one of the following options:
- **Automatic**: When you resize the Statistics window, automatically adjusts between a one and two column display, based on current window width.
- **One**: Counters are always displayed in a single column within the Statistics window.
- **Two**: Counters are always displayed in two columns within the Statistics window.

Click here {button ,AL("Display in stats",0,`',`')} for more information.

To reset counters in the Statistics window:

- On the View menu in the Statistics window, click **Reset Values**.

Click here {button ,AL("Display in stats",0,`',`')} for more information.

To save statistics to a text file:

1. On the File menu in the Statistics window, click **Save**.
2. Specify a location and name for the text file.

To print current statistics information:

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

To remove a site or domain from the list of sites configured for web filtering:

- To remove a site name or domain name from the site list in the left pane on the Web tab, click it in the list and then click Remove Site. Norton Internet Security prompts for confirmation before it removes the entry.

  Removing a domain does not remove any site entries that are beneath that domain. If you remove a domain, all of the site entries beneath that domain are "promoted" within the site list hierarchy to become second-level entries.

  When a site or domain is removed, the site-specific or domain-specific ad blocking list and the privacy and active content settings are discarded.

Click here {button ,AL("Managing block list",0,`',`')} for more information.

To change web settings for a site:

1 In the Norton Internet Security Advanced Settings dialog box, click the **Web** tab.

2 In the site list in the left pane, click the site name.

The settings shown on the Ad Blocking, Privacy, and Active Content tabs apply to the site that is currently selected in the site list (in the left pane).

3 Click a tab to make its controls visible.

4 Modify any web settings for the site, then click **Apply** to put the changes into effect.

Click here {button ,AL("Managing block list",0,`',`')} for more information.

To specify which ports to monitor for HTTP communication:

1 Open the Norton Internet Security Advanced Settings dialog box.

2 Click the Other tab.

3 In the Other dialog box, you can do the following:

- To add a port to the HTTP Port List: Click **Add**, then enter the number of the port that you want the Norton Internet Security to monitor for HTTP communication.
- To remove a port from the HTTP Port List: Click the port number in the **HTTP Port List**, then click **Remove**.

Tips

- Network services (such as HTTP or FTP) use specific ports on your PC. For example, HTTP communication is usually conducted through port 80. Norton Internet Security filters all HTTP communication sent and received through the ports in the **HTTP Port List**, applying the blocking options that you have enabled.
- Your PC may connect to the Internet through a proxy server, which causes all HTTP communication to go through the port used by the proxy server. Or you may use an application that performs HTTP communication through a nonstandard port. If HTTP communication is conducted through a non-standard port or a proxy server, you should add the port to the **HTTP Port List**.

To determine whether Norton Internet Security works with your proxy server:

Check Norton Internet Security Statistics to see if Norton Internet Security is doing HTTP filtering.

1 Click **Options** in the Norton Internet Security toolbar.

2 Click **Internet Security**.

3 Click **View Statistics**.

2 In the Web category, look at the Bytes Processed counter.

3 Confirm that Ad blocking is enabled:

- **a** In the Status window, confirm that Norton Internet Security is enabled.
- **b** Check **Ad Blocking**.

4 Use your browser to connect to a Web site.

5 If Norton Internet Security is filtering, the Bytes Processed counter in the Statistics window should increase as you access web pages:

● If the Bytes Processed counter stays at 0 and Ad blocking filtering is enabled, then Norton Internet Security is probably not monitoring the port used by your proxy server. Click here for help to determine what port to monitor for HTTP communication.

● If the Bytes Processed counter increases when you access web pages but you are not seeing ad blocking, try clearing your browser cache completely to make sure the web pages are not coming from the browser cache.

Click here {button ,AL("proxy config",0,`',`')} for more information.

To determine what port to monitor for HTTP communication:

1 Make a connection to a Web site.

2 In the Event Log, click the Connections tab.

3 Look at the information in the Remote column.

   There should be a port number next to the IP address of the site you accessed with your browser. This number is the port number that was used to access your proxy server for your web connection.

4 Norton Internet Security needs to perform filtering on this port number. You might need to add the port number to the list of ports that are filtered.

   a Open the Other tab in the Norton Internet Security Advanced Settings dialog box.

   b The **HTTP Port List** shows all the ports that the Ad Blocker monitors for HTTP communication when ad blocking is enabled.

   c Click Add to add a port number to the list.

Click here {button ,AL("proxy config",0,`',`')} for more information.

To set up default settings for privacy rules:

You can configure Norton Internet Security so that it uses a set of default privacy rules at all sites for which no site-specific or domain-specific privacy rules are defined.

To set up default privacy rules:

1 Open the Web tab in the Norton Internet Security Advanced Settings dialog box.

2 In the site list in the left pane, click **(Defaults)**.

3 Use options on the Privacy tab to specify default rules for **Cookies,** and for the HTTP Header fields: **Referer**, **Browser (User-agent)**, and **E-mail (From)**.

Norton Internet Security uses privacy rules from (Defaults) when no site-specific or domain-specific privacy rules are defined and the Cookie Assistant disabled.

Click here {button ,AL("Privacy tab",0,`',`')} for more information.

To see what privacy rules are in effect at a site:

1 Open the Web tab in the Norton Internet Security Advanced Settings dialog box.

2 Click the site in the site list (left pane). If the **Use These Rules For <site>** check box is unchecked, a message appears at the bottom of the Privacy tab indicating how Norton Internet Security is determining what Privacy rules to use.

Click here {button ,AL("Privacy tab",0,`',`')} for more information.

To create privacy rules for a specific Web site:

You can configure site-specific privacy rules for Norton Internet Security to use whenever you visit a particular Web site.

To set up site-specific privacy rules:

1 Open the Web tab in the Norton Internet Security Advanced Settings dialog box.

2 In the site list in the left pane, click the site that you want to work with.

3 Click the **Use These Rules For <site>** check box.

4 Use options on the Privacy tab to specify site-specific rules for Cookies, and for the HTTP Header fields: Referer, Browser (User-agent), and E-mail (From).

Tips

- Norton Internet Security ignores all privacy rules if Privacy is not enabled.
- When the privacy filter is enabled and the Use These Rules For <site> check box is checked, Norton Internet Security will use the site's privacy rule settings whenever you visit the current site.
- If the Use These Rules For <site> check box is unchecked, a message appears at the bottom of the Privacy tab indicating how Norton Internet Security is determining what Privacy rules to use.

Click here {button ,AL("Privacy tab",0,`',`')} for more information.

To create privacy rules for web servers within a domain:

You can configure domain-specific privacy rules for Norton Internet Security to use whenever you visit any site within the specified domain. To set up domain-specific privacy rules:

1 Open the Web tab in the Norton Internet Security Advanced Settings dialog box.

2 Click the **Privacy** tab.

3 In the site list in the left pane, click the domain that you want to work with.

4 Click the **Use These Rules For <domain>** check box.

5 Use options on the Privacy tab to specify domain-specific rules for Cookies, and for the HTTP Header fields: Referer, Browser (User-agent), and E-mail (From).

Click here {button ,AL("Privacy tab",0,`',`')} for more information.

To specify default settings for Norton Internet Security's active content rules:

You can configure Norton Internet Security so that it uses a set of default active content rules at all sites for which no site-specific or domain-specific active content rules are defined.

To set up default active content rules:

1 Open the Web tab in the Norton Internet Security Advanced Settings dialog box.

2 Open the Active Content tab.

3 In the site list in the left pane, click **(Defaults)**.

4 Use options on the Active Content tab to specify default rules to handle Java and ActiveX content and to control animated images.

Norton Internet Security uses active content rules from (Defaults) when no site-specific or domain-specific active content rules are defined and the Java/ActiveX Assistant is not enabled.

Click here {button ,AL("Active Content tab",0,`',`')} for more information.

To create active content rules for a specific Web site:

You can configure site-specific active content rules for Norton Internet Security to use whenever you visit that site.

To set up site-specific active content rules:

1 Open the Web tab in the Norton Internet Security Advanced Settings dialog box.

2 Open the Active Content tab.

3 In the site list in the left pane, click the site that you want to work with.

4 Click the **Use These Rules For <site>** check box.

5 Specify site-specific rules to handle Java and ActiveX content and to control animated images.

Click here {button ,AL("Active Content tab",0,`',`')} for more information.

To permit the display of all ads and images at a specific site:

You can set up a single site-specific permit rule that allows the display of all ads and images at a particular site.

1 Open the Web tab in the Norton Internet Security Advanced Settings dialog box.

2 Open the Ad Blocking Content tab.

3 In the site list in the left pane, click the site that you want to work with.

3 Click **Add**.

4 In the Add New HTML String dialog box, click **Permit.**

5 In the text box type a forward slash character ("/").

Permit rules take precedence over Block rules for any given site.

All web addresses use the "/" (forward slash character). Setting up a permit rule for HTML display codes that contain "/" effectively gives blanket permission to display all images and ads at the site.

Click here {button ,AL("Active Content tab",0,`',`')} for more information.

To permit the display of some ads and images at a specific site:

You can set up site-specific permit rules that override a matching block rule in the (Defaults) block list.

1. Open the Web tab in the Norton Internet Security Advanced Settings dialog box.
2. Open the Ad Blocking Content tab.
3. In the site list in the left pane, click the site that you want to work with.
4. Click **Add**.
5. In the Add New HTML String dialog box, click **Permit.**
6. Enter the HTML string to permit.

   The HTML string you specify is added to the ad blocking list maintained for the selected site.

   Permit rules take precedence over Block rules for any given site.

To specify what ads and images to block at all sites:

Norton Internet Security provides a pre-defined (Defaults) ad blocking list that is applied globally to the content of all Web sites.

To make additions to this global ad blocking list:

1 Open the Norton Internet Security Advanced Settings dialog box and click the Web tab.

2 In the site list in the left pane, click **(Defaults)**.

The Ad Blocking tab displays all of the HTML strings that are currently defined for the (Defaults) block list.

3 On the Ad Blocking tab, click **Add**.

4 Enter an HTML string to block.

The HTML string you specify is added to the (Defaults) ad blocking list.

Tips

● When ad blocking is enabled, all HTML pages are scanned for the HTML strings specified in the (Defaults) list. Norton Internet Security looks for the block strings within HTML tags that are used to present graphics and advertising. The HTML structures that contain a matching string are removed from the page by Norton Internet Security before the page is interpreted and displayed in the web browser.

● On a per site basis, you can override the blocking effect of any string in the (Defaults) block list. Simply add the same string to the site-specific ad blocking list and define it as a Permit string. Then, when Norton Internet Security scans the HTML pages from that site, any HTML statement that contains a matching HTML string is allowed to remain on the page.

Click here {button ,AL("Ref graphics",0,`',`')} for more information.

To specify what ads and images to block at a single site:

You can maintain site-specific ad blocking lists with Norton Internet Security. A site-specific block list is applied only to the content of web pages from a specified Web site.

Automatically create site-specific block lists

You can drag images and ads to the ad trashcan or paste image or link location information in the ad trashcan. Before Norton Internet Security adds the new block list entry, you can choose if you want to block the entire string or if you want to highlight a portion of the string so that it applies to more than one image or link location.

To manually create a site-specific block list:

1 Open the Norton Internet Security Advanced Settings dialog box and click the Web tab.

2 On the left pane, click **Add Site**.

3 Enter the Web site name, for example, "www.ajax.com." To create a block list to all web servers within a domain, enter the domain name, for example, "ajax.com."

The new site or domain name is added to the site list displayed in the left pane on the Web tab.

To manually add to the ad blocking list that applies to a specific Web site:

1 Open the Norton Internet Security Advanced Settings dialog box and click the Web tab.

2 Open the Ad Blocking tab.

2 In the site list in the left pane, click the site that you want to work with.

3 Click **Add**.

4 Enter an HTML string to block or to permit. The HTML string you specify is added to the ad blocking list maintained for the selected site.

Click here {button ,AL("Ref graphics",0,`',`')} for more information.

To add a string to an ad blocking list:

1. Open the Norton Internet Security Advanced Settings dialog box and click the Web tab.
2. In the left pane, click the site you want to work with:
   - To add a string to the (Defaults) blocking list, click **(Defaults)** in the site list.
   - To add a string to a site-specific blocking list, click the site or domain name in the site list.
3. On the Ad Blocking tab, click **Add**.
4. Type the HTML string you want to add and then specify whether you want to block or permit this string when it is found on web pages.

   HTML strings in the (Defaults) list are always used for blocking purposes. You cannot create a Permit string in the (Defaults) list.

To change an HTML string in an ad blocking list:

1 Open the Norton Internet Security Advanced Settings dialog box and click the Web tab.

2 In the left pane, click the site you want to work with:

- To add a string to the (Defaults) blocking list, click **(Defaults)** in the site list.
- To add a string to a site-specific blocking list, click the site or domain name in the site list.

The HTML strings for the selected ad blocking list are displayed in the Ad Blocking tab.

3 In the HTML string list, click the string you want to modify.

4 Click **Modify**, and then type your changes to replace the current string. For site-specific ad blocking lists, you can specify whether this HTML string should be blocked or permitted.

Click here {button ,AL("URL info",0,`',`')} for more information.

To remove an HTML string from an ad blocking list:

1 Open the Norton Internet Security Advanced Settings dialog box and click the Web tab.

2 In the left pane, click the site you want to work with:

- To add a string to the (Defaults) blocking list, click **(Defaults)** in the site list.
- To add a string to a site-specific blocking list, click the site or domain name in the site list.

The HTML strings for the selected ad blocking list are displayed in the Ad Blocking tab.

3 In the HTML string list, click the string you want to remove.

4 Click **Remove**.

You are asked to confirm that you want to remove the string from the list.

Click here {button ,AL("Managing block strings",0,`',`')} for more information.

To enable Automatic Firewall Rule Creation:

1 Open the Norton Internet Security Advanced Settings dialog box and click the Other tab.

2 On the Other tab, click the **Enable Automatic Firewall Rule Creation** check box.

When Enable Automatic Firewall Rule Creation is enabled, Norton Internet Security will automatically create a new firewall rule for applications it knows about. If this option is not checked, you will be prompted to create the rule when the application is run.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

To temporarily disable a firewall rule:

1. Open the Norton Internet Security Advanced Settings dialog box and click the Firewall tab.
2. In the list of rules, a check mark next to the rule specifies whether or not the rule is currently in effect. To temporarily disable a rule, uncheck it.
3. To permanently disable a rule, remove it from the list (click the rule and then click Remove).

   Norton Internet Security will ignore all firewall rules if Security is not enabled.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

To open the Add Firewall Rule dialog box:

1 Open the Norton Internet Security Advanced Settings dialog box.

2 On the Firewall tab in the Norton Internet Security Advanced Settings dialog box, click **Add**.

To get to the Application tab in the Add Firewall Rule dialog box:

1. Open the Norton Internet Security Advanced Settings dialog box.
2. On the Firewall tab, click **Add** (for a new rule) or click an existing rule and then click Modify.
3. Click the **Application** tab.

To get to the Type tab in the Add Firewall Rule dialog box:

1 Open the Norton Internet Security Advanced Settings dialog box.

2 On the Firewall tab, click **Add** (for a new rule) or click an existing rule and click **Modify**.

3 In the Protocol box, click **ICMP**.

4 Click the **Type** tab.

To get to the Service tab in the Add Firewall Rule dialog box:

1 Open the Norton Internet Security Advanced Settings dialog box.

2 On the Firewall tab, click **Add** (for a new rule) or click an existing rule and then click **Modify**.

3 Click the **Service** tab.

To get to the Logging tab in the Add Firewall Rule dialog box:

1. Open the Norton Internet Security Advanced Settings dialog box.
2. On the Firewall tab in the Norton Internet Security Settings dialog box, click **Add** (for a new rule) or click an existing rule and then click **Modify**.
3. Click the **Logging** tab.

To get to the Address tab in the Add Firewall Rule dialog box:

1. Open the Norton Internet Security Advanced Settings dialog box.
2. On the Firewall tab, click **Add** (for a new rule) or click an existing rule and click **Modify**.
3. Click the **Address** tab.

To manually add the default ICMP firewall rules:

ICMP filtering will not be activated until you manually add an ICMP firewall rule as described:

1 Right-click the Norton Internet Security icon in the Windows system taskbar, then click **Settings**.

2 On the Firewall tab, click **Add**.

3 Create an outbound ICMP rule. In the Add Firewall Rule dialog box, fill in the following:

Name: Default Outbound ICMP

Action: Permit

Direction: Outbound

Protocol: ICMP

4 Then, on the Type tab click **Any Type**.

5 Click OK to add the rule.

6 Create an inbound ICMP rule. In the Add Firewall Rule dialog box, fill in the following:

Name: Default Outbound ICMP

Action: Permit

Direction: Outbound

Protocol: ICMP

7 On the Type tab click **Any Type**.

8 Click OK to add the rule.

To add a firewall rule:

You can maintain a list of firewall rules that specify what types of network communications are permitted with this PC.

1 Open the Norton Internet Security Advanced Settings dialog box.

2 On the Firewall tab, click Add.

Use options in the Add Firewall Rule dialog box to specify the network communication rule.

3 To move a rule in the firewall list order, click it and then use the up arrow or down arrow button to change its location in the order.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

To change a firewall rule:

1 Open the Norton Internet Security Advanced Settings dialog box and click the **Firewall** tab.

2 In the Firewall Rule list, click the rule you want to modify.

3 Click **Modify**, and then use options in the Modify Firewall Rule dialog box to make desired changes.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

To remove a firewall rule:

1 Open the Norton Internet Security Advanced Settings dialog box and click the **Firewall** tab.

2 In the Firewall Rule list, click the rule you want to remove.

3 Click **Remove**.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

To change the order in which firewall rules are processed:

1 Open the Norton Internet Security Advanced Settings dialog box and click the Firewall tab.

2 In the Firewall Rule list, click the rule you want to move, and then use the up arrow or down arrow button to change its location in the order.

Tips

● When the firewall is enabled, the rules in the firewall rules list are processed in the order in which they are listed.

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

● If an Ignore rule is matched, the type of communication that was attempted is logged to the firewall event log and then the rule processing continues until another match occurs. If there is no match, the communication is either blocked by default or the Rule Assistant is invoked.

● For an Ignore rule to work effectively, it must appear in the firewall rule list above any related Permit or Block rule for that type of communication. It's a good idea to move all Ignore rules to the top of the firewall rule list.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

To test the firewall:

1 Open the Norton Internet Security Advanced Settings dialog box.

2 On the Firewall tab, click **Test**.

3 In the Test Firewall dialog box, you can test whether a specified type of network communication would be permitted or would be blocked by existing firewall rules.

   You do not have to enable the firewall in order to test the firewall rules.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

To add a site or domain to the list of sites configured for web filtering:

1. Open the Norton Internet Security Advanced Settings dialog box and click the **Web** tab.
2. On the left pane, click **Add Site**.
3. Do one of the following:

- To create web filtering rules that apply to a specific Web site, enter the Web site name. For example, enter www.symantec.com.
- To create web filtering rules that apply to all servers within a domain, enter the domain name. For example, enter symantec.com.

The new site or domain name is added to the site list displayed in the left pane on the Web tab.

To access Norton Internet Security Advanced Settings:

1. On the toolbar, click **Options**.
2. Click **Internet Security**.
3. Click **Advanced Options**.

To access the Event Log:

1 On the toolbar, click **Options**.

2 Click **Internet Security**.

3 Click **View Event Log.**

About the Statistics window

Norton Internet Security Statistics shows you the real time state of the Norton Internet Security system. It displays several sets of counters indicating web- and firewall-related activity for the current session.

Use the View menu to do the following:

- To keep the Statistics window in view while you work in other applications, select Always on Top. A check next to this option indicates that it is active. To turn off this feature, click the command again.
- To choose the number of columns in the statistics window, point to columns on the view menu, then choose a one column display, a two column display, or let the display determine columns automatically based on the size of the Statistics window.
- To reset counters to zero, click Reset Values. All counters except those associated with Network Connections and Estimated Single Graphic Size are reset.
- To specify which set of counters is displayed, click Options on the View menu.

Choose a topic for details about the statistics counters:

- Network
- Web
- Web Graphics Blocked
- Firewall TCP Connections
- Firewall UDP Datagrams
- Firewall Rules
- Network Connections
- Last 60 Seconds

About Web Statistics

The Statistics window shows you real time counters indicating web-related activity for the current session.

To see the web counters, on the View menu, click **Options** > **Web**.

- Graphics Blocked

  Number of graphics (banners and images) blocked by Norton Internet Security.

- Cookies Blocked

  Number of outbound cookies blocked by Norton Internet Security’s HTTP Privacy filter.

- Refer Req Blocked

  Number of refer requests rejected by Norton Internet Security's HTTP privacy filter. This behavior is configured using the Referer setting.

- Bytes Processed

  Number of bytes processed by Norton Internet Security's HTTP ad blocker and privacy filters.

- Packets Processed

  Number of packets processed by Norton Internet Security's HTTP ad blocker and privacy filters.

- KB/Second Processed

  Number of kilobytes processed per second by Norton Internet Security's HTTP ad blocker and privacy filters. In addition, a red line indicates the highest number kilobytes per second processed since Norton Internet Security started. The number at the far right shows the scale used for this graphic indicator.

- Open Connections

  Number of HTTP connections currently open. In addition, a red line indicates the highest number of HTTP connections that have been open at the same time since Norton Internet Security started. The number at the far right shows the scale used for this graphic indicator.

About Web Graphics Blocked

If you have Ad Blocking enabled, you can view details about the web graphics that have been blocked.

- Estimated Single Graphic Size

  Norton Internet Security uses 14 kilobytes as the average graphic size when estimating Web Graphics Blocked statistics.

- Estimated Kbytes Blocked

  This counter is based on the number of graphics blocked times the estimated graphic size.

- Time Saved

  Shows the time saved by not loading the graphics that have been blocked. The time is shown in hh:mm:ss format for several connection speeds:

14.4	28.8
33.6	56

About Firewall TCP Connections Statistics

The Norton Internet Security Statistics window shows you real time counters indicating firewall-related TCP activity. To configure this behavior, use options on the Firewall tab in the Settings dialog box to define firewall rules.

To see the firewall TCP counters, on the View menu, click **Options** > **Firewall TCP Connections**.

- Inbound Permitted

  Counter shows the number of inbound TCP connections that were permitted.
- Inbound Blocked

  Counter shows the number of inbound TCP connections that were blocked.
- Outbound Permitted

  Counter shows the number of outbound connections that were permitted.
- Outbound Blocked

  Counter shows the number of outbound connections that were blocked.
- Total Permitted

  Counter shows the sum of all permitted connections (both inbound and outbound).
- Total Blocked

  Counter shows the sum of all blocked connections (both inbound and outbound).

About Firewall UDP Datagrams Statistics

The Norton Internet Security Statistics window shows you real time counters indicating firewall-related UDP activity for the current session. To configure this behavior, use options on the Firewall tab in the Settings dialog box to define firewall rules.

To see the firewall UDP counters, on the View menu, click **Options** > **Firewall UDP Datagrams**.

- Inbound Permitted

  Counter shows the number of inbound datagrams that were permitted.
- Inbound Blocked

  Counter shows the number of inbound datagrams that were blocked.
- Outbound Permitted

  Counter shows the number of outbound datagrams that were permitted.
- Outbound Blocked

  Counter shows the number of outbound datagrams that were blocked.
- Total Permitted

  Counter shows the sum of all permitted datagrams (both inbound and outbound).
- Total Blocked

  Counter shows the sum of all blocked datagrams (both inbound and outbound).

About the Firewall Rule Statistics

The Norton Internet Security Statistics window shows you real time counters indicating firewall-related activity for the current session.

To see the firewall rule statistics, on the View menu, click **Options** > **Firewall Rules**.

The Firewall Rule Stats window lists all of the rules defined for your firewall. Three counters are maintained for each rule: Permitted, Blocked, and Passed Along. A running total for all rules indicates how many communication attempts were permitted, how many were blocked, and how many were passed along.

Each time network communication occurs, the counters are updated to indicate how the firewall reacted to the communication. Each network communication attempt is checked against the existing firewall rules starting from the top of the list and progressing on to the botton. If the communication is permitted by a rule, the Permitted counter increments. If the communication is blocked by a rule, the Blocked counter increments. If the communication does not match a rule, then information about the connection is passed on to the next rule and the Passed Along counter increments.

About Network Connection Statistics

The Norton Internet Security Statistics window shows you real time counters indicating network connection information for the current session. This information is also available from the Norton Internet Security status bar. You can also terminate a connection here: Right-click a connection and then click Terminate Connection on the popup menu.

To see the network connection statistics, on the View menu, click **Options** > **Network Connections**.

Protocol TCP or UDP. The icon associated with the protocol indicates the connection status (listening, connected/outgoing).

Executable The application that is using the network connection.

Remote The address or host name of the remote site and the service or port number. This information is available for TCP connections only.

Local The local address or machine name and the service or port number being used by the application.

Sent Number of bytes sent since the connection started.

Recv Number of bytes received since the connection started.

Time The amount of time that the connection has been active.

About Last 60 Second Statistics

You can see a graphic representation of network activity for the last 60 seconds. Four different counters are represented in a line graph on a second by second basis. This allows you to note the speed of various network connection types.

HTTP Connections	red graph line
Net Connections	green graph line
HTTP KBytes/Sec	blue graph line
Net Kbytes/Sec	black graph line

About Network Statistics

The Norton Internet Security Statistics window shows you real time network counters since the program started.

To see the web counters, on the View menu, click **Options** > **Network**.

- TCP Bytes Sent

  The number of TCP bytes sent over network connections since Norton Internet Security started.

- TCP Bytes Received

  The number of TCP bytes received over network connections since Norton Internet Security started.

- UDP Bytes Sent

  The number of UDP bytes sent over network connections since Norton Internet Security started.

- UDP Bytes Received

  The number of UPD bytes received over network connections since Norton Internet Security started.

- All Bytes Sent

  The number of NDIS bytes sent over network connections since Norton Internet Security started.

- All Bytes Received

  The number of NDIS bytes received over network connections since Norton Internet Security started.

- Open Connections

  The current number of network connections. In addition, a red line indicates the highest number of simultaneous open network connections since Norton Internet Security started. The number at the far right shows the scale used for this graphic indicator.

When checked, the program icon displays in the notification area on the Windows taskbar (by default, in the right corner at the bottom of the screen). You can click the icon to open the main menu.

The options under Startup determine whether Norton Internet Security starts automatically or must be started manually.

If you want complete control over when Norton Internet Security runs on your PC, click Manual. You must start Norton Internet Security to use it.

The options under Startup determine whether the firewall starts automatically or must be started manually.

If you are using a networked PC or have a continuous Internet connection and you want the firewall protection available at all times, click Run at System Startup. The firewall starts automatically when you start up your PC.

The options under Startup Options determine whether the firewall starts automatically or must be started manually.

The firewall has three web filters: Ad blocking, Privacy, and Active content.

Displays a hierarchical site list showing each of the domains and sites for which web settings have been defined.

When you click a site in the list, the Ad Blocking, Privacy, and Active Content tabs update to show the settings defined for that site. Use options on the Ad Blocking, Privacy, and Active Content tabs to maintain site-specific settings for the currently selected site.

Opens the New Site/Domain dialog box, which you use to add a new site or domain to the hierarchical site list in the left pane.

After adding the site, you can click it in the site list and then use settings on the Ad Blocking, Privacy, and Active Content tabs to specify rules and block list entries that only run when you visit this Web site.

Removes the currently selected site or domain from the site list. The firewall prompts for confirmation before it removes the entry.

When a site or domain is removed, the site-specific or domain-specific ad blocking list and the privacy and active content settings are discarded.

If you remove a domain, all of the site entries beneath that domain are promoted within the site list hierarchy to become second-level entries.

Opens the Web (HTTP) Filters dialog box where you can selectively enable or disable the ad blocking, privacy, and active content web filters, the Cookie Assistant, and the Java/ActiveX Assistant.

In addition, you can manage the list of ports that the firewall monitors for HTTP communication when ad blocking is enabled.

When clicked, the Cookie Assistant prompts for a response each time a cookie is requested by a Web site that doesn't have a cookie rule.

The Cookie Assistant gives you the option to block or permit the return of a cookie, and to create a cookie rule that applies to all future requests for cookies by this site.

If the Privacy check box is unchecked, the Cookie Assistant setting is unavailable.

When clicked, the Java/ActiveX Assistant prompts for a response each time JavaScript, a Java applet, or an ActiveX control is received from a Web site that doesn't have any site-specific active content rules.

The Java/ActiveX Assistant gives you the option to block or permit Java or ActiveX program execution, and to create an active content rule that applies to all future attempts to run this type of program by this site.

If the Active Content check box is unchecked, the Java/ActiveX Assistant setting is unavailable.

Select this check box to turn on the ad blocking filter, which prevents images and ads from displaying on web pages opened in your browser. To specifically turn off the ad blocking filter, uncheck this check box.

Specifies whether the privacy filter is enabled. The privacy filter uses the rules on the Privacy tab to block or permit the return of user information and cookies to Web sites.

If you are concerned with privacy, click the Privacy check box and then use the settings on the Privacy tab to specify how you want the rules to be enforced.

Specifies whether the active content filter is enabled. The active content filter uses the rules on the Active Content tab to control whether web pages run JavaScript, Java applets, ActiveX controls and display animated images.

The Use These Rules for <site> check box determines whether the active content rules apply specifically to the current site.

When checked, Use These Rules For <site> specifies that you want to use site-specific active content settings for the current site. You can change each of the active content settings for the site as desired.

When the Use These Rules For <site> check box is unchecked, the active content settings are unavailable.

This message indicates how active content rules are determined for the currently selected site. There are several possibilities:

- Norton Internet Security will use rules from <domain>
  Active Content rules are defined for the domain to which this site belongs.
- Norton Internet Security will use rules from (Defaults)
  No site- or domain-specific active content rules are defined and the Java/ActiveX Assistant is not enabled. Norton Internet Security uses the (Default) active content rules.
- Norton Internet Security will alert you with an Assistant
  No site- or domain-specific active content rules are defined. The Java/ActiveX Assistant is enabled. When you visit this site, the Java/ActiveX Assistant will help you to create an active content rule for the site or for the domain that contains the site.

If you want to set up site-specific rules, click the Use These Rules For <site> check box, and then click the rule options you want to use for this site.

When clicked, prevents web pages from running JavaScript. Norton Internet Security comments out all of the HTML code within <script> </script> tags to block execution of JavaScript.

Lets you add a new HTML string to the ad blocking list that is currently active.

Lets you remove an HTML string from the ad blocking list that is currently active.

Lets you change an HTML string in the ad blocking list that is currently active.

Shows the ad blocking list defined for the site that is currently selected in the Sites list (in the left pane). The ad blocking list consists of HTML strings that are used by the Ad Blocking filter to prevent ads and images from being displayed on web pages.

When ad blocking is enabled and you connect to a Web site, Norton Internet Security scans HTML pages at the site for the strings specified in the ad blocking list for that site. In addition, It checks for strings that match those that are specified in the ad blocking list for (Defaults). Norton Internet Security looks for matching strings within the kind of HTML tags that are used to present graphics and advertising. Norton Internet Security removes any matching strings before the page is displayed in the web browser.

The settings shown on the Ad Blocking, Privacy, and Active Content tabs apply to the site that is currently selected in the Sites list (in the left pane). Click a tab to make the controls on the tab visible.

Lists the rules that are in effect when the firewall is enabled. Rules are processed in the order in which they are listed.

You can add, modify, remove, or change the order of a rule in the list. You can also enable or disable any rule in the list.

When the firewall is enabled, any TCP/IP communication that is not covered by existing firewall rules is blocked by default.

Opens the Add Firewall Rule dialog box where you can specify a rule to permit a specific type of network communication.

Opens the Modify Firewall Rule dialog box where you can change the characteristics of a rule.

Prompts you to confirm that you want to delete the currently selected rule from the connection permission list. If you answer Yes, the rule is permanently removed.

Opens the Test Firewall dialog box, where you can test whether a specified type of network communication would be permitted or would be blocked by existing firewall rules.

You don't have to enable the firewall in order to test the firewall rules.

Specifies whether the rule permits, blocks, or ignores the type of network communication defined within the rule.

Specifies whether the rule applies to inbound network communication, outbound network communication, or network communication in either direction.

Specifies what communications protocol the rule applies to: TCP, UDP, both TCP and UDP, or ICMP.

Categorizes the type of application for use with the Parental Control feature.

If you want to treat an application differently from others in the same category, place it in either User Category 1 or User Category 2. For example, if you want to permit certain games but block the majority of them, place acceptable games in User Category 1. When you configure applications in the Parental Control window, you could permit User Category 1 applications but block Games.

Enter a descriptive name that identifies the rule you want to add. This rule name will appear in the Firewall Rule column in the rules list on the Firewall tab.

Click a tab to display the options on the tab.

Shows the type of network communication being attempted.

Indicates the application that is attempting to communicate.

For most ICMP network communication, no application is associated with an ICMP message. Consequently, Application will show N/A, meaning not applicable.

For TCP or UDP network communication, indicates the remote service that the application is communicating with.

For ICMP network communication, indicates the type of ICMP message that is being communicated.

Indicates the remote address that the application or ICMP message is communicating with.

Blocks this single instance of network communication. A firewall rule is not created.

Permits this single instance of network communication. A firewall rule is not created.

Enter the location and name of the application executable file to which you want this rule to apply. This setting is not available if Any Application is checked.

Specifies that the rule applies to the application identified in the Application box.

Specifies that the rule applies to all applications on the local PC.

Other button.

Opens the Add Application From File System dialog box, where you can click the application that will be affected by the rule.

Lists the services to which the current rule applies. Use the Add and Remove buttons to create and maintain the list of services for this rule.

Lists the services to which the current rule applies. Use the Add and Remove buttons to create and maintain the list of services for this rule.

Click this option if you want the rule to apply to a single type of local service. Then, identify the service in the Service Name or Port box.

Click this option if you want the rule to apply to a range of port numbers.

Removes the currently selected service from the list of services.

Click this option if you want the rule to apply to a defined list of services. Use the Add and Remove buttons to create the list of services.

Click this option if you want the rule to apply to any local service.

Opens the Service dialog box, where you can specify a service name (for example HTTP or FTP) or enter the port number used by that service. The service you specify is added to the list of services to which this rule applies.

If you clicked Single Service, enter the service name (for example HTTP or FTP) or enter the port number used by that service.

If you clicked Service Range, enter the first (lowest) port number in the range.

If you clicked Service Range, enter the last (highest) port number in the range.

Click this option if you want the rule to apply to a single type of remote service. Then, identify the service in the Service Name or Port box.

Click this option if you want the rule to apply to a range of port numbers.

Click this option if you want the rule to apply to any remote service.

Click this option if you want the rule to apply to a defined list of services. Use the Add and Remove buttons to create the list of services.

Click this option if you want the rule to apply to a specific IP address for your PC. Then specify the IP address or the name of the host PC in the Address or Host Name box.

Click this option if you want the rule to apply to communication to or from any IP address used by your local PC.

Enter the local IP address, PC host name, or local interface name to which you want this rule to apply. This option is not available if Any Address is clicked.

Click this option if you want the rule to apply to a single remote IP address. Then specify the IP address or the name of the host in the Address or Host Name box.

Click this option if you want the rule to apply to a set of addresses (for example, all the PCs on a particular subnet). In the Address and Subnet Mask boxes, enter the IP address and subnet mask that define the network address.

Click this option if you want the rule to apply to a range of IP addresses. In the First Address box, enter the first (lowest) IP address in the range. In the Last Address box, enter the last (highest) IP address in the range.

Click this option if you want the rule to apply to communication to or from any remote address.

If you clicked Host Address, enter the remote IP address or host name to which you want this rule to apply.

If you clicked Network Address, enter the IP address, which is used in conjunction with the Subnet Mask to define the network address.

If you clicked Address Range, enter the first (lowest) IP address in the range.

If you clicked Network Address, enter the subnet mask, which is used in conjunction with the IP address specified in the Address box to define the network address.

If you clicked Address Range, enter the last (highest) IP address in the range.

Click this option if you want the rule to apply to a single type of ICMP message. Then click the message type in the Type box.

Click this option if you want the rule to apply to a defined list of ICMP message types. Use the Add and Remove buttons to create the list of Types.

Click this option if you want the rule to apply to any type of ICMP message.

Specifies what type of ICMP message the rule applies to.

Lists the types of ICMP messages to which the current rule applies. Use the Add and Remove buttons to create and maintain the list of message types for this rule.

Opens the ICMP Type dialog box, where you can specify an ICMP message type. The message type you specify is added to the list of ICMP message types to which this rule applies.

Removes the currently selected ICMP message type from the list of types.

Opens a time scheduler dialog box where, for each day of the week, you can specify a time interval during which this rule will be in effect.

Click this button to specify that the current rule is in effect all day (24 hours) for the day indicated in the dialog box title.

Click this button to specify that the rule is never in effect for the day indicated in the dialog box title.

Indicates the starting time at which the current rule becomes active. To change the starting time, click the button and then make hour and minute selections.

Indicates the ending time at which the current rule ceases to be active. To change the ending time, click the button and then make hour and minute selections from the time list boxes.

To specify the hour at which the current rule becomes active, click the Start Time button and then click a time in this list box.

To specify the hour at which the current rule ceases to be active, click the End Time button and then click a time in this list box.

To specify the minute within the selected hour at which the current rule becomes active, click the Start Time button and then click a minute time in this list box.

To specify the minute within the selected hour at which the current rule ceases to be active, click the End Time button and then click a minute time in this list box.

When clicked, specifies that the currently defined time interval applies to every day of the week. The current rule becomes active each day during the specified time interval.

Click this option if you want to create a cookie rule that will apply to cookie requests from all Web sites within the domain identified on the right.

Identifies the domain within which the currently active Web site resides. Click this option if you want to create a cookie rule that will apply to all Web sites within the domain.

Click this option if you want to create a cookie rule that will apply to all cookie requests from the specific Web site identified on the right.

Identifies the name of the host for the Web site that is requesting a cookie. Click this option if you want to create a cookie rule that will apply only to the current site.

Indicates the time and date when the cookie request occurred.

Blocks this single cookie request. A cookie rule is not created.

Permits this single cookie request. A cookie rule is not created.

Creates a rule that prevents your browser from returning cookies to the identified Web site or domain upon request.

Click Domain to specify that the rule applies to cookie requests from all Web sites within the specified domain. Click Site to specify that the rule applies to cookie requests from the identified Web site only.

The rule is applied for the current cookie request and for all future requests.

A rule for the current site or domain is added to the Privacy tab in the Settings dialog box. To see or modify the cookie rule for the current site, click the site on the Web tab and then click the Web tab.

Creates a rule that permits your browser to return cookies to the identified Web site or domain upon request.

Click Domain to specify that the rule applies to cookie requests from all Web sites within the specified domain. Click Site to specify that the rule applies to cookie requests from the identified Web site only.

The rule is applied for the current cookie request and for all future requests.

A rule for the current site or domain is added to the Privacy tab in the Settings dialog box. To see or modify the cookie rule for the current site, click the site on the Web tab and then click the Web tab.

Shows the type of programming code that the web page is attempting to run.

Click this option if you want to create a rule that will apply to all Web sites within the domain identified on the right.

Identifies the domain within which the currently active Web site resides. Click this option if you want to create a rule that will apply to all Web sites within the domain.

Click this option if you want to create a rule that will apply to the specific Web site identified on the right.

Indicates the time at which the Java/ActiveX alert occurred.

Identifies the name of the host for the Web site that wants to run the Java or ActiveX code. Click this option if you want to create a rule that will apply only to the current site.

For one time only, the script is blocked and won’t run. A rule is not created.

For one time only, the script is permitted to run. A rule is not created.

Creates a rule that prevents web pages received from the specified site or domain from running this type of Java or ActiveX code.

Click this option if you want to create a rule that blocks this type of code.

Creates a rule that permits web pages received from the specified site or domain to run this type of Java or ActiveX code.

Click this option if you want to create a rule that allows this type of code to run.

You must specify either that the rule applies only to the application indicated, or that it should be applied to all applications that attempt this type of network communication.

Click this option if you want the rule to apply only to the identified application.

Click this option if you want the rule to apply to all applications that attempt this type of network communication.

For TCP or UDP network communication, you must specify either that the rule as currently defined applies only to communications made using the service and port indicated, or that it should be applied to communications made using any service or port.

For ICMP network communication, you must specify either that the rule as currently defined applies only to communications made using the ICMP message type indicated, or that it should be applied to communications made using any ICMP message type.

For TCP or UDP network communication, click this option if you want the rule to apply only to communications made using the identified service or port.

For ICMP network communication, click this option if you want the rule to apply only to communications made using the identified ICMP message type.

You must specify either that the rule as currently defined applies only to communications made while connected to the address indicated, or that it should be applied to communications made while connected to any address.

Click this option if you want the rule to apply only to communication made when connected to the identified address.

Click this option if you want the rule to apply to communication made when connected to any address.

The Rule Assistant proposes a name for the rule you are creating. If you want to enter a different name for the rule, type it in the box.

Shows the application to which the rule applies or shows that the rule applies to all applications. (Not applicable for ICMP communication.)

For TCP or UDP network communication, shows the service to which the rule applies or shows that the rule applies when communicating using any services.

For ICMP network communication, shows the ICMP message type to which the rule applies or shows that the rule applies when communicating using any message type.

Shows the address to which the rule applies or shows that the rule applies when connected to any address.

Shows you the type of rule you are creating and the properties of the rule that are currently defined. By default, the communications rule applies to only the application, service or ICMP message type, and address indicated. The Rule Assistant will present a series of choices that let you modify the rule properties, making the rule more restrictive or more permissive.

Indicates the application that is attempting to communicate. (Not applicable for ICMP network communication.)

For TCP or UDP network communication, indicates the remote service that the application is communicating with.

For ICMP network communication, indicates the ICMP message type used for communication.

Indicates the remote IP address or host name of the machine that your PC wants to communicate with.

Specifies that the test should simulate communication coming from a machine that is connecting to your PC.

Specifies that the test should simulate communication going from your PC to another machine.

Specifies that the test should simulate TCP inbound or outbound connections.

Specifies that the test should simulate use of inbound or outbound UDP packets.

Specifies that the test should simulate use of inbound or outbound ICMP packets.

Specifies that the test should simulate communication using the specified remote service. Enter the name of the service or the port number used for the service. For example, under most circumstances, to test outbound FTP communication, specify FTP as the remote service or specify port number 21.

When clicked, specifies that the test should simulate inbound communication using any remote service.

When unchecked, you must specify the remote service or port number that would be used by the machine connecting to your PC.

Specifies that the test should simulate communication using the specified local service. Enter the name of the service or the port number used for the service. For example, under most circumstances, if you want to test a rule that should affect remote users connecting to the FTP server that runs on your local PC, you can specify FTP as the local service or specify port number 21.

When clicked, specifies that the test should simulate outbound communication using any local service.

When unchecked, you must specify the local service or port number that would be used by your PC to connect to the remote machine.

Specifies that the test should simulate outbound communication using the specified remote IP address. Enter the IP address or host name. For example, to test outbound FTP communication to an FTP server running on a specific remote host, enter the remote host's IP address or host name.

When clicked, specifies that the test should simulate inbound communication from any remote address.

When unchecked, you must specify the remote IP address or host name used by the machine that would be communicating with your PC.

Specifies that the test should simulate communication using the specified local IP address or machine name. Enter the local IP address or the machine name. For example, if you want to test a rule that should affect remote users connecting to the FTP server that runs on your local PC, you should specify the local IP address they will use to connect to the FTP server.

By default, your current PC IP address or machine name appears in the Local address box.

If your PC has network cards supporting multiple IP addresses, this setting lets you simulate communication using a specific IP address.

When clicked, specifies that the test should simulate outbound communication from any local address.

When unchecked, you must specify the local IP address or machine name used by your PC to connect to the remote server. If your PC has network cards supporting multiple IP addresses, this lets you simulate communication using a specific IP address.

If you want to test communications rules for a specific application, uncheck the Any Application check box. Then enter the location and name of the application executable file.

Opens the Add Application From File System dialog box, where you can select an application. The test will simulate either inbound or outbound communication with that application.

When clicked, specifies that the test will simulate either inbound or outbound communication with any application.

When unchecked, the test will simulate either inbound or outbound communication with the application specified in the Application box.

Indicates whether the type of communication you are testing would be blocked or permitted.

Indicates the name of the rule that either permits or blocks the type of communication you are testing.

If no rule matches the test condition, the Test Result reports that the communication is blocked by the implicit block rule: when the firewall is enabled, any communication for which there is no rule defined is blocked by default.

When you perform a firewall test, if a rule matches the test condition, that rule is highlighted in the rules list on the Firewall tab in the Settings dialog box.

Click Test to see how the firewall works with the type of communication you've specified in the Test Firewall dialog box.

The Test Result indicates whether the type of communication you are testing would be blocked or permitted. It also shows the name of the rule that matches the type of communication you are testing.

If no rule matches the test condition, the Test Result reports that the communication is blocked by the implicit block rule: when the firewall is enabled, any communication for which there is no rule defined is blocked by default.

When you perform a firewall test, if a rule matches the test condition, that rule is highlighted in the rules list on the Firewall tab in the Settings dialog box.

Re-enter the password. To provide security, the string that you type here displays as asterisks.

The Firewall Rule Stats window lists all of the rules defined for your firewall. Three counters are maintained for each rule: Permitted, Blocked, and Passed Along. A running total for all rules indicates how many communication attempts were permitted, how many were blocked, and how many were passed along.

You must supply a password to open the Settings dialog box, the Event Log viewer, or the Statistics window.

The password you enter must match the password that was specified on the General tab in the Settings dialog box.

Type the HTML string that you want to add to the block list. Then choose whether to permit or block HTML image statements that contain this string.

The way that you define HTML strings in the ad blocking list will affect how restrictive or unrestrictive the firewall will be in its filtering of HTML data. Here are some examples:

Specifies that the HTML string should be used to block display of an ad or image.

When you create a block string, any HTML statement that contains a matching HTML string is removed before the page is interpreted and displayed in the web browser.

Specifies that the HTML string should be used to permit display of an ad or image.

You can create a permit string only in a site-specific list. The permit string is used to override a block string in the (Defaults) block list.

When you create a permit string, any HTML statement that contains a matching HTML string is allowed to remain on the page.

This message indicates the status of ad blocking. There are two possibilities:

The Ad Blocking filter is not enabled: The (Defaults) ad blocking list and any site-specific ad blocking list will be ignored because the ad blocking is not turned on. To enable it, click Ad Blocking in the Status window.

(Defaults) block list also applies: When you visit a Web site, Norton Internet Security uses two ad blocking lists: the (Defaults) list plus the site-specific list. Norton Internet Security provides a pre-defined (Defaults) ad blocking list that is applied globally to the content of all Web sites. You can add, modify, and remove strings in the (Defaults) block list.

You can add either a site entry or a domain entry to the site list.

Adding a domain entry lets you configure privacy and active content web setting defaults for all the web servers within the domain.

Adding a site entry lets you configure privacy and active content web settings for a single web server.

The Use These Rules For <site> check box determines whether the privacy rules apply specifically to the current site.

When clicked, Use These Rules For <site> specifies that you want to use site-specific privacy settings for the current site. You can change each of the privacy settings for the site as desired.

When the Use These Rules For <site> check box is unchecked, the privacy settings are unavailable.

If the Use These Rules For <site> check box is unchecked, a status message displays at the bottom of the Privacy tab indicating how Norton Internet Security will determine privacy rules for the current site.

This message indicates how Privacy rules are determined for the currently selected site.

Norton Internet Security can block, permit, or alter HTTP header information that is passed in each request that the browser sends to a web server. You can use Norton Internet Security to control the information passed in the following HTTP header fields: Referer, Browser (User-agent), and E-mail (From).

If you chose to replace Browser (User-agent) field information with a Reply, type the string that you want to use for the reply. This string will be sent as the content of the User-agent field each time the site requests data from a server.

This Browser (User-agent) Reply box is only available when you click Reply in the Browser (User-agent) list box.

These settings specify whether a site is provided with information about what kind of browser and operating system you are using when you request for data from their server. Normally, this information is passed in the User-agent field as part of the data request:

Block: When clicked, Norton Internet Security does not let your browser identify the browser and operating system you are using when it requests data from a server.

Permit: When clicked, Norton Internet Security permits your browser to identify the browser and operating system you are using when it requests data from a server.

Reply: When clicked, Norton Internet Security returns the string specified in the Browser (User-agent) box instead of the identity of the browser and operating system you are using.

If the Use These Rules For <site> check box is unchecked, the Browser (User-agent) settings are not available. In this case, a message below the Use These Rules For <site> check box indicates how Norton Internet Security determines which Privacy rules to use.

If you chose to replace E-mail (From field) information with a Reply, type the string that you want to use for the reply. This string will be sent as the content of the From field each time the site requests data from a server.

This E-mail (From) Reply box is only available when you click Reply in the E-mail (From) list box.

These settings specify whether sites are given the email address that your browser uses to identify you as the sender of mail. This information may be passed in the From field as part of the data request:

Block: When clicked, Norton Internet Security does not let your browser provide the email address that is used to identify you as the sender of mail.

Permit: When clicked, Norton Internet Security permits your browser to provide the email address that is used to identify you as the sender of mail.

Reply: When clicked, Norton Internet Security returns the string specified in the E-mail (From) box instead of the email address that your browser uses to identify you as the sender of mail.

If the Use These Rules For <site> check box is unchecked, the E-mail (From) settings are not available. In this case, a message below the Use These Rules For <site> check box indicates how Norton Internet Security is determining which privacy rules to use.

If you chose to handle cookie requests with a Reply, type the string that you want to use for the reply. This string will be sent instead of a cookie each time the site makes a cookie request.

This Cookie Reply box is only available when you click Reply in the Cookies list box.

Some advertisers use cookies to track users on a variety of sites and send the information back to their corporate server. This setting specifies how requests for cookies are handled for the currently clicked site.

Block: When clicked, Norton Internet Security prevents your browser from returning cookies.

Permit: When clicked, Norton Internet Security permits your browser to return cookies

Reply: When clicked, Norton Internet Security returns the string specified in the Cookie box instead of the cookie.

If the Use These Rules For <site> check box is unchecked, the Cookies settings are unavailable. In this case, a message below the Use These Rules For <site> check box indicates how Norton Internet Security is determining which privacy rules to use.

If you chose to replace the Referer field information with a Reply, type the string that you want to use for the reply. This string will be sent as the content of the Referer field each time the site requests data from a server.

This Referer Reply box is only available when you click Reply in the Referer list box.

These settings specify whether third-party sites are provided with the identity of the site that triggered a request for data from their server:

Block: When clicked, Norton Internet Security prevents your browser from identifying the site you were visiting.

Permit: When clicked, Norton Internet Security permits your browser to identify the site you were visiting.

Reply: When clicked, Norton Internet Security returns the string specified in the Referer box instead of the identity of the site you were visiting.

If the Use These Rules For <site> check box is unchecked, the Referer settings are not available. In this case, a message below the Use These Rules for <site> check box indicates how Norton Internet Security determines which privacy rules to use.

When clicked, a notification icon displays in the Status window when a network communication event matches this rule.

If you want to limit the frequency with which a rule match triggers notification on the Status window, increase the Log Event After <n> Matches setting.

Note: This setting is unavailable if event logging for this rule is disabled. To enable event logging, click the Write An Event Log Entry When This Rule Is Matched check box.

Lets you limit the frequency with which a rule match triggers a log event.

Specify the number of times a network communication event should match this firewall rule before a firewall event is logged or a Status window notification occurs. Norton Internet Security counts how many times the rule is matched and writes a log event when the count reaches the number that you enter here.

Specifies that an entry is logged to the firewall event log when network communication of the type described by the rule occurs.

Use the Log Event After <n> Matches setting to control how often an event is logged for this rule.

Specifies that you want the whole string that is shown in the box to be added to the block list for the identified site.

Specifies that you want only the part of the string that is highlighted in the box to be added to the block list for the identified site.

Shows you the HTML string that you put into the trashcan.

Examine the string and consider whether it will accomplish the type of blocking you want.

To use the entire string as a block list entry, click Add the whole string to the block list.

To use only a portion of the HTML string as a block list entry, select the portion you want. Then, click Add the portion of the string highlighted below to the block list.

Shows you the HTML string that you put into the trashcan and indicates whether the string would be added to the block list for a specific site or for all sites.

Click to move a rule up in the list. Firewall rules are processed in the order in which they are listed.

Click to move a rule down in the list. Firewall rules are processed in the order in which they are listed.

About blocking graphic images

Click a topic for information about how to use Norton Internet Security to block graphic images on web pages.

- How browsers load graphics and how Norton Internet Security blocks them.
- How Norton Internet Security uses the ad blocking lists.
- What's the difference between Link Location and Image Location?
- How to edit entries in the block list.
- How to tell if you're blocking too little or too much.
- What happens with animated gifs?
- Why is there sometimes an empty square or rectangle on the page?
- When I turn Norton Internet Security on and reload a page, it doesn't block images.

How browsers load graphics and how Norton Internet Security blocks them

When you go to a web page, your browser might receive something like this:

“Greetings! This is the Ajax company home page: <img src="http://www.ajax.com/nifty_images/image7.gif">”

When your browser sees that, it prints the text "Greetings! This is the Ajax company home page:" on the screen, and then it connects to www.ajax.com and asks it for a file called "/nifty_images/image7.gif". If www.ajax.com has such a file, it sends it to the browser, which displays the image.

When Norton Internet Security blocks graphics, it's blocking the outbound request that the browser makes for the image. The blocked data is never transferred, so pages load faster and the Internet has less clutter.

The options on the Web Ad Blocking tab in the Norton Internet Security Settings dialog box let you maintain the (Defaults) ad blocking list and site-specific ad blocking lists, which are used to prevent ads and images from being displayed on web pages.

When the ad blocking enabled and you connect to a Web site, Norton Internet Security scans HTML pages at the site for the strings specified in the ad blocking list for that site. In addition, Norton Internet Security checks for matches to the strings specified in the ad blocking list for (Defaults). Norton Internet Security looks for matching strings within the kind of HTML tags that are used to present graphics and advertising. The HTML structures that contain a matching string are removed from the page by Norton Internet Security before the page is interpreted and displayed in the web browser.

Click here for information about how Norton Internet Security uses the ad blocking lists.

Click here {button ,AL("Ref graphics",0,`',`')} for more information.

Link location versus image location

When you click some images, they take you to other pages. What really happens is that your browser just loads a new page that was associated with the image you clicked.

The URL that your browser uses to fetch the image is the Image Location, and the URL that your browser uses to fetch the new page is the Link Location. You can block an image by adding a string that matches either its Image Location or the Link Location associated with it.

If you want to customize a particular page, be specific about the Image Location by adding an HTML string to the site-specific block list. For example, you could add the HTML string "nifty_images/image7.gif" to the site-specific list for the www.ajax.com site to specifically block image7.gif on any pages at the www.ajax.com Web site.

In contrast, if you want to block all of the images that take you to a site whose only purpose is to sell you shoes for your pet wombat, it often works well to add a very general block list string, like "www.wombatshoes.com", or even just "wombatshoes.com" to the (Defaults) block list. Adding "www.wombatshoes.com" would block all images that link to the web server at www.wombatshoes.com. Adding "wombatshoes.com" would block all images that link to any web server within the wombatshoes.com domain.

Be careful that what you put into the (Defaults) block list isn't too general. Adding something like "www" is not a good block list string. It matches far too many URLs and you'd rarely see anything. Strings that are cut from the middle of a URL, such as "cgi-bin/redir/" are very general and may block things that you want to see on other pages. Click here for help on how to tell what you may be blocking.

Click here {button ,AL("Ref graphics",0,`',`')} for more information.

How to tell if you're blocking too little or too much

Norton Internet Security logs all the ads and images that it blocks to the Ad Blocking event log.

If you are looking at a page and it doesn't seem quite right, you can look at the Ad Blocking tab in the Event Log and see the web page elements that Norton Internet Security removed most recently. Clicking a particular line displays more information about it in a pane at the bottom of the Event Log viewer:

- Removed shows the HTML element that the browser was prevented from retrieving.
- From shows the URL of the web page you were looking at that the blocked element would have been requested from.
- Because shows the string in the block list that caused the ad or image to be blocked.

If you see a large number of images being removed from several different From locations all for the same Because reason, it could be an indication that the Because string is too general, and you might consider removing it from your block list.

Note: Be sure to clear your browser's web page cache before doing this test, or you won't see any changes.

Click here {button ,AL("Ref graphics",0,`',`')} for more information.

What happens with animated gifs

When image animation is disabled, an animation graphic series displays only once when a page is accessed.

Animation blocking only applies to gifs that were not blocked in the first place. All of the frames of an animated GIF are fully downloaded. If animation blocking is enabled, the gifs will run through a single cycle of animation and then stop.

Aside from reducing the visual distraction on some pages, this can also dramatically reduce disk thrashing, which occurs when the browser stores all of the animation frames in its cache and continuously re-reads them in order to display them. For laptops, that can mean increased battery life.

Click here {button ,AL("Ref graphics",0,`',`')} for more information.

Why does an empty square or rectangle occasionally appear on the page?

In some cases, Norton Internet Security blocks an image by replacing it with a transparent GIF. If the unblocked GIF would have had a border around it, the transparent GIF gets one also. In those cases, the link is usually still present, meaning that it's possible to click the empty area and go to the web page associated with the blocked image request.

Click here {button ,AL("Ref graphics",0,`',`')} for more information.

When I turn on Norton Internet Security and reload a page, it doesn't block images

The most likely cause is that the reloaded page is coming from your browser's local history of web pages (the cache) and not from the actual server. You need to clear your web browser's cache.

About the Web Browser's Cache

Because transferring web pages over the Internet from a web server to your computer takes time, the people who create browsers used caching to speed up the displaying of pages. Before your browser sends a request to a web server for a page, it first checks to see if it has seen that same web page recently. This occurs more often than you might think, such as when you click the Back button in Netscape or Internet Explorer.

If the web page is in your browser's list of recently visited pages (cache), then it is read right from your hard disk. This is much faster than retrieving it from the web server.

However, reading the web page from your hard disk also bypasses your computer's network software, which also means that Norton Internet Security will not see any requests going to web servers and won't have anything to block. If the web page in the browser's cache is full of images you want to block, you'll need to clear the cache before Norton Internet Security can block them. The reverse can also be true: If the web page in your cache has already had images blocked and you want to disable blocking, you'll need to clear the cache or your browser won't realize that there are now new images to be retrieved.

Click here {button ,AL("Ref graphics",0,`',`')} for more information.

About Norton Internet Security privacy features

Click a topic for information about the privacy features provided by Norton Internet Security.

- What are cookies?
- How Norton Internet Security blocks cookies
- Why does my browser keep warning me about accepting cookies?
- How to block some cookies but not others
- What are referer fields?
- How do I block referer fields?

What are cookies?

Cookies are bits of information that web servers store on your computer for their later use. Web servers can use cookies to keep track of how many times you've visited and when, and what sort of information you've been surfing for on their site. They can even use cookies to pass that information on to other web servers, such as advertisement servers.

On the positive side, cookies can be used to store your own Web site configuration, to remember items placed in your shopping cart at an online shopping site, or to store account and password information for subscription sites. You may not want to block all cookies, which is why Norton Internet Security lets you permit or block cookies on a per-site basis.

Click here {button ,AL("Cookies",0,`',`')} for more information.

How Norton Internet Security blocks cookies

Cookies are blocked on the way out of your computer, not on the way in. Incoming cookies are accepted, but the information that they contain is not allowed to be sent back to a web server unless you explicitly put the domain name of the server into the cookie permission list.

There are several ways for web servers to set cookies on your computer, but there's only one way that browsers give cookies back to web servers. If they're blocked on the way out, the blocker catches all of them.

Click here {button ,AL("Cookies",0,`',`')} for more information.

Why does my browser keep warning me about cookies?

You' probably have your browser configured to warn you before accepting a cookie. Since Norton Internet Security prevents cookies from being sent to web servers, and logs what it blocked and what it permitted, it's safe to change your browser configuration so that it accepts cookies without notifying you.

Click here {button ,AL("Cookies",0,`',`')} for more information.

How to block some cookies but not others

You can specify site-specific cookie blocking using the Norton Internet Security Advanced Settings.

- To set up site-specific cookie rules, click the site in the site list, click **Use these rules for <site>**, and then use the Cookies setting to specify a cookie rule that applies to the current site only.
- To discard site-specific rules and inherit the rules defined for the site domain or for (Defaults), click to uncheck the **Use these rules for <site>** check box. Norton Internet Security uses privacy rules from (Defaults) when site-specific or domain-specific privacy rules are defined and the Cookie Assistant is not enabled.

To see what privacy rules are in effect at a site, select the site in the **Site** list. If the **Use these rules for <site>** check box is unchecked, a message appears at the bottom of the Privacy tab indicating how Norton Internet Security is determining what Privacy rules to use.

Click here for details on how to set up privacy rules for a site.

Click here {button ,AL("Cookies",0,`',`')} for more information.

What are referer fields?

When you click a link to a web page, your browser makes a quick note of what page you are currently viewing. When it sends the request for the new page, it passes that information on to the new server. That lets web servers that you visit to know where you've just been, which is information that you might prefer to keep to yourself.

When referer fields are permitted, your browser tells a web server that you are visiting that you clicked a link to get to them. It also tells the server what page it was that you were just visiting. When referer fields are blocked, however, the web server that you are getting a page from has no more information than if you just typed the URL into your browser or clicked it in your bookmarks.

Click here {button ,AL("Referer",0,`',`')} for more information.

How do I block referer fields?

Referer field blocking is controlled by the Referer setting on the Web Privacy tab in the Norton Internet Security Settings dialog box.

The **Referer** setting specifies whether third-party sites are provided with information about what site triggered a request for data from their server.

For example, a Web site page may present an advertisement by including an image source tag in an HTML statement. When the page is rendered for display, the image source tag directs your browser to obtain the advertisement from a separate advertising site. As part of your browser's request for the advertisement, it provides information to the advertising site about the identity of the site you visited that triggered the request. You can prevent your browser from telling the advertising site what site you were visiting by setting **Referer** to **Block**.

Click here {button ,AL("Referer",0,`',`')} for more information.

About firewalls and safety

- What the Norton Internet Security Firewall does
- How the Firewall blocks connections
- How to use Ignore rules
- Why Rule Assistant alerts pop up
- What to do when a Rule Assistant alert pops up
- What are services and what are port numbers?
- What's the difference between TCP connection attempts and UDP packets?
- What is ICMP filtering and how do I enable it?
- Will the Rule Assistant alert me about ICMP packets?
- What should I do when alerted about connection attempts made to non-listening server ports?
- Why are there default Firewall rules automatically set up for me?

What does the Personal Firewall do?

The Personal Firewall is a filter that, when enabled, intercepts both inbound and outbound connection attempts on your computer and decides whether to permit or block them based on a list of rules. The Personal Firewall can protect against data being transmitted without your knowledge. It can warn you about attempts to use resources on your computer that you might otherwise not know about, help you learn about the resources your computer makes available to others on the Internet, and provide you with a way to control what connects to your computer and what your computer can connect to.

In most cases you do not need to configure the Personal Firewall directly●Norton Internet Security creates and maintains a set of firewall rules for you, based primarily on the settings in the Security window.

If you want to fine tune Personal Firewall settings or see what firewall rules are in effect, open Norton Internet Security’s Advanced Settings and click the Firewall tab.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

How the firewall blocks connections

The firewall consults a list of rules, visible in the Firewall tab of the Settings dialog box, when it needs to decide how to deal with a connection. Each firewall rule prescribes an action for a specific type of network communication. The rule can block, permit, or ignore that specific type of communication.

With each new connection or packet, the firewall goes down the list of rules, in order, looking for the first rule that matches the connection or packet type in question.

- Once a **block** or **permit** rule is matched, all remaining rules are ignored. In other words, additional rules that match this type of communication are ignored if they appear below the first rule that matches.
- If an **ignore** rule is matched, the type of communication that was attempted is logged to the firewall event log and then the rule processing continues until another match occurs.

If no match is found, the connection or packet is denied. However, if the Rule Assistant is enabled, an alert gives you several options on how to deal with this communications attempt.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

How to use ignore rules

When you define a firewall rule with the Add Firewall Rule dialog box, the **Action** setting specifies whether the rule permits, blocks, or ignores the type of network communication defined within the rule. The **Ignore** option lets you log some type of communication activity prior to enforcing a Permit rule or Block rule that applies to that type of communication.

When an Ignore rule is matched, logging occurs and firewall processing continues in an attempt to match the communication to a subsequent Permit or Block firewall rule.

Note: For an Ignore rule to work effectively, it must appear in the firewall rule list above any related Permit or Block rule for that type of communication. It's a good idea to move all Ignore rules to the top of the firewall rule list. To move a rule in the list order, click it and use the up arrow or down arrow button to change its location in the order.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

Why Rule Assistant alerts pop up

If the Norton Internet Security firewall and Rule Assistant are enabled, and network communication is being attempted to or from your computer, the Rule Assistant will indicate several things to you:

- If your computer is establishing communications with a remote computer (outbound) or if some remote computer is establishing communications with your computer (inbound)
- The name of the application on your computer that is responsible for the communications attempt
- The inbound or outbound service name or port number
- The address of the other computer communicating with your computer

The most common reason for an alert to display is that you ran an application that is trying to establish an outbound connection with another computer. (The Rule Assistant will always indicate to you what application is making the attempt.) In this case, you probably want to permit the outbound connection, and you might even want to create a rule to permit it in the future so that you aren't warned every time you try to use that application. Once you have Rule Assistant create a rule to always permit outbound communication with this application, you are giving this application permission to establish any outbound communications.

If, on the other hand, the application is something that you think should not be communicating with another computer, such as a newly installed text editor or a paint program you downloaded from the Internet, you may want to create a rule to block communications for that application.

If the communication was inbound, the Rule Assistant will indicate what application is responsible for the communications attempt. Before you get too suspicious of remote computers trying to connect to yours, bear in mind that programs often create more than one connection and some client programs that you run communicate with remote servers by asking them to connect back into your computer. An FTP client is a good example of this; when you run an FTP client to connect to an FTP server, one alert usually tells you about an outbound connection. Then, more alerts tell you about the remote FTP server connecting back to your FTP client whenever you send a command to the FTP server to do something.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

What to do when a Rule Assistant alert pops up

First, determine what communication happened that made it pop up. Then decide whether to permit or block the communication. Finally, decide whether to have the Rule Assistant create a rule that Norton Internet Security can apply for future communications attempts.

The application name shown in the Rule Assistant alert dialog box is usually enough to give you an idea of what happened, especially when the communication is coming from a program that you just ran. The Rule Assistant alert also gives you the service or port number to consider, and the address or name of the remote host computer as well.

You can block or permit the connection for "just this attempt" until you get a feel for how often the communication occurs. You can also check the Event Log viewer Firewall tab to see events logged by the firewall, including how rules are being processed and what connections were permitted or blocked.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

What are services and port numbers?

Many host computers that are connected to the Internet offer services. Services are protocols that are used to allow one computer to access a particular kind of data stored in another computer.

A computer that is connected to the Internet is usually assigned a 4-byte Internet Protocol address (an IP address) that is used to distinguish it from all other computers connected to the Internet. When you connect to a web server, for example, you may tell your browser to connect to www.symantec.com, but your computer ultimately has to translate the name to its IP address, 216.32.116.201, before the connection can be made.

When the connection is made, you also need a way to tell the computer to which you're connecting about the services in which you're interested. The host computer may be running both an HTTP server and an FTP server, and if you're connecting to the host computer using a web browser, you'll want to connect to the HTTP server and not the FTP server. This is done using port numbers. Since HTTP servers usually listen on port number 80, and FTP servers usually listen on port number 21, the web browser will connect to the correct server on the www.symantec.com computer if it connects to port 80 of the computer at 216.32.116.201 rather than to port 21. Port numbers are arbitrarily chosen numbers associated with particular services, and are always used in conjunction with IP addresses when establishing connections to host computers.

Click here to see the port and service assignments used by Norton Internet Security and the Rule Assistant when displaying messages about connections.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

What's the difference between TCP connection attempts and UDP packets?

A connection attempt is just a TCP packet that is asking to establish a connection to or from your computer. The connection may last anywhere from milliseconds to hours. A UDP packet, on the other hand, is a single packet used to transmit information without the promise of any additional information being transmitted. Your computer can send or receive a single UDP packet to exchange information without any connection being established.

Both kinds of packets are being used when you use a web browser to download a web page. If you go to http://www.symantec.com, for example, your computer first sends a UDP packet out to try to find out what the 4-byte Internet Protocol address is for the computer called www.symantec.com. The protocol used to do that is called DNS, or Domain Name Service, and the queries and replies take place without any persistent TCP connections being made.

Having a rule to permit this is important or your computer wouldn't be able to talk to other machines at all. UDP, or connectionless communication, works well for DNS because the queries and replies are very small and can be completed in single packets.

Once the web client gets the 4-byte IP address for www.symantec.com, it needs to establish a persistent connection with the site in order to fetch the web page and images because there's more data to be moved than will fit in a single packet. That's where TCP connections come into play; a TCP SYN (synchronize a connection) packet is sent to the web server, the server replies with a TCP ACK (acknowledgment). This creates a connection between the two computers, and the data starts to flow.

By default, when the Norton Internet Security firewall is enabled, inbound and outbound UDP packets are permitted. This can always be changed by editing one of the Norton Internet Security firewall rules.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

What is ICMP filtering and how do I enable it?

ICMP is a component of TCP/IP that passes control messages to and from your PC. You can set up firewall rules to filter the following types of ICMP messages:

Echo Reply (ping reply)

Destination Unreachable

Source Quench

Redirect

Echo Request (ping request)

Router Advertisement

Router Solicitation

Time Exceeded (used by Traceroute)

Parameter Problem

Timestamp Request

Timestamp Reply

Information Request

Information Reply

Address Mask Request

Click here {button ,AL("firewall faq",0,`',`')} for more information.

Will the Rule Assistant alert me about ICMP packets?

By default, Norton Internet Security provides two ICMP firewall rules that permit all inbound and outbound ICMP packet traffic. If you want to use the Rule Assistant to alert you to ICMP activity and to help create rules for specific types of ICMP messages, you should disable (or remove) the default ICMP rules.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

Responding to alerts about connection attempts made to non-listening server ports

The Rule Assistant in Norton Internet Security provides notification of inbound UDP and TCP connection attempts made to non-listening server ports. Connection attempts to non-listening server ports are detected by the NDIS filter. Alerts about such connection attempts are displayed by the Rule Assistant.

The alert indicates the type of packet used for network communication (UDP or TCP), the local service that was targeted for the connection, the remote address and service making the connection attempt and the fact that there was no service on your machine actively listening for communication sent to that service port.

Your response to the alert will depend on the way you typically use software on your PC:

- If you never run the type of server identified by the alert (such as an FTP server, finger server, telnet, or web server), then you can simply create a rule to block this type of incoming communication. In this case, the Norton Internet Security firewall will discard the incoming communication packet instead of passing it on to the TCP/IP network software.

  Note: The rule blocks connection attempts when the server is running as well as when it is not. So if you later decide to run the type of service specified by the rule, you might want to modify the rule to allow inbound connections to that service.

- If you sometimes run the type of server identified by the alert, you should create a rule to permit this type of incoming communication. The Norton Internet Security firewall will pass the incoming communication packet to the TCP/IP network software. The TCP/IP network software knows that no software is listening on the port that the connection attempt was made on, and it will reject the connection.
- If you are not sure about the connection attempt, click the **Block this one time** option to see if all of your applications still run properly after blocking the inbound connection attempt. If this is the case, then in the future, it is okay to create a rule to block this unnecessary communication.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

Why are there firewall rules automatically set up for me?

A number of default rules are defined for the firewall. When the firewall is enabled, these rules are in effect.

Default Inbound DNS
Default Outbound DNS

These two default UDP firewall rules are needed by most home and corporate users to permit the use of the domain name service (DNS).

Default Inbound Bootp
Default Outbound Bootp

These two default UDP firewall rules are needed by most home and corporate users to permit the use of the bootp service (bootp is short for bootstrap protocol, which enables a machine to discover its own IP address).

Default Inbound NetBIOS
Default Outbound NetBIOS

These two default UDP firewall rules are needed by most corporate users to permit the use of the NetBIOS name service and the NetBIOS datagram service used in file sharing on the Microsoft Network.

Default Inbound Loopback
Default Outbound Loopback

These two default TCP or UDP firewall rules permit inbound and outbound loopback connections to the localhost address of 127.0.0.1. It is usually safe to permit loopback or local connections, because the connection originator is typically a trusted application on your own PC. Even with this firewall rule enabled, remote machines will always be blocked access to the localhost address by the underlying network.

Default Block Back Orifice

This default UDP firewall rule protects you from attacks by Back Orifice.

Default Block NetBus

This default TCP firewall rule protects you from attacks by NetBus.

Default Inbound ICMP
Default Outbound ICMP

These two default ICMP firewall rules permit all types of inbound and outbound ICMP messaging through the NDIS layer.

Click here {button ,AL("firewall faq",0,`',`')} for more information.

Active content

Active content is content that changes on your web pages, such as a weather map or a stock ticker. Most web pages provide active content by including Java scripts, Java applets, or ActiveX controls in the HTML code that defines the page.

ActiveX controls

ActiveX controls are programs designed to run over the Internet. Unlike Java Applets that run in a restricted environment, however, ActiveX technology has no built-in security. As a result, ActiveX controls have the potential to take complete control of your PC and perform destructive acts on your data or system software.

Address

In networking, an address is a numerical identifier for distinguishing one node from another.

Address mask

A technique used to select bits from an Internet address for subnet addressing. Masks are often used to help identify a range of addresses.

Adult settings

Accounts based on the Adult profile will allow users to change their own account settings but not the settings of others. Here are the settings provided by the Adult profile:

- Security settings: Applications are allowed to access the network unless they match the profile of a malicious program. Java Applets and ActiveX controls are allowed to run normally.
- Privacy settings: The user is prompted before confidential information is sent from the PC to a Web site. Cookies are not blocked. Web sites are prevented from finding out the sites that the user visited or the user’s email address.

Banner ad

An advertising graphic that appears at the top of the browser window and runs across the page.

Animated GIF

To display an animated image on a web page, a series of graphic images is shown. The series of images is displayed repeatedly to create the animation effect.

Personal Firewall

The Personal Firewall lets you control access in and out of your PC. It protects you against unauthorized transfers of data from your machine and prohibits attempts by intruders to gain access to critical or personal data on your machine.

Cache

In the context of web browsers, a web browser cache is a location on your hard disk where web pages and files (such as graphics) are stored as you view them. This speeds up the display of web pages you frequently visit or have already seen, because the browser can open them from your hard disk instead of from the Web.

Child settings

An account based on the Child profile will be restricted so that the child cannot change any settings. The Child profile has the following settings:

- Security settings: Applications are allowed to access the network unless they match the profile of a known malicious program. Java Applets and ActiveX controls are allowed to run normally.
- Privacy settings: Confidential information cannot be sent from the PC to a Web site. Cookies are not blocked. Web sites are prevented from finding out the sites that the user visited or the user’s email address.
- Parental Control settings: Blocks all of the Web site categories except sports and game sites. Gives only a few types of programs the ability to access the Internet (email, games, web browsers, and parent-approved categories).

Connection

A method of data exchange that allows a reliable transfer of data between two computers.

Connection attempt

The data transfer that requests the opening of a connection.

Cookie

Cookies are bits of information that web servers store on your computer for their later use. Web servers can use cookies to keep track of how many times you've visited and when, and what sort of information you've been surfing for on their site. They can even use cookies to pass that information on to other web servers, such as advertisement servers.

On the positive side, cookies can be used to store your own Web site configuration, to remember items placed in your “shopping cart” at an online shopping site, or to store account and password information for subscription sites.

Domain

A group of computers on a network administered as a unit. Within the Internet, subdomains or hosts sharing a common part of an IP address are said to be in the same domain.

Domain name

A domain name locates an organization or other entity on the Internet. For example, the domain name www.symantec.com locates an Internet address for a domain name where "symantec.com" is the domain and the particular host server is "www." Together, "www.symantec.com" constitutes a fully-qualified domain name.

Domain name server

A node that resolves Internet addresses for network hosts. Domain Name Service is a protocol that is part of the Internet Protocol Suite, and uses UDP. Another mechanism used to resolve Internet addresses is a Hosts file.

Echo

A computer is said to "echo" if it immediately transmits each character that it receives back to the source. An echo serves as a confirmation of receipt. TCP and UDP use port 7 for echo.

Email

Electronic mail. A method of sending messages to other people via computer networks.

Email is one of the protocols included with the TCP/IP suite of protocols. A popular protocol for sending email is SMTP and a popular protocol for receiving it is POP3.

Fileshare

A file system resource available through a network connection. Fileshare uses UDP ports 137 and 138 and TCP port 139. If you block TCP port 139, no fileshares are allowed.

Using fileshare is acceptable in a trusted office environment, but it is inappropriate for an Internet connection. Allow inbound if you want to receive broadcasts and see people in your "Network Neighborhood." Allow outgoing connections if you want to share another system's resources. Block outbound to the Internet. Block incoming connections unless you want to share your system resources.

Firewall rule

A set of parameters that defines a type of data packet or network communication to look for, and what to do (permit it or block it) when it is found.

Norton Internet Security provides a set of firewall rules that protects your PC from known attacks by malicious hackers. Using the Live Update feature, you can download the latest firewall rules to protect your system against new forms of attack.

FTP

File Transfer Protocol. The Internet standard high-level protocol for transferring files from one machine to another over TCP/IP networks. FTP uses ports 20 and 21. FTP is commonly used to download programs and other files to your computer from other servers. It is also used to transfer Web page files.

FTP Server: Providing FTP as a service invites hacking attempts. Use the security of your FTP server and operating system to control access (e.g. usernames, passwords, file access control). In the firewall, you can decide if you can filter by remote IP and allow access only to the local IP addresses. Block inbound connection attempts unless you have an FTP server.

FTP Client: If you are accessing an FTP server, try to use passive mode. Passive mode FTP allows you to block incoming FTP connection attempts. Check all downloaded files for viruses.

GIF

Graphics Interchange Format files, a bit-mapped graphics format used on the World Wide Web.

HTML

HyperText Markup Language. A standard set of "markup" symbols or codes inserted in a file intended for display on a World Wide Web browser. The markup tells the Web browser how to display a Web page's words and images for the user and defines hypertext links between documents.

HTTP

HyperText Transport Protocol. A set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Requires an HTTP client program on one end, and an HTTP server program on the other end. HTTP is the most important application protocol used in the World Wide Web. HTTP uses TCP port 80.

If you block HTML, you won't be able to surf the web. You may want to allow Java or ActiveX on trusted sites only.

ICMP

Internet Control Message Protocol. A protocol used by the Internet Protocol to report errors, give limited routing advice, and provide simple low-level services over TCP/IP networks.

ICMP is often used to disrupt IRC Chatgroup users. A malicious user can determine your IP address and then send false ICMP messages to your system which promptly drops your IRC connection. If you use IRC Chat, consider blocking incoming Destination Unreachable messages, as they are frequently used for this purpose.

ICMP Types:

Echo Reply (ping reply)

Destination Unreachable

Source Quench

Redirect

Echo Request (ping request)

Router Advertisement

Router Solicitation

Time Exceeded (used by Traceroute)

Parameter Problem

Timestamp Request

Timestamp Reply

Information Request

Information Reply

Address Mask Request

Identification

A service that provides user information to another system, so they can try to verify your identity. Uses TCP port 113. If you block it, other systems may refuse you their services, such as email.

Inbound communication

An attempt by an external computer to open a connection to your PC. The connection can be used to send data to and from your PC.

The Rule Assistant alerts you whenever a new type of inbound network communication occurs. You can then specify whether to allow or prohibit the communication, and you can define a firewall rule for that type of communication.

Inbound packet

A data packet arriving from a remote computer or network.

Incoming connection

A connection established by a remote computer to you. This is easily identifiable in the TCP protocol.

Internet Protocol (IP)

The essential network protocol by which data is sent from one computer to another on the Internet. It supports TCP, UDP, ICMP and many others. The Norton Internet Security firewall filters TCP and UDP. IP is a packet-oriented protocol that does not guarantee delivery.

Internet

A collection of networks and gateways (including the ARPANET, and NSFnet) using the TCP/IP protocol suite and functioning as a single cooperative virtual network.

Intranet

A network that uses TCP/IP protocols and other Internet technology within an organization. Especially applied to the use of World Wide Web technology for internal applications.

An intranet is a network of networks that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network. Typically, an intranet includes connections through one or more gateway computers to the outside Internet. The main purpose of an intranet is to share company information and computing resources among employees. An intranet can also be used to facilitate working in groups and for teleconferences.

An intranet uses TCP/IP, HTTP, and other Internet protocols and in general looks like a private version of the Internet.

Typically, larger enterprises allow users within their intranet to access the public Internet through firewall servers that have the ability to screen messages in both directions so that company security is maintained.

IP address

The Internet address, or IP address, is a 32-bit address assigned to hosts using TCP/IP. Most Internet addresses consist of a network portion and a node portion. The address for a host must be unique on the network. When you connect to a web server, for example, you may tell your browser to connect to www.symantec.com, but your computer ultimately has to translate the name to its IP address, 216.32.116.201, before the connection can be made.

ISP

Internet Service Provider. A company that provides individuals and other companies access to the Internet and other related services such as Web site building and hosting.

Categorized list of Web sites

Symantec's categorized list of Web sites is organized according to content—crime, intolerance, sex, violence, and so on. This list is updated on a regular basis and is made available through Norton Internet Security's LiveUpdate feature.

A description of each content category is available on Symantec's Web site.

Local (address or port)

Refers to your machine, as opposed to a remote machine.

Logging on to Norton Internet Security

Norton Internet Security grants users specific Internet access rights and other privileges. Before these rights and privileges go into effect, the user must log into Norton Internet Security.

There are several ways to log on to Norton Internet Security:

- Click the Norton Internet Security icon in the system tray and choose **Account Login**.
- Navigate to Norton Internet Security's Accounts window and click **Log In**.
- If a user's account has been set up as the Startup, the user is automatically logged on each time the program starts.

Java applet

Java applets are small programs that run in a restricted environment managed by your browser (sometimes referred to as a “sandbox”). Typically Java applets are downloaded to your computer when you visit a Web site. For example, you might download a stock ticker during a visit to a financial Web site.

While the vast majority of Java applets are designed to add functionality to basic HTML-based web pages, in some cases they may have a malicious intent such as password stealing.

Log

A listing of events related to network activity. The Norton Internet Security Event Log, available from the Norton Internet Security icon, provides a detailed event history.

Modem

Device that carries a data signal, typically over a telephone or ISDN line.

Name resolution

The process of mapping a domain name into the corresponding IP address.

NetBEUI

Short for NetBIOS Extended User Interface. The implementation of the NetBIOS transport protocol available with the Client for Microsoft Networks. This local-area protocol operates underneath the NetBIOS interface and lets computers communicate within a local area network.

The Norton Internet Security default firewall rules allow inbound and outbound NetBIOS.

NetBIOS

Short for Network Basic Input Output System, an application programming interface (API). An interface specification for PC local area networks used with the Client for Microsoft Networks and other LANs. Application programs use NetBIOS for client/server or peer-to-peer communications in support of file and print shares.

This protocol can be carried over TCP and UDP.

Network address

The network portion of an IP address. Most IP addresses have a network portion and a node portion.

Non-listening server port

When a service (server program) initially is started, it "binds" to a designated port number, which it then uses for network communication. If no service is bound to the port number that a client attempts to connect to, then the client is requesting a connection to a "non-listening server port." In other words, the client is attempting to connect to a server that is not running.

If the Norton Internet Security Firewall Rule Assistant is enabled, you will be alerted about inbound UDP and TCP communication attempting to connect to a non-listening server port.

Normal Users

A Normal User can change his or her own Norton Internet Security settings but not the settings of any other users. Normal Users cannot create or delete user accounts.

NTP

Network Time Protocol. A service that supplies the time. Uses port 123.

Allowing access for this protocol has potential risk if your system has time-sensitive services or applications and it uses the time that is supplied.

NTTP

Network News Transfer Protocol used for managing the notes posted on Usenet newsgroups. The NNTP client may is included as part of your Netscape, Internet Explorer, Opera, or other Web browser or you may use a separate client program called a newsreader. Allow inbound connections only if you are running a news server.

Outbound communication

An attempt by your PC to open a connection with an external computer. The connection can be used to send data to and from your PC.

The Rule Assistant alerts you whenever a new type of outbound network communication occurs. You can then specify whether to allow or prohibit the communication, and you can define a firewall rule for that type of communication.

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet. A packet contains information that enables computers on a network to determine whether to receive it, in addition to the data being transmitted.

When any file (email message, HTML file, GIF file, URL request, and so forth) is sent from one place to another on the Internet, the Transport Control Protocol (TCP) layer of TCP/IP divides the file into chunks (packets). Each of these packets includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet; when they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

Password

A secret character sequence used for authentication. Norton Internet Security supports password control to prevent another user on the PC from changing settings or having access to the Statistics and Event Log.

Permit/Block (rules)

The action taken if a packet matches a rule. Block means the packet is not sent/received. Permit means it is sent/received.

Personal Firewall

The Personal Firewall prevents outsiders from accessing your own private data resources and controls what outside resources its own users have access to. To do this, the Personal Firewall filters all network packets to determine whether to forward them toward their destination.

POP3

Post Office Protocol, version 3. which is used to transfer email. Uses TCP port 110.

Risks related to email are the spreading of viruses in files that are attached, and 'spam', the junk-mail of the Internet. Allow inbound connections if you are running a POP3 mail server.

Port

A "logical connection" place. A transport user identification used by a client program to specify a particular server program on a computer. Higher-level applications that use TCP/IP, such as the web protocol HTTP, have ports with preassigned numbers. Other application processes are given port numbers dynamically for each connection. When a service (server program) initially is started, it is said to bind to its designated port number. As any client program wants to use that server, it also must request to bind to the designated port number.

See also non-listening port.

Port number

Each TCP/IP application program has unique port numbers associated with it. The port number identifies the logical communications channel that is to be used by this application. Some protocols, use a well known port (for example, HTTP uses port 80) though this too can be configurable. Port numbers are always used in conjunction with IP addresses when establishing connections to host computers.

The host computer may be running both an HTTP server and an FTP server. If you're connecting to the host computer using a web browser, you'll want to connect to the HTTP server and not the FTP server. Since HTTP servers usually listen on port number 80, and FTP servers usually listen on port number 21, the web browser will connect to the correct server on the www.symantec.com computer if it connects to port 80.

Protocol

A protocol is the special set of rules for communicating that the end points in a connection use when they send signals back and forth. Both end points must recognize and observe the protocol.

On the Internet, there are the TCP/IP protocols, consisting of:

- TCP (Transmission Control Protocol), which uses a set of rules to exchange messages with other Internet points at the information packet level.
- IP (Internet Protocol), which uses a set of rules to send and receive messages at the Internet address level.
- HTTP, FTP, and other protocols, each with defined sets of rules.

Proxy

A mechanism allowing one system to “front” for another system when responding to protocol requests. Security applications in firewalls use proxy services to screen the secured network from users on the Internet.

Proxy server

A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server (separating the enterprise network from the outside network) and a firewall server (protecting the enterprise network from outside intrusion).

A proxy server receives a request for an Internet service (such as a Web page request) from a user. If the proxy server is also a cache server, it can use its local cache of previously downloaded Web pages. to provide the page without forwarding the request to the Internet. If the page is not in the cache, the proxy server, uses one of its own IP addresses to request the page from the server out on the Internet. When the page is returned, the proxy server relates it to the original request and forwards it on to the user.

To the user, all Internet requests and returned responses appear to be directly with the addressed Internet server. The proxy IP address has to be specified as a configuration option to the browser or other protocol program.

RAS

Remote Access Service, support for dialup connections.

Remote access is the ability to get access to a computer or a network from a remote distance. A remote access server is the computer and associated software that is set up to handle users seeking access to network remotely. Sometimes called a communication server, a remote access server usually includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network.

Referer field

Referer fields are used to provide "third-party" sites with information about the site that triggered a request for data from their server. Referer fields allow web servers to know where you've just been, which is information that you might prefer to keep to yourself.

For example, a web page may present an advertisement by including instructions for the browser to request the advertisement from a third-party site. As part of your browser's request for the advertisement, it provides the advertising site information about the site you visited that triggered the request. This information is passed in a referer field in the "HTTP GET" header (which the browser uses to make the request).

When you choose to block referer fields, information about what page you are currently viewing is not passed on. When your browser connects to a new web server, it appears that you just typed the URL into your browser or selected it from your bookmarks.

Restricted Users

Restricted Users cannot make any changes to their own accounts or the accounts of others. They are prevented from viewing security settings or the information stored by the Confidential Information Guardian.

Rule Assistant

The Rule Assistant provides an interactive learning mode in which Norton Internet Security automatically prompts for your input and creates rules that permit or block network communication based on the way you use software on your PC.

When the Rule Assistant is enabled, you are prompted for input whenever an application on the PC attempts to make a new type of network communication. Based on your response, Norton Internet Security permits or blocks the network communication and may create a firewall rule that applies to all future attempts to perform this type of network communication.

Services

Services are protocols that are used to allow one computer to access a particular kind of data stored in another computer. Many host computers that are connected to the Internet offer services. For example, HTTP servers use the HyperText Transfer Protocol to provide World Wide Web service, FTP servers offer File Transfer Protocol services, SMTP servers use the Simple Mail Transport Protocol to send mail, and POP servers use the Post Office Protocol to retrieve mail.

Services file

A text file that lists the port number of network services available to Windows sockets applications.

SMTP

Simple Mail Transfer Protocol. A TCP/IP protocol governing electronic mail transmission and reception. This is one of the most popular email services. Uses TCP/IP port 25. Risks related to email are the spreading of viruses in files that are attached, and 'spam', the junk-mail of the Internet.

Allow inbound connections only if you are running an SMTP mail server. Allow outbound to your SMTP mail server.

SOCKS

A mechanism by which a secure proxy data channel can be established between two computers in a client/server environment.

SOCKS is a protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet. Socks uses sockets to represent and keep track of individual connections. The client side of Socks is built into certain Web browsers and the server side can be added to a proxy server.

A socks server handles requests from clients inside a company's firewall and either allows or rejects connection requests, based on the requested Internet destination or user identification. Once a connection and a subsequent "bind" request have been set up, the flow of information exchange follows the usual protocol (for example, the Web's HTTP protocol).

Startup account

Norton Internet Security starts with one account automatically logged in. The various settings for the account (Security, Privacy, Parental Control, and Ad Blocking) go into effect immediately.

To change the startup account, open the Accounts window, click the user’s account and then click **Properties**.

Subscription content

If your subscription content is current, you can use Symantec’s Live Update feature to obtain content updates for Norton Internet Security. Content updates include updated Web site block lists and new rules for the Personal Firewall that protect you from the latest forms of Internet-based attacks.

Supervisor settings

Accounts based on the Supervisor profile will allow users to change their own settings and those of any other user. The Supervisor profile has the following settings:

- Security settings: Applications are allowed to access the network unless they match the profile of a known malicious program. Java Applets and ActiveX controls are allowed to run normally.
- Privacy settings: The user must give permission before confidential information is allowed to go out to a Web site, but cookies are not blocked. Web sites are prevented from retrieving the address of the last Web site visited or the email address used by the browser.

Supervisor

A user with supervisor rights can change any setting in the program and also add, remove, and modify other user accounts. More than one user can have supervisor rights.

Teenager settings

An account based on the Teenager profile will be restricted so that they cannot change any settings. The Teenager profile has the following settings:

- Security settings: Applications are allowed to access the network unless they match the profile of a known malicious program. Java Applets and ActiveX controls are allowed to run normally.
- Privacy settings: Confidential information is blocked from going out to Web sites (HTTP), but cookies are not blocked. Web sites are prevented from retrieving the address of the last Web site visited or the email address used by the browser.
- Parental Control settings: Blocks most categorized Web sites but does allow sports, games, finance, chat, job search, and news sites. Allows most types of programs to access the Internet (newsreaders and file transfer programs are blocked).

TCP

Transmission Control Protocol. The Internet standard transport-level protocol, providing reliable, full duplex, stream service. Software implementing TCP usually resides in the operating system and uses the IP protocol to transmit information across the Internet.

Examples of TCP-based applications and services are FTP, web browsing, email and IRC.

TCP/IP

Transport Control Protocol/Internet Protocol. Generally refers to the Internet Protocol Suite, which includes TCP and IP, as well as several other protocols, used by computers to communicate with each other. TCP/IP is the standard protocol used on the Internet. It can also be used as a communications protocol in the private networks called intranets and in extranets.

TCP/IP is a two-layered program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

Telnet

Telnet is a TCP-based service that supports remote logins (usually to UNIX systems). Telnet uses port 23.

With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific applications and data on that computer. Telnet is most likely to be used by program developers and anyone who has a need to use specific applications or data located at a particular host computer. Telnet has the risk of that you are sending your username and password over a network, which may be stolen by someone and used to break in.

UDP

User Datagram Protocol. A transport layer in TCP/IP networks. UDP is a low-overhead protocol that uses IP to deliver its packets.

Examples of services and applications that use UDP are DNS, NetBIOS (for broadcasts etc.).

URL

Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web.

The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

A sample URL is http://www.symantec.com/index.html, where http is the protocol, www.symantec.com is the domain name, and index.html is the document.

Web browser

A software application used to make navigating the Internet easy for the user by providing a graphical user interface so the user can click menus, icons, or buttons rather than learning difficult computer commands. Also called a web client because the browser application resides on the client, or the computer of the individual using it, rather than residing on a web server.

Two widely used web browsers are Microsoft's Internet Explorer and Netscape Navigator.

Web page

A single document on the World Wide Web that is specified by a unique address or URL and that contains text, hyperlinks, and graphics.

Web server

Computer where web pages are stored and accessed by others using web client software, or the computer software that allows the user to access the web pages.

Web site

A group of similar web pages linked by hyperlinks and managed by a single company, organization, or individual. A Web site may include text, graphics, audio and video files, and hyperlinks to other web pages.

World Wide Web

The World Wide Web (WWW or simply Web) is all the resources and users on the Internet that are using the Hypertext Transport Protocol (HTTP). The Web gives universal access to a vast collection of documents. The Web's protocols are a superset of many of the most common Internet application services. Web servers exist for libraries, corporations, and a wide variety of other sites.

Port and service assignments

When displaying messages about connections, Norton Internet Security uses the port and service assignments listed in your PC's Services file (if present) and those in the following table. (The Services file is a text file located in your Windows directory.)

Service	Port Number	Description
http	80	HTTP
www	80	HTTP
www-http	80	HTTP
http-alt	800	HTTP
http-alt-1	8008	HTTP
http-proxy	8080	Often used as HTTP proxy
http-proxy-1	8088	Often used as HTTP proxy
http-mgmt	280	HTTP management
https	443	HTTP server
gss-http	488	HTTP misc
fmpro-http	591	HTTP misc
ftp-data	20	File Transfer
ftp	21	File Transfer
http-rpc-epmap	593	HTTP misc
bootps	67	Bootstrap Protocol Server
bootpc	68	Bootstrap Protocol Client
dcom	135	Microsoft RPC end point to end point mapping
ldap	389	Lightweight Directory Access Protocol
video	458	Connectix and Quick Time Streaming protocols
video-1	545	Connectix and Quick Time Streaming protocols
rtsp	554	Real Time Stream Protocol
mountd	709	NFS mount daemon
pcnfsd	721	PC NFS Daemon
irc	194	Internet Relay Chat protocol
irc-serv	529	Internet Relay Chat protocol
ircs	994	Internet Relay Chat protocol
ircu	6665	Internet Relay Chat protocol
ircu-1	6666	Internet Relay Chat protocol
ircu-2	6667	Internet Relay Chat protocol
ircu-3	6668	Internet Relay Chat protocol
ircu-4	6669	Internet Relay Chat protocol
socks	1080	Socks
lotusnote	1352	Lotus
ms-sql-s	1433	Microsoft misc
ms_sql-m	1434	Microsoft misc
ms-sna-server	1477	Microsoft misc
ms-sna-base	1478	Microsoft misc
orasrv	1525	Oracle
tdisrv	1527	Oracle
coauthor	1529	Oracle

nsvt	1537	HP's NSVT native protocol
nsvt-stream	1570	HP's NSVT TCP stream mode
remote-winsock	1745	Remote Winsock Proxy
netshow	1755	Microsoft's NetShow
SMTP	25	Simple Mail Transfer
telnet	23	Telnet
Pop3	110	Post Office Protocol
icq	4000	ICQ chat program
aol	5190	America Online
aol-1	5191	America Online
aol-2	5192	America Online
aol-3	5193	America Online
aol-4	11523	America Online
Back-Orifice	31337	Back Orifice
NetBus	12345	Netbus
NetBus-2	12346	Netbus2
pc-anywhere-data	5631	pcAnywhere data port
pc-anywhere-status	5632	pcAnywhere status port
xserver	6000	X Server
vdolive	7000	VDOLive Player
msbd	7007	Microsoft MSBD (related to NetShow)
realaudio	7070	Real Networks Real Audio
quake	26000	Quake server game
quake2	27910	Quake2 server game
quake2-2	27911	Quake2 server game