

McAfee®

# personal firewall plus

## User Guide

---



## COPYRIGHT

Copyright © 2004 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the McAfee legal department at: 5000 Headquarters Drive, Plano, Texas 75024, or call +1-972-963-8000.

## TRADEMARK ATTRIBUTIONS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (AND IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFFEE, MCAFFEE (AND IN KATAKANA), MCAFFEE AND DESIGN, MCAFFEE.COM, MCAFFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NETS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

## LICENSE INFORMATION

### License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE, INC. OR THE PLACE OF PURCHASE FOR A FULL REFUND.

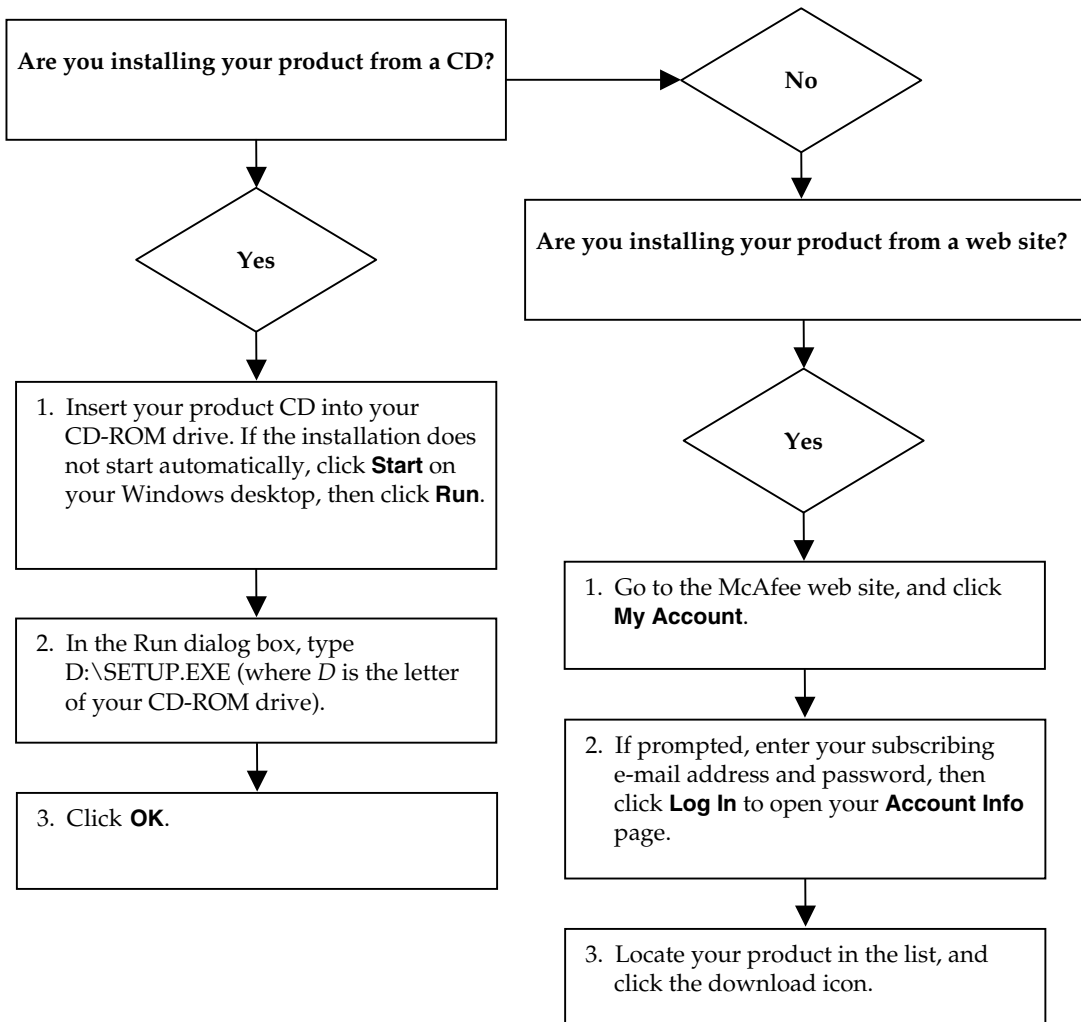
### Attributions

This product includes or may include:

♦ Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). ♦ Cryptographic software written by Eric A. Young and software written by Tim J. Hudson. ♦ Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee, Inc. provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. ♦ Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier. ♦ Software written by Douglas W. Sauder. ♦ Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at [www.apache.org/licenses/LICENSE-2.0.txt](http://www.apache.org/licenses/LICENSE-2.0.txt). ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others. ♦ Software developed by CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. ♦ FEAD® Optimizer® technology, Copyright Netop Systems AG, Berlin, Germany. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000. ♦ Software copyrighted by Expat maintainers. ♦ Software copyrighted by The Regents of the University of California, © 1989. ♦ Software copyrighted by Gunnar Ritter. ♦ Software copyrighted by Sun Microsystems®, Inc. © 2003. ♦ Software copyrighted by Gisle Aas. © 1995-2003. ♦ Software copyrighted by Michael A. Chase, © 1999-2000. ♦ Software copyrighted by Neil Winton, © 1995-1996. ♦ Software copyrighted by RSA Data Security, Inc., © 1990-1992. ♦ Software copyrighted by Sean M. Burke, © 1999, 2000. ♦ Software copyrighted by Martijn Koster, © 1995. ♦ Software copyrighted by Brad Appleton, © 1996-1999. ♦ Software copyrighted by Michael G. Schwern, © 2001. ♦ Software copyrighted by Graham Barr, © 1998. ♦ Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. ♦ Software copyrighted by Frodo Looijaard, © 1997. ♦ Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at [www.python.org](http://www.python.org). ♦ Software copyrighted by Beman Dawes, © 1994-1999, 2002. ♦ Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software copyrighted by Simone Bordet & Marco Cravero, © 2002. ♦ Software copyrighted by Stephen Purcell, © 2001. ♦ Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). ♦ Software copyrighted by International Business Machines Corporation and others, © 1995-2003. ♦ Software developed by the University of California, Berkeley and its contributors. ♦ Software developed by Ralf S. Engelschall <[rsengelschall.com](mailto:rsengelschall@engelschall.com)> for use in the mod\_ssl project (<http://www.modssl.org/>). ♦ Software copyrighted by Kevin Henney, © 2000-2002. ♦ Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. ♦ Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation. ♦ Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. ♦ Software copyrighted by Boost.org, © 1999-2002. ♦ Software copyrighted by Nicolai M. Josuttis, © 1999. ♦ Software copyrighted by Jeremy Siek, © 1999-2001. ♦ Software copyrighted by Daryle Walker, © 2001. ♦ Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. ♦ Software copyrighted by Samuel Krempp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history. ♦ Software copyrighted by Doug Gregor ([gregod@cs.rpi.edu](mailto:gregod@cs.rpi.edu)), © 2001, 2002. ♦ Software copyrighted by Cadenza New Zealand Ltd., © 2000. ♦ Software copyrighted by Jens Maurer, © 2000, 2001. ♦ Software copyrighted by Jaakko Järvi ([jaakko.jarvi@cs.utu.fi](mailto:jaakko.jarvi@cs.utu.fi)), © 1999, 2000. ♦ Software copyrighted by Ronald Garcia, © 2002. ♦ Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001. ♦ Software copyrighted by Stephen Cleary ([shammah@voyager.net](mailto:shammah@voyager.net)), © 2000. ♦ Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001. ♦ Software copyrighted by Paul Moore, © 1999. ♦ Software copyrighted by Dr. John Maddock, © 1998-2002. ♦ Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. ♦ Software copyrighted by Peter Dimov, © 2001, 2002. ♦ Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. ♦ Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

# Quick Start Card

If you are installing your product from a CD or the web site, print this convenient reference page.



McAfee reserves the right to change Upgrade & Support Plans and policies at any time without notice. McAfee and VirusScan are registered trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries.  
© 2004 Networks Associates Technology, Inc. All rights reserved.

### For more information

To view the User Guides on the product CD, make sure you have Acrobat Reader installed; if not, install it now from the McAfee product CD.

- 1 Insert your product CD into your CD-ROM drive.
- 2 Open Windows Explorer: Click **Start** on your Windows desktop, and click **Search**.
- 3 Locate the Manuals folder, and double-click the User Guide .PDF you want to open.

### Registration benefits

We recommend that you follow the easy steps within your product to transmit your registration directly to us. Registration ensures that you receive timely and knowledgeable technical assistance, plus the following benefits:

- FREE electronic support
- Virus definition (.DAT) file updates for one year after installation when you purchase VirusScan software  
Go to <http://www.mcafee.com> for pricing of an additional year of virus signatures.
- 60-day warranty that guarantees replacement of your software CD if it is defective or damaged

- SpamKiller filter updates for one year after installation when you purchase SpamKiller software

Go to <http://www.mcafee.com> for pricing of an additional year of filter updates.

- McAfee Internet Security Suite updates for one year after installation when you purchase MIS software

Go to <http://www.mcafee.com> for pricing of an additional year of content updates.

### Technical Support

For technical support, please visit <http://www.mcafeehelp.com/>.

Our support site offers 24-hour access to the easy-to-use Answer Wizard for solutions to the most common support questions.

Knowledgeable users can also try our advanced options, which include a Keyword Search and our Help Tree. If a solution cannot be found, you can also access our FREE Chat Now! and E-mail Express! options. Chat and e-mail help you to quickly reach our qualified support engineers through the Internet, at no cost. Otherwise, you can get phone support information at <http://www.mcafeehelp.com/>.

# Contents

<b>Quick Start Card</b> .....	<b>iii</b>
<b>1 Getting Started</b> .....	<b>7</b>
New features .....	7
System requirements .....	8
Uninstalling other firewalls .....	9
Setting the default firewall .....	9
Setting the security level .....	10
Testing McAfee Personal Firewall Plus .....	11
Using McAfee SecurityCenter .....	12
<b>2 Using McAfee Personal Firewall Plus</b> .....	<b>13</b>
About the Summary page .....	13
About the Internet Applications page .....	17
Changing permissions .....	18
Changing applications .....	18
About the Inbound Events page .....	19
Understanding events .....	20
Showing events in the Inbound Events log .....	22
Responding to inbound events .....	24
Managing the Inbound Events log .....	27
About alerts .....	29
Red alerts .....	29
Green alerts .....	34
Blue alerts .....	35
<b>Index</b> .....	<b>37</b>



Welcome to McAfee Personal Firewall Plus.

McAfee Personal Firewall Plus software offers advanced protection for your computer and your personal data. Personal Firewall establishes a barrier between your computer and the Internet, silently monitoring Internet traffic for suspicious activities.

With it, you get the following features:

- Defends against potential hacker probes and attacks
- Complements anti-virus defenses
- Monitors Internet and network activity
- Alerts you to potentially hostile events
- Provides detailed information on suspicious Internet traffic
- Integrates Hackerwatch.org functionality, including event reporting, self-testing tools, and the ability to email reported events to other online authorities
- Provides detailed tracing and event research features

## New features

- **Enhanced HackerWatch.org Integration**  
Reporting potential hackers is easier than ever. McAfee Personal Firewall Plus improves the functionality of HackerWatch.org, which includes event submission of potentially malicious events to the database.
- **Extended Intelligent Application Handling**  
When an application seeks Internet access, Personal Firewall first checks whether it recognizes the application as trusted or malicious. If the application is recognized as trusted, Personal Firewall automatically allows it access to the Internet so you do not have to. This database has been enhanced to provide users with more details about the applications connecting to the Internet.
- **Advanced Trojan Detection**  
McAfee Personal Firewall Plus combines application connection management with an enhanced database to detect and block more potentially malicious applications, such as Trojans, from accessing the Internet and potentially relaying your personal data.

### ■ **Improved Visual Tracing**

McAfee Personal Firewall Plus includes an updated intruder-tracing tool known as Visual Trace. Visual Trace includes easy-to-read graphical maps showing the originating source of hostile attacks and traffic worldwide, including detailed contact/owner information from originating IP addresses and all subsequent steps to your computer. McAfee Personal Firewall Plus has added more geographical data to the Visual Trace feature which enhances location details and provides more visual pin-pointed locations of intruders. Visual Trace allows users to visually track where intrusions originate, and with this new data, users are able to see a better graphical representation of their searches.

### ■ **Improved Usability**

McAfee Personal Firewall Plus includes a Setup Assistant and a User Tutorial to guide users in the setup and use of their firewall. Although the product is designed to use without any intervention, McAfee provides users with a wealth of resources to understand and appreciate what the firewall provides for them.

### ■ **Enhanced Intrusion Detection**

Personal Firewall's Intrusion Detection System (IDS) detects common attack patterns and other suspicious activity. Intrusion detection monitors every data packet for suspicious data transfers or transfer methods and logs this in the event log.

### ■ **Enhanced Traffic Analysis**

McAfee Personal Firewall Plus offers users a view of both incoming and outgoing data from their computers, as well as displaying application connections including applications that are actively "listening" for open connections. This allows users to see and act upon applications that might be open for intrusion.

## System requirements

- Microsoft® Windows 98, Me, 2000, or XP
- Personal computer with processor  
Windows 98 or Me: Pentium 150 MHz or higher  
Windows 2000 or XP: Pentium 233 MHz or higher
- RAM  
Windows 98: 32 MB (64 MB recommended)  
Windows Me, 2000, or XP: 64 MB (128 MB recommended)
- 35 MB hard disk space
- Microsoft® Internet Explorer 5.5 or later

### **NOTE**

To upgrade to the latest version of Internet Explorer, visit the Microsoft Web site at

<http://www.microsoft.com/worldwide/>.



## Uninstalling other firewalls

Before you install McAfee Personal Firewall Plus software, you must uninstall any other firewall programs on your computer. Please follow your firewall program's uninstall instructions to do so.

### NOTE

If you use Windows XP, you do not need to disable the built-in firewall before installing McAfee Personal Firewall Plus. However, we recommend that you do disable the built-in firewall. If you do not, you will not receive events in the Inbound Events log in McAfee Personal Firewall Plus.

## Setting the default firewall

McAfee Personal Firewall can manage permissions and traffic for Internet applications on your computer, even if Windows Firewall is detected as running on your computer.

When installed, McAfee Personal Firewall automatically disables Windows Firewall and sets itself as your default firewall. You then experience only McAfee Personal Firewall functionality and messaging. If you subsequently enable Windows Firewall via Windows Security Center or Windows Control Panel, letting both firewalls run on your computer might result in partial loss of logging in McAfee Firewall as well as duplicate status and alert messaging.

### NOTE

If both firewalls are enabled, McAfee Personal Firewall does not show all the blocked IP addresses in its Inbound Events tab. Windows Firewall intercepts most of these events and blocks those events, preventing McAfee Personal Firewall from detecting or logging those events. However, McAfee Personal Firewall might block additional traffic based upon other security factors, and that traffic will be logged.

Logging is disabled in Windows Firewall by default, but if you choose to enable both firewalls, you can enable Windows Firewall logging. The default Windows Firewall log is `C:\Windows\pfirewall.log`

To ensure that your computer is protected by at least one firewall, Windows Firewall is automatically re-enabled when McAfee Personal Firewall is uninstalled.

If you disable McAfee Personal Firewall or set its security setting to **Open** without manually enabling Windows Firewall, all firewall protection will be removed except for previously blocked applications.

## Setting the security level

You can configure security options to indicate how Personal Firewall responds when it detects unwanted traffic. By default, the **Standard** security level is enabled. Use this setting if you are a novice firewall user. If you are an experienced firewall user, you can use other settings. In **Standard** security level, when an application requests Internet access and you grant it access, you are granting the application Full Access. Full Access allows the application the ability to both send data and receive unsolicited data on non-system ports.

To configure security settings:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, then click **Utilities**.
- 2 Click the **Security Settings** icon.
- 3 Set the security level by moving the slider to the desired level.

If you are a novice firewall user, accept the default **Standard** setting. The security level ranges from Lockdown to Open:

- ◆ **Lockdown Connection** — All traffic is stopped. This is essentially the same as unplugging your Internet connection. You can use this setting to block ports you configured to be open in the System Services page.
- ◆ **Tight Security** — An application requests only the type of access to the Internet that it explicitly needs (for example, Outbound Only Access), and you either grant access or block it. If the application later requests Full Access, you either grant Full Access or keep it limited to Outbound Only Access. Use this setting if you are an experienced firewall user.
- ◆ **Standard Security (recommended)** — When an application requests Internet access and you grant it access, you are granting the application Full Access. Full Access allows the application the ability to both send data and receive unsolicited data on non-system ports. Use this setting if you are a novice firewall user.
- ◆ **Trusting Security** — All applications are automatically trusted when they first attempt to access the Internet. However, you can choose to be notified about new applications on your computer with alerts. Use this setting if you find that some games or streaming media do not work.
- ◆ **Open** — Your firewall is effectively disabled. This setting allows all traffic through Personal Firewall with no filtering.

### NOTE

Previously blocked applications continue to be blocked when the firewall is set to the **Open** security setting or **Disabled**. To prevent this from occurring, you can either change the application's permissions to **Full Access** or simply delete the **Blocked** permission rule in the **Permissions** list.

- 4 Select additional security settings:

**NOTE**

If your computer runs Windows XP and multiple XP users have been added, these options are available only if you are logged on to your computer as an administrator.

- ◆ **Record Intrusion Detection (IDS) Events in Inbound Events Log** — If you select this option, events detected by IDS will appear in the Inbound Events log. The Intrusion Detection System detects common attack types and other suspicious activity. Intrusion detection monitors every inbound and outbound data packet for suspicious data transfers or transfer methods. It compares these to a "signature" database and automatically drops the packets coming from the offending computer.

IDS looks for specific traffic patterns used by attackers. IDS checks each packet that your machine receives to detect suspicious or known-attack traffic. For example, if Personal Firewall sees ICMP packets, it analyzes those packets for suspicious traffic patterns by comparing the ICMP traffic against known attack patterns.

- ◆ **Accept ICMP ping requests** — ICMP traffic is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. If you select this option, Personal Firewall allows all ping requests without logging the pings in the Inbound Events log. If you do not select this option, Personal Firewall blocks all ping requests and logs the pings in the Inbound Events log.
- ◆ **Allow restricted users to change Personal Firewall settings** — If your computer runs Windows XP and multiple XP users have been added, make sure this checkbox is selected if you want to allow restricted XP users to modify Personal Firewall settings.

- 5 Click **OK** if you are finished making changes.

## Testing McAfee Personal Firewall Plus

To test Personal Firewall:

- 1 Right-click the McAfee icon , point to **Personal Firewall**, then click **Test Firewall**.
- 2 Personal Firewall opens Internet Explorer and goes to <http://www.hackerwatch.org/>, a web site maintained by McAfee. Please follow the directions on the Hackerwatch.org Probe page to test Personal Firewall.

### NOTE

If you connect to the Internet through a proxy server or Network Address Translation server, as is the case in most office networks (LANs), you will not get a proper reading. Hackerwatch.org's firewall tester looks for which computer asked for the firewall test and tests that computer. If you connect through a proxy or NAT server, it simply relays your computer's request for the firewall test, and Hackerwatch.org will test the wrong computer. The results that you get belong to the proxy server—not to your computer.


## Using McAfee SecurityCenter


McAfee SecurityCenter is your one-stop security shop, accessible from its icon in your Windows system tray or from your Windows desktop. With it, you can perform these useful tasks:

- Get free security analysis for your computer.
- Launch, manage, and configure all your McAfee subscriptions from one icon.
- See continuously updated virus alerts and the latest product information.
- Receive free trial subscriptions to download and install trial versions directly from McAfee using our patented software delivery process.
- Get quick links to frequently asked questions and account details at the McAfee web site.


### NOTE

For more information about its features, click **Help** in the **SecurityCenter** dialog box.


While SecurityCenter is running and all of the McAfee features installed on your computer are enabled, a red M icon  appears in the Windows system tray. This area is usually in the lower-right corner of the Windows desktop and contains the clock.

If one or more of the McAfee applications installed on your computer are disabled, the McAfee icon changes to black .


To open the McAfee SecurityCenter:

- 1 Right-click the McAfee icon .
- 2 Click **Open SecurityCenter**.

To access a Personal Firewall feature:

- 1 Right-click the McAfee icon .
- 2 Point to **Personal Firewall**, then click the feature you want to use.

To open Personal Firewall:

Right-click the McAfee icon , point to **Personal Firewall**, and click **View Summary**, **Internet Applications**, **Inbound Events**, or **Utilities**.

## About the Summary page




The Personal Firewall Summary includes four summary pages: Main Summary, Application Summary, Event Summary, and HackerWatch Summary. The Summary pages contain a variety of reports on recent inbound events, application status, and world-wide intrusion activity reported by HackerWatch.org. You will also find links to common tasks performed in Personal Firewall.

To open the Personal Firewall Summary pages, right-click the McAfee icon, point to **Personal Firewall**, then click **View Summary**. The Main Summary page appears (Figure 2-1).



Figure 2-1. Main Summary page

Click the following to navigate to different Summary pages:

Item	Description
Change View	Click <b>Change View</b> to open a list of Summary pages. From the list, select a Summary page to view.
 Right arrow	Click the right arrow icon to view the next Summary page.
 Left arrow	Click the left arrow icon to view the previous Summary page.
 Home	Click the home icon to return to the <b>Main Summary</b> page.

The Main Summary page provides the following information:

Item	Description
Security Setting	The security setting status tells you the level of security at which the firewall is set. Click the link to change the security level.
Blocked Events	The blocked events status displays the number of events that have been blocked today. Click the link to view event details from the Inbound Event page.
Application Rule Changes	The application rule status displays the number of application rules that have been changed recently. Click the link to view the list of allowed and blocked applications and to modify application permissions.
What's New?	<b>What's New?</b> shows the latest application that was granted full access to the Internet.
Last Event	<b>Last Event</b> shows the latest inbound events. You can click a link to trace the event or to trust the IP address. Trusting an IP address allows all traffic from the IP address to reach your computer.
Daily Report	<b>Daily Report</b> displays the number of inbound events that Personal Firewall blocked today, this week, and this month. Click the link to view event details from the Inbound Event page.
Active Applications	<b>Active Applications</b> displays the applications that are currently running on your computer and accessing the Internet. Click an application to view which IP addresses the application is connecting to.
Common Tasks	Click a link in <b>Common Tasks</b> to go to Personal Firewall pages where you can view firewall activity and perform tasks.

To view the Application Summary page, click **Change View**, then select **Application Summary**. The Application Summary page provides the following information:

Item	Description
Traffic Monitor	The <b>Traffic Monitor</b> shows inbound and outbound traffic volume across your Internet connection in the last ten minutes. Click the graph to view traffic monitoring details.
Active Applications	<b>Active Applications</b> shows the bandwidth usage of your computer's most active applications during the last 24 hours. <b>Application</b> —The application accessing the Internet. <b>%</b> —The percentage of bandwidth used by the application. <b>Permission</b> —The type of Internet access that the application is allowed. <b>Rule Created</b> —When the application rule was created.
What's New?	<b>What's New?</b> shows the latest application that was granted full access to the Internet.
Active Applications	<b>Active Applications</b> displays the applications that are currently running on your computer and accessing the Internet. Click an application to view which IP addresses the application is connecting to.
Common Tasks	Click a link in <b>Common Tasks</b> to go to Personal Firewall pages where you can view application status and perform application-related tasks.

To view the Event Summary page, click **Change View**, then select **Event Summary**. The Event Summary page provides the following information:

Item	Description
Port Comparison	<b>Port Comparison</b> shows a pie chart of the most frequently attempted ports on your computer during the past 30 days. You can click a port name to view details from the Inbound Events page. You can also move your mouse pointer over the port number to see a description of the port.
Top Offenders	<b>Top Offenders</b> shows the most frequently blocked IP addresses, when the last inbound event occurred for each address, and the total number of inbound events in the past thirty days for each address. Click an event to view event details from the Inbound Events page.
Daily Report	<b>Daily Report</b> displays the number of inbound events that Personal Firewall blocked today, this week, and this month. Click a number to view the event details from the Inbound Events log.

Item	Description
Last Event	<b>Last Event</b> shows the latest inbound events. You can click a link to trace the event or to trust the IP address. Trusting an IP address allows all traffic from the IP address to reach your computer.
Common Tasks	Click a link in <b>Common Tasks</b> to go to Personal Firewall pages where you can view details of events and perform event-related tasks.

To view the HackerWatch Summary page, click **Change View**, then select **HackerWatch Summary**. The HackerWatch Summary page provides the following information:

Item	Description
World Activity	<b>World Activity</b> shows a world map identifying recently blocked activity monitored by HackerWatch.org. Click the map to open the Global Threat Analysis Map in HackerWatch.org.
Event Volume	<b>Event Volume</b> shows the number of inbound events submitted to HackerWatch.org.
Global Port Activity	<b>Global Port Activity</b> shows the top ports, in the past 5 days, that appear to be threats. Click a port to view the port number and port description.
Common Tasks	Click a link in <b>Common Tasks</b> to go to HackerWatch.org pages where you can get more information on world-wide hacker activity.



## About the Internet Applications page

Use the Internet Applications page to view the list of allowed and blocked applications.

Right-click the McAfee icon, point to **Personal Firewall**, then click **Internet Applications**. The Internet Applications page appears (Figure 2-2).

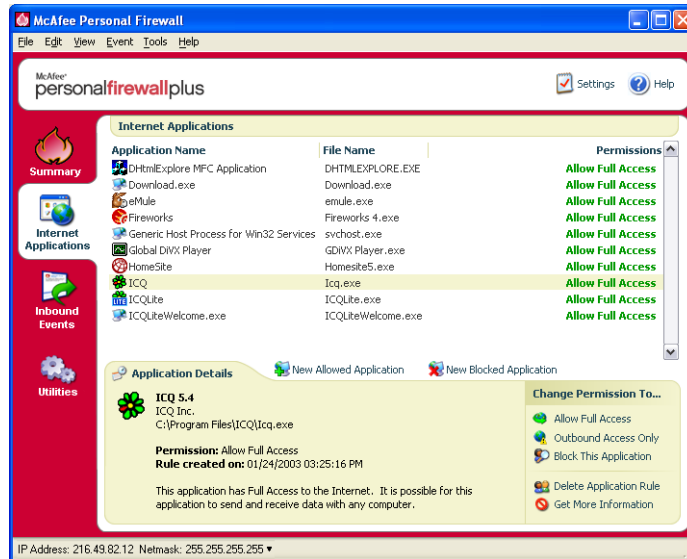


Figure 2-2. Internet Applications page

The Internet Applications page provides the following information:

- Application names
- File names
- Current permission levels
- Application details: pathnames, permission timestamps, and explanations of permission types

## Changing permissions

Personal Firewall lets you set the permission level for each application that requests Internet access.

To change a permission level:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, then click **Internet Applications**.
- 2 In the **Permissions** list, right-click the permission level for an application, and choose a different level:
  - ◆ Click **Allow Full Access** to allow the application to both send and receive data.
  - ◆ Click **Outbound Access Only** to prevent the application from receiving data.
  - ◆ Click **Block This Application** to prevent the application from sending or receiving data.

### NOTE

Previously blocked applications continue to be blocked when the firewall is set to the **Open** security setting or **Disabled**. To prevent this from occurring, you can either change the application's permissions to **Full Access** or simply delete the **Blocked** permission rule in the **Permissions** list.

To delete a permission level:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, then click **Internet Applications**.
- 2 In the **Permissions** list, right-click the permission level for an application, and click **Delete Application Rule**.

The next time the application requests Internet access, you can set its permission level to re-add it to the list.

## Changing applications

To change the list of allowed and blocked Internet applications:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, then click **Internet Applications**.
- 2 Add or remove applications from the **Application Name** list:
  - ◆ To add a new "Allowed" application, click **New Allowed Application**, select the application to allow, then click **Open**.
  - ◆ To add a new "Blocked" application, click **New Blocked Application**, select the application to block, then click **Open**.
  - ◆ To remove an application from the list, click **Delete Application Rule**.

## About the Inbound Events page

Use the Inbound Events page to view the Inbound Events log generated when Personal Firewall blocks unsolicited Internet traffic.

Right-click the McAfee icon, point to **Personal Firewall**, then click **Inbound Events**. The Inbound Events page appears (Figure 2-3).

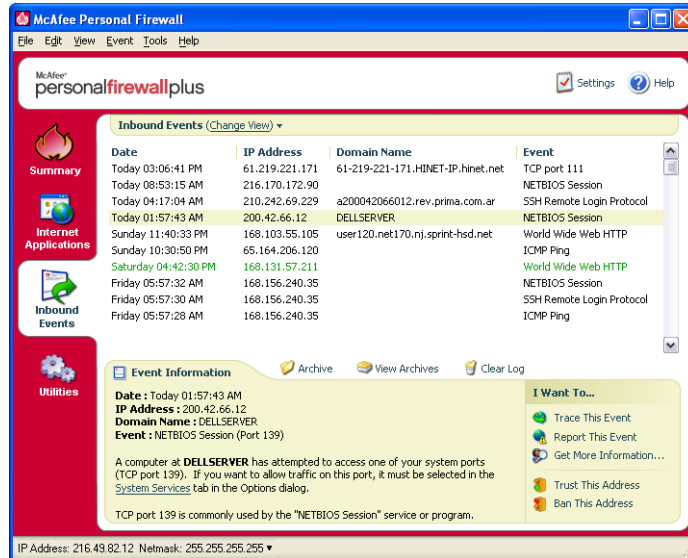


Figure 2-3. Inbound Events page

The Inbound Events page provides the following information:

- Timestamps
- Source IPs
- Hostnames
- Service or application names
- Event details: connection types, connection ports, and explanations of port events

## Understanding events

### About IP addresses

IP addresses are numbers: four numbers each between 0 and 255 to be precise. These numbers identify a specific place that traffic can be directed to on the Internet.

### Special IP addresses

Several IP addresses are unusual for various reasons:

**Non-routable IP addresses** — These are also referred to as "Private IP Space." These IP addresses cannot be used on the Internet. Private IP blocks are 10.x.x.x, 172.16.x.x - 172.31.x.x, and 192.168.x.x.

**Loop-back IP addresses** — Loop-back addresses are used for testing purposes. Traffic sent to this block of IP addresses comes right back to the device generating the packet. It never leaves the device, and is primarily used for hardware and software testing. The Loop-Back IP block is 127.x.x.x.

**Null IP address** — This is an invalid address. When it is seen, it indicates that the traffic had a blank IP address. This is obviously not normal, and frequently it indicates that the sender is deliberately obscuring the origin of the traffic. The sender will not be able to receive any replies to their traffic unless the packet is received by an application that understands the contents of the packet that will include instructions specific to that application. Any address that starts with 0 (0.x.x.x) is a null address. For example, 0.0.0.0 is a null IP address.

### Events from 0.0.0.0

If you see events from IP address 0.0.0.0, there are two likely causes. The first, and most common, is that for some reason your computer received a badly formed packet. The Internet isn't always 100% reliable, and bad packets can occur. Since Personal Firewall sees the packets before TCP/IP can validate them, it might report these packets as an event.

The other situation occurs when the source IP is spoofed, or faked. Spoofed packets might be a sign that someone is scanning around looking for Trojans, and they happened to try your computer. It's important to remember that Personal Firewall blocked this attempt, so your computer is safe.

### Events from 127.0.0.1

Events will sometimes list their source IP as 127.0.0.1. It's important to note that this IP is special, and is referred to as the loopback address.

Basically, no matter what computer you're on, 127.0.0.1 always refers to yourself. This address is also referred to as localhost, as the computer name localhost will always resolve back to the IP address 127.0.0.1.

Does this mean that your computer is attempting to hack itself? Is some Trojan or spyware taking over your computer? Not likely. Many legitimate programs use the loopback address for communication between components. For example, many personal mail or web servers let you configure them via a web interface that is usually accessible through something like `http://localhost/`.

However, Personal Firewall allows traffic from these programs, so if you see events from 127.0.0.1, it most likely means that the source IP address is spoofed, or faked. Spoofed packets are usually signs of someone scanning for Trojans. It's important to remember that Personal Firewall blocked this attempt, so your computer is safe. Obviously, reporting events from 127.0.0.1 won't do any good, so there's no need to do so.

That said, some programs, most notably Netscape 6.2 and higher, require you to add 127.0.0.1 to the Trusted IP Addresses list. These programs' components communicate between each other in such a manner that Personal Firewall cannot determine if the traffic is local or not.

In the example of Netscape 6.2, if you do not trust 127.0.0.1, then you will not be able to use your buddy list. Therefore, if you see traffic from 127.0.0.1 and all of the applications on your computer work normally, then it is safe to block this traffic. However, if a program (like Netscape) is having problems, add 127.0.0.1 in the Trusted IP Addresses list in Personal Firewall, then find out if the problem is resolved.

If placing 127.0.0.1 in the trusted IP list fixes the problem, then you need to weigh your options: if you trust 127.0.0.1, your program will work, but you will be more open to spoofed attacks. If you do not trust the address, then your program will not work, but you will remain protected against such malicious traffic.

## Events from computers on your LAN

Events can be generated from computers on your local area network (LAN). To show that these events are coming from somewhere "close to home," Personal Firewall displays them in green.

In most corporate LAN settings, you'll want to select **Make all computers on your LAN Trusted** in the Trusted IP Addresses options.

However, it's important to note that in some situations, your "local" network can be as dangerous, or even more dangerous, than the outside network. This is especially true if you are on a high-bandwidth public network, such as DSL or cable modems. In such a scenario, it's best not to select the **Make all computers on your LAN Trusted** option.

If you are on a home network connected to broadband, you should instead manually add the IP addresses of your local computers to the Trusted IP Addresses list. Remember, you can use .255 style addresses to trust an entire block. For example, you can trust your entire ICS (Internet Connection Sharing) network by trusting the IP 192.168.255.255.

## Events from private IP addresses

IP addresses of the format 192.168.xxx.xxx, 10.xxx.xxx.xxx, and 172.16.0.0 - 172.31.255.255 are referred to as non-routable or private IP addresses. These IP addresses should never leave your network, and can be trusted most of the time.

The 192.168 block is used with Microsoft Internet Connection Sharing (ICS). If you are using ICS, and see events from this IP block, you might want to add the IP address 192.168.255.255 to your Trusted IP Addresses list. This will trust the entire 192.168.xxx.xxx block.

If you are not on a private network, and see events from these IP ranges, the source IP address might be spoofed, or faked. Spoofed packets are usually signs that someone is scanning for Trojans. It's important to remember that Personal Firewall blocked this attempt, so your computer is safe.

Since private IP addresses refer to different computers depending on what network you are on, reporting these events will have no effect, so there's no need to do so.

## Showing events in the Inbound Events log

The Inbound Events log allows you to conveniently display events in a number of ways. The default view limits the view to events occurring on the current day. You can also view events that occurred during the past week, or view the complete log.

Personal Firewall also lets you display inbound events from specific days, from specific Internet addresses (IP addresses), or events that contain the same event information.

For information about an event, click the event, and the information appears in the **Event Information** area at the bottom of the Inbound Events page.

### Showing today's events

To show only events occurring today:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, then click **Inbound Events**.
- 2 From the **View** menu, click **Show Today's Events**.

The Inbound Events log displays events occurring today only.

### Showing this week's events

To show events occurring in the past week:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, then click **Inbound Events**.
- 2 From the **View** menu, click **Show This Week's Events**.

The Inbound Events log displays events occurring this week only.

## Showing the complete Inbound Events log

To show all of the events in the Inbound Events log:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 From the **View** menu, click **Show Complete Log**.

The Inbound Events log displays all events, not including archives, from the Inbound Events log.

## Showing only events from the selected day

This is useful when you want to look only at events from a specific day. All events not occurring on that day are hidden.

To show all of the events from a specific day:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, then click **Inbound Events**.
- 2 From the **View** menu, click **Show Only Events from Selected Day**.

Today's events appear on the Inbound Events log.

## Showing only events from the selected Internet address

This is useful when you want to see other events originating from a specific Internet address. All other events are hidden.

To show all of the events from a specific Internet address:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, then click **Inbound Events**.
- 2 From the **View** menu, click **Show Only Events from Selected Internet Address**.

Events originating from the selected Internet address appear in the Inbound Events log.

## Showing only events with the same event information

This is useful when you need to see if there are other events in the Inbound Events log that have the same information in the **Event Information** column as the event you selected. You can find out how many times this event happened, and if it is from the same source. The Event Information column provides a description of the event and, if known, the common program or service that uses that port.

To show all of the events with the same event information:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 From the **View** menu, click **Show Only Events with the Same Event Information**.

Events with the same Event Information appear in the Inbound Events log.

## Responding to inbound events

In addition to getting details about events in the Inbound Events log, you can try to perform a Visual Trace of the IP addresses for an event in the Inbound Events log, or get event details at the anti-hacker online community HackerWatch.org web site.

### Tracing the selected event

You can try to perform a Visual Trace of the IP addresses for an event in the Inbound Events log:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 Right-click the event you want to trace, then click **Trace Selected Event**.

You can also double click an event to perform a trace.

By default, Personal Firewall begins a Visual Trace using the integrated Visual Trace program.

### Getting advice from HackerWatch.org

You can also try to get more information about an event from the anti-hacker online community HackerWatch.org:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 Locate and click the event about which you want more information.
- 3 From the **Event** menu, click **More Information on Event**.

Your web browser opens and goes to the HackerWatch.org web site at <http://www.hackerwatch.org/> to get details about the event type and advice about whether to report the event.



## Reporting an event

To report an event that you think was an attack on your computer:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 Click the event you want to report, then click **Report This Event** in the lower right pane.

Personal Firewall reports the event to the HackerWatch.org web site using your unique ID.

## Signing up for HackerWatch.org

When you first open the Summary page, Personal Firewall contacts HackerWatch.org to generate your unique user ID. If you are an existing user, your sign-up is automatically validated. If you are a new user, you must enter a nickname and email address, then click the validation link in the confirmation email from HackerWatch.org to be able to use the event filtering/e-mailing features at its web site.

You can report events to HackerWatch.org without validating your user ID. However, to filter events and email events to a friend, you must sign up for the service.

Signing up for the service allows your submissions to be tracked and lets us notify you if HackerWatch.org needs more information or further action from you. We also require you to sign up because we must confirm any information we receive for that information to be useful.

All email addresses provided to HackerWatch.org are kept confidential. If a request for additional information is made by an ISP, that request is routed through HackerWatch.org; your email address is never exposed.

## Trusting an address

If you see an event in the Inbound Events log that contains an IP address that you need to allow, you can have Personal Firewall allow connections from it at all times:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 Right-click the event whose IP address you want trusted, and click **Trust the Source IP Address**.
- 3 Verify that the IP address displayed in the Trust This Address confirmation message is correct, and click **OK**.

The IP address is added to the **Trusted IP Addresses** list.

To verify that the IP address was added:

- 1 Click the **Utilities** tab.
- 2 Click the **Trusted & Banned IPs** icon, then click the **Trusted IP Addresses** tab.

The IP address appears in the **Trusted IP Addresses** list.

### Banning an address

If an IP address appears in your Inbound Events log, this indicates that traffic from that address was blocked. Therefore, banning an address adds no additional protection unless your computer has ports that are deliberately opened through the System Services feature, or unless your computer has an application that has permission to receive traffic.

Add an IP address to your banned list only if you have one or more ports that are deliberately open and if you have reason to believe that you must block that address from accessing open ports.

If you see an event in the Inbound Events log that contains an IP address that you want to ban, you can have Personal Firewall prevent connections from it at all times:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 Right-click the event whose IP address you want to ban, and click **Ban the Source IP Address**.
- 3 Verify that the IP address displayed in the Ban This Address confirmation message is correct, and click **OK**.

The IP address is added to the **Banned IP Addresses** list.

To verify that the IP address was added:

- 1 Click the **Utilities** tab.
- 2 Click the **Trusted & Banned IPs** icon, then click the **Banned IP Addresses** tab.

The IP address appears in the **Banned IP Addresses** list.

## Managing the Inbound Events log

You can use the Inbound Events page to manage the events in the Inbound Events log generated when Personal Firewall blocks unsolicited Internet traffic.

### Archiving the Inbound Events log

You can archive the current Inbound Events log in a file on your hard drive. We recommend that you archive your event log periodically because the event log can get quite large.

To archive the Inbound Events Log:

- 1 Right-click the McAfee icon, point to **Personal Firewall**, then click **Inbound Events**.
- 2 From the **File** menu, click **Archive Log**.
- 3 Click **Yes** on the confirmation message.
- 4 Click **Save** to save the archive in the default location, or browse to a location where you want to save the archive.

### Viewing an archived Inbound Events log

You can view any Inbound Events log that you previously archived.

#### NOTE

Before you view your archives, you must archive your current Inbound Events log. Failure to do so will clear your current Inbound Events log when you view an archive.

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 From the File menu, click **View Archived Logs**.
- 3 Click the archive file name (you might have to browse to it) and click **Open**.

The archived data appears in the Inbound Events log.

### Clearing the Inbound Events log

You can clear all information from the Inbound Events log.

#### NOTE

Once you clear the Inbound Events log, you cannot recover it. If you think you will need the event log in the future, you should archive it instead.

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 From the **File** menu, click **Clear Log**.
- 3 Click **Yes** on the confirmation box to clear the log.

The Event Log is now empty.

## Exporting displayed events

You can export your event log to a text file in case you need to share it with your ISP, technical support, or law enforcement officials.

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 From the File menu, click **Export Displayed Events**.
- 3 Browse to the location to which you want to save the events.
- 4 Rename the file if necessary, then click **Save**.

Your events are saved to a .txt file in the location you chose.

## Copying an event to the Clipboard

You can copy an event to the clipboard so that you can paste it in a text file using Notepad.

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 Click the event in the Inbound Events log that you need to export.
- 3 From the **Edit** menu, click **Copy Selected Event to Clipboard**.
- 4 Open Notepad:  
Click the Windows Start button, point to Programs, then Accessories, then click Notepad.
- 5 From the **Edit** menu, click **Paste**. The event appears in Notepad. Repeat this step until you have all of the necessary events.
- 6 Save the Notepad file in a safe place.

## Deleting the selected event

You can delete events from the Inbound Events log.

- 1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
- 2 Click the event in the Inbound Events log that you want to delete.
- 3 From the **Edit** menu, click **Delete Selected Event**.

The event is deleted from the Inbound Events log.

## About alerts

We strongly recommend that you become familiar with the types of alerts you will encounter while using Personal Firewall. Review the following types of alerts that can appear and the possible responses you can choose, so that you can confidently respond to an alert.

### NOTE

Recommendations on alerts help you decide how to handle an alert. For recommendations to appear on alerts, click the **Utilities** tab, click the **Alert Settings** icon, then select either **Use Smart Recommendations** (the default) or **Display Smart Recommendations only** from the **Smart Recommendations** list.

## Red alerts

Red alerts contain important information that requires your immediate attention:

- **Internet Application Blocked** — This alert appears if Personal Firewall blocks an application from accessing the Internet. For example, if a Trojan program alert appears, McAfee automatically denies this program access to the Internet and recommends that you scan your computer for viruses.
- **Application Wants to Access the Internet** — This alert appears when Personal Firewall detects Internet or network traffic for new applications. (Standard or Tight Security)
- **Application Has Been Modified** — This alert appears when Personal Firewall detects that an application you have previously allowed to access the Internet has changed. If you have not recently upgraded the application in question, you should be careful about granting the modified application access to the Internet. (Trusting, Standard, or Tight Security)
- **Application Requests Server Access** — This alert appears when Personal Firewall detects that an application you have previously allowed to access the Internet has requested Internet access as a server. (Tight Security)

### NOTE

The Windows XP SP2 default Automatic Updates setting downloads and installs updates for the Windows OS and other Microsoft programs running on your computer without messaging you. When an application has been modified from one of Windows silent updates, McAfee Personal Firewall alerts appear the next time the Microsoft application is run.

### IMPORTANT

You must grant access to applications that require Internet access for online product updates (such as McAfee services) to keep them up-to-date.

## Internet Application Blocked alert

If a Trojan program alert appears (Figure 2-4), Personal Firewall automatically denies this program access to the Internet and recommends that you scan your computer for viruses.

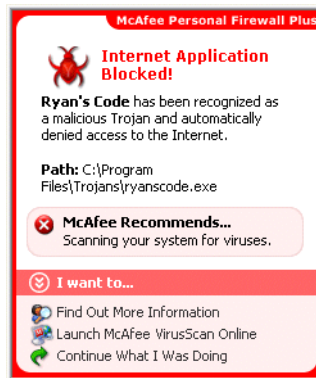


Figure 2-4. Internet Application Blocked alert

View a brief description of the event, then choose from these options:

- Click **Find Out More Information** to get details about the event through the Inbound Events log (see [About the Inbound Events page on page 19](#) for details).
- Click **Launch McAfee VirusScan Online** to scan your computer for viruses.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.

## Application Wants to Access the Internet alert

If you selected **Standard** or **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 2-5) when it detects Internet or network traffic for new or modified applications.

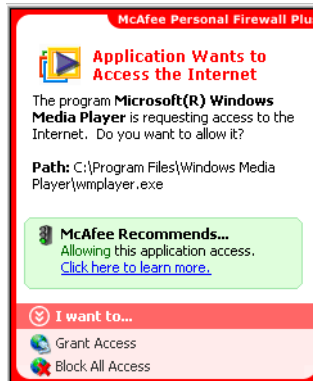


Figure 2-5. Application Wants to Access the Internet alert

If an alert appears recommending caution in allowing the application Internet access, you can click **Click here to learn more** to get more information about the application. This option appears on the alert only if Personal Firewall is configured to use Smart Recommendations.

McAfee might not recognize the application trying to gain Internet access (Figure 2-6).



Figure 2-6. Unrecognized Application alert

Therefore, McAfee cannot give you a recommendation on how to handle the application. You can report the application to McAfee by clicking **Tell McAfee about this program**. A web page appears and asks you for information related to the application. Please fill out as much information as you know.

The information you submit is used in conjunction with other research tools by our HackerWatch operators to determine whether an application warrants being listed in our known applications database, and if so, how it should be treated by Personal Firewall.

View a brief description of the event, then choose from these options:

- Click **Grant Access** to allow the application to both send data and receive unsolicited data on non-system ports.
- Click **Block All Access** to prevent the application from sending or receiving data.

### Application Has Been Modified alert

If you selected **Trusting**, **Standard**, or **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 2-7) when Personal Firewall detects that an application you have previously allowed to access the Internet has changed. If you have not recently upgraded the application in question, be careful about granting the modified application access to the Internet.

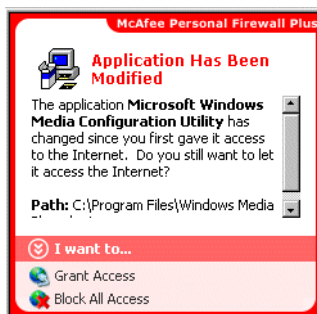


Figure 2-7. Application Has Been Modified alert

View a brief description of the event, then choose from these options:

- Click **Grant Access** to allow the application to both send data and receive unsolicited data on non-system ports.
- Click **Block All Access** to prevent the application from sending or receiving data.



## Application Requests Server Access alert

If you selected **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 2-8) when it detects that an application you have previously allowed to access the Internet has requested Internet access as a server.

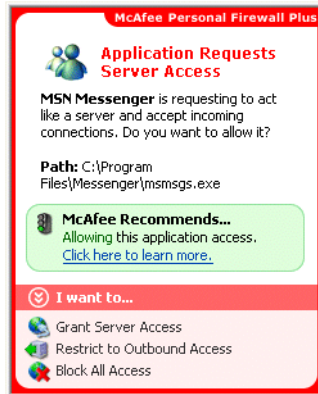


Figure 2-8. Application Requests Server Access alert

For example, an alert appears when MSN Messenger requests server access to send a file during a chat.

View a brief description of the event, then choose from these options:

- Click **Grant Server Access** to allow the application to both send and receive data.
- Click **Restrict to Outbound Access** to prevent the application from receiving data.
- Click **Block All Access** to prevent the application from sending or receiving data.

## Green alerts

Green alerts inform you of changes that have been made to Personal Firewall. For example, green alerts can inform you of applications to which Personal Firewall has automatically granted Internet access, or inform you of any new application rules.

**Program Allowed to Access the Internet** — This alert appears when Personal Firewall automatically grants Internet access for all new or modified applications, then notifies you (Trusting Security). An example of a modified application is one with modified rules to automatically allow the application Internet access.

### Application Allowed to Access the Internet alert

If you selected **Trusting** security in the Security Settings options, Personal Firewall automatically grants Internet access for all new or modified applications, then notifies you with an alert (Figure 2-9).

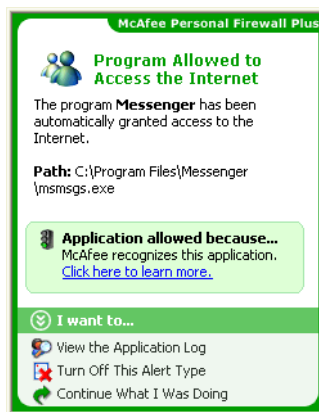


Figure 2-9. Program Allowed to Access the Internet

View a brief description of the event, then choose from these options:

- Click **View the Application Log** to get details about the event through the Internet Applications Log (see *About the Internet Applications page on page 17* for details).
- Click **Turn Off This Alert Type** to prevent these types of alerts from appearing.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.

## Blue alerts

Blue alerts contain information, but require no response from you.

- **Connection Attempt Blocked** — This alert appears when Personal Firewall blocks unwanted Internet or network traffic. (Trusting, Standard, or Tight Security)

### Connection Attempt Blocked alert

If you selected **Trusting, Standard, or Tight** security, Personal Firewall displays an alert (Figure 2-10) when it blocks unwanted Internet or network traffic.

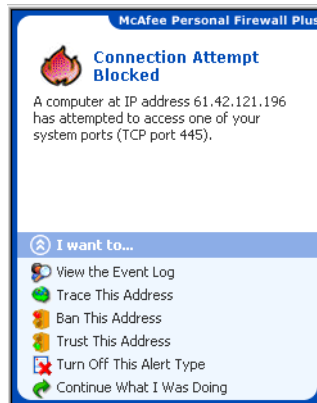


Figure 2-10. Connection Attempt Blocked alert

View a brief description of the event, then choose from these options:

- Click **View the Event Log** to get details about the event through the Personal Firewall Inbound Events log (see [About the Inbound Events page on page 19](#) for details).
- Click **Trace This Address** to perform a Visual Trace of the IP addresses for this event.
- Click **Ban This Address** to block this address from accessing your computer. The address is added to the Banned IP Addresses list.
- Click **Trust This Address** to allow this IP address to access your computer.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.



# Index

## A

### alerts

- Application Has Been Modified, [29](#)
- Application Requests Internet Access, [29](#)
- Application Requests Server Access, [29](#)
- Connection Attempt Blocked, [35](#)
- Internet Application Blocked, [29](#)
- New Application Allowed, [34](#)

## D

- default firewall, setting the, [9](#)

## E

### Event Log

- about, [19](#)
- managing, [27](#)
- viewing, [27](#)

### events

- about, [19](#)
- archiving the Event Log, [27](#)
- clearing the Event Log, [27](#)
- copying, [28](#)
- deleting, [28](#)
- exporting, [28](#)
- from 0.0.0.0, [20](#)
- from 127.0.0.1, [20](#)
- from computers on your LAN, [21](#)
- from private IP addresses, [22](#)
- HackerWatch.org advice, [24](#)
- loopback, [20](#)
- more information, [24](#)
- reporting, [25](#)
- responding to, [24](#)

### showing

- all, [23](#)
- from one address, [23](#)
- one day's, [23](#)
- this week's, [22](#)
- today's, [22](#)
- with same event info, [24](#)

### tracing

- understanding, [19](#)
- viewing archived Event Logs, [27](#)

## G

- getting started, [7](#)

## H

### HackerWatch.org

- advice, [24](#)
- reporting an event to, [25](#)
- signing up, [25](#)

## I

### Internet applications

- about, [17](#)
- changing applications, [18](#)
- changing permissions, [18](#)

### IP addresses

- about, [20](#)

## M

- McAfee SecurityCenter, [12](#)

## N

- new features, [7](#)

## P

### Personal Firewall

- testing, [11](#)

using, 13

## Q

Quick Start Card, iii

## R

reporting an event, 25

## S

showing events in the Event Log, 22

Summary Page, 13

system requirements, 8

## T

testing Personal Firewall, 11

tracing an event, 24

## U

uninstalling

    other firewalls, 9

## W

Windows Automatic Updates, 29

Windows Firewall, 9

