Web options

The Web tab lets you 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 appearing on Web pages.
- Privacy: On this tab, you can define both global and site-specific settings to control the information that your browser sends in the referer field, user-agent field, and email field when getting pages from a Web site. (Blocking the user-agent field is not recommended.) You can also define how cookies are handled.
- 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. You can also specify that animated images on Web pages not repeat the animation sequence.

For more information:

Add Site

Remove Site

Ad Blocking

Privacy

Active Content

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Add site

Opens 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.

After adding a site, you can select it in the site list. Use the various tabs to specify the settings to be used when you visit this Web site.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Remove site

Removes the selected site name or domain name from the site list on the Web tab.

When a site or domain is removed, the site-specific or domain-specific settings are discarded.

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

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Web Settings: 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 appearing on Web pages.

When ad blocking is enabled, all HTML pages are scanned for the HTML strings specified in the site-specific blocking list and the (Defaults) blocking list. An HTML string is a sequence of text characters that are part of an advertisement URL; for example: www.site.com/ads/newcar.html. Any HTML string that contains a matching HTML blocking string is removed from the page before the page appears in the Web browser.

If you want to see an item that ad blocking has removed from a Web site, add a HTML string to permit that element to appear.

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

The controls on this tab include:

- Add: Opens the Add New HTML String dialog box where you can add a new HTML string to the selected blocking list.
- Modify: Opens the Modify HTML String dialog box for the selected string.
- Remove: Removes the selected HTML string.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Web Settings: Privacy Tab

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

Use these rules for <site> must be checked for the following settings to be available:

- Cookies: Specifies how the program handles requests for cookies when you visit a site.
- Referer: Specifies whether third-party sites are sent the address of the Web site from which you came.
- Browser (User-agent): Specifies whether sites are provided with information about the kind of browser that you are using. (Blocking the user-agent field is not recommended.)
- E-mail (From): Specifies whether sites are given the email address that your browser uses. Newer browsers do not send your email address, so in most cases this option is not necessary.

For more information:

Cookies

Referer

Browser (User-agent)

E-mail (From)

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Cookies

Sites may use cookies to store your own Web site configuration, to remember items placed in a 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.

Some advertisers use cookies to track your Web usage and send the information back to their corporate server. This setting specifies how the program handles requests for cookies for the selected site.

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

- Permit: The program permits your browser to return cookies.
- Block: The program prevents your browser from returning cookies.
- Reply: The program returns the string specified in the Cookie box instead of the cookie.

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

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Referer

Specifies whether third-party sites are sent the address of the Web site from which you came. By default, the Referer field is blocked.

For example, a Web page may have an advertisement that comes from a third-party site. As part of your browser's request for the advertisement, it provides the address of the Web page to the advertising site. 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 revealing the URL of the page that 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.

Note: 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 on 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 of the BeBop site—then the BeBop Web server can be configured to refuse to respond to the server request.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Browser (User-agent)

Specifies whether sites are provided with information about the type of browser and operating system you are using. If you enable Privacy Control, 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 the type of browser and operating system that you are using.
- Block: Prevents your browser from revealing the type of browser and operating system that 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.

Note: 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. Misidentifying your operating system can make it more difficult for a hacker to identify an effective attack.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

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.

Note: Newer browsers do not send your email address, so in most cases this option is not necessary.

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 sender's 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.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Web Settings: 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 not repeatedly display the animation sequence.

For more information:

Script Blocking

Binary Executable Blocking

Miscellaneous Blocking

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Script Blocking

Some Web pages use JavaScript or VBScript to display advertising, open secondary (pop-up) 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).

There are four script-blocking options:

- Block all script: Prevents JavaScript and VBScript from running. When this option is selected, the program comments out all of the HTML code within <script> </script> tags to block the execution of these scripts.
- Block script popups only: Prevent scripts from displaying secondary or pop-up windows but lets them perform other actions. When this option is selected, the program examines the strings within HTML <script> </script> tags, and removes any open method JavaScript calls.
- Allow all script to execute: Lets JavaScripts and VBScripts work normally.
- Use default script behavior: Let (Defaults) control the blocking behavior of an individual site. Click (Defaults) to view the default script blocking setting.

Note: When Block all script is enabled, a JavaScript error may appear when you open a Web page. In most cases, you can click OK to dismiss the error and continue viewing the Web page. Some Web pages may not work correctly if JavaScript or VBScript is blocked.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Binary Executables

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 and ActiveX blocking behavior of individual sites.

There are three options for Java applets and ActiveX controls:

- Block Java applets and Block ActiveX controls: Prevents these types of active content from running.
- Allow Java applets to execute and Allow ActiveX controls to execute: Lets these programs work normally.
- Use default Java applet behavior and Use default ActiveX behavior: Lets (Defaults) control the blocking behavior of the individual site. Click (Defaults) to view the Java applet and ActiveX settings.

To change the Binary Executable settings for (Defaults), in the Personal Firewall Settings window, use Custom Level to change the Java applet and ActiveX control security settings.

Troubleshooting tips

If either Block Java applets or Block ActiveX controls is enabled, an error may appear when you open a Web page. In most cases, you can click OK to dismiss the error and continue viewing the Web page.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Miscellaneous (Animated images)

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.

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

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Other options

HTTP Port List: The HTTP Port List shows the HTTP port numbers being filtered for Java and ActiveX blocking, script blocking, confidential information and so on. The default list contains the standard HTTP ports, but you can add ports if you use applications that perform HTTP communication through nonstandard ports. For example, your computer may connect to the Internet through a proxy server that causes all HTTP communication to go through the port used by the proxy server. Web applications that use ports not covered in this list are not filtered for content blocking.

Block IGMP Protocol: Blocks the use of the Internet Group Management Protocol, a standard for IP multicasting on the Internet. Attackers sometimes exploit this protocol to freeze a victim's computer once they obtain its IP address.

Note: You must restart your computer for a change in this setting to take effect.

Stealth Blocked Ports: Causes blocked ports to not respond at all to inquiries from the Internet. When your computer receives an inquiry on a blocked port, it can respond that the port is closed, or it can not respond at all. If your computer responds that the port is closed, it passes an important piece of information to the inquiring computer: that there is a computer there. If your computer does not respond at all (stealth), the inquiring computer learns nothing.

Block Fragmented IP Packet Headers: Blocks 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.
Note: You must restart your computer for a change in this setting to take effect.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Content Blocking log

Messages in the Content Blocking log provide information about ads, images, Java applets and ActiveX controls that have been blocked. The messages indicate the HTML code that was removed in order to block ads and images, the Web page that it was removed from, and the URL string that triggered the blocking activity.

Refresh updates the display with current information.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Connections log

The Connections log shows a history of all TCP/IP network connections made with this computer. Connections are logged when the connection is closed.

In addition to the date and time columns, the following information is available:

- User: The name of the account that made the connection.
- Remote: The address or host name of the remote site and the service or port number.
- Local: The local address or computer name and the service or port number being used by the application.
- Sent Bytes: Number of bytes sent while the connection was active.
- Recv Bytes: Number of bytes received while the connection was active.
- Elapsed Time: The length of time that the connection was active.

Refresh updates the display with current information.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Firewall log

The Firewall log provides information about network communication intercepted by the firewall and rules that were processed. It shows alerts displayed to the user, unused ports blocked, and AutoBlock events.

Refresh updates the display with current information.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Privacy log

This Privacy log provides information about cookies that were blocked. 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 locked, including the address of the site from which you linked and the name of the site to which you linked.

Refresh updates the display with current information.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Restrictions log

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

Refresh updates the display with current information.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

System log

The System log provides information about the program’s activity as a Windows service (a program that performs a specific task to support other programs) and error messages.

System events are identified by type. Options on the System tab let you specify the following types of event to display:

- Error: These messages include the highest severity system errors.
- Warning: These messages cover cases in which software is operating in less than optimum conditions. For example, when resource usage is too high.
- Information: These messages include information about the current status of IP filtering.
- Alert: These messages notify the user of network interactions detected. For example, if the Rule Assistant is enabled, the program displays a user alert any time a new type of inbound or outbound network communication is attempted. An alert message is recorded in the 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: These messages indicate whether the program started as a Windows service on the computer.

Refresh updates the display with current information.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Web History log

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

You can review the sites your children have visited with the Web history log.

Go to opens the selected site in your browser.

Refresh updates the display with current information.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Alerts log

The Alerts log lists security alerts. This provides a history of possible attacks on your system.

Refresh updates the display with current information.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

active content

Material on a Web page that changes with time or in response to user action, such as a weather map or a stock ticker. Active content is implemented through ActiveX controls, VB Script, JavaScript, and Java applets in the HTML code that defines the page.

ActiveX controls

Programs that are designed to run over the Internet. ActiveX controls don’t run in a restricted environment like Java applets do, so they have the potential to take control of your computer. Malicious hackers can use this capability to steal or destroy your data or system software.

address mask

A code, in the form of an IP address, that computers use to determine which parts of an IP address identify the network and subnet (that is, parts that are common to all computers on the network) and which parts identify individual computers on that network. Masks are often used to help identify a range of addresses.

Adult account

Accounts based on the Adult profile let users change their own account settings but not the settings of other accounts.

banner ad

An advertising graphic that appears on a Web page and often contains a link to the advertiser's Web site.

cache

A location on your hard disk in which data is stored for reuse. A Web browser cache stores Web pages and files (such as graphics) as you view them. Web pages that you frequently visit or have already seen appear quicker because the browser opens them from your hard disk instead of from the Web.

categorized list of Web sites

A list of Web sites maintained by Symantec that is organized according to content—crime, intolerance, sex, violence, and so on. This list is updated regularly and is made available as part of your Internet security subscription service.

Child account

An account based on the Child profile is restricted so that the child cannot change any settings.

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.

connection-based protocol

A protocol, such as TCP, that requires a connection before information packets are transmitted.

connectionless protocol

A protocol, such as UDP, that sends a transmission to a destination address on a network without establishing a connection.

cookie

Information that Web servers store on your computer and subsequently retrieve when you revisit a site. Web servers can use cookies to store your personal information and preferences so that you don’t need to reenter them each time you visit. Cookies are often used to remember items you place in your shopping cart at an online store. However, cookies can also be used to monitor when you visit a site and which pages you view; cookies can be used to pass that information on to other Web servers, such as advertisement servers.

cracker

A person who attempts unauthorized access of other people's computers for the purpose of obtaining information on those computers or to do damage to those computers.

cyberpunk

Originally a science fiction subgenre focusing on computers, technology, and the Internet, now sometimes used to describe a person who uses applications written by others to gain unauthorized access to other people’s computers.

DHCP

Dynamic Host Configuration Protocol. DHCP automatically assigns a temporary IP address to each device on a network. Many Internet service providers use DHCP to assign addresses to dialup and some broadband customers.

DNS

Domain Name System. A hierarchical naming system that correlates domain names (such as www.symantec.com) with IP addresses (such as 206.204.212.71).

DNS server

Domain Name System server. A computer that keeps a database of domain names and their corresponding IP addresses. When a computer sends a domain name to a DNS server, the server returns the IP address for that domain.

domain

On the Internet, the common address for a single company or organization (such as symantec.com), which might have multiple hosts.

domain name

Locates an organization or other entity on the Internet. For example, 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.

echo

To immediately transmit each character that a computer receives back to the source, serving as a confirmation of receipt. TCP and UDP use port 7 for echo. Echoing can be used to test the quality of a network connection between two computers.

email

Electronic mail. A method of exchanging messages and files with other people via computer networks. A popular protocol for sending email is SMTP (Simple Mail Transfer Protocol). Popular protocols for receiving email are POP3 (Post Office Protocol 3) and IMAP4 (Internet Message Access Protocol 4). Web-based email services use HTTP (HyperText Transfer Protocol) for sending and receiving email.

File and Printer Sharing for Microsoft Networks

A service that allows sharing of files and printers through a network connection. File and Printer Sharing for Microsoft Networks uses UDP ports 137 and 138, and TCP port 139. If you block TCP port 139, no shared resources are allowed.

Norton Internet Security and Norton Personal Firewall block port 139 by default. This prevents file sharing by any computer not in the Trusted zone.

fingerprint

An encrypted digital signature used to uniquely identify a specific application version. Used by Automatic Internet Access Control to ensure that it creates rules only for known applications.

firewall

A security system that uses rules to block or allow connections and data transmissions between your computer and the Internet. A desktop firewall, like Norton Personal Firewall, protects an individual computer, typically a computer used at home. A conventional (corporate) firewall protects a network of computers, typically at a business.

If you use a computer at work that is protected by a corporate firewall, you probably don’t need a desktop firewall. If you use a computer that is connected to the Internet and isn’t protected by a firewall, you should use a desktop firewall.

Your computer is especially vulnerable to hacking and other threats if you do not use a firewall and you have an always-on Internet connection, such as a DSL (Digital Subscriber Line) or a cable modem. One potential threat is hackers using your computer to launch malicious actions against other computers, without you ever knowing it. Norton Personal Firewall protects your computer from such actions by monitoring data sent over the Internet from your computer.

firewall rule

A set of parameters that specifies a type of data packet or network communication and an action to perform (permit it or block it) when it is found.

fragment

An IP packet that has been split into two or more parts, or fragments. When the size of an IP packet exceeds the maximum frame size of a network that it crosses, the packet must be divided into smaller packets, or fragments.

FTP

File Transfer Protocol. A standard protocol for copying files to and from remote computers over TCP/IP networks, such as the Internet. 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 upload Web page files to your own Web site.

hacker

A person who attempts unauthorized access of other people’s computers for the purpose of obtaining information on those computers or to do damage to those computers.

host name

The name that identifies a computer on a network. For example, www.symantec.com is the host name for the Symantec Web site. Host names are translated to IP addresses by the DNS.

HTML

HyperText Markup Language. A standard language for documents on the World Wide Web. Codes inserted in a text file instruct the Web browser on how to display a Web page's words and images for the user, and defines hypertext links between documents.

HTTP

HyperText Transfer Protocol. A set of rules for requesting pages from a Web server and transmitting pages (including text, graphic images, sound, video, and other multimedia files) to the requesting Web browser. HTTP is the most widely used application protocol on the World Wide Web. HTTP uses TCP port 80.

HTTPS

HyperText Transfer Protocol Secure. A variation of HTTP that uses encryption to transmit data securely. HTTPS uses TCP port 443.

ICMP

Internet Control Message Protocol. A protocol used on the Internet to report errors, give limited routing advice, and provide simple low-level services over TCP/IP networks. Some IP troubleshooting tools, such as ping and traceroute, use ICMP.

identification

A service that provides user information to another system, also known as IDENT, Authentication, or AUTH. Some email servers, news servers, and IRC servers use this service to verify your identity before allowing access. Identification uses TCP port 113.

IGMP

Internet Group Membership Protocol. A protocol used to establish memberships in multicast groups on a single network. Multicasting is a means of sending messages to a select group. It is often used as a way to teleconference over the Internet.

inbound communication

An attempt by an external computer to open a connection to your computer. The connection can be used to send data to and from your computer.

inbound packet

A data packet arriving from a remote computer or network.

incoming connection

A connection established by a remote computer to your computer.

Internet

A collection of networks and gateways (including ARPANET and NSFnet) using the TCP/IP protocol suite and functioning as a single cooperative virtual network.

intranet

A network within an organization that uses TCP/IP protocols and other Internet technology. It may include many interlinked local area networks and also use leased lines in a wide area network. The purpose of an intranet is to share company information and computing resources among employees.

IP

Internet Protocol. The essential protocol by which data is sent from one computer to another on the Internet. IP routes packets to the appropriate destinations.

IP address

Internet Protocol address. A 32-bit numeric address assigned to hosts that use TCP/IP. The address for a host must be unique on the network. IP addresses are usually expressed as four decimal numbers, each ranging from 0 to 255, separated by periods. For example, 206.204.52.71.

ISP

Internet Service Provider. A company that supplies Internet access to individuals and companies. Most ISPs offer other Internet connectivity services, such as Web site hosting.

Java applet

A small program that runs in a restricted environment (sometimes referred to as a sandbox) that is managed by your browser. Most Java applets are used to add multimedia effects, interactivity, or other functionality to a Web page, but they can be used for malicious purposes, such as password stealing.

JavaScript

A scripting language that is similar to, but less capable than, Java. JavaScript code can be included in Web pages to add interactivity and other functionality.

local

A term that refers to your computer, as opposed to a remote computer.

Logging on

When you start Norton Internet Security, it uses the settings from the startup account, or, if you are using Windows accounts, the settings for the account you use to log on to Windows. To use a different account, you have to log off of the current account and log on to another account.

log

A list of events related to network activity. Using the log, you can monitor your firewall's actions and see any attempts to break into your computer.

modem

Device that modulates (converts to analog) and demodulates (converts from analog) digital data for transmission over a telephone line. Also commonly used to refer to interface devices for digital connections to the Internet, such as ISDN, cable, and DSL.

name resolution

The process of mapping a domain name to a corresponding IP address.

NAT

Network Address Translation. A method of converting IP addresses used on an intranet or local area network into Internet IP addresses. This lets many computers share an Internet IP address. More importantly, it hides the IP addresses of internal network computers from outsiders. The Internet Connection Sharing (ICS) feature included with recent versions of Windows uses NAT.

NetBEUI

NetBIOS Extended User Interface. The implementation of the NetBIOS transport protocol available with the Client for Microsoft Networks. A network protocol that lets computers communicate within a local area network. This protocol is not routed over the Internet.

NetBIOS

Network Basic Input Output System. An interface specification for local area networks that is used with the Client for Microsoft Networks and other LAN operating systems. 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 portion of an IP address that is common to all computers on a particular network or subnet.

nonlistening server port

A port that doesn’t have a service bound to it. When a service (server program) is started, it binds to a designated port number, which it then uses for network communication. When a port is bound, only the service bound to it can use that port.

Adult account

Users of an Adult account can change their own settings but not the settings of any other accounts. Adult accounts cannot create or delete accounts.

NNTP

Network News Transfer Protocol. A protocol used by news servers and newsreaders for managing the messages posted on Usenet newsgroups. NNTP usually uses port 119.

NTP

Network Time Protocol. A protocol used for services that supply the time. NTP uses port 123.

outbound communication

An attempt by your computer to open a connection with a remote computer. The connection can be used to send data to and from your computer.

packet

A unit of data that is routed between an origin and a destination on the Internet. In addition to the data being transmitted, a packet contains information that enables computers on a network to determine whether to receive it.

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 Transmission Control Protocol (TCP) layer of TCP/IP divides the file into smaller pieces (packets). Each of these packets includes the Internet address of the destination. The individual packets for a file may travel different routes over the Internet; when they have all arrived, they are reassembled into the original file by the TCP layer on the receiving end.

Packets can also be sent over UDP, ICMP, or IGMP.

packet monkey

An unsophisticated hacker who uses preexisting programs to infiltrate other people’s computers.

packet-switching network

A network of computers (such as the Internet) that transmits files by breaking them into small units (packets) and routing each packet along the best available route between the source and destination, relaying the packets through computers along the route. Packets in a file may not all take the same route and they may arrive at the destination at different times and out of sequence. Network protocols (such as TCP/IP) reassemble the packets into a file on the receiving end.

Sometimes packets may be subdivided or "fragmented" during the route.

password

A character sequence entered by users to verify their identity to a network or program. The most secure passwords are difficult to guess or find in a dictionary, and contain a combination of capital letters, lowercase letters, numbers, and symbols.

POP3

Post Office Protocol, version 3. A commonly used protocol for transmitting email. POP3 uses TCP port 110.

port

A logical communications channel or channel endpoint used by a client program to specify a particular server program on a computer. Also called a service or socket.

Higher-level applications that use TCP/IP, such as the Web protocol HTTP, have ports with preassigned numbers. (For example, the Web protocol HTTP usually uses port 80.) Other application processes are given port numbers dynamically for each connection. When a service (server program) is started, it binds to its designated port number. When a client program wants to use that server, it also must request to bind to the designated port number. *See also* service.

port number

A logical communications channel to be used by a particular TCP/IP application. Each application has unique port numbers associated with it. By convention, some protocols use a well-known port number (for example, HTTP uses port 80), although this is configurable. Port numbers are always appended to IP addresses when establishing connections to host computers, but most applications don’t display the port number.

port scan

An attempt to gain access to a computer by searching for open ports. Usually done by an automated program that sends a request to each port at an IP address, listening for responses that could reveal a vulnerability. If a port scan is detected and AutoBlock is enabled, all communications from the scanning computer are stopped for 30 minutes.

PPP

Point-to-Point Protocol. A method of connecting to the Internet via dial-up connection. Some broadband connections use a variant of PPP called PPPoE (PPP over Ethernet).

protocol

A set of rules for communicating across a network. Both end points must recognize and observe the protocol.

Internet communications rely on several protocols, including:

- TCP (Transmission Control Protocol): A set of rules to exchange messages with other Internet points at the information packet level.
- IP (Internet Protocol): A set of rules to send and receive messages at the Internet address level.
- HTTP, FTP, and other application-layer protocols: Rules that are used by applications, such as Web browsers, file-transfer programs, and email programs.

proxy

A mechanism allowing one system to act on behalf of 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 is 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 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 from the addressed Internet server. The proxy IP address must be specified as a configuration option on the browser or other protocol program.

referer field

Information included with a request for data that tells a server what site you’re visiting when you make the request. Referer fields let Web servers know where you've been on the Internet.

When you choose to block referer fields, information about the page you are currently viewing is not passed on. When your browser connects to a new Web server, it appears that you typed the URL in your browser or selected it from your bookmarks.

Norton Internet Security and Norton Firewall block referer fields by default to protect your privacy.

router

A device on a network that links computers or interconnected networks. A router receives packets and forwards them to their destination via the best available route.

script kiddie

A person who attempts unauthorized access of other people’s computers for the purpose of obtaining information on those computers or to do damage to those computers. Typically one that uses applications written by others to attack computers on the Internet.

service

Protocols that let one computer access a type of data stored on 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 exchange email, and POP servers use the Post Office Protocol to exchange email. *See also* port.

SMTP

Simple Mail Transfer Protocol. A TCP/IP protocol governing electronic mail transmission and reception. This is one of the most popular email services. SMTP   uses TCP/IP port 25.

sneakernet

A method of moving data between computers that are not connected by a network. A user copies the data onto removable media (such as floppy disks) and physically carries the media to another computer.

socket

An identifier for a particular service on a particular computer. A socket consists of the IP address of the computer followed by a colon and the port number. *See also* port.

startup account

When Norton Internet Security starts, one account is automatically logged on. This account is known as the startup account. The various settings for the startup account (Security, Privacy, Parental Control, and so on) go into effect immediately.

If you are using multiple accounts created in Norton Internet Security, you can specify which account is the startup account. If you are using Windows accounts as Norton Internet Security accounts, the startup account is the one currently logged on to Windows.

subnet

A local area network that is part of a larger intranet or the Internet.

subnet mask

A code, in the form of an IP address, that computers use to determine which parts of an IP address identify the subnet (that is, parts that are common to all computers on the subnet) and which parts identify an individual computer on that subnet.

Using the subnet number, it is possible to identify which addresses are in your local network and should be protected.

Supervisor account

Accounts based on the supervisor profile let users change their own settings and those of any other account.

Supervisor

An account with supervisor rights can change any setting in the program and also add, remove, and modify other accounts. More than one account can have supervisor rights.

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 over 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 intranets and 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.

Teenager account

An account based on the Teenager profile is restricted so users cannot change any settings.

Telnet

A TCP-based service that supports remote logons to computers connected to a network. This lets you log on to a remote computer as a regular user with the privileges that you have been granted to the applications and data on that computer. Since a person logged on remotely to a computer can make possibly dangerous changes to files, be very careful to whom you give telnet access.

Windows includes a telnet client (telnet.exe) that can be used to log on to remote computers. Telnet uses port 23.

top-level domain

The last part of a domain name, which identifies the type of entity that owns the address (such as .com for commercial organizations or .edu for educational institutions) or the geographical location of the address (such as .ca for Canada or .uk for United Kingdom).

Trojan horse

A program masquerading as a legitimate program that is harmful to the computer.

A Trojan horse neither replicates nor copies itself, but damages or compromises the security of the computer. Typically, it relies on someone emailing it to you; it does not email itself. A Trojan horse might arrive disguised as useful software of some sort. Some Trojan horse programs perform malicious actions on the computer on which they are run, while others, such as Back Orifice, provide remote-control capabilities for hackers.

UDP

User Datagram Protocol. A connectionless protocol that operates at the transport layer to provide functionality similar to TCP, but with less reliability. UDP uses IP to deliver its packets, but it does not establish a connection before sending and it does not verify that packets are properly received. Internet radio and other streaming media often use UDP because of the lower overhead.

URL

Uniform Resource Locator. The global address of documents and other resources on the World Wide Web. The first part of a URL indicates the 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. A sample FTP site URL is ftp://ftp.symantec.com, where ftp is the protocol and ftp.symantec.com is the domain name.

virus

A program designed to replicate and spread, generally without the user’s knowledge.

A virus replicates itself by attaching itself to another program, a boot sector, a partition sector, or a document that supports macros. Many viruses just replicate; many also do damage. A virus can arrive in a document that you receive by email.

vulnerability

An opening through which an attack or damage might occur.

Web browser

A software application that makes navigating the Internet easy for the user by providing a graphical user interface. This lets the user click menus, icons, or buttons rather than learn difficult computer commands. Also called a Web client.

Two widely used Web browsers are Microsoft Internet Explorer and Netscape Navigator.

Web page

A single document on the World Wide Web that is specified by a unique address or URL. A Web page can contain text, hyperlinks, and graphics.

Web server

A computer on which Web pages are stored and accessed by others using Web client software, or the computer software that lets the user access the Web pages.

Three widely used Web servers are Apache, Internet Information Server, and Personal Web Server.

Web site

A group of Web pages 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.

well-known ports

Ports in the numeric range 0 through 1023 that are assigned to applications by Internet convention.

World Wide Web

The collection of hypertext documents that are stored on HTTP servers around the world. Also called WWW or simply the Web. The Web allows universal access to a vast collection of documents stored in HTML format as Web pages.

worm

A program that makes copies of itself, for example, from one disk drive to another, or by sending itself through email. It may do damage or compromise the security of the computer. A worm might arrive as an attachment to an email.

zombie program

A dormant program secretly placed on a computer. Later, it is awakened to aid in a collective attack on another system. Zombie programs don't normally damage the computer on which they reside, but are used to attack other computers. A zombie program might arrive as an email attachment.

About the Current Status window

In the Current Status window you can.

- See who is currently logged on.
- Temporarily enable or disable all protection.
- View realtime statistics or temporarily suspend protection features.
- See when your Internet security subscription service expires.

Many of the counters on this page are reset when you restart your computer. The others are reset when you clear the corresponding event log.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

About the Reporting window

In the Reporting window you can control the amount of information that you receive from Alert Tracker.

Use the Reporting slider to set one of the following Reporting Levels:

Reporting Level	**Information Provided**	**Alert Tracker Messages**	**Security Alerts**	**Notifies you when…**
Minimal	Critical Internet events	None	None	Internet Access Control rules are created automatically Port scans occur Confidential information is blocked Remote access Trojan horse program is encountered
Medium	Important Internet events	Medium number	None	Same notification as Minimal, plus: Applications access the Internet
High	Complete program activities	Many	Displayed	Same notification as Medium, plus: Unused ports are blocked Cookies and content are blocked

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

About the Security Check window

The Security Check window enables you test your computer’s vulnerability to security intrusions. The Scan for Security Risks link connects you to the Symantec Security Check web page, where you can get information on what Security Check scans for before running the scan.

To run Security Check, click the Scan for Security Risks link.

About the Personal Firewall Settings window

In the Personal Firewall Settings window you can view, modify, and enable Internet security settings.

If a selected account is not currently logged on, the account name appears in red and the settings do not go into effect until the account logs on to Norton Internet Security. This allows you to edit other users' settings.

Use the Security Level slider to set one of the following Security Levels:

- High: The Personal Firewall security setting is set to High, which blocks everything until you allow it. Java applet and ActiveX control security settings are set to Medium, which prompts you each time one is encountered. Unused ports do not respond to connection attempts, giving them a stealth appearance.
- Medium: The Personal Firewall security setting is set to High, which blocks everything until you allow it. ActiveX control and Java applet security settings are set to None, which allows all ActiveX controls and Java applets to run. Unused ports do not respond to connection attempts, giving them a stealth appearance.
- Minimal: The Personal Firewall security setting is set to Medium, which blocks known malicious applications. ActiveX control and Java applet security settings are set to None, which allows all ActiveX controls and Java applets to run. Unused ports respond normally to connection attempts.

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

Other controls in this window include:

- Custom Level: Controls specific Security settings.
- Default Level: Reverts the Security settings to the original settings.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Customize Security Settings

This dialog box lets you create a customized level of security.

- Personal Firewall: Specifies how firewall rules are applied.
- Java Applet Security: Lets you 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.)
- Enable Internet Access Control Alerts: Provides discretionary control when an application tries to connect to the network but no firewall rule exists for it. You will be able to permit or block the application from accessing the Internet.

  Disable this option if you want to block applications from accessing the network when there are no specific firewall rules in place for them.

- Alert when unused ports are accessed: Alerts you when an attempt is made to access an unused port on your computer. These alerts are useful for solving problems when you are configuring advanced programs and features such as Internet Connection Sharing. Disable to avoid alerts about unsolicited connection attempts.

Choose an item for more information:

Personal Firewall settings

Java Applet Security settings

ActiveX Control Security settings

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Personal Firewall settings

The Personal Firewall has three settings:

- High: Blocks all communication that you do not specifically allow. You must create firewall rules for every application that requests Internet access. If you have done an Application Scan, you should not be interrupted frequently.
- Medium: Blocks many ports used by harmful applications, but may also block useful applications when they use the same ports. This setting uses rules that are supplied by Symantec and kept current by LiveUpdate. You should not change these rules without specific knowledge of the effect that your changes will have on your protection.
- None: Disables the firewall and allows all Internet communications.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Java Applet Security settings

The Java Applet Security control has three settings:

- High: Blocks your browser from running any Java applets over the Internet. This is the safest, but most inconvenient option. Web sites that rely on these elements might not operate properly using this setting.
- Medium: Prompts you when Java applets are encountered. This lets you temporarily or permanently allow or block each Java applet that you encounter. It can be bothersome to respond every time you come across a Java applet, but it lets you decide which ones to run.
- None: Lets Java applets run whenever you encounter them.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

ActiveX Control Security settings

The ActiveX Control Security control has three settings:

- High: Blocks your browser from running any ActiveX controls over the Internet. This is the safest, but most inconvenient option. Web sites that rely on these elements might not operate properly using this setting.
- Medium: Prompts you when ActiveX controls are encountered. This lets you temporarily or permanently allow or block each ActiveX control that you encounter. It can be bothersome to respond every time you come across an ActiveX control, but it lets you decide which ones to run.
- None: Lets ActiveX controls run whenever you encounter them.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

About the Internet Access Control window

In the Internet Access Control window you can control how applications on your computer access the Internet.

Configure changes the following system-wide settings:

- System-Wide Settings: Changes firewall rules that apply to the entire system rather than to a particular application. For example, the rules that control Microsoft networking are found here. You can add system-wide rules to monitor communications.
- Trojan Settings: Provides protection for a large number of remote access Trojan horse programs. LiveUpdate updates this protection. You can view the list of rules that protects you from remote access Trojan horses, but do not change these rules without specific knowledge of the affect that your changes will have.
- Application Scan: Scans for Internet-enabled applications. This is the quickest way to set up Internet Access Control for all of your applications. The Application Scan checks your computer for Internet-enabled applications that it recognizes and then lets you choose settings for each application.
- Enable Automatic Internet Access Control: Creates a new firewall rule for low-risk applications that it recognizes the first time that they are run. Only enable Automatic Internet Access Control if you run LiveUpdate weekly to keep your Internet and virus protection current. New rules will only be created for applications that have been identified as posing little risk to your computer.

In the list of applications, you can modify Internet access for each application:

- Application: The name of the application, or the name of the application's executable file.
- Internet Access: The type of control placed on the application. Click this entry to change the type of control.
- Category: The category that this application is placed in for Parental Control. Click this entry to change the category.

You can also add, modify, or remove Internet access controls for any of the applications in the list.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

About the Internet Zone Control window

In the Internet Zone Control window you can identify computers that you trust, and computers that you want to restrict from accessing your computer at all.

You can place computers in either of two zones:

- Trusted zone: Computers not regulated by Norton Internet Security. They have as much access to your computer as they would have if Norton Internet Security were not installed. Place computers on your local network with which you need to share files and printers in the Trusted zone.

  If a computer in your Trusted zone is successfully attacked, and a hacker takes control of it, it poses a risk to your computer.

- Restricted zone: Computers prevented from accessing your computer at all. Add computers that attempt to attack you to the Restricted zone. The Restricted zone provides the highest level of protection, beyond the normal protection provided by Norton Internet Security. You cannot interact with computers in the Restricted zone.

You can add computers to or remove computers from either zone.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

About the Intrusion Protection window

In the Intrusion Protection window you can review and control the reaction to attacks.

Intrusion Protection stops hacker attacks as they occur. The program monitors Internet communications, looking for patterns of communications that are typical of a hacker attack. For example, if a computer tries to connect to a series of ports on your computer, Intrusion Protection recognizes it as a port scan, which is a common method of attack.

Intrusion Protection also detects attempts to connect to ports used by remote-access Trojan horse programs.

When the program detects an attack, it warns you and blocks all communications from the attacking computer for 30 minutes. This automatic blocking of communications is called AutoBlock.

AutoBlock stops all communication from the remote computer for 30 minutes. It does not stop you from communicating to the remote computer.

Computers in the Trusted and Restricted zones are not subject to AutoBlock. Computers in the Trusted zone are never blocked, while computers in the Restricted zone are permanently blocked.

Some normal Internet activities will be repeatedly recognized by Norton Personal Firewall as an attack. For example, some Internet service providers scan the ports of client computers to ensure that they are within their service agreements.

To prevent normal activities from interrupting your Internet use, you can exclude certain computers from being blocked by AutoBlock.

- Detect Port Scan Attempts: Blocks the attack and notifies you when the program detects a port scan.
- Enable AutoBlock: Stops all communication from attacking computers for 30 minutes.

AutoBlock stops all communication from the remote computer. It does not stop you from communicating to the remote computer.

In some cases, normal activity might be recognized as an attack. If you can’t communicate with a computer that you should be able to communicate with, see if it is on the list of Computers currently blocked by AutoBlock.

You can unblock single computers, unblock all blocked computers, or exclude computers from being blocked by AutoBlock.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Exclusions

To prevent normal activities from interrupting your Internet use, you can exclude certain computers from being blocked by AutoBlock.

The controls include:

- Exclude: Adds the item selected in the Currently Blocked list to the Excluded Computers list.
- Add: Adds new IP addresses to the Excluded Computers list.
- Remove: Removes the selected computer from the Excluded Computers list.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

About the Privacy Control window

In the Privacy Control window you can view, modify, and enable Internet privacy settings.

Use the Privacy Level slider to set one of the following Privacy Levels:

- High: Blocks all confidential information from being sent to nonsecured (HTTP) Web sites. You are prompted each time a cookie is sent to a Web site. Browser privacy is 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 you each time confidential information is sent from the computer to a nonsecured (HTTP) Web site (restricted accounts are prevented from sending confidential information). Cookies are sent to Web sites without requiring permission from you. 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 address of the last Web site 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.

Other controls in this window include:

- Confidential Info: Protects credit card information and other sensitive data from being sent out over the Web
- Custom Level: Controls specific Privacy settings
- Default Level: Reverts the Security settings to the original settings

---

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Customize Privacy Settings

This dialog box lets you create a customized level of privacy.

- Confidential Information: Specifies how confidential information is handled when you enter it on a Web page or in a supported instant messaging program.

  High: Blocks all outgoing confidential information to unsecure Web sites.

  Medium: Alerts you each time you attempt to send confidential information to an unsecure Web site.

  None: Allows all outgoing confidential information.
- Cookie Blocking: Specifies how cookies are handled when a Web site requests them.

  High: Blocks all cookies.

  Medium: Prompts you each time a Web site requests a cookie.

  None: Allows all cookies.
- Enable Browser Privacy: Prevents a Web site from retrieving your email address or the address of the last Web site visited.
- Enable Secure Connections (HTTPS): Lets you access Web sites using HTTPS, a secure protocol that is often required for credit card purchases. If this option is active, confidential information will not be blocked.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Confidential Information

The Confidential Information feature lets you block specific information from going out to Web sites and supported instant messaging programs. 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.

The program blocks confidential data sent to Web sites by means of HTTP only. 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 ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Add or Modify Confidential Information

Use this dialog box to place confidential information in the database for protection.

The confidential data is located in a single database. Any confidential information you enter can be seen and accessed by accounts with adult or supervisor rights.

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

Entering partial information has two advantages. First, you are not entering your complete credit card number where someone might find it. Second, it lets the program block your private information on sites that use multiple boxes for credit card numbers.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Confidential Information Length

You have specified confidential information of less than 5 characters. Specifying a short sequence of characters may cause frequent false alerts if the sequence happens to match normal Internet communication, such as part of a web site’s URL.

To prevent this notice from displaying when you enter a short sequence of confidential information, select Do not show this dialog again.

Click OK to close the dialog box. To make the confidential information less likely to cause false alerts, enter a longer string of characters in the Modify Confidential Information dialog box, Information to protect field.

About the Ad Blocking window

Many sites use banner ads on their Web pages that often include animated graphics to get visitors' attention. If you find banner ads to be distracting, you can block them. You can also use Ad Blocking to block specific ads that are featured on a Web page.

Turning on Enable Ad Blocking can reduce the amount of time it takes to display a Web page, especially with dial-up connections.

The Trashcan icon enables you create a customized list of ads to block. You can drag, or cut and paste, the graphic from the web site into the ad trashcan dialog box to add its URL to the list.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

About the Parental Control window

In the Parental Control window, you can create a safer, more child-friendly Internet environment for your family members.

If a selected account is not currently logged on, the account name appears in red and the settings do not go into effect until the account logs on to Norton Internet Security.

By default, children's accounts do not block any Internet applications but they do restrict access to certain categories of Web sites.

The controls in this window include:

- Sites: Blocks objectionable Web sites by restricting the types of Web sites you can access. The basis of the Norton Internet Security Web filtering feature is an extensive categorized list of Web sites that is created and maintained by Symantec. Using this list as a starting point, you can customize Web access settings for each individual in your household.
- Applications: Blocks access to specific Internet-based applications. You can configure children's accounts to let them browse the Web, but prevent them from accessing the Internet with several categories of applications.

  The Personal Firewall must be set to High to restrict the use of selected Internet-based programs.
- Defaults: Reverts the Parental Control settings to the original settings.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Specify Sites

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:

- Specify permitted sites: Blocks all sites except those that you specify as acceptable. Use this option to let family members visit handpicked sites only.

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

  When you specify a list of permitted Web sites, content from all other Web sites is blocked. If a site references graphics or other elements from other sites, these items are blocked even though they appear to be from the same Web site.

- Specify blocked sites: Lets children visit any Web site except for those that you block. The basis of this feature is an extensive categorized list of Web sites that is created and maintained by Symantec. Children can visit the majority of sites on the Web except for those that fall into certain categories.

  You can block a site that is not in the category list by adding it to the Additional Sites to Block list.

  To block applications that appear outside your browser, close this dialog box and click Applications.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Exceptions

This list of Web sites overrides the categorized list of Web sites that is maintained by Symantec and permits them to be viewed.

If there are sites on the categorized list of Web sites that you want to permit your children to view, add them to this list.

If you add a domain to the list, all Web sites within the domain are excepted. For example, if you add the domain msn.com, it allows your children to view all the Web sites at that domain, such as www.msn.com and messenger.msn.com. If you add messenger.msn.com, it only allows your children to view the messenger.msn.com Web site.

The controls in this window include:

- Add: Adds new Web sites to the Exceptions list.
- Remove: Removes the selected Web site from the Exceptions list.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} 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 that you select.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Applications

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 the types of Internet programs—if any—that you want your children to use.

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

Norton Internet Security doesn't prevent restricted programs from running. It prevents them from communicating over the Internet.

To block applications that appear in your browser, such as some chat rooms, close this dialog box and click Sites.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Notice

Security and the Personal Firewall must be enabled to protect you from Internet risks.

The following features are disabled when the Personal Firewall is disabled:

- Parental Control cannot restrict applications.
- Privacy Control cannot block secure connections.

Enable Security in the Personal Firewall Settings window. If you have selected custom security settings, the Personal Firewall must be set to Medium or High.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

About the Accounts window

In the Accounts window you can manage the accounts for your family. Options available in the Accounts window vary depending upon whether you are using your Windows operating system account(s), or accounts created specifically for Norton Internet Security.

Accounts with supervisor rights can create Norton Internet Security accounts. Accounts are created using options in the Accounts window; Internet rights and privileges are set in the Security, Privacy, and Parental Control windows.

The controls in this window include:

- Parental Control Wizard: Clicking this link displays the Account Manager, where you can set the option to use your Windows account(s) or use accounts you create specifically for Norton Internet Security. You can also set account types (Child, Teenager, Adult, or Supervisor) in the Account Manager.
- Log On: Logs you on to an account. The Internet rights and privileges of that account are active. This option is not available if you are logged on under a Windows account.
- Log Off: Logs off the current account so you can change accounts. When the current account 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. This option is not available if you are logged on under a Windows account.
- Change Password: Changes the logged on account's password. This option is not available if you are logged on under a Windows account.

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

- Create Account: Creates new Norton Internet Security accounts for family members. This option is not available if you are logged on under a Windows account.
- Delete Account: Removes the selected Norton Internet Security account. This option is not available if you are logged on under a Windows account.
- Properties: Changes the account settings for the selected account.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Create Accounts

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

The controls in this window include:

- Account Name: The name by which you want to identify the account.
- Password/Confirm Password: The password for the account. Passwords are case sensitive. You do not have to use a password.
- Base Account On: The 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 account's settings in the Security, Privacy, Parental Control, and Ad Blocking windows.
- Make this the startup account: Norton Internet Security starts with this account logged on.

Click here {button ,AL("About the Accounts window",0,`',`')} for more information

Account Properties

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

- Password/Confirm Password: The password for the account. Passwords are case sensitive. You do not have to use a password.
- Account Type: Type of account—adult, teenager, child, or Supervisor.
- Make this the startup account: Norton Internet Security starts with this account logged on.

Click here {button ,AL("About the Accounts window",0,`',`')} for more information

General Options

Use these options to control general configuration settings.

- Show Taskbar Icon: Places the program icon in the system tray. You can right-click the icon to log on and off, exit the program, or perform other tasks.
- Show the Alert Tracker: Displays the half-globe Alert Tracker icon at the side of your screen. You can double-click the Alert Tracker to see recent messages.
- Startup: Select from two startup options:
- Manual: The program does not start automatically.
- Run at System Startup: The program starts when you start your Computer.
- View Event Log: Shows a log containing information on content blocking, connections, firewall activity, and other events.
- View Statistics: Shows realtime, detailed statistics that indicate how the program is protecting your system.
- Clear Statistics: Resets the realtime statistics shown in the Status window and the Statistics window. Log-based statistics are cleared when you clear the associated Event Log.
- Advanced Options: Changes advanced settings for the Personal Firewall and other features such as Privacy and Active Content.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Tray Menu Options

Use these options to control the options available in the menu that appears when you right-click the program icon in the notification area of the Windows taskbar. The tray menu gives you direct access to Norton Internet Security features you use often.

The following menu items can appear on the menu:

- Options: Displays the Norton Internet Security Options dialog box for access to general settings, statistics, the event log, and tray menu settings.
- Advanced Options: Displays the Norton Internet Security Advanced Options dialog box for changing security settings for individual web sites, as well as other miscellaneous settings.
- View Event Log: Displays the log containing information on content blocking, connections, firewall activity, and other events.
- View Statistics: Displays realtime, detailed statistics that indicate how the program is protecting your system.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Cookie Alert

Cookies are small files that are stored on your computer that Web sites use to track your visits.

Cookie alerts appear when you encounter a cookie and you have the Privacy Level set to High or Cookie Blocking set to Medium: Prompt me each time.

Read the alert and then select one of the available options:

- Permit this cookie. Allows the return of cookie information to the Web site. Cookies from the Web site that you are visiting are usually harmless, and may be necessary for proper operation of the Web pages.
- Block this cookie. Blocks the return of cookie information to the Web site. Expect repeated cookie alerts from pages on which you block cookies. Cookies that are from Web sites other than the one you are visiting are commonly used to track your Internet usage, and can usually be blocked without affecting the functioning of the Web site that you are visiting.

Because cookies are used so often and present a small risk, you should not block cookies from the site you are visiting.

If you want to block all cookies and not see cookie alerts, set Cookie Blocking to High: Block Cookies.

You can set cookie handling for specific Web sites in Advanced Options.

Java/ActiveX Alert

Java applets and ActiveX controls are Web page components that do more than display text or graphics. Common applications are pop-up menus and up-to-date stock quotes. However, these components can potentially be used for malicious purposes as well.

ActiveX and Java Alerts appear when a Java applet or ActiveX control is encountered and you have the Security Level set to High, or have Java Applet Security or ActiveX Control Security set to Medium: Prompt me each time.

Read the alert and then select one of the available options:

- Permit this ActiveX control (or Java applet). Permits this ActiveX control or Java applet to run. Unless the Threat level is high, select this option on sites you trust, since these elements are required for many Web pages to function correctly.
- Block this ActiveX control (or Java applet). Prevents this ActiveX control or Java applet from running. While this is always the safer option, it might prevent the Web page from functioning correctly.

If you select block, and the Web page does not function correctly, click your browser's Refresh button and choose Permit.

You can set Java applet and ActiveX control handling for specific Web sites in Advanced Options.

Security Alert

Security Alerts appear when someone attempts to access your computer. It may be a hacker or someone on your own network.

Read the alert and evaluate the risk. You can get more information about this kind of attack. Most Security alerts trigger AutoBlock, preventing the computer from communicating with your computer for 30 minutes.

Ensure that the alert describes a real attack and not a legitimate attempt to access your computer. If the attempt is legitimate, add the computer that is attempting to connect to you to the Trusted zone or use Internet Access Control to allow the type of connection described in the alert.

Don’t assume that every security alert represents an attempt to hack your computer. There are many more-or-less harmless events on the Internet that cause security alerts. Answering the following questions may be helpful in determining if a Security alert represents an attack or more-or-less normal Internet activity.

- Is the connection attempt from an unknown computer?
- Does the Security alert describe a clearly threatening behavior? Accessing a single closed port is not as threatening as a complete port scan.
- Is the attempt part of a pattern of threatening attempts from the same computer?

If you answer yes to all of these questions, you may be under attack. If you answer no to one or more of these questions, you are probably not under attack. However, you might be seeing a hacker’s scan of a number of computers looking for vulnerabilities. With Security enabled, your computer does not appear vulnerable to the hacker. In fact, your computer may not appear to exist to the hacker.

Confidential Information Alert

Confidential Information alerts appear when you attempt to send protected information to a Web site or via a supported instant messaging program that does not use secure, encrypted communications.

The alert contains the information that you are attempting to send, and the Web site to which it is being sent. Details provides the specific entry that triggered the Confidential Information alert.

Read the alert and then select one of the available options:

- Permit this confidential information to be sent. Sends the information.
- Block this confidential information from being sent. Blocks the information from being sent.

Note: This alert can be triggered by non-confidential information transmitted to or from your computer that happens to match your confidential information. Some web sites may transmit numbers or text as part of their normal operation, which may happen to match your confidential information. For example, a web site has the numbers "1234" as part of its URL, which happens to match the "1234" you have entered as your confidential "Credit Card" information. This alert does not necessarily mean that the web site is trying to obtain your credit card information. Similarly, an alert can be triggered if you have designated "Washington" as part of your confidential address and you enter "Washington" in a web search engine. In such cases, you can permit the confidential information to be sent.

Internet Access Control Alert

Internet Access Control alerts appear when you need to make a decision about a program on your computer that is attempting to access the Internet.

Norton Internet Security helps you assess the potential threat posed by the program by displaying a threat level: no risk, low risk, medium risk, or high risk. The threat level is based on characteristics of the program, such as the location of the program on your computer, whether it contains a virus or other malicious threat, whether the program is from a known company, and other criteria. Click the Details link to view information about the program.

Read the alert information and then select one of the available options:

- Automatically configure Internet access. The application is recognized and there are appropriate access rules in the database. This is usually the best option.
- Permit this application to access the Internet. Provides the application with full access to the Internet. This is not as safe as choosing Automatic, but it is appropriate for many applications that are not recognized. If you recognize the application and trust it to be safe, then this is the appropriate choice.
- Block this application from accessing the Internet. Blocks all Internet access for the application. This is the appropriate choice if you don’t recognize the application and the risk is high.
- Customize Internet access for this application. Lets you create specific rules for the application’s Internet access. Select this option if you understand how the application accesses the Internet and you want to create specific rules to control its access. Selecting this option starts the Add Rule wizard.

You can minimize the number of Internet Access Control alerts you see by enabling Automatic Internet Access Control. When this option is enabled, Norton Internet Security automatically creates a new firewall rule for applications that it has digital signatures (fingerprints) for the first time the applications are run.

Choose Application Category

Choose a category for the application. These categories appear in the Parental Control Settings > Applications dialog box, where you can select the categories of applications your children are permitted to use online. You can change an application’s category at any time from the Internet Access Control window by clicking the Category entry.

Automatic Internet Access Control

When Automatic Internet Access Control is enabled, Norton Internet Security creates a new firewall rule for applications that it has digital signatures (fingerprints) for the first time the applications are run. Disable this option if you want to be notified when a new application attempts to access the Internet. Be sure to run LiveUpdate weekly to keep your Internet and virus protection current. New rules will be created only for applications that have been identified as posing little risk to your computer.

If you want specific control over individual applications, use Application Scan instead of Automatic Internet Access Control.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Change Password

Changes the password of the currently logged in account. This option is not available if you are logged in under a Windows account.

- Old Password: The current password for the account. Not necessary for supervisor accounts.
- New Password: The new password.
- Confirm Password: The new password again, for confirmation.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Log on

Accounts are granted specific Internet access rights and other privileges. Before these rights and privileges go into effect, the account must log on.

To automatically log on the account each time the program starts, make the account the Startup Account.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Action

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

- Permit Internet Access: Lets communication of this type take place.
- Block Internet Access: Prevents communication of this type from taking place.
- Monitor Internet Access: 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.

Monitor Internet Access lets you log communication activity. For example, suppose you have a Permit firewall rule that lets your FTP server communicate with any network address. You could track how often users at a particular network address connect to your FTP server by setting up a monitor rule to log instances of FTP server communication to and from that network address. The FTP server monitor rule must precede the FTP server permit rule.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Connections

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

- Connections to other computers: The rule applies to outbound connections from your computer to other computers.
- Connections from other computers: The rule applies to inbound connections from other computers to your computer.
- Connections to and from other computers: The rule applies to inbound connections as well as outbound connections.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Computers

Specifies the computers and network adapters to which this rule applies.

The computers you specify are other computers with which you want to control communications with your computer.

- Any computer: The rule applies to all computers.
- Only computers specified below: The rule applies to all computers, sites and domains listed. Add adds computers to the list.

Adapters

Applies the rule to a specific network adapter in your computer.

This is useful if your computer has more than one IP address. If, for example, your computer has a connection to a local network as well as a connection to the Internet, then it probably has two IP addresses.

This setting lets you apply rules to one of your computer's IP addresses. For example, if your computer is connected to a home network and also connects to the Internet, you might want to set up a rule that permits file sharing on the home network, and another rule that blocks file sharing across the Internet.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Communications

Defines the methods of communication to which this rule applies.

Protocols

Specifies the communications protocols that this rule controls.

- TCP: The rule applies to TCP (Transport Control Protocol) communications.
- UDP: The rule applies to UDP (User Datagram Protocol) communications.
- TCP and UDP: The rule applies to both TCP and UDP communications.
- ICMP: The rule applies to ICMP (Internet Control Message Protocol) communications. This option is only available for system-wide rules

Ports

Specifies the types of communications, or ports, that are controlled by this rule.

- All types of communications (all ports): The rule applies to communications using any port.
- Only the types of communications or ports listed below: The rule applies to the ports listed. You can add ports to or remove ports from the list.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Tracking

Specifies whether the program should notify you or create an event log entry when a network communication event matches the criteria set for this rule.

- Create an event log entry: An entry is created in the Firewall event log when a network communication event matches this rule.
- Notify me with an Alert Tracker message: An Alert Tracker message appears when a network communication event matches this rule. You can review recent Alert Tracker messages by double-clicking the Alert Tracker half globe.
- Create Security Alert: Depending on the level of reporting chosen, a Security Alert dialog box appears when a network communication event matches this rule.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Description

The description that you enter appears in the Application Rule Summary dialog box so that you can distinguish this rule from other rules. Since some applications require multiple rules, you should enter a specific description. This description may show up in the log and alert tracker.

Category

Identifies the type of application. Parental Control uses these categories to determine which applications and types of communication your children can use online.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Rule Summary

Shows the rules for the category in which you are working. Rules are in one of the following categories:

- System-wide settings: There is one list of system-wide rules.
- Application scan: Each application has its own list of rules.
- Trojan horse settings: These rules are supplied by Symantec and kept current by LiveUpdate. You should not change these rules without specific knowledge of the effect that your changes will have on your protection.

To temporarily disable a rule, without removing it from the list, uncheck the checkbox for that rule.

Other controls in this window include:

- Add: Adds a new rule to the list.
- Modify: Changes the selected rule.
- Remove: Deletes the selected rule.
- Move Up: Moves the selected rule up in the list. Rules are executed in the order in which they appear in the list. Those higher in the list are executed first.
- Move Down: Moves the selected rule down in the list. Rules are executed in the order in which they appear in the list. Those higher in the list are executed first.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Network Adapters

If you have multiple adapters on your computer, you can specify the network adapters to which this rule applies.

The network adapters that you specify are on your computer.

The options are:

- Any adapter: The rule applies to all network adapters.
- Only adapters specified below: The rule applies to the network adapters listed. Add adds adapters to the list.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Specify Computers

The Specify Computers dialog box lets you specify computers in three ways: individual computers, a range of computers, and all computers on a subnet. In each of these three you can use IP addresses to identify computers.

Individually

Specify the name or IP address of a single computer.

IP addresses are 32-bit numbers expressed as four decimal numbers, each ranging from 0 to 255, and separated by periods. For example: 206.204.52.71.

The computer name you enter can be a URL (Uniform Resource Locator) such as service.symantec.com, or a Microsoft Network computer name, such as Mojave. You can find the names of computers on your local network in Network Neighborhood or Network Places.

Using A Range

Specify the starting (lowest numerically) IP address and the Ending (highest numerically) IP address. All the computers within that range of IP addresses are included.

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

Using A Network Address

Specify an IP address and a subnet mask. This specifies all the IP addresses on that subnet.

The IP address you enter can be any one in the subnet you are identifying. The appropriate subnet mask is almost always 255.255.255.0.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Specify ICMP Commands

Filter by: Specifies the methods of communication, or ports, to which this rule applies.

- Known ports from list: The rule applies to the selected ports in the list. Check each port to which you want this rule to apply.
- Individually specified ports: The rule applies to the ports that you enter. You can enter multiple port numbers separated by spaces.
- Port range: The rule applies to a series of ports. Enter the starting (lowest) port number and the ending (highest) port number.

Locality: This rule can be applied to local and remote ports. Local ports are those on your computer that are usually used for inbound connections. Remote ports are on the computer with which your computer is communicating. They are usually used for outbound connections.

The Command list specifies the ICMP commands to which you want to apply this rule.

Check each command to which the rule should apply.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Specify Ports

Specifies the methods of communication, or ports, to which this rule applies:

- Known ports from list: The rule applies to the selected ports in the list. Check each port to which you want this rule to apply.
- Individually specified ports: The rule applies to the ports that you enter. You can enter multiple port numbers separated by spaces.
- Port range: The rule applies to a series of ports. Enter the starting (lowest) port number and the ending (highest) port number.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

There are important reasons why you should renew your subscription

Keeping your Symantec software updated to protect your computer against the latest Internet threats is always quick and easy. This product uses Symantec’s LiveUpdate technology to check for updates online and download them to your computer. Symantec’s Internet security experts update Personal Firewall continuously to protect against the latest Internet threats. This product includes a complimentary Internet security subscription service. After your complimentary subscription expires, you can renew your subscription annually to ensure you have the most up-to-date protection for your computer.

What is the virus definition service?

Virus definitions are essential in keeping your computer protected from the latest viruses. The virus definition service allows Norton AntiVirus to detect new viruses and remove them from your computer before they cause damage or spread out and infect other computers. Your Norton Internet Security subscription service includes the virus definition service.

What is the firewall rule service?

Firewall rules are necessary to defend your computer against the latest security intrusions and privacy threats. They are a set of instructions that Norton Personal Firewall uses to inspect the nature of data travelling between your computer and the Internet and determine if it should be blocked or permitted.

What is the Web filtering service?

The Web filtering service updates the categorized list of Web sites that Norton Internet Security uses to block access to inappropriate Web sites and keep your children safe on the Internet.

For more information visit www.symantec.com/avcenter

Internet Access Control

Choose one of the available options for the application shown.

- Automatically configure Internet access: The application is recognized if it digitally matches an entry in Symantec's database and there are appropriate access rules in the database. This is usually the best option.
- Permit this application to access the Internet: Provides the application with full access to the Internet. This is not as safe as choosing Automatic, but it is appropriate for many applications that are not recognized. If you recognize the application and trust it to be safe, select this option.
- Block this application from accessing the Internet: Blocks all Internet access for the application. Select this option if you don't recognize the application and the risk is high.
- Customize Internet access for this application: Lets you create specific rules for the application's Internet access. Select this option if you understand how the application accesses the Internet and you want to create specific rules to control its access. Selecting this option starts the Add Rule wizard.

You can minimize the number of Internet Access Control alerts you see by enabling Automatic Internet Access Control. Automatic Internet Access Control creates a new firewall rule for applications that it has digital signatures (fingerprints) for the first time the applications are run.

This option is enabled by default when you install.

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Security Alert

Security Alerts appear when someone attempts to access your computer. It may be a hacker or someone on your own network.

Read the alert and evaluate the risk. You can get more information about this kind of attack. Most Security alerts trigger AutoBlock, preventing the computer from communicating with your computer for 30 minutes.

Ensure that the alert describes a real attack and not a legitimate attempt to access your computer. If the attempt is legitimate, add the computer that is attempting to connect to you to the Trusted zone or use Internet Access Control to allow the type of connection described in the alert.

Don’t assume that every security alert represents an attempt to hack your computer. There are many more-or-less harmless events on the Internet that cause security alerts.

This alert is warning you about a possible remote access Trojan horse program. A Trojan horse program masquerades as a legitimate program and damages or compromises the security of your computer.

Some Trojan horse programs perform malicious actions on the computer on which they are run, while others, such as Back Orifice, provide remote-control capabilities for hackers.

For more information, visit www.symantec.com/avcenter

About the Statistics window

The Statistics window shows you the realtime state of the system. It shows several sets of counters indicating Web- and firewall-related activity for the current session.

The View menu has the following commands:

- Always on Top: Keeps the Statistics window in view while you work in other applications. A check next to this option indicates that it is active.
- Columns: Specify the number of columns in the statistics window. You can select a one-column display, a two-column display, or let the program determine the number of columns automatically based on the size of the Statistics window.
- Reset Values: Resets the statistics to zero. All statistics, except those associated with Network Connections and Estimated Single Graphic Size, are reset.
- Options: Specifies which statistics are displayed.

For more information on the available statistics:

Network

Web

Web Graphics/Banner Ads Blocked

Firewall TCP Connections

Firewall UDP Datagrams

Firewall Rules

Network Connections

Last 60 Seconds

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Network

The Network group shows the following realtime network statistics since the program started.

- TCP Bytes Sent: The number of TCP bytes sent over network connections since the program started.
- TCP Bytes Received: The number of TCP bytes received over network connections since the program started.
- UDP Bytes Sent: The number of UDP bytes sent over network connections since the program started.
- UDP Bytes Received: The number of UDP bytes received over network connections since the program started.
- All Bytes Sent: The number of NDIS bytes sent over network connections since the program started.
- All Bytes Received: The number of NDIS bytes received over network connections since the program started.
- Open Connections: The current number of network connections. In addition, a red line indicates the highest number of simultaneous open network connections since the program started. The number at the far right shows the scale used for this graphic indicator.

{button ,CW(`SUB')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Web

The Web group shows the following realtime statistics indicating Web-related activity for the current session.

- Graphics Blocked: Number of graphics blocked by the program.
- Cookies Blocked: Number of outbound cookies blocked by the program’s HTTP Privacy filter.
- Refer Req Blocked: Number of refer requests rejected by the program's HTTP privacy filter. This behavior is configured using the Referer setting.
- Bytes Processed: Number of bytes processed by the program’s HTTP filters.
- Packets Processed: Number of packets processed by the program’s HTTP filters.
- KB/Second Processed: Number of kilobytes processed per second by the program’s HTTP filters. In addition, a red line indicates the highest number of kilobytes per second processed since the program 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 the program started. The number at the far right shows the scale used for this graphic indicator.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Web Graphics / Banner Ads Blocked

The Web Graphics / Banner Ads Blocked group shows the following statistics about the Web graphics and banner ads 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.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Firewall TCP Connections

The Firewall TCP Connections group shows the following realtime statistics indicating firewall-related TCP activity. To configure this behavior, use the Internet Access Control window to define firewall rules.

- 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).

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Firewall UDP Datagrams

The Firewall UDP Datagrams group shows the following realtime statistics indicating firewall-related UDP activity for the current session. To configure this behavior, use the Internet Access Control window to define firewall rules.

- Inbound Permitted: Shows the number of inbound datagrams that were permitted.
- Inbound Blocked: Shows the number of inbound datagrams that were blocked.
- Outbound Permitted: Shows the number of outbound datagrams that were permitted.
- Outbound Blocked: Shows the number of outbound datagrams that were blocked.
- Total Permitted: Shows the sum of all permitted datagrams (both inbound and outbound).
- Total Blocked: Shows the sum of all blocked datagrams (both inbound and outbound).

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Firewall Rules

The Firewall Rules group shows the following realtime statistics indicating firewall-related activity for the current session.

The Firewall Rule group lists all of the rules defined for your firewall. Three statistics are maintained for each rule: Permitted, Blocked, and No Match. A running total for all rules indicates how many communication attempts were permitted, how many were blocked, and how many were not matched.

Each time that network communication occurs, the statistics 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 to the bottom. If the communication is permitted by a rule, the Permitted statistic increases. If the communication is blocked by a rule, the Blocked statistic increases. If the communication does not match a rule, then information about the connection is passed on to the next rule and the No Match statistic increases.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Network Connections

The Network Connection group shows the following realtime statistics indicating network connection information for the current session.

You can terminate a connection from this group. To terminate a connection, right-click the connection you want to terminate and then click Terminate Connection.

The information shown includes:

- 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.

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} for more information

Last 60 Seconds

The Last 60 Seconds group shows a graphic representation of network activity for the last 60 seconds.

To see the last 60 seconds statistics: On the View menu, click **Options** and check the **Last 60 Seconds** check box.

Four statistics are represented in a line graph on a second-by-second basis. This lets you note the speeds 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

{button ,CW(`')} Back

Click here {button ,EF(`hh.exe',`ms-its:NIS.chm',5,`')} 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 Java applets and ActiveX controls are not blocked.

Click to set up customized Security settings for the account.

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

Click to set up customized Privacy settings for the account.

Click to enable or disable Privacy protection for the account.

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

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

Click to specify any confidential data that you do not want to send over the Web (HTTP).

Click to enable or disable all of the Parental Control features.

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 that 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.

Your computer does not currently have Windows Multi-user Settings enabled. Multi-user Settings enable you to set up multiple user accounts, so that more than one person can use your computer.

To enable Windows Multi-user Settings, click the Windows Start menu, point to Settings, and then click Control Panel. Double-click the Users icon to display the Wizard that helps you create a new user account.

Click to enable or disable all of the Ad Blocking protection features.

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

Check to show the program icon in the notification area on the Windows taskbar (by default, in the bottom-right corner of the screen). You can click the icon to open a menu.

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

If you are using a networked computer 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 computer.

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

If you want to control when the program runs on your computer, click Manual. You must start the program to use it.

Click to add a new HTML string to the selected ad blocking list.

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 Ad Blocking to prevent ads and images from appearing on Web pages.

When ad blocking is enabled and you connect to a Web site, the program 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). The program looks for matching strings within the HTML tags that are used to present graphics and advertising. The program removes any matching strings before the page appears in the Web browser.

Click to change an HTML string in the ad blocking list that is currently active.

Click to remove an HTML string from the ad blocking list that is currently active.

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 a site, you can select it in the site list and then use settings on the 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 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 a hierarchical site list showing each of the domains and sites for which Web settings have been defined.

When you select a site in the list, the tabs update to show the settings defined for that site. Use options on these tabs to maintain site-specific settings for the currently selected site.

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 Ad Blocking is not turned on. To enable it, in the Ad Blocking window, check Enable Ad Blocking.

(Defaults) block list also applies: When you visit a Web site, the program uses two ad blocking lists: the (Defaults) list and the site-specific list. The program provides a predefined (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.

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

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 selected site.

Block: Prevents your browser from returning cookies.

Permit: Permits your browser to return cookies.

Reply: Returns the string specified in the Cookie box instead of the cookie.

When Use These Rules For <site> is unchecked, the cookies settings are unavailable.

If you choose to handle cookie requests with a Reply, type the string that you want to use for the reply. This string is sent instead of a cookie each time the site makes a cookie request.

This cookie reply box is available only when you select Reply in the Cookies list box.

The program 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 the program to control the information passed in the following HTTP header fields: Referer, Browser (User-agent), and E-mail (From).

These settings specify whether third-party Web sites are provided with the address of the Web site from which you came.

Block: Prevents your browser from identifying the site you were visiting.

Permit: Permits your browser to identify the site you were visiting.

Reply: Returns the string specified in the Referer box instead of the identity of the site from which you came.

When Use These Rules For <site> is unchecked, the Referer settings are not available.

If you choose to replace the Referer field information with a reply, type the string that you want to use for the reply. This string is sent as the content of the Referer field each time the site requests data from a server.

The Referer reply box is only available when you select Reply in the Referer list box.

When checked, a notification icon appears 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, check Write An Event Log Entry When This Rule Is Matched.

If you choose to replace Browser (User-agent) field information with a reply, type the string that you want to use for the reply. This string is sent as the content of the User-agent field each time the site requests data from a server.

The Browser (User-agent) Reply box is only available when you select Reply in the Browser (User-agent) 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: Prevents your browser from providing the email address that is used to identify you as the sender of mail.

Permit: Permits your browser to provide the email address that is used to identify you as the sender of mail.

Reply: 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.

When Use These Rules For <site> is unchecked, the E-mail (From) settings are not available.

If you choose to replace E-mail (From) information with a Reply, type the string that you want to use for the reply. This string is sent as the content of the From field each time the site requests data from a server.

The E-mail (From) Reply box is only available when you select Reply in the E-mail (From) list box.

Indicates how Privacy rules are determined for the currently selected site.

These tabs control site-specific settings. Select a site in the site list, then use the controls on these tabs to make site-specific settings.

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 pop-up 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), in the Personal Firewall Settings window, use Custom Level to change the Java applet and ActiveX control security settings.

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

Shows the HTTP ports monitored by the program. The default list contains the standard HTTP ports. You can add ports if you use applications that perform HTTP communication through nonstandard ports.

Add a new HTTP port to the list.

Remove the selected HTTP port from the list.

Blocks all forms of IGMP (Internet Group Management Protocol) communications, a protocol sometimes exploited by attackers to stop a victim’s computer from responding.

Stops blocked ports from responding to inquiries from the Internet.

Blocks 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 the program automatically create firewall rules for you when an attempt to connect to the network occurs 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 using the Add Rule wizard.

The current settings for this account are shown in the Personal Firewall, Privacy, and Parental Control windows. If the account is not logged on, the name appears in red; if the account is logged on, the name is shown in blue.

If you are logged on to the program and have supervisor rights, you can select any account from the list and then make changes to the account's Personal Firewall, Privacy, and Parental Control settings. Any changes that you make are automatically saved but don't go into effect until the user logs on.

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

Click to log on or log off of the program.

Click to change the password of the logged-on account.

The list shows the names and types of accounts:

- A Supervisor account can change the settings of any account.
- An Adult account can change only its own accounts.
- A Teenager or Child account cannot make changes to any accounts.
- The Not Logged In account is a built-in account that prevents network access. This account becomes active when a user logs off.
- The Startup account is automatically logged on each time the program starts up. Any account can be identified as the startup account.

Click to create a new account.

Click to remove the selected account.

Click to change the basic properties of the selected account.

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

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

Select any categories in the list to block. If a category in the list is unchecked, the account can visit sites in that category.

Click to add any exceptions to the category list.

Sites in this list are blocked in addition to Web sites in checked categories. To add sites to this list, click Add.

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

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

Specifies how confidential information is treated when an account attempts to enter it on a Web site.

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

Check to prevent Web sites from obtaining your email address and the address of the last site that you visited.

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

Check the categories of Internet-based applications to which you want your child to have access.

Description, type, and content of the confidential information blocked by the program.

Click to add information to block from going out to nonsecured Web sites (HTTP).

Click to remove the confidential information entry in the list.

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

The Personal Firewall has these settings:

- **None**: Disables the firewall and allows all Internet communications.
- **Medium**: Blocks many ports used by harmful applications. However, it can also block useful applications when they use the same ports.
- **High**: Blocks all communications that you do not specifically allow. You must create firewall rules for every application that requests Internet access. If you have done an Application Scan, you should not be interrupted frequently.

Using the following settings, you can control how Java applets run on your computer:

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

Using the following settings, you can control how ActiveX controls run on your computer:

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

Check to give the user 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 permit 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 this option, applications that are not covered by firewall rules are blocked from accessing the network.

Check to see alert messages when an inbound connection attempt is made to a port with no corresponding listening service. These alerts are useful for solving problems when you are configuring advanced programs and features such as Internet Connection Sharing. Disable to avoid alerts about harmless connection attempts.

Click to suspend or resume the Security protection features.

Drag the slider to change the Reporting Level. Higher settings report more security events.

Click if you have customized the account’s Reporting Level settings and want to revert back to the original default setting.

Click to adjust system-wide firewall settings, including Trojan protection, to do an Application Scan, or to enable automatic Internet Access Control.

Click to add an application and configure its Internet access. When added, the application appears in the list above.

Click to change the selected application in the list above.

Click to remove the selected application from the list above.

Lists applications already configured for Internet access control.

Click to add a computer or site to which to permit access.

Click to remove the selected computer or site from the list above.

Lists computers or sites already controlled.

Click to add an application behavior.

Click to change an application behavior selected from the list above.

Click to remove the selected application behavior from the list above.

Click to move the selected application behavior up in the list.

Click to move the selected application behavior down in the list.

Enables or disables any of the options selected below.

Sets 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**: Lets animated GIF files run on your computer.
- **Block animations repeating**: Blocks animated GIF files from running on your computer. Only the first frame of the GIF appears.

Set the ActiveX blocking options for individual sites or for (Defaults):

- **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 computer.
- **Allow ActiveX controls to execute**: Lets ActiveX controls run on your computer.

To change the Binary Executable settings for (Defaults), in the Personal Firewall Settings window, use Custom Level to change the Java applet and ActiveX control security settings.

Set the Java applet options for individual sites or for (Defaults):

- **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 computer.
- **Allow Java applets to execute**: Lets Java applets run on your computer.

To change the Binary Executable settings for (Defaults), in the Personal Firewall Settings window, use Custom Level to change the Java applet and ActiveX control security settings.

Type the HTML string that you want to add to the block list. Choose whether to permit or block HTML image statements that contain this string.

How you define HTML strings in the ad blocking list affects how restrictive or unrestrictive the firewall will be in its filtering of HTML data. More specific HTML strings will filter data more precisely.

Specifies that the HTML string is 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 appears in the Web browser.

Specifies that the HTML string is used to permit 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 a page in that site.

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 of the Web servers within the domain.

Adding a site entry lets you configure privacy and active content Web settings for a single Web server.

These settings specify whether a site is provided with information about the type of browser and operating system that you are using when you request data from their server. Normally, this information is passed in the User-agent field as part of the data request:

Block: Blocks the identity of the browser and operating system you are using when it is requested by a server.

Permit: Lets your browser identify the type of browser and operating system that you are using when it requests data from a server.

Reply: Returns the string specified in the Browser (User-agent) box instead of the identity of the browser and operating system you are using.

If Use These Rules For <site> is not checked, the Browser (User-agent) settings are not available.

The address of the Web site.

The name of the account you want to create.

The password for the account.

The password for the account repeated for verification.

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

Check to have the account log on automatically each time that the program starts.

Check to have the account log on automatically each time that the program starts.

The name of the account.

The type of account:

- Administrators can change the settings of any account.
- Adult accounts can change only their own account settings.
- Teenager or Child accounts cannot change the settings of any account.

The current password.

The new password for the account.

The new password for the account repeated for verification.

The type of information that you want to block from being sent over the Web (HTTP).

The name for the information that you want to block.

The exact sequence of characters, including spaces, that you want to block.

Sites in this list are not blocked, even if they are in the blocked category list provided by Symantec.

Click to add a site to the exceptions list. Sites in this list are not blocked, even if they are in a blocked category list provided by Symantec.

Click to remove the selected site from the exceptions list.

The account is allowed to visit only the sites that appear in this list—access to all other sites is blocked.

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

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

Select the account from the drop-down list.

The password for the account.

Adds the Options command to the menu that appears when you right-click the program icon in the notification area on the Windows taskbar.

Adds the Display Advanced Options command to the menu that appears when you right-click the program icon in the notification area on the Windows taskbar.

Adds the Display View Event Log command to the menu that appears when you right-click the program icon in the notification area on the Windows taskbar.

Adds the View Statistics command to the menu that appears when you right-click the program icon in the notification area on the Windows taskbar.

Displays the Alert Tracker half-globe at the side of your screen.