Symantec™ Client Firewall Implementation Guide

symantec™

Symantec™ Client Firewall Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

Trademarks

Symantec, the Symantec logo, and LiveUpdate are U.S. registered trademarks of Symantec Corporation. Symantec Client Firewall, Symantec Client Security, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT
SYMANTEC CLIENT FIREWALL

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE.

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

YOU MAY:

A. use the Software in the manner described in the Software documentation and in accordance with the License Module. If the Software is part of an offering containing multiple Software titles, the aggregate number of copies You may use may not exceed the aggregate number of licenses indicated in the License Module, as calculated by any combination of licensed Software titles in such offering. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single machine;

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

C. use the Software on a network or to protect a network such as at the gateway or on a mail server, provided that You have a license to the Software for each computer that can access the network;

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

E. use the Software in accordance with any additional permitted uses set forth in Section 8, below.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

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

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

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

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

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

G. use the Software in any manner that contradicts any additional restrictions set forth in Section 8, below.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which You have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit You to obtain and use Content Updates.

3. LIMITED WARRANTY:

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

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

4. DISCLAIMER OF DAMAGES:

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

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

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

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

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

6. EXPORT REGULATION:

Export, re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. The original of this Agreement has been written in English and English is the governing language of this Agreement. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A. or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

8. ADDITIONAL RESTRICTIONS FOR SPECIFIED SOFTWARE:

i.If the product You have licensed is Symantec AntiVirus Scan Engine, Symantec AntiVirus for NetApp® Filer/NetCache®, or Symantec AntiVirus for Inktomi® Traffic Edge™, the following additional restrictions apply to Your use of the Software:

A. Symantec AntiVirus for NetApp Filer/NetCache may only be used to scan and repair files accessed through NetApp Filer/NetCache.

B. Symantec AntiVirus for Inktomi Traffic Edge may only be used to scan and repair files accessed through Inktomi Traffic Edge.

C. Symantec AntiVirus Scan Engine may not be used to scan and repair files accessed through NetApp Filer/NetCache or Inktomi Traffic Edge.

ii.If the product You have licensed is Symantec Web Security, independent of version or operating platform designation, upon the expiration of Your right to acquire Content Updates, the filtering definitions corresponding with all previous Content Updates will be entirely deleted and will no longer be available for use with the Software. Upon the expiration of Your right to acquire Content Updates, access to updated virus definitions will no longer be available, however, Licensee may continue to use virus definitions previously acquired.

NetApp and NetCache are registered trademarks of Network Appliance, Inc. in the U.S. and other countries. Inktomi and Traffic Edge are trademarks or registered trademarks of Inktomi Corporation in the United States and other countries.

This Software utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators. Copyright © 1996-1999. Silicon Graphics Computer Systems, Inc. Copyright © 1994. Hewlett-Packard Company.

SUN MICROSYSTEMS, INC. BINARY CODE LICENSE AGREEMENT

READ THE TERMS OF THIS AGREEMENT AND ANY PROVIDED SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT") CAREFULLY BEFORE OPENING THE SOFTWARE MEDIA PACKAGE. BY OPENING THE SOFTWARE MEDIA PACKAGE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THESE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO YOUR PLACE OF PURCHASE FOR A REFUND OR, IF THE SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" BUTTON AT THE END OF THIS AGREEMENT.

1. LICENSE TO USE.

Sun grants you a non-exclusive and non-transferable license for the internal use only of the accompanying software and documentation and any error corrections provided by Sun (collectively "Software"), by the number of users and the class of computer hardware for which the corresponding fee has been paid.

2. RESTRICTIONS.

Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Except as specifically authorized in any Supplemental License Terms, you may not make copies of Software, other than a single copy of Software for archival purposes. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Software is not designed, licensed, or intended for use in the design, construction, operation, or maintenance of any nuclear facility. Sun disclaims any express or implied warranty of fitness for such uses. No right, title, or interest in or to any trademark, service mark, logo, or trade name of Sun or its licensors is granted under this Agreement.

3. LIMITED WARRANTY.

Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software.

4. DISCLAIMER OF WARRANTY.

UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

5. LIMITATION OF LIABILITY.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose.

6. TERMINATION.

This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Upon Termination, you must destroy all copies of Software.

7. EXPORT REGULATIONS.

All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

8. U.S. GOVERNMENT RESTRICTED RIGHTS.

If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

9. GOVERNING LAW.

Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

10. SEVERABILITY.

If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

11. INTEGRATION.

This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations, and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

For inquiries please contact: Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303

JAVA™ 2 RUNTIME ENVIRONMENT VERSION 1.3 SUPPLEMENTAL LICENSE TERMS

These supplemental license terms (“Supplemental Terms”) add to or modify the terms of the Binary Code License Agreement (collectively “Agreement”). Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Agreement, or in any license contained within the Software.

1. LICENSE TO DISTRIBUTE.

Subject to the terms and conditions of this Agreement, including, but not limited to, Section 2 (Redistributables) and Section 3 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license to reproduce and distribute the Software in binary code form only, provided that you (i) distribute the Software complete and unmodified, only as part of and for the sole purpose of running your Java applet or application (“Program”) into which the Software is incorporated, (ii) do not distribute additional software intended to replace any component(s) of the Software, (iii) do not remove or alter any proprietary legends or notices contained in the Software, (iv) only distribute the Program subject to a license agreement that protects Sun’s interests consistent with the terms contained in this Agreement, and (v) agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts, and/or expenses (including attorneys’ fees) incurred in connection with any claim, lawsuit, or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

2. REDISTRIBUTABLES.

In addition to the license granted in Paragraph 1 above, Sun grants you a non-exclusive, non-transferable, limited license to reproduce and distribute, only as part of Software, those files specifically identified as redistributable in the Software “README” file (“Redistributables”) provided that: (a) you distribute the Redistributables complete and unmodified (unless otherwise specified in the applicable README file), and only bundled as part of the JavaTM applets and applications that you develop (“Programs”); (b) you do not distribute additional software intended to supersede any component(s) of the Redistributables; (c) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables; (d) you only distribute the Redistributables pursuant to a license agreement that protects Sun’s interests consistent with the terms contained in the Agreement; and (e) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts, and/or expenses (including attorneys’ fees) incurred in connection with any claim, lawsuit, or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

3. JAVA TECHNOLOGY RESTRICTIONS.

You may not modify the Java Platform Interface (“JPI”, identified as classes contained within the “java” package or any subpackages of the “java” package) by creating additional classes within the JPI or otherwise causing the addition to or modification of the classes in the JPI. In the event that you create an additional class and associated API(s) which (i) extends the functionality of a Java platform, and (ii) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. You may not create or authorize your licensees to create additional classes, interfaces, or subpackages that are in any way identified as “java”, “javax”, “sun”, or similar convention as specified by Sun in any class file naming convention.

4. TRADEMARKS AND LOGOS.

You acknowledge and agree as between you and Sun that Sun owns the Java trademark and all Java-related trademarks, service marks, logos, and other brand designations including the Coffee Cup logo and Duke logo (“Java Marks”), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Java Marks inures to Sun’s benefit.

5. SOURCE CODE.

Software may contain source code that is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed.

6. TERMINATION.

Sun may terminate this Agreement immediately should any Software become, or in Sun’s opinion be likely to become, the subject of a claim of infringement of a patent, trade secret, copyright, or other intellectual property right.

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
    - Error messages/log files
    - Troubleshooting performed prior to contacting Symantec
    - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manual

Contents

Chapter 3 Creating rules

Chapter 4 Using pRules

Chapter 5 Controlling access to protected computers

Chapter 6 Customizing intrusion detection

Chapter 7 Configuring client settings

Chapter 8 Managing client log data

Index

Chapter 1

Implementing Symantec Client Firewall

This chapter includes the following topics:

- About Symantec Client Firewall
- System requirements
- Installing Symantec Client Firewall client components

About Symantec Client Firewall

Symantec Client Firewall protection includes a client application to protect workstations and administration programs to simplify the management of protection.

Symantec Client Firewall includes three key components:

- Symantec Client Firewall client
- Symantec Client Firewall Administrator
- Symantec Packager

About Symantec Client Firewall client

With Symantec Client Firewall client, you create and enforce firewall policies that are derived from usage requirements for workstations. At any time, you can roll out more restrictive policies, including complete blocking, in response to attacks or other unwanted behavior.

Symantec Client Firewall client includes data and default rules to validate and permit well-known applications to access the Internet. At the same time, the rules block the activity of known Trojan horse programs, which masquerade as useful programs while performing unwanted back-door activity. Symantec provides updated data as necessary.

You enable or disable intrusion detection signatures based on vulnerability exposure. Symantec supplies intrusion detection signatures, which are known, detectable network traffic patterns that are derived from previously identified exploits, attacks, or anomalous activities that are outside of expected behavior or traffic. Symantec provides updated signatures as necessary.

About Symantec Client Firewall Administrator

Symantec Client Firewall Administrator is a standalone application used to configure client policies. Symantec Client Firewall Administrator includes most of the settings needed to configure firewalls, and the means to save the settings in a policy package that is rolled out to the clients.

With Symantec Client Firewall Administrator, you can do the following:

- Configure and edit firewall rules and client settings for multiple installations of the client.
- Save different configurations in multiple packages for roll out to different groups of firewalls.
- Import configuration data from a local firewall, and save the data to a rules package.
- Display and configure firewall rules by the following rule categories:
    - System-Wide rules
    - Application rules
    - Trojan Horse rules
- Verify the authenticity of applications that access the Internet.
- Configure client settings, which include the following:
    - User access level: Determines the extent to which users can modify firewall rules, configure the firewall, and view firewall data.
    - Degree of firewall protection: Protects against potential Internet threats, such as ActiveX controls, Java applets, and communications aimed at unused ports.
    - Intrusion Detection: Monitors inbound and outbound network communications for packet patterns that are characteristic of an attack.
    - Accessibility: Specifies client access options through the firewall.
    - Blocking: Determines blocking of ports, fragmented IP packets, and the Internet Group Membership Protocol (IGMP).
- Create trusted and restricted zones for IP addresses.

About Symantec Packager

Symantec Packager lets you create, modify, and build custom installation packages that you distribute to target systems. Using Symantec Packager, you can tailor installations to fit your corporate environment, building packages that contain only the features and settings that your users need.

Symantec products included in installation packages are protected by copyright law and the Symantec license agreement. Distribution of packages requires a license for each user who installs the package.

You can also create custom commands in conjunction with a supported program, such as Symantec Client Firewall client, to create and roll out firewall policy packages.

System requirements

A number of hardware and software requirements are necessary to install and run Symantec Client Firewall client components.

Symantec Client Firewall client requirements

The Symantec Client Firewall client has the following minimum requirements:

- Windows 98/98 SE/Me; Windows NT 4.0 Workstation with Service Pack 6a; Windows 2000 Professional; Windows XP Home/Professional

  Server operating systems, such as Windows 2000 Server, are not supported.
- 64 MB of RAM minimum
- 70 MB disk space
- Internet Explorer 5 or later
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

Note: Symantec firewall product versions other than Symantec Client Firewall 5.x, Symantec Desktop Firewall version 2.01, Norton Personal Firewall version 2.5, and Norton Personal Firewall version 2002 must be uninstalled prior to installation.

Symantec Client Firewall Administrator requirements

The Symantec Client Firewall Administrator has the following minimum requirements:

- Windows NT 4.0 with Service Pack 6a; Windows 2000; Windows XP
- 64 MB of RAM minimum
- 15 MB disk space
- Microsoft Internet Explorer 5.5 Service Pack 2 or later
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

- Java Runtime Environment 1.4.0 (Installed with the Symantec Client Firewall Administrator)
- 115 MB for Java Runtime Environment 1.4.0 install

Symantec Packager requirements

Symantec Packager runs only on Microsoft 32-bit operating systems and has the following system requirements:

- Supported operating systems:
  - Windows NT Workstation 4.0/Server 4.0 with Service Pack 6a
  - Windows 2000 Professional/Server with Service Pack 2
  - Windows XP Professional
- Microsoft Internet Explorer 5.5 or later
- Windows Installer 2.0

  If Windows Installer 2.0 is not present, Symantec Packager installs it during installation.
- Pentium II 300 processor (or faster)
- 64 MB RAM (128 MB recommended)
- 60 MB disk space
- CD-ROM or DVD-ROM drive

System requirements for installation packages

Although Symantec Packager runs only on Windows NT/2000/XP operating systems, packages that you create using Symantec Packager can be installed on the following operating systems:

- Windows NT 4.0 with Service Pack 6a
- Windows 98
- Windows Millennium Edition (Me)
- Windows 2000
- Windows XP Home Edition/Professional Edition

The Deployment Depot component and Package Deployment Tool can only be used for deployment to Windows NT/2000/XP computers.

Installing Symantec Client Firewall client components

To get the Symantec Client Firewall client and administration software up and running, you must install several separate components:

- Symantec Client Firewall Administator
- Symantec Packager
- Symantec Client Firewall client

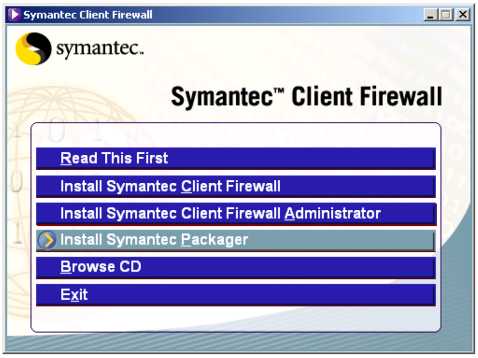
Installing Symantec Client Firewall Administrator

When you install Symantec Client Firewall Administrator, the Java Runtime Environment is installed automatically if it is not already present.

To install Symantec Client Firewall Administrator

1 Insert the Symantec Client Firewall CD into the CD-ROM drive.

If the installation program does not start automatically, run Setup.exe from the root folder of the CD.


Symantec Client Firewall
symantec.
Symantec™ Client Firewall
Read This First
Install Symantec Client Firewall
Install Symantec Client Firewall Administrator
Install Symantec Packager
Browse CD
Exit

2 In the Symantec Client Firewall window, click **Install Symantec Client Firewall Administrator**.

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

Installing Symantec Packager

By default, Symantec Packager is installed to the \Program Files \Symantec\Packager folder.

To install Symantec Packager

1. Insert the Symantec Client Firewall client CD into the CD-ROM drive.

   If the installation program does not start automatically, run Setup.exe from the root folder of the CD.
2. In the Symantec Client Firewall Installation window, click **Install Symantec Packager**.
3. Follow the on-screen instructions to complete the installation.

Installing Symantec Client Firewall client

Symantec Client Firewall client can be installed from the distribution CD or the SCF.exe installation package can be run directly.

To install Symantec Client Firewall client

1. Insert the Symantec Client Firewall client CD into the CD-ROM drive.

   If the installation program does not start automatically, run Setup.exe from the root folder of the CD.
2. In the Symantec Client Firewall client Installation window, click **Install Symantec Client Firewall**.
3. Follow the on-screen instructions to complete the installation.

The SCF.exe installation package is located on the distribution CD in the \SCF folder. SCF.exe can be deployed and run by any convenient method on a client computer.

Deploying Symantec Client Firewall client using the Package Deployment Tool

The Package Deployment Tool, which is part of Symantec Packager, can be used to deploy Symantec Client Firewall client to remote Windows NT/2000/XP computers.

For detailed information about the Package Deployment Tool, refer to the *Symantec Packager Implementation Guide* in the Docs folder on the Symantec Client Firewall CD.

To deploy Symantec Client Firewall client using the Package Deployment Tool

1. In the folder in which Symantec Packager is installed, launch PackageDeploy.exe.

   By default, Symantec Packager is installed in \Program Files\Symantec\Packager.

2. In the Package Deployment window, in the File deployment sequence group, click **Add**.

3. In the Open dialog box, locate the SCF.exe installation package, then click **Open**.

4. In the Target computers group, do one of the following:

   - In the Enter computer name or IP address text box, type the computer name or IP address for the target computer, then click **Add**.
   - Click **Search** to browse for computers, select them, then click **OK**.

     It may take a few moments for the Select Computers dialog box to appear.
   - Click **Import List** to use a preconfigured list of target computers. Select the file, then click **Open**.

5. In the Package Deployment Tool, click **Deploy**.

6. In the Deployment Credentials dialog box, add the requested information, then click **OK**.

   The Deployment Status dialog box reports the progress of the deployment.

Chapter 2

Managing policies

This chapter includes the following topics:

- About policies
- Configuring policies
- Distributing policies

About policies

Centralized firewall management lets you provide the maximum amount of firewall protection while minimizing maintenance and client user involvement. This is achieved by rolling out Symantec Client Firewall client policies, which are sets of configured firewall rules and settings to govern firewall operation.

Policy management lets you do the following:

- Customize Symantec Client Firewall clients to better accommodate your organization's needs.
- Configure the Symantec Client Firewall clients differently for different groups, departments, or users in your organization.
- Update firewall rules to accommodate changing conditions on your corporate intranet and threats on the Internet.

Policies, which are native .xml or compressed .cfp (Client Firewall Policy) files, contain all of the firewall rules, intrusion detection signatures, and configuration settings for a given policy.

Policy components

Key components of a firewall policy include the following:

- Rules
- pRules
- Zones
- IDS exclusions
- Client settings

Rules

Firewall rules include System-Wide, Application, and Trojan Horse rules.

System-Wide firewall rules apply to all of the network communications of Symantec Client Firewall clients that access the Internet. These rules are based on port numbers and IP addresses rather than specific applications or Trojan horses, which are handled separately.

Application rules permit or block communications between specific client applications and the Internet. You can configure an application rule that is specific to communications on a particular port or address, or one that applies to multiple IP ports and addresses.

Trojan horses are malicious programs that are disguised as useful applications. Symantec Client Firewall Administrator Trojan Horse rules examine the network communications of Symantec Client Firewall clients that access the Internet, looking for signs of these malicious programs. If one is detected, the firewall rule takes immediate action against this type of threat.

See "About rules" on page 36.

pRules

Application rules are created in the registry of the client when the firewall policy is rolled out. If all clients are similarly configured, this is an efficient method of providing uniform protection. If client workstations use widely divergent sets of applications, pRules are appropriate.

With pRules, or potential rules, data about applications is installed on the client workstation, but the rules themselves are not created in the registry. When an application first attempts to access the Internet, the pRule is invoked. If the application matches the pRule criteria, then a new application rule is created from the pRule data in the registry of the client workstation.

See "About pRules" on page 54.

Zones

With Zones, you can identify computers that you can trust, and those that you want to restrict from accessing a client computer.

- Computers that are in the Trusted Zone are not regulated by Symantec Client Firewall client, and have total access to the client computer.
- Computers that are in the Restricted Zone are prevented from accessing client computers.
- Computers that are not placed in any Zone are regulated by all other settings of the firewall policy.

Use the Trusted Zone to list computers on your local network with which you need to share files and printers. Add computers to the Restricted Zone that have attempted to attack computers in your organization. The Restricted Zone provides the highest level of protection provided by Symantec Client Firewall. Clients cannot interact with any computers that are in the Restricted Zone.

See "About Zones" on page 70.

IDS exclusions

Intrusion detection is based on signatures. A signature defines or describes a network traffic pattern. Intrusion Detection System (IDS) signatures detect traffic patterns that are derived from previously detected exploits or attacks, or an anomalous pattern that is outside of the realm of expected traffic patterns and could be destructive.

Symantec supplies and periodically updates the set of signatures that are monitored.

Because each signature has a small corresponding resource impact, you can exclude specified signatures from being processed. For example, you may not need protection against certain attack signatures because your environment does not contain the systems or components that they are known to attack. Once you exclude an IDS attack signature, the signature can cross the firewall and is not logged. You can also exclude specific IP addresses for a signature. For example, the addresses may already be specified for automatic blocking by the firewall or it is possible that the threat from an IP address has been eliminated, and you want information from the IP to flow across the firewall.

See "About the Intrusion Detection System (IDS)" on page 76.

Symantec Client Firewall client settings

You can customize client settings for each firewall policy to enable or disable specific components of firewall protection, which include the following:

- User access level: Determines the extent to which users can modify firewall rules, configure firewall behavior outside of administrator control, and view firewall data
- Degree of firewall protection: Protects against potential Internet threats, such as ActiveX controls, Java applets, and communications aimed at unused ports
- Intrusion Detection: Monitors inbound and outbound network communications for packet patterns that are characteristic of an attack
- Privacy control: Protects confidential information, blocks cookies, enforces browser privacy, and forces secure communications (HTTPS)
- Blocking: Determines blocking of ports, fragmented IP packets, and the IGMP protocol

In addition, you specify whether firewall icons appear on the workstation.

See "About client configuration settings" on page 84.

About Symantec Client Firewall Administrator

Symantec Client Firewall Administrator is a policy configuration tool for tuning, customization, and setting user-level settings. It is a separate application with its own user interface for use by firewall and system administrators. You use Symantec Client Firewall Administrator to create or to import policy files for modification, then save the policy files for distribution to Symantec Client Firewall clients.

Configuring policies

Typically, to prepare a policy, you install the Symantec Client Firewall client on a representative computer for a group of users. For example, members of the accounting group may require different protection settings than the art department. Use this representative computer to run all applications that access the Internet in as varied a trial as possible. The computer's firewall settings are then imported into Symantec Client Firewall Administrator. You can create as many different policies for rollout as necessary.

The most efficient method to create firewall policies is to install both the firewall and Symantec Client Firewall Administrator on the same computer.

Note: To use a firewall installation as the basis for creating a policy, do not use a computer that is also running the Symantec System Center. A Symantec System Center computer requires firewall rules that are not appropriate for client workstations.

From Symantec Client Firewall Administrator, you can save a policy for distribution in one of two formats:

- .xml: Stores all configuration information except IDS exclusion data in a native .xml format file. If IDS exclusion settings are not part of a policy distribution, the .xml format is significantly smaller in size than the corresponding .cfp format file.
- .cfp (Client Firewall Policy): Stores all configuration information in a compressed policy file. If a policy contains Intrusion Detection System settings, use the .cfp format.

How you import a policy into Symantec Client Firewall Administrator for configuration depends on the following:

- Whether you want to use configuration data from the Active Client, which is the firewall application running on the same computer as Symantec Client Firewall Administrator. When you import data from the Active Client, you import its current configuration settings.
- Whether to import rule and settings information from existing policy files.

When you import settings from the Active Client, Intrusion Detection System settings are not included. This is because importing Active Client data is done through an intermediate .xml file. Only .cfp files contain IDS settings.

Creating a policy with Symantec Client Firewall Administrator

Customizing a policy with Symantec Client Firewall Administrator requires the following actions:

- Opening an existing policy for modification or creating an entirely new policy in Symantec Client Firewall Administrator.
- Importing one or more groups of policy settings from other policy files or the Active Client.
- Customizing the policy within Symantec Client Firewall Administrator to add, modify, or delete Rules, pRules, Zones, IDS Exclusions, and Client Settings.
- Exporting the policy file to the Active Client for testing.
- Saving the modified policy as a .cfp or .xml file for distribution to firewall installations.

The Active Client is the local instance of Symantec Client Firewall client that is installed on the same computer as Symantec Client Firewall Administrator. You can use the Active Client to help develop, test, and clarify the rules and configuration settings of a policy package.

Create policies

When importing a policy, you have the option of importing all settings categories or selected settings categories. This convenience lets you build a new policy using existing settings that do not require change and configure only those categories that do require change.

To create an entirely new policy

- In Symantec Client Firewall Administrator, on the File menu, click **New**.

New policies are created from the ScfaDefaultPolicy.cfp template.

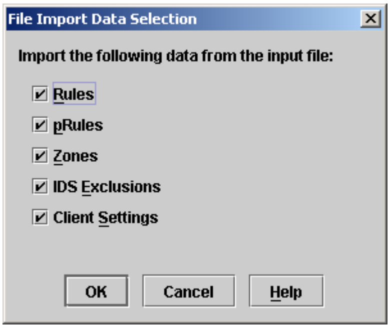
To open an existing policy

1. In Symantec Client Firewall Administrator, on the File menu, click **Open**.
2. Navigate to the .xml or .cfp policy file.
3. Click **Open**.

The initial firewall policy that is installed with the firewall is copied to the \Program Files\Symantec\Symantec Client Firewall Administrator\Data folder on the computer on which Symantec Client Firewall Administrator is installed. The policy is called ScfInitialPolicy.cfp.

To import data from an existing policy into Symantec Client Firewall Administrator

1. In Symantec Client Firewall Administrator, on the File menu, click **Import**.



File Import Data Selection

Import the following data from the input file:

☑ Rules
☑ pRules
☑ Zones
☑ IDS Exclusions
☑ Client Settings

2. In the File Import Data Selection dialog box, select the categories of configuration data that you want to import.
3. Click **OK**.
4. In the Open dialog box, navigate to the policy file that contains the data you want to import.
5. Click **Open**.

When importing settings from the Active Client, IDS Exclusions settings are not available.

To import policy data using the Active Client

1. In Symantec Client Firewall Administrator, on the File menu, click **Import from Active Client.**
2. In the File Import Data Selection dialog box, select the categories of configuration data that you want to import.
3. Click **OK.**
4. In the Open dialog box, navigate to the policy file that contains the data you want to import.
5. Click **Open.**

Saving a policy

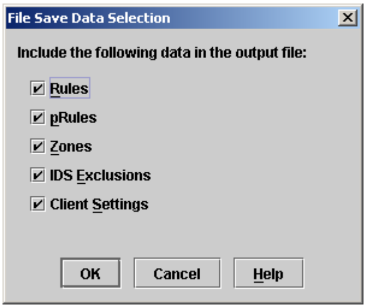
After you finish configuring a policy, you save it for later distribution to Symantec Client Firewall clients.

Save a policy

By default, policy files are saved to the \Program Files\Symantec\Symantec Client Firewall Administrator\Data folder on the computer on which Symantec Client Firewall Administrator is installed. You can, however, choose to save in any location.

To save an imported policy to the same policy file name

1. In Symantec Client Firewall Administrator, on the File menu, click **Save.**



File Save Data Selection

Include the following data in the output file:

☑ Rules
☑ pRules
☑ Zones
☑ IDS Exclusions
☑ Client Settings

2. In the File Save Data Selection dialog box, select the categories of configuration data that you want the policy to contain.
3. Click **OK.**

   Only the selected categories are saved.

With the Save As option, you can specify whether to save the policy as an .xml or .cfp policy file.

To save an imported policy to a new policy file name

1. In Symantec Client Firewall Administrator, on the File menu, click **Save As.**
2. In the File Save Data Selection dialog box, select the categories of configuration data that you want the policy to contain.
3. Click **OK.**

   Only the selected categories are saved.
4. In the Save dialog box, specify the location and file name for the policy.
5. In the Save dialog box, in the Files of Type drop-down list, select one of the following file types:
   - Policy Packages (*.cfp)
   - XML files (*.xml)
6. Click **Save.**

Exporting policy data to the Active Client

If you want to use the Symantec Client Firewall Administrator Active Client to test and customize a policy that was created in Symantec Client Firewall Administrator, you must export the policy data.

Note: Make sure to install a Symantec Client Firewall client on the same computer as Symantec Client Firewall Administrator before using the Export to Active Client option.

To export policy data to the Active Client

1. In Symantec Client Firewall Administrator, on the File menu, click **Export to Active Client.**
2. In the Export Data Selection dialog box, select the categories of configuration data that you want to export.
3. Click **OK.**

   Zones and IDS Exclusions are always checked by default, whether or not information was added to the categories. If the Zones and IDS Exclusions contain no configuration information and are left checked, any information in those categories on the Active Client is erased upon export.

Distributing policies

Policy distribution is the process of rolling out a new policy to one or more groups of Symantec Client Firewall client. Once a policy is rolled out, all client firewalls that receive the policy are updated to the new set of Rules, pRules, Zones, IDS exclusions, and Client Settings that are saved in the policy.

Distribution mechanisms include the following:

- Fio.exe policy import/export tool
- Policy package created with Symantec Packager
- Web-based policy package distribution
- Login scripts
- Third-party distribution tools

How a policy update affects rules and settings

When a policy update is distributed to the Symantec Client Firewall client, the previous rules and settings used by clients are modified by those in the new policy according to the following precedence rules:

- If the new policy includes rules, all existing Admin type firewall rules are replaced by the Admin type rules in the new policy.
- All existing client settings are replaced by those in the new policy.
- Zone data is replaced by the Zone data in the new policy.
- Intrusion Detection System exclusion data is replaced by the IDS exclusion data in the new policy.
- All pRules are overwritten.
- Existing User type rules on a Symantec Client Firewall client are neither deleted nor replaced.

  For any client, if the user access level supports configuring User type rules, the user can keep the existing User rules, delete them, or reconfigure them.

Note: A policy may include only subsets of data from one or more of the policy categories (Rules, pRules, Zones, IDS Exclusions, Client Settings). If a category is not included in the policy update, the existing client data for that category or group of categories is preserved.

Using the policy file import/export utility

Fio.exe is command-line utility that is installed with the Symantec Client Firewall client. You can use it to import an .xml file containing the policy update into a single, local firewall. Additionally, you can use Fio.exe to export the policy of the firewall to an .xml file. Fio.exe must be run on the client computer.

Note: The exported policy does not include IDS and IP automatic blocking exclusions, which are not saved in an .xml file.

The command syntax for the file import/export utility is as follows:

fio.exe i | o [path]package_filename

where path is the optional full path to the policy file, and package_filename is the .xml policy file. When Fio.exe is run, it locates the Symantec Client Firewall client to update automatically.

Table 2-1 describes the parameters.

Table 2-1 File import/export utility parameters

Parameter	Description
i	Imports the specified policy
o	Exports the rules and configuration settings from the current Symantec Client Firewall client to an .xml file

For example, to update a Symantec Client Firewall client with a policy named NewAdminPkg.xml in the directory C:\Admin\Packages, type the following at a command prompt:

fio i c:\Admin\Packages\NewAdminPkg.xml

To export a policy to be named NewAdminPkg.xml to the directory C:\Admin\Misc, where the policy contains the rules and settings of the current Symantec Client Firewall client, type the following at a command prompt:

fio o c:\Admin\Packages\NewAdminPkg.xml

Creating a policy file package

Using Symantec Packager, you can create a policy package to update Symantec Client Firewall clients.

Create a package

The package contains one of the following:

- The policy file for distribution and the Fio.exe utility.
- The policy file for distribution and a command to launch the local copy of Fio.exe.

  This is the preferred method, but will only work if the location of Fio.exe is known on the Symantec Client Firewall client.

Note: Fio.exe exports User rules as well as Admin rules; therefore, packages created with Fio.exe may contain User rules.

To create a policy package with Fio.exe

1. In Symantec Packager, on the Configure Products tab, click **File** > **New Custom Command**.
2. In the Command Editor dialog box, on the Parameters tab, select **Description**, then click **Modify**.
3. Type a description for the package, then click **OK**.
4. On the Parameters tab, select **Command line**, then click **Modify**.
5. In the Command Line Specification dialog box, in the Command line and switches text box, type the command you want to run on the Symantec Client Firewall client.

   For example, type the following:

   fio.exe i newpolicy.xml
6. Click **OK.**
7. On the Parameters tab, in the Add files group, click **Add**.
8. In the Open dialog box, navigate to select Fio.exe, then click **Open**.
9. In the Open dialog box, navigate to select the policy file (for example, newpolicy.xml), then click **Open**.

10 On the Parameters tab, click **Build**.

11 In the Save As dialog box, specify the location and name (for example, newpolicy) to create the policy package, then click **Save**.

The package is saved as both a .pcg file for edit in Symantec Packager and as an executable policy package for distribution to Symantec Client Firewall clients.

If you know the location of Fio.exe on the Symantec Client Firewall client, you do not have to include Fio.exe in the package.

To create a policy package without Fio.exe

1 In Symantec Packager, on the Configure Products tab, click **File** > **New Custom Command**.

2 In the Command Editor dialog box, on the Parameters tab, select **Description**, then click **Modify**.

3 Type a description for the package, then click **OK**.

4 On the Parameters tab, select Command line, then click **Modify**.

5 In the Command Line Specification dialog box, in the Command line and switches text box, type the command you want to run on the Symantec Client Firewall client.

For example, type the following, then click **OK**:

c:\Program Files\Symantec Client Firewall\fio.exe i newpolicy.xml

6 On the Parameters tab, in the Add files group, click **Add**.

7 In the Open dialog box, navigate to select the policy file (for example, newpolicy.xml), then click **Open**.

8 On the Parameters tab, click **Build**.

9 In the Save As dialog box, specify the location and name (for example, newpolicy) to create the policy package, then click **Save**.

The package is saved as both a .pcg file for edit in Symantec Packager and as an executable policy package for distribution to Symantec Client Firewall clients.

The policy package is an executable file that can be distributed by a variety of methods, including the following:

- The Deployment Depot component of Symantec Packager, which can be used to roll out the package to Windows NT/2000/XP Symantec Client Firewall clients.
- Web-based policy package distribution.
- Login scripts.
- Third-party distribution tools.

See the Symantec Packager documentation for distribution details.

Chapter 3

Creating rules

This chapter includes the following topics:

- About rules
- Manually creating a firewall rule
- Automatic creation of rules on the client
- Enabling and disabling logging for a firewall rule
- Combining firewall rules
- Testing application rules

About rules

Rules are the components of a policy that control how the Symantec Client Firewall client protects your network from malicious incoming traffic, applications, and Trojan horses. The firewall automatically checks all incoming and outgoing data for a computer in the network against these rules. It compares this information against the sets of conditions specified in its rules.

Rules are ordered in a sequential list, from highest to lowest priority. Incoming or outgoing data is compared against this rules list, one rule at a time, from the highest priority rule to the lowest priority rule.

A firewall rule executes when its conditions are met by incoming or outgoing data. Once a rule is invoked, the firewall action specified by the rule is taken. Subsequent rules of lower priority in the rules list are not evaluated.

Upon execution, a rule triggers one of the following actions when its criteria are matched:

- Permits the transmission to complete
- Blocks the transmission
- Monitors and logs the transmission

The Symantec Client Firewall client automatically creates rules for a client computer as it communicates with the Internet, either silently (with the Internet Access Control setting enabled) or by prompting the user. Firewall administrators can also create new firewall rules manually using Symantec Client Firewall Administrator. They can then distribute these rules to clients in policies.

The Symantec Client Firewall client automatically creates many of the rules that your network needs. You can also manually add your own rules to a policy using Symantec Client Firewall Administrator.

Rule categories

Rules are classified into the following three categories:

- System-Wide rules: Apply to all network communications of firewalls accessing the corporate network or Internet. For example, the rules that provide protection against someone connecting to a Symantec Client Firewall client using Microsoft networking are System-Wide rules.
- Application rules: Apply to a client application's access to the Internet. Use Application rules for a Symantec Client Firewall client that needs access to the corporate network or Internet.
- Trojan Horse rules: Apply to a category of malicious programs that are disguised as useful programs. When a Trojan horse runs, it appears to be performing a helpful function, but it is actually damaging the host computer's operating system and may damage other connected network resources.

  The Symantec Client Firewall client supplies a set of Trojan Horse rules that apply to the characteristics of known Trojan horse threats.

Rule types

Rules are categorized as either Admin rules or User rules. Table 3-1 describes the meaning of the categorization and how Admin and User rules are managed by the different user access levels.

Table 3-1 Rule types and descriptions

Rule type	Description
Admin	■ Created and configured by users with an access level of Administrator and rolled out to groups of clients. ■ Can be viewed by users with Normal access level; cannot be viewed by users with Restricted access level. ■ When a new policy is rolled out to clients, all existing Admin rules on the clients are overwritten. ■ Any System-Wide rules, Application rules, and Trojan Horse rules created with Symantec Client Firewall Administrator are defined as Admin rules.

Table 3-1 Rule types and descriptions

Rule type	Description
User	■ Created and configured using the Symantec Client Firewall client user interface by users with an access level of Administrator or Normal. ■ Maintained on an individual client. ■ Cannot be configured or viewed by users with a Restricted access level. ■ When a new policy is rolled out to clients, all existing User rules on clients are preserved. ■ Not editable with Symantec Client Firewall Administrator.

Rule processing order

Rules are processed in an order based on their types and the users who created them. Rules are evaluated one after the other until the conditions specified in a rule are met. When the first match occurs, the action specified by the rule is triggered and all further rule evaluation stops.

Within a rule category (System-Wide, Application, or Trojan Horse), Admin rules have priority and are always processed before User rules.

The order of priority for rule categories is shown in Table 3-2.

Table 3-2 Rule processing priority

Priority	Rule category	User type
First	System-Wide	Admin
Second	Application	Admin
Third	System-Wide	User
Fourth	Application	User
Fifth	Trojan Horse	Admin
Sixth	Trojan Horse	User

Rules can be reordered only within their own priority categories.

The firewall administrator may want to order the rules within priority categories so that evaluation occurs in the most logical sequence. Order rules so that they are evaluated according to exclusivity, with the most restrictive rules evaluated first and the most general rules evaluated last.

Default System-Wide rules

A number of rules are predefined and enabled when you install the Symantec Client Firewall client. The default System-Wide rules for the Symantec Client Firewall client are listed in Table 3-3.

Table 3-3 Default System-Wide rules

Rule	Traffic allowed/user protected from	Consequences of changing rule state
Default Inbound ICMP	Allows locally generated network probing (ping, traceroute); allows responses to come back to the computer.	Ping, traceroute will fail.
Default Outbound ICMP	Allows locally generated network probing (ping, traceroute); allows queries to go out.	Ping, traceroute will fail.
Default Inbound DNS	Receives responses to DNS requests.	DNS will fail. For more security, change this rule to allow the DNS to and from the user's primary DNS only.
Default Outbound DNS	Allows DNS queries.	DNS will fail. For more security, change this rule to allow the DNS to and from the user's primary DNS only.
Default Inbound NetBIOS Name	Prevents lookup of the computer's name via NetBIOS.	Name profiling can be done via NetBIOS.
Default Inbound NetBIOS	Blocks Windows file and print sharing.	Some NetBIOS file and print sharing information will be mappable.
Default Outbound NetBIOS	Allows Windows file and print sharing on other servers (the client can access someone else's share).	Prevents and prompts on attempts to connect to someone else's file share.
Default Inbound Loopback	Allows localhost communication.	A significant number of programs which use IP to communicate between processes on the same computer will fail or prompt.

Table 3-3 Default System-Wide rules

Rule	Traffic allowed/user protected from	Consequences of changing rule state
Default Outbound Loopback	Allows localhost communication.	A significant number of programs which use IP to communicate between processes on the same computer will fail or prompt.
Block Access to Secure Sites	Keyed to the Enable secure HTTP connections option in Privacy Control on the Symantec Client Firewall client.	The Enable secure HTTP connections option in Privacy Control on the Symantec Client Firewall client will stop working.
Default Block Inbound and Outbound ICMP	Blocks any ICMP not permitted by the default permit rules.	Ping and traceroute will fail.
Block Windows File Sharing	Blocks Windows file and print sharing. The intent of this rule is to provide a simple switch for turning on file and printer sharing.	Attempts to connect to this computer for file and printer sharing will fail or prompt the user.
Default Inbound Bootp	Allows a response to a request for a dynamic IP address assignment via BootP or DHCP.	Computers without a static IP address will not be able to get an IP address assigned.
Default Outbound Bootp	Allows requests for a dynamic IP address assignment via BootP or DHCP.	Computers without a static IP address will not be able to get an IP address assigned.
Default Block Microsoft Windows 2000 SMB	Blocks SMB, which can be used as an alternate file and print sharing mechanism.	SMB connection attempts will cause alerts or be permitted.
Default Block EPMAP	Blocks EPmap, which can be used to remotely configure some services.	EPmap connections will cause alerts or be permitted.

Elements of a rule

The Symantec Client Firewall Administrator lets you specify the specific conditions that must be present for the rule to be triggered on the firewall client and the action that will be taken.

Action options

Action options let you specify whether the rule permits, blocks, or monitors the type of network communication defined within the rule.

Table 3-4 describes the available Action options.

Table 3-4 Action options

Option	Description
Permit	Allows communication of this type to take place.
Block	Prevents communication of this type from taking place.
Monitor	Updates the Firewall tab in the Symantec Client Firewall client Event Log. Rule processing then continues until a match is found. If there is no match, the communication is either blocked by default or an Internet Access Control alert appears.

The resulting action of configuring a rule to monitor rather than permit or block depends on how a few client settings are configured. For example, if Client Firewall Level is set to High, Access Control Alerts is set to Enable, and Automatic Internet Access Control is set to Enable, Symantec Client Firewall automatically and transparently creates a rule that permits known applications to access the Internet on the client computer. Other combinations of client settings cause the firewall to transparently block traffic that is configured with a Monitor action, or cause the firewall to prompt users to decide whether to permit or block the traffic.

Table 3-5 shows the resulting actions that the firewall takes when the Client Firewall Level is set to High, along with possible combinations of enabled or disabled Access Control Alerts and Automatic Internet Access Control settings.

Table 3-5 Monitor action results with Client Firewall Level set to High

Access Control Alerts status	Automatic Internet Access Control status	Resulting firewall action
Disabled	Disabled	Block.
Enabled	Disabled	Permit or block (user choice).

Table 3-5 Monitor action results with Client Firewall Level set to High

Access Control Alerts status	Automatic Internet Access Control status	Resulting firewall action
Disabled	Enabled	Permit. Permit rule is automatically created for known applications.
Enabled	Enabled	Permit or block for unknown applications (user choice). Permit rule is automatically created for known applications.

Table 3-6 shows the resulting actions that the firewall takes when the Client Firewall Level is set to Medium, along with possible combinations of enabled or disabled Access Control Alerts and Automatic Internet Access Control settings.

Table 3-6 Monitor action results with Client Firewall Level set to Medium

Access Control Alerts status	Automatic Internet Access Control status	Resulting firewall action
Disabled	Disabled	Permit.
Enabled	Disabled	Permit.
Disabled	Enabled	Permit. Permit rule is automatically created for known applications.
Enabled	Enabled	Permit. Permit rule is automatically created for known applications.

See “About client configuration settings” on page 84.

Note: When using a block all rule that prevents network traffic from getting through to clients, two additional permit rules must be enabled and applied before the block all rule. These two rules are the Inbound BootP and Default Outbound BootP System-Wide rules that are supplied by default with Symantec Client Firewall client.

This action is necessary so that DHCP will function properly, renewing IP addresses on computers affected by the block all rule and reestablishing communication between those computers and the network when the block all rule is disabled.

Direction options

Direction options let you specify whether the rule applies to inbound network communication, outbound network communication, or network communication in both directions.

Table 3-7 describes the available Direction options.

Table 3-7 Direction options

Option	Description
Connections to other computers	The rule applies to outbound connections from your computer to another computer.
Connections from other computers	The rule applies to inbound connections from another computer to your computer.
Connections to and from other computers	The rule applies to inbound connections as well as outbound connections.

Computers options

Computers options let you specify the computers and network adapters to which a rule applies. The computers that you specify are computers with which you want to control communications.

Table 3-8 describes the available Computers options.

Table 3-8 Computers options

Option	Description
Any computer	The rule applies to all computers.

Table 3-8 Computers options

Option	Description
Computer list specified below	The rule applies to one computer, to multiple computers with IP addresses in a specified range, or to multiple computers in a domain.
Network Adapters	The rule applies to a specific network adapter in your computer. The IP address of the network adapter to which the rule should apply is specified.

Protocol options

Protocol options let you specify the communications protocols that a rule controls.

Table 3-9 describes the available Protocol options.

Table 3-9 Protocol options

Option	Description
TCP	The rule applies to Transmission Control Protocol (TCP) communications.
UDP	The rule applies to User Datagram Protocol (UDP) communications.
TCP and UDP	The rule applies to both TCP and UDP communications.
ICMP	The rule applies to Internet Control Message Protocol (ICMP) communications. ICMP applies to System-Wide rules and Trojan Horse rules only.

Ports options

Ports options let you specify the types of communications, or ports, that are controlled by a rule.

Table 3-10 describes the available Ports options.

Table 3-10 Ports options

Option	Description
All types of communications (all ports)	The rule applies to communications using any port.

Table 3-10 Ports options

Option	Description
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.

Tracking options

Tracking options let you specify whether the program should notify you or create an Event Log entry when a network communication event matches the criteria set for this rule.

Table 3-11 describes the available Tracking options.

Table 3-11 Tracking options

Option	Description
Do not track this rule	No record of the actions of this rule is made.
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 AlertTracker message	An AlertTracker message appears when a network communication event matches this rule.
Display Security Alert	A Security Alert dialog box appears when a network communication event matches this rule.

Type

Type lets you view or specify whether a pRule is an Admin or User type pRule.

Description

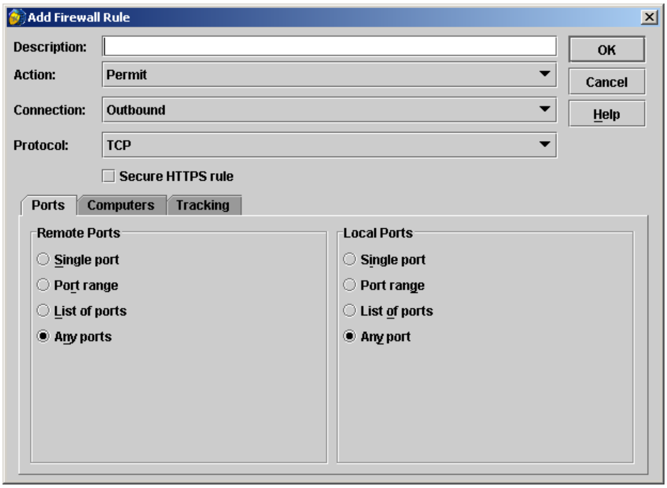
Description lets you specify the name of the rule so that you can distinguish it from other rules.

Manually creating a firewall rule

Firewall rules can be built using Symantec Client Firewall Administrator, saved to a new policy, and distributed to firewalls. Firewall rules can also be created on the Symantec Client Firewall client, if the user has the proper access level.

To create an application rule for an application

1. In Symantec Client Firewall Administrator, on the Rules tab, on the Application Rules tab, under Application, select the application for which you want to create a rule.
2. Under Rules, click **Add**.



Add Firewall Rule

Description:

Action: Permit

Connection: Outbound

Protocol: TCP

□ Secure HTTPS rule

Remote Ports

○ Single port

○ Port range

○ List of ports

● Any ports

Local Ports

○ Single port

○ Port range

○ List of ports

● Any port

3. In the Add Firewall Rule dialog box, in the Action list, select whether you want to Block, Permit, or Permit and monitor the communication.
4. In the Connection list, select whether the rule applies to inbound communications, outbound communications, or both inbound and outbound communications.
5. In the Protocol list, select whether the rule applies to TCP communications, UDP communications, TCP and UDP communications, or ICMP communications.

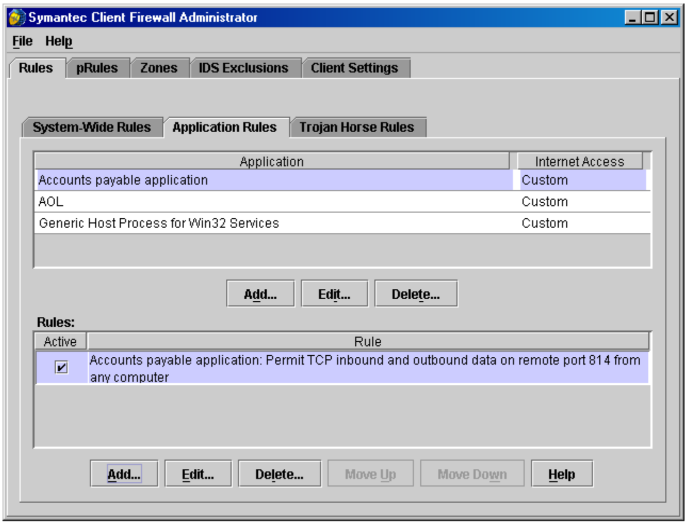
6 On the Ports tab, select whether the rule applies to all ports or one or more particular ports, and whether the rule applies to remote ports (communications from other computers) or local ports (communications from the same computer).

7 On the Computers tab, identify the IP addresses to which the rule applies.

8 On the Tracking tab, specify whether you want a log entry to be written when the rule is triggered, and whether you want the Alert Tracker utility to be turned on.

9 Click **OK**.

After you finish configuring a rule, the new rule appears in Symantec Client Firewall Administrator, on the Application Rules tab, under Rules.



Application	Internet Access
Accounts payable application	Custom
AOL	Custom
Generic Host Process for Win32 Services	Custom

Active	Rule
☑	Accounts payable application: Permit TCP inbound and outbound data on remote port 814 from any computer

Automatic creation of rules on the client

The Symantec Client Firewall client maintains a list of Internet applications that are generally safe to use in the pRules database. When Automatic Internet Access Control is enabled, the Symantec Client Firewall client automatically creates new access rules for recognized applications the first time that they run. This process is invisible to the client user.

If an unknown application on a Symantec Client Firewall client attempts to access the network or Internet, a number of events may occur, depending on how the client is configured:

- The Symantec Client Firewall client triggers an alert. The client user must then choose whether to allow or block Internet access for the application, then configure a rule for the event that triggered the alert by selecting choices from several panels.
- The connection is blocked, and the client user does not manage the alert or configure a rule for the application. For this to occur, the access level for the client users must be Restricted.

To enable Automatic Internet Access Control

◆ In Symantec Client Firewall Administrator, on the Client Settings tab, under Global, in the Value column for Automatic Internet Access Control, click **Enable**.

Enabling and disabling logging for a firewall rule

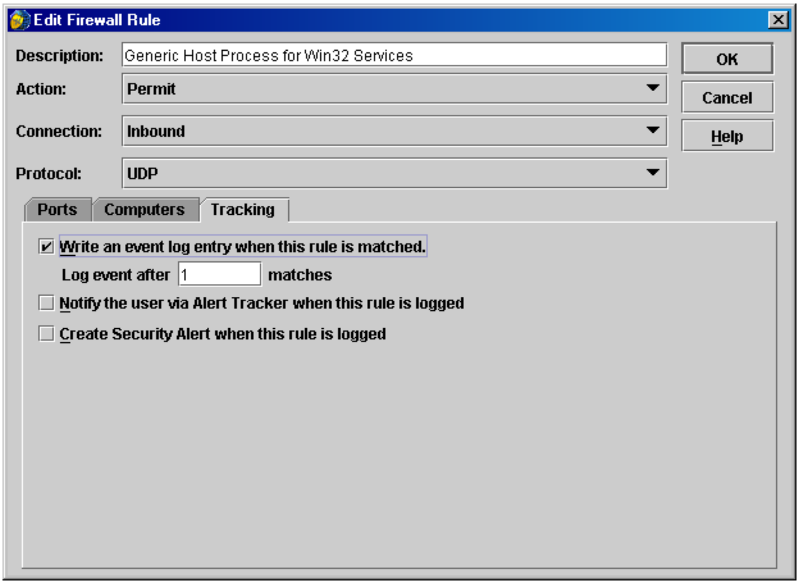
The firewall administrator can enable or disable logging for a selected rule when creating or modifying a policy.

To enable or disable logging for a firewall rule

1. In Symantec Client Firewall Administrator, on the Rules tab, select the tab for the rule category containing the rule that you want to modify.
2. Scroll through the rules list and click to select the rule.
3. Under Rules, click **Edit**.

4 In the Edit Firewall Rule dialog box, on the Tracking tab, check **Write an event log entry when this rule is matched** to enable logging for the rule. Uncheck the rule to disable logging.

5 If you're enabling logging for the rule, type the number of rule matches that you want to occur before the event is logged.



Edit Firewall Rule

Description: Generic Host Process for Win32 Services

Action: Permit

Connection: Inbound

Protocol: UDP

☑ Write an event log entry when this rule is matched.

Log event after 1 matches

☐ Notify the user via Alert Tracker when this rule is logged

☐ Create Security Alert when this rule is logged

Combining firewall rules

In some cases, you can combine existing rules to simplify firewall management using settings in the Edit Firewall Rule dialog box. Table 3-12 shows examples of combining two rules into a single rule.

Table 3-12 Examples of combining firewall rules

Setting	Values to combine	Scenario
Connection	Inbound and outbound connections	Rule 1 blocks all inbound UDP traffic on port 20, and Rule 2 blocks all outbound UDP traffic on port 20. To combine the rules, you would do the following: ■ On the appropriate Rules tab, select a rule that you want to combine with another. ■ Click Edit. ■ In the Edit Firewall Rule dialog box, change the Connection setting value to Inbound and outbound. ■ Click OK. ■ On the Rules tab, delete the associated rule that you did not select.
Protocol	UDP protocol and TCP protocol	Rule 1 blocks all inbound UDP traffic on port 20, and Rule 2 blocks all inbound TCP traffic on port 20. To combine the rules, you would do the following: ■ On the appropriate Rules tab, select a rule that you want to combine with another. ■ Click Edit. ■ In the Edit Firewall Rule dialog box, change the Protocol setting value to UDP and TCP. ■ Click OK. ■ On the Rules tab, delete the associated rule that you did not select.

Testing application rules

After an application has been run several times on a Symantec Client Firewall client and all of its features have been used, many rules will have been built. It is important to exercise every possible use, connection, port, and operation of the application to get the most complete characterization of the application. It is helpful if you can determine in advance how an application is accessing the Internet. For example, some applications call for the use of consecutive ports, while others use random ports.

Chapter 4

Using pRules

This chapter includes the following topics:

- About pRules
- Guidelines for using pRules
- Symantec-supplied pRules
- Configuring pRules
- Configuring pRules to support Active Directory

About pRules

Application rules are created in the registry of the Symantec Client Firewall client when the firewall policy is rolled out. This is an efficient method of providing uniform protection if all clients are similarly configured. If client workstations use divergent sets of applications, pRules are appropriate. With pRules, data about applications is installed on the client workstation, but the rules themselves are not created in the registry.

A pRule, or potential rule, contains the data required to validate an Internet-enabled application and then create an Application rule on the firewall client. The first time that an application is run, its corresponding pRule is processed. If the application matches the pRule criteria, the Symantec Client Firewall client creates an Application rule in the client registry using rule data for the application that is also contained in the pRule.

Once an Application rule is generated from a pRule on a client computer, the pRule is never applied again because the Application rule has a higher processing priority than the pRule. Using pRules lets the Symantec Client Firewall client generate Application rules as they are needed rather than creating a large number of Application rules that may never be used.

pRules are not used on a Symantec Client Firewall client until an application is run on the client and there is either:

- No Application rule for the application already in place.
- A rule in place, but the rule does not cover all the access that the application needs; for example, the rule allows only outbound TCP access on remote port 80 for Internet Explorer, but the application needs access to remote port 443.

A set of Symantec-supplied pRules, corresponding to many commonly used Internet-enabled applications, is installed on a firewall client when the default policy package is rolled out. This default set of pRules should be customized by an administrator using the Symantec Client Firewall Administrator or extended to include administrator-created, custom pRules for additional internal corporate or external applications and then rolled out to clients as part of a policy package.

pRules and rule types

Like System-Wide, Application, and Trojan Horse rules, pRules have a rule type. The default rule type for a pRule is User. Any Application rule generated from a pRule on the client is, by default, also of rule type User.

Unlike Administrator rules, User rules are not replaced when a policy package is rolled out to a client. Any Application rules generated from pRules that are of type User will remain in force on the client.

You can edit the rule type of a pRule using Symantec Client Firewall Administrator. For example, you may want an Application rule generated from a pRule to be of type Admin so that it will have a higher rule priority. Any Application rules generated from pRules that are of type Admin will be replaced when a new policy with Administrator rules is rolled out to clients. If the pRule is still on the client, a new application rule will be created on the client when the application is next run.

Note: Several Symantec Client Firewall client pRules associated with Symantec components are defined as type Admin rules. Do not change these rules to type User in Symantec Client Firewall Administrator, as doing so will affect the correct order in which the firewall rules are supposed to execute.

Using a digest value to identify an application

A pRule can include a digest, or application signature, that the Symantec Client Firewall client uses to validate the application’s executable file before applying any rule criteria. The digest is an encrypted hash value based on unique internal information about the application’s executable file.

For the set of pRules supplied with the Symantec Client Firewall client, the application digests are guaranteed to identify authentic copies of the application.

For pRules that you create for new applications with Symantec Client Firewall Administrator, you generate the digests, or application signatures, based on the executable files that you specify. Before creating a new pRule, make certain that the executable file referred to is the genuine application and has not been replaced or altered by a Trojan horse.

The digest is the most stringent means with which to securely identify an application. This capability is useful for preventing threats, such as malicious programs impersonating genuine applications from executing on the network.

Priority of pRule evaluation

A pRule is evaluated after all Zones, AutoBlocking lists, and Application rules are evaluted, as shown Table 4-1.

Table 4-1 Client application evaluation order

Order	SCF Process	Result
1	Match the IP address associated with the application against IP addresses in the Zones and AutoBlocking lists.	If a match occurs, perform the action (permit, block, or permit and monitor) and stop any further processing. If no match occurs, continue with rule processing.
2	Check all rules in the following order of priority: ■ System-Wide Admin rules ■ Application Admin rules ■ System-Wide User rules ■ Application User rules ■ Trojan Horse Admin rules ■ Trojan Horse User rules	The first time that a match occurs, perform the action (permit, block, or permit and monitor) and stop any further rule processing. If no match occurs, continue with pRule processing.
3	Check pRules of type Admin in order of priority, then all pRules of type User in order of priority.	If a match occurs, and a pRule exists for the application, then create the Application rule defined from the pRule data on the client and perform the specified action (permit, block, or permit and monitor).

Application rules and pRules

A pRule also contains information about the rules that determines the conditions under which an application is permitted to connect to the Internet.

In most cases, rule sets for pRules are designed to permit, rather than block, Internet access. The rule sets defined when creating a pRule are usually such that only expected behaviors by the application, such as communicating through the application’s default port, are permitted.

If a pRule does not exist for an application and the application is launched on a client, two possible courses of events can take place:

- If the Automatic Internet Access Control setting is enabled on the client, the Symantec Client Firewall client silently creates both a pRule for the application and a corresponding rule set that includes permitting the application to communicate with the Internet using the application's designated port.
- If the Automatic Internet Access Control setting is not enabled on the client, a sequence of alerts and messages is displayed on the client that require user input for configuring the application. The client is queried as to whether to create a pRule for the application, and which rule settings to use when the application is launched.

You must include the application's digest in a pRule file in order for the rules within the pRule to be created automatically. If the application digest is not being monitored and the client's access level is Admin or Normal, the client will receive an Internet Access Control alert and can configure rules for the application.

In most cases, using the Automatic Internet Access Control setting for firewalls is recommended. This minimizes the number of firewall alerts and firewall configuration requests that users receive.

Note: A client user must have a system account with access to the Windows registry to use Automatic Internet Access Control, otherwise that setting must be disabled.

Guidelines for using pRules

Following are some guidelines and recommendations for using pRules:

- pRules are most useful when there are many computers in an organization using a divergent set of applications. When many clients in an organization are using the same small set of applications, using Application rules instead of pRules is simpler.
- When deciding whether to create an Application rule or a pRule, consider that in an Application rule you must specify the fully qualified path. Therefore, the location of the executable file must be correct on all the client computers that use the information. A pRule is path independent; that is, you only have to specify the executable file name.

- If a client user has access rights to create local rules on the Symantec Client Firewall client (for example, a user of type Normal) and creates a rule for an application before its pRule is executed, the pRule will never be triggered. When the application is run on the client, the Application rule, being of a higher priority, will always be applied before the pRule.

  In cases such as these, make certain there is no conflict of intent between the Application rule and the pRule. For example, the pRule specifying to block a communication and the Application rule created by the user specifying to permit a communication.

- Any time that a version update is made to an application with a pRule, the pRule must be reconfigured through Symantec Client Firewall Administrator. If the pRule is not reconfigured, the Symantec Client Firewall client cannot match the pRule against the application executable and the firewall will block the application from running and will post alerts (users with an access level of Restricted will not receive alerts). When updating an application version, it is possible to retain information about earlier versions so that they can still execute.

- If clients are using applications that are updated frequently, consider not creating a pRule digest entry for the application to simplify administration. If the application is updated occasionally, consider creating a pRule that applies to different application versions. If you use a digest match criterion in the pRule for the application, you can optionally use other rules along with the match criterion to regulate the application's Internet connection behavior.

  See "Digest match criteria" on page 65.

- pRules are most useful for clients with an access level of Restricted. They are less useful for clients with an access level of Normal or Admin, because clients with those access levels can create their own rules.

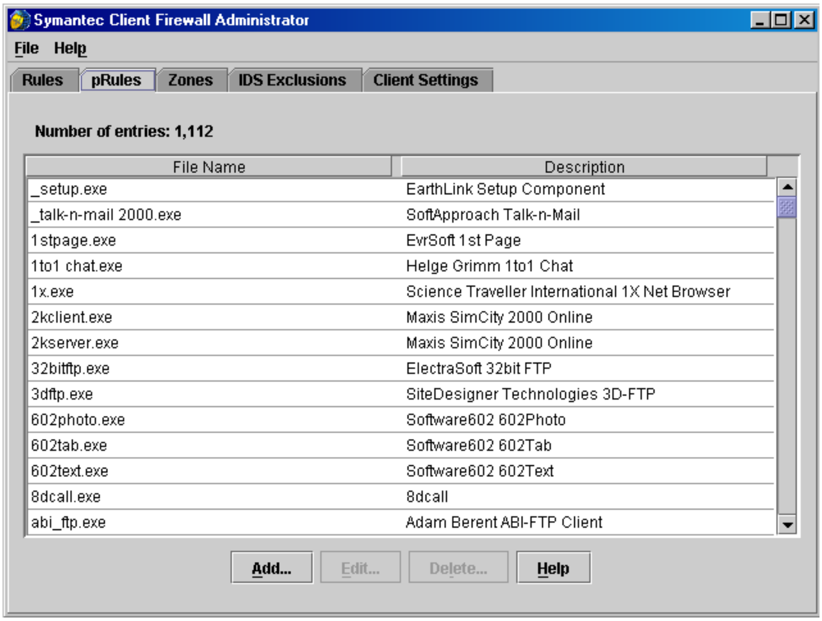
  If a user creates, for example, a local Application rule for the same application covered by a pRule, the Application rule, being of a higher priority will always execute before the pRule, rendering the pRule irrelevant. To ensure that application rules are used, it is best to create an application rule of type Admin instead of a pRule for a policy. This consideration applies more to users with Normal access rights, since users with Admin access rights have complete access to the firewall and can modify both Admin and User rules.

Symantec-supplied pRules

The default policy package for firewalls contains a set of pRules that provide coverage for many commonly used commercially available applications, as well as Windows subsystem executables. You can view the list of pRules in the current policy package loaded into Symantec Client Firewall Administrator.

To view the pRules in the current policy package

◆ In Symantec Client Firewall Administrator, on the pRules tab, scroll through the list to view the current pRules or see if a specific executable file for an application is secured by a pRule.



Number of entries: 1,112

File Name	Description
_setup.exe	EarthLink Setup Component
_talk-n-mail 2000.exe	SoftApproach Talk-n-Mail
1stpage.exe	EvrSoft 1st Page
1to1 chat.exe	Helge Grimm 1to1 Chat
1x.exe	Science Traveller International 1X Net Browser
2kclient.exe	Maxis SimCity 2000 Online
2kserver.exe	Maxis SimCity 2000 Online
32bitftp.exe	ElectraSoft 32bit FTP
3dftp.exe	SiteDesigner Technologies 3D-FTP
602photo.exe	Software602 602Photo
602tab.exe	Software602 602Tab
602text.exe	Software602 602Text
8dcall.exe	8dcall
abi_ftp.exe	Adam Berent ABI-FTP Client

Configuring pRules

In addition to the Symantec-supplied set of pRules, you can create new pRules using Symantec Client Firewall Administrator. This capability lets you add protection for commercially available applications for which pRules are not supplied and for internal corporate applications.

You create or modify a pRule for distribution to firewalls by configuring the following four sets of options for the pRule:

- Application identity: Specify the application's executable file and supply a brief description of the application.
- Match names: Generate application match names, which label sets of match criteria that are used to authenticate an application's executable file. Each match name for the pRule has separate associated match criteria.
- Match criteria: Configure the values the pRule uses to verify the application before allowing it to run. You can configure one or more sets of match criteria for an individual pRule, with each match set containing one or more match criteria. You choose from among the following match criteria:

  File Version — Specify a version number or range of version numbers for the application to use as a match.

  Version Data — Specify file resource property values to use as match criteria. After you select this option, you can select one of the following: Comments, Company name, File description, Internal name, Original file name, Product name, Product version, Legal copyright, or Legal trademarks.

  Required Digest — Specify an encrypted pRule digest value to use for matching the Internet-enabled application.

  Using a required digest match means that the application executable must be authenticated by the digest or a security alert is triggered. It is the strongest method of verifying the authenticity of an application.

  Optional Digest — Specify an encrypted pRule digest value to use for matching the application. Using an optional digest match means that if the application executable is not validated by the digest, other match criteria, such as company name, can be applied without triggering a security alert, for example.

  File Size — Specify an application executable file size or a range of possible file sizes to use for matching the application.

  By default, Symantec Client Firewall Administrator uses the executable file name as a match criterion for the application when a pRule is added.

- Rules: Configure the Application rule that will be created on the Symantec Client Firewall client once the executable file specified by the pRule has been validated.

Create new pRules or edit existing pRules

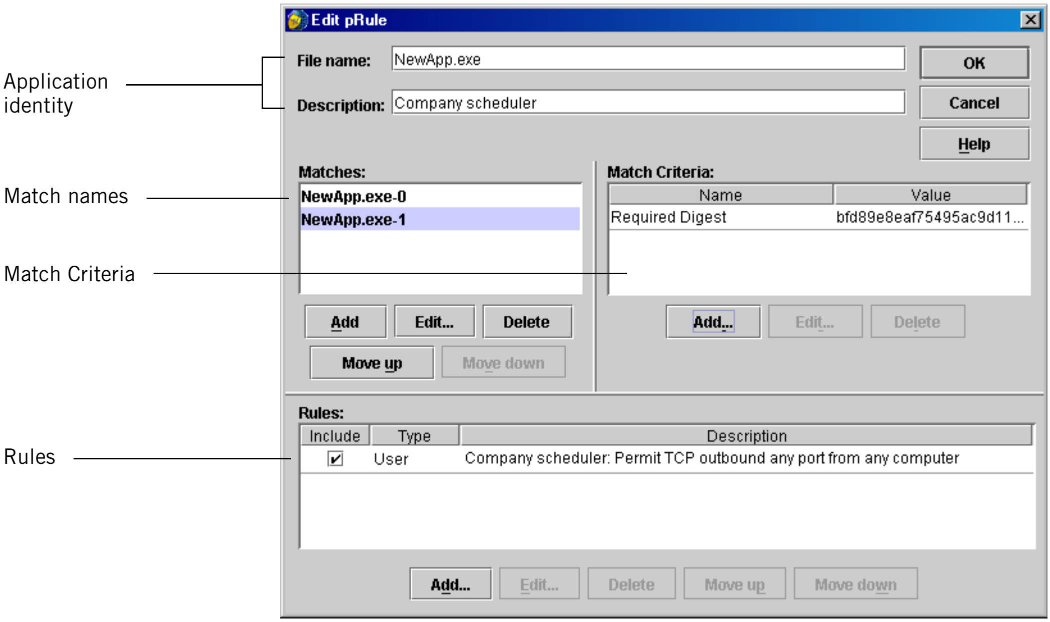
Create new pRules or modify existing pRules as follows.

To create a new pRule

- In Symantec Client Firewall Administrator, on the pRules tab, click **Add**.

To edit an existing pRule

- In Symantec Client Firewall Administrator, on the pRules tab, select an existing pRule, then click **Edit**.



File name: NewApp.exe

Description: Company scheduler

Matches:

NewApp.exe-0
NewApp.exe-1

Match Criteria:

Name	Value
Required Digest	bfd89e8eaf75495ac9d11...

Rules:

Include	Type	Description
☑	User	Company scheduler: Permit TCP outbound any port from any computer

Specifying the Application identity for a pRule

The application identity is the executable name of the application.

To specify the application identity for a pRule

1 In the Add or Edit pRule dialog box, in the File name text box, type or confirm the executable name of the application.

Do not type the path to the executable file (for example, NewApp.exe).

2 In the Description text box, type a description of the application.

Adding or editing match names for a pRule

Each match name for the pRule is associated with a set of match criteria that the pRule uses to validate the executable file including file size, file version, version information, and digest value.

To add or edit match names for a pRule

- In the Add or Edit pRule dialog box, under Matches, do one of the following:
  - To add a match name, click **Add**.

    By default, the Match name is the file name with a sequential number appended (for example, NewApp.exe-0). You can rename the Match name by clicking Edit and changing the name in the Edit Match Name dialog box.

    By default, the associated match criteria is set to Any Version. This value is overwritten when a new value is set.
  - To modify an existing match name, select the match name, then click **Edit**.

Configuring match criteria

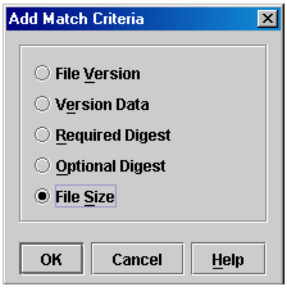
The match criteria are the types of information used to validate an application and their values.

Work with match criteria and values

You begin working with match criteria by selecting from among five types of available criteria. Each of the match criteria types has a dialog box that requests appropriate information. For example, File Size allows you to enter one or more file sizes or a size range that the application must match when the pRule is processed on the Symantec Client Firewall client.

To specify new Match Criteria

1. In the Add pRule or Edit pRule dialog box, under Matches, select a match name.
2. Under Match Criteria, click **Add**.



○ File Version
○ Version Data
○ Required Digest
○ Optional Digest
● File Size

3. In the Add Match Criteria dialog box, select one of the five match criteria, then click **OK**.

To modify existing match criteria

1. In the Add pRule or Edit pRule dialog box, under Matches, select a match name.
2. Under Match Criteria, select the item, then click **Edit**.

To specify the match criteria

1. In the displayed Add or Edit pRule Match Criteria dialog box, enter the requested information and click **Add**.
2. Do one of the following:
   - If this is the only value that you want validated, click **OK** to close the Add pRule Match Criteria dialog box.
   - To add additional values, in the Add or Edit pRule Match Criteria dialog box, enter the information and click **Add** after each value. When finished, click **OK** to close the Add pRule Match Criteria dialog box.

File version match criteria

File version match criteria can include specific file versions for the application as well as file version ranges. When you configure version match criteria, you can specify one of the following for file matching:

- A single version number
- A list of nonconsecutive version numbers
- A range of version numbers

You can use either the standard four-part version naming convention for version data (four numbers separated by three periods, for example, 8.0.0.1) or as few digits as are necessary to specify the version or versions that you want.

If you specify fewer than four digits, the remaining digits are wildcards. For example, if you specify a value of 2.0, it matches any value from 2.0.0.0 to 2.0.9.9.

Version data match criteria

Version data match criteria includes the following resource properties that are associated with the application:

- Comments: Use the value of the comments property that is associated with the application's executable file.
- Company name: Use the value of the company name property that is associated with the application executable, if one exists.
- File description: Use the value for the description property of the application's executable file.
- Internal name: Use the value of the internal name property of the application executable, if one exists. If no internal file name value was specified before the application was compiled, this value defaults to the application file name without the file suffix.
- Original file name: Use the name that the application executable was created with, before any renaming of the file happened.
- Product name: Use the product name that was distributed with this version of the application's executable file.
- Product version: Use the version of the product with which the application's executable file is distributed. A product version number is a 64-bit number displayed according to the format major number.minor number.build number.private part number, such as the value 9.0.3517.0.

- Legal copyright: Use the property value that represents the legal copyright of the application.
- Legal trademarks: Use the property value that represents the trademarks of the application.

A file property that is listed under Resource Name may or may not exist for a given executable file. Examine the Version page of an application's property box, viewable in Windows Explorer, to check which file properties are available.

Digest match criteria

A pRule digest is an application signature that is derived from a scan of the code sections of an application's executable file. A digest value uniquely identifies an application's executable file with an encrypted key. When the pRule is invoked on the Symantec Client Firewall client, the application's digest value is recomputed and compared to the stored digest value of the pRule. For a match to occur, the digest of the launched application on the Symantec Client Firewall client must exactly match that of its digest entry.

Using a digest as a match criterion provides high-level security for verifying the authenticity of an application. A required digest provides the maximum level of security possible, while an optional digest provides a lower level of security, but greater flexibility in handling different versions of an application. To enable rules to be automatically generated on a client computer the first time that an application is run, you need to have already defined a pRule for the application with a digest.

The executable file name used in a pRule can be associated with more than one application. The same file name can correspond to different applications on a client (for example, Setup.exe) or different versions of an application (for example, Internet Explorer). In this case, you can create several match names, each with a required digest value corresponding to a different executable.

Note: There can be only one digest value per application match name. Anytime that an application is updated, either the pRule digest value must also be updated or an additional match name with a new digest must be added to the pRule. If this is not done, the new version of the application will be blocked from executing.

Required digest match criteria

When you use the required digest match selection, and the application associated with the pRule is run, the Symantec Client Firewall client checks the required digest value for each match name according to the match name order:

- If a match occurs with a required digest value the first time that an application is launched on a client, the Application rule is created silently in the Windows registry of the client computer.
- If the Symantec Client Firewall client is unable to match the application against any required digest value in the pRule, a security alert is posted, and a sequence of dialog boxes prompts the user to configure rules for the application.

Note: Restricted users are not able to configure application rules.

Note that once a pRule becomes an Application rule, the path locations for the executable files associated with the pRule cannot be changed, or the Application rule will not work.

Optional digest match criteria

The optional digest match selection works similarly to the required digest match selection. However, if the optional digest match fails, other match criteria in the same set are checked. If another criterion in the match set containing the optional digest is matched, no security alert is triggered.

You can use the optional digest value as the only match criterion in a match set. When you do so, and the associated application is run, one of the following behaviors can occur:

- If a match occurs between the application and the optional digest value, the rules for the application will silently autocreate on the client.
- If a match does not occur, the user receives a prompt, and can choose whether to allow the Symantec Client Firewall client to automatically configure a rule for the application (using the pRule data), or manually configure the rule by completing the Symantec Client Firewall client prompts.

Using the NoVerifyDigest setting

If you enable the NoVerifyDigest client configuration setting, any required digest or optional digest values for pRules will be ignored. If no other match criteria exist for an application associated with a pRule, a rule for the application will be silently created on the client. If other match criteria exist for the application, then those criteria will be applied.

This setting is available in the event that you have applications from trusted sources and want to disable digest checking; however, this setting should be used with caution.

File size match criteria

You can specify either a list of nonconsecutive file size values, or a range of file sizes to use for matching.

Adding an Application rule to a pRule

Once a pRule is triggered and the corresponding application run, any application rules associated with the pRule are saved into the Windows registry on the client. Effectively, the pRule becomes an Application rule, and is governed by the rules associated with Application rules.

See “Rule categories” on page 37.

To add an Application rule to a pRule

1. In the Add pRules dialog box, under Rules, click **Add**.
2. In the Add Firewall Rule dialog box, enter the necessary information to create the rule.

Configuring pRules to support Active Directory

Typically, a Windows 2000/NT client in a Windows 2000 network uses the following processes for networking in an Active Directory environment:

C:\Winnt\System32\Lsass.exe	Supports Kerberos, LDAP, EPmap, and Nterm
C:\Winnt\System32\Services.exe	Supports NTP, Bootp, Kerberos, DNS, and EPmap
C:\Winnt\Explorer.exe	Supports LDAP
C:\Winnt\System32\Winlogon.exe	Supports LDAP
Windows Subsystem	Supports NetBIOS and SMB

Table 4-2 shows a rulebase that supports Windows 2000 networking in an Active Directory environment. All rules are permitted, admin-level, bi-directional rules unless indicated in the Description column.

Table 4-2 Sample application rulebase

Executable	Description	Protocol	Remote ports	Local ports
Lsass.exe	Kerberos EPmap LDAP Nterm	UDP TCP TCP, UDP TCP	88 135 389 1026	1025-5000 1025-5000 1025-5000 1025-5000
Services.exe	DNS Bootp Kerberos NTP EPmap	TCP, UDP UDP UDP UDP TCP	53 67, 68 88 123 135	1025-5000 67, 68 1025-5000 1025-5000 1025-5000
Explorer.exe	LDAP	TCP, UDP	389	1025-5000
Winlogon.exe	LDAP	TCP, UDP	389	1025-5000
System	NetBIOS NetBIOS to 139 (inbound only) SMB (microsoft-ds)	TCP, UDP TCP TCP	137, 138, 139 1025-5000 445	1025-5000 139 1025-5000

You can create one pRule for all executables or one pRule for each executable. Additionally, be sure to verify that admin-level, system-wide rules are not blocking protocols, such as SMB and EPmap, and that the upper port range of 5000 is satisfactory in your environment.

Chapter 5

Controlling access to protected computers

This chapter includes the following topics:

- About Zones
- Enabling file and printer sharing

About Zones

Symantec Client Firewall monitors all connections, including those made among computers across your organization. Controlling access to clients and groups of clients allows you to completely block access to known malicious IP addresses or Internet sites. You can also allow computers in your organization to share files, printers, and other resources.

Symantec Client Firewall lets you organize computers on your network and the Internet into two Zones: Trusted (the firewall is ignored) and Restricted (all external communications are blocked). If a computer has not been placed in the Trusted Zone or Restricted Zone, then all existing rules apply to external communications to and from the computer.

The firewall always checks Zones before it checks rules. If a match with an IP address in a Zone occurs, no further rule evaluation beyond whether to permit the communication (Trusted Zone) or block the communication (Restricted Zone) takes place.

Computers that you place in the Trusted Zone are not regulated by Symantec Client Firewall. They have as much access to your computer as they would have if Symantec Client Firewall was not installed. Only use the Trusted Zone for computers on your local network with which you need to share files and printers. If a computer in your Trusted Zone is attacked, and an attacker takes control of it, it poses a risk to your computer and all other computers in your Trusted Zone.

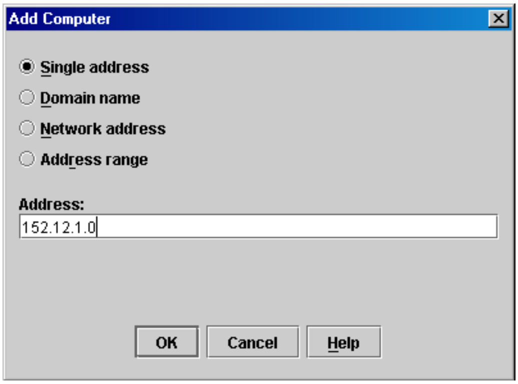
Computers that you place in the Restricted Zone are prevented from accessing your computer at all. If a computer is in the Restricted Zone, all communication among it and any computers that you have protected with Symantec Client Firewall is automatically blocked.

Adding a computer to the Trusted Zone

In most cases, you will want to add all of the computers in your organization to the Trusted Zone. Only add external computers to your Trusted Zone if you know that their users can be trusted and they have firewall software installed.

To add a computer to the Trusted Zone

1 In Symantec Client Firewall Administrator, on the Zones tab, on the Trusted Zone tab, click **Add**.



Add Computer

● Single address

○ Domain name

○ Network address

○ Address range

Address:
152.12.1.0

2 In the Add Computer dialog box, select one of the following:

- Single address: A single, 32-bit number that identifies the computer.
- Domain name: A domain name that contains the IP address of the computer.
- Network address: An inclusive range of IP addresses, created by entering one IP address and a subnet mask.
- Address range: An inclusive range of IP addresses, from starting IP address to ending IP address.

3 In the Address text box, type the IP addresses of the computers that you want to place in the Trusted Zone.

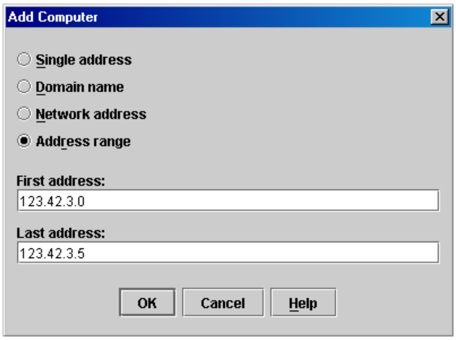
4 Click **OK**.

Adding a computer to the Restricted Zone

Computers that you place in the Restricted Zone are prevented from accessing your computer.

To add a computer to the Restricted Zone

1 In Symantec Client Firewall Administrator, on the Zones tab, on the Restricted Zone tab, click **Add**.



○ Single address
○ Domain name
○ Network address
● Address range

First address: 123.42.3.0

Last address: 123.42.3.5

2 In the Add Computer dialog box, select one of the following:

- Single address: A single, 32-bit number that identifies the computer.
- Domain name: A domain name that contains the IP address of the computer.
- Network address: An inclusive range of IP addresses, created by entering one IP address and a subnet mask.
- Address range: An inclusive range of IP addresses, from starting IP address to ending IP address.

3 Do one of the following:

- If you only want to add one computer, in the First address text box, type the IP address.
- If you want to add a range of computers, in the First address text box, type the first IP address, then in the Last address text box, type the last IP address.

4 Click **OK**.

Enabling file and printer sharing

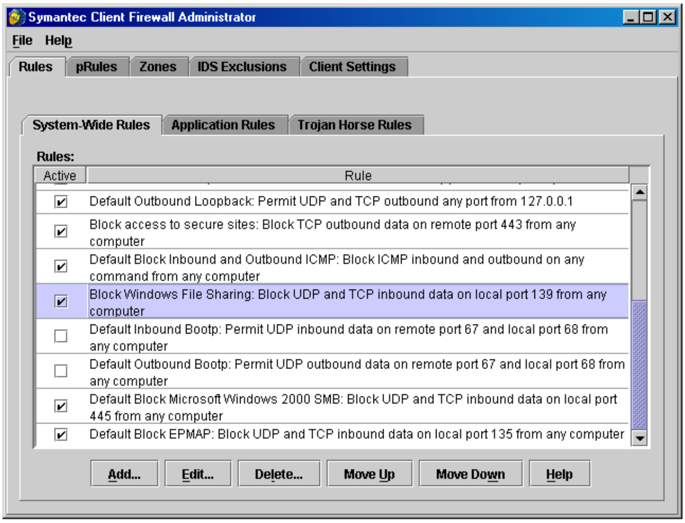
Microsoft networking provides file and printer sharing. By default, Symantec Client Firewall prevents any computers from accessing these services on a protected computer.

To share files and give access to printers for the administrative group covered by the policy, you can enable file and printer sharing. If you enable these features, they are still protected from malicious users on the Internet.

Note: Before enabling file and printer sharing for the administrative group covered by the policy, ensure that each shared resource is protected by a secure password.

To enable file and printer sharing

◆ In Symantec Client Firewall Administrator, on the Rules tab, on the System-Wide Rules tab, under Rules, uncheck **Block Windows File Sharing: Block UDP and TCP inbound data on local port 139 from any computer**.



Rules:

Active	Rule
☑	Default Outbound Loopback: Permit UDP and TCP outbound any port from 127.0.0.1
☑	Block access to secure sites: Block TCP outbound data on remote port 443 from any computer
☑	Default Block Inbound and Outbound ICMP: Block ICMP inbound and outbound on any command from any computer
☑	Block Windows File Sharing: Block UDP and TCP inbound data on local port 139 from any computer
□	Default Inbound Bootp: Permit UDP inbound data on remote port 67 and local port 68 from any computer
□	Default Outbound Bootp: Permit UDP outbound data on remote port 67 and local port 68 from any computer
☑	Default Block Microsoft Windows 2000 SMB: Block UDP and TCP inbound data on local port 445 from any computer
☑	Default Block EPMAP: Block UDP and TCP inbound data on local port 135 from any computer

Chapter 6

Customizing intrusion detection

This chapter includes the following topics:

About the Intrusion Detection System (IDS)

The Intrusion Detection System (IDS) used in the Symantec Client Firewall client scans each packet that enters and exits its host computer for *attack signatures* (arrangements of information that identify an attacker's attempt to exploit a known operating system or application vulnerability).

Because attacks may span packets, Intrusion Detection examines packets in two different ways. It scans each packet individually looking for patterns that are typical of an attack. It also monitors the packets as a stream of information, which lets it identify attacks spread across multiple packets.

If the information matches a known attack, Intrusion Detection automatically discards the packet and severs the connection with the computer that sent the data. This protects computers on your network from being affected in any way.

You can modify how Intrusion Detection responds to attacks by excluding specific attack signatures from being monitored and by excluding specific computers from AutoBlock, which automatically blocks all communication from an attacking computer.

Intrusion Detection relies on an extensive list of attack signatures to detect and block suspicious network activity. This list is displayed in Symantec Client Firewall Administrator, and you can control whether or not to exclude any attack signature on the list from blocking. The list of known threats is Symantec-supplied and can be updated on the Symantec Client Firewall client using the Symantec LiveUpdate facility.

About customizing Intrusion Detection

The default Intrusion Detection System (IDS) settings should provide your Symantec Client Firewall client computers with adequate protection against a wide variety of threats. If the default settings do not completely address the needs of your network, you can customize Intrusion Detection settings in one or more of the following ways:

- Enable or disable Intrusion Detection.
- Exclude specific attack signatures from being monitored.
- Enable or disable AutoBlock.
- Exclude specific computers from IDS AutoBlocking.

Warning: Each exclusion leaves your computer vulnerable to attacks. Use the utmost care when excluding attacks. Only exclude behavior that is always benign.

Excluding attack signatures from firewall protection

Following are reasons for disabling firewall protection against specific attack signatures:

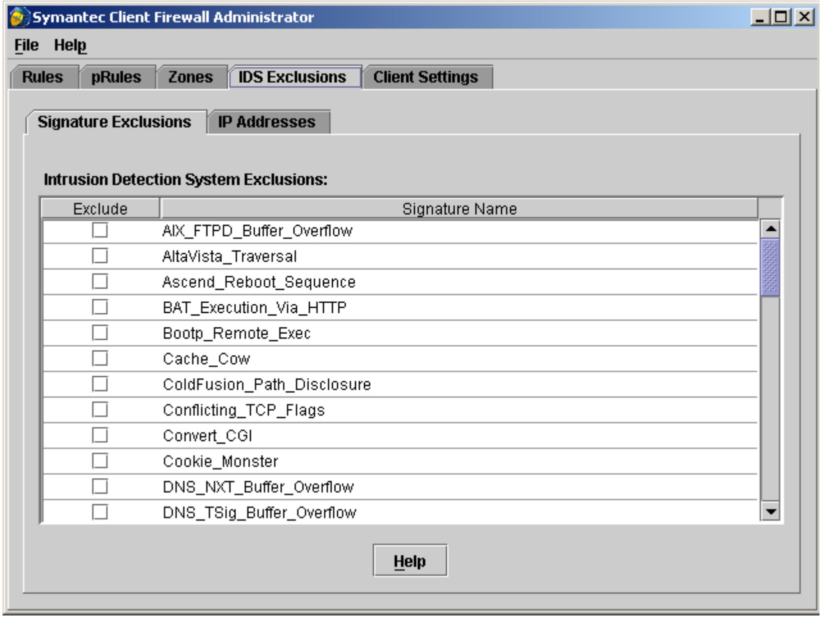
- Your network may not need protection against certain attack signatures because your environment does not contain the applications or network components that are targeted for attack.
- In some cases, benign network activity may appear similar to a Symantec Client Firewall client attack signature. If you receive repeated warnings about possible attacks, and you know that these attacks are being triggered by safe behavior, you can create an exclusion for the attack signature that matches the benign activity.
- There is a need to reduce resource consumption on your system. Lowering the number of attack signatures checked for by the Symantec Client Firewall client lowers the amount of resource consumption by the firewall. However, you must be certain that an attack signature poses no threat before excluding it from blocking.

Exclude attack signatures for clients

You can enable and disable the blocking of IDS attack signatures for firewalls using Symantec Client Firewall Administrator.

To exclude an IDS attack signature from being blocked

- In Symantec Client Firewall Administrator, on the IDS Exclusions tab, on the Signature Exclusions tab, under Intrusion Detection System Exclusions, check the attack signatures that you want to exclude from firewall blocking.



Intrusion Detection System Exclusions:

Exclude	Signature Name
□	AIX_FTPD_Buffer_Overflow
□	AltaVista_Traversal
□	Ascend_Reboot_Sequence
□	BAT_Execution_Via_HTTP
□	Bootp_Remote_Exec
□	Cache_Cow
□	ColdFusion_Path_Disclosure
□	Conflicting_TCP_Flags
□	Convert_CGI
□	Cookie_Monster
□	DNS_NXT_Buffer_Overflow
□	DNS_TSig_Buffer_Overflow

To restore attack signatures that have previously been excluded

1. Before restoring the attack signatures, you need to have previously saved the policy that contains the signatures.

   You save a policy with IDS exclusions in Symantec Client Firewall Administrator by using **File** > **Save**, then making sure the IDS Exclusion box is checked, and then saving the policy file with a .cfp extension.

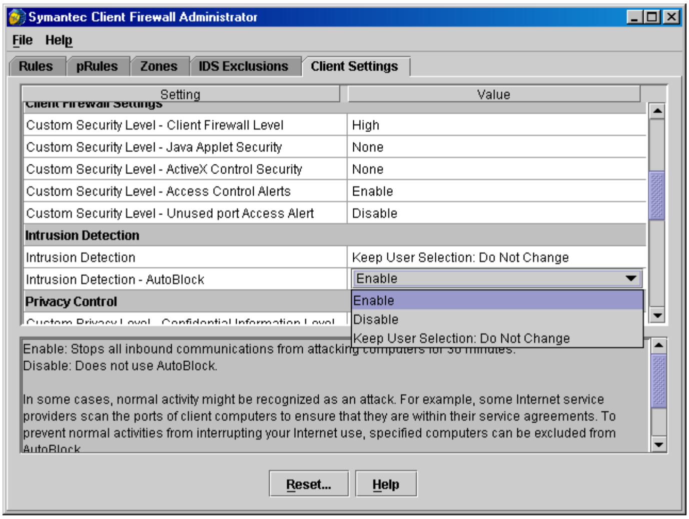
2. When you want to add the attack signatures back in for client monitoring, click **File** > **Import**.
3. Browse to the directory containing the .cfp policy file, then click to open it.
4. On the IDS Exclusions tab, on the Signature Exclusions tab, uncheck the Intrusion Detection System Exclusions that you want to monitor.
5. Save the policy.
6. Roll out the policy to clients.

Configuring AutoBlock

When the Symantec Client Firewall client detects an attack, it automatically blocks the connection to ensure that your computer is safe. The program can also activate AutoBlock, which automatically discards all incoming communication from the attacking computer for a set period of time, even if the incoming communication does not match an attack signature. By default, AutoBlock stops all inbound communications from the attacking computer for 30 minutes. While AutoBlock stops all incoming communication from the remote computer, it does not stop you from sending information to the attacking computer.

To configure AutoBlock

1 In Symantec Client Firewall Administrator, on the Client Settings tab, under Intrusion Detection, click the Value cell for Intrusion Detection - AutoBlock.



Setting	Value
Client Firewall Settings	
Custom Security Level - Client Firewall Level	High
Custom Security Level - Java Applet Security	None
Custom Security Level - ActiveX Control Security	None
Custom Security Level - Access Control Alerts	Enable
Custom Security Level - Unused port Access Alert	Disable
Intrusion Detection	
Intrusion Detection	Keep User Selection: Do Not Change
Intrusion Detection - AutoBlock	Enable
Privacy Control	
Custom Privacy Level - Confidential Information Level	

Enable: Stops all inbound communications from attacking computers for 30 minutes.
Disable: Does not use AutoBlock.

In some cases, normal activity might be recognized 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, specified computers can be excluded from AutoBlock

2 In the drop-down list, select one of the following:

- Enable
- Disable
- Keep User Selection: Do Not Change

3 Roll out the policy file out to clients.

Excluding computers from AutoBlock

Some normal Internet activities will be repeatedly recognized by the Symantec Client Firewall client as attacks. For example, some Internet service providers scan the ports of your computer to ensure that you are within their service agreements.

If client computers can't communicate with computers they should be able to connect to, the destination computers may be blocked by AutoBlock. Depending on the circumstances, you can disable the AutoBlock setting on clients, preventing attacking computers from being added to the AutoBlock list, or you can exclude specific computers from AutoBlock.

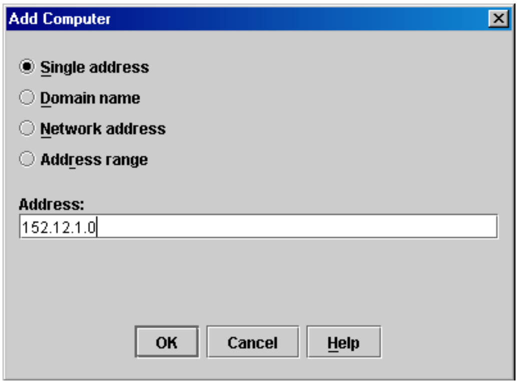
Exclude computers from AutoBlock

Use the following procedures to exclude IP addresses from being blocked, or to turn off exclusion.

To exclude computers from being blocked

1 In Symantec Client Firewall Administrator, on the IDS Exclusions tab, on the AutoBlock tab, click **Add**.

2 In the Add Computer dialog box, in the Address text box, type the IP addresses that you want to exclude from firewall protection.

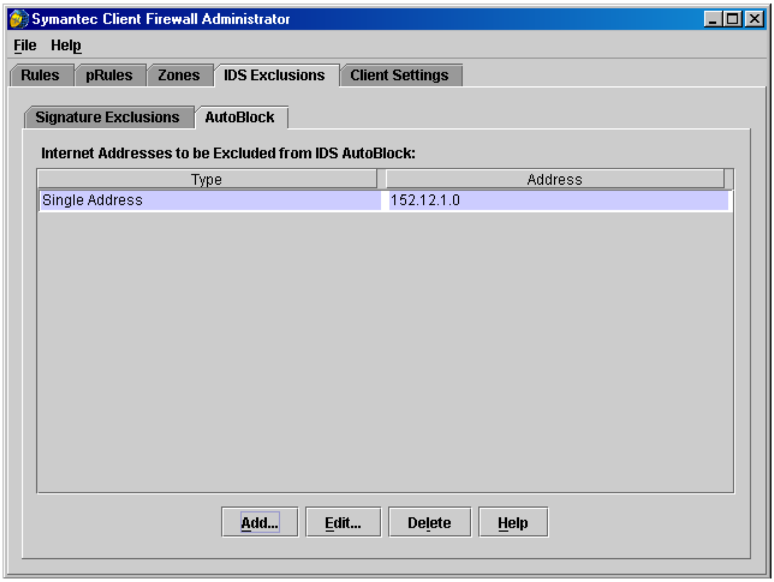


● Single address
○ Domain name
○ Network address
○ Address range

Address: 152.12.1.0

3 Click **OK**.

The addresses that you added appear on the AutoBlock tab, under Internet Addresses to be Excluded from IDS AutoBlock.



Type	Address
Single Address	152.12.1.0

To turn off exclusion of a computer

1 In Symantec Client Firewall Administrator, on the IDS Exclusions tab, on the AutoBlock tab, under Address, select the IP address or address range for the computer or computers that you want to remove from the AutoBlock exclusion list.

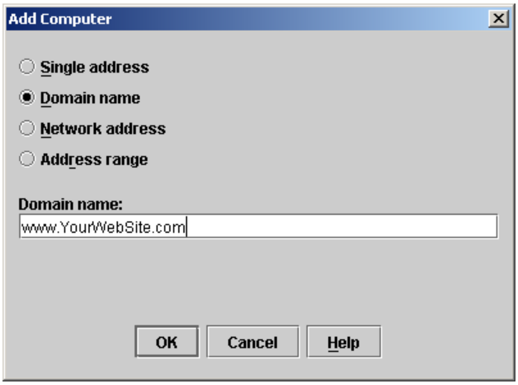
2 Click **Delete**.

Restricting a blocked computer

You can add a blocked computer to an administrative Restricted Zone to permanently prevent that computer from accessing other computers. Computers that are added to the Restricted Zone do not appear on the blocked list on the Symantec Client Firewall client because the firewall automatically rejects any connection attempts by restricted computers.

To restrict a blocked computer

1 In Symantec Client Firewall Administrator, on the Zones tab, on the Restricted Zone tab, click **Add**.



Domain name: www.YourWebSite.com

2 In the Add Computer dialog box, select one of the following:

- Single address
- Domain name
- Network address
- Address range

3 In the Domain name text box, type the IP address information or domain information for the blocked computers that you want to add to the Restricted zone.

Chapter 7

Configuring client settings

This chapter includes the following topics:

About client configuration settings

Symantec Client Firewall Administrator includes settings for overall operation of the Symantec Client Firewall client, the extent to which a client user is allowed to configure the firewall (access level), whether to automatically generate rules, security levels for various Internet communications, and any ports or IP addresses that will be blocked or filtered on the client.

The complete list of client settings that are configurable through Symantec Client Firewall Administrator, and brief descriptions of each setting, are provided in the following tables, organized by category.

Note: The selection Keep User Selection: Do Not Change is available for many client configuration settings. This selection retains whatever value (for example, Enabled or Disabled) is already selected in the client user interface.

Access level settings

Table 7-1 describes the Access level client configuration settings.

Table 7-1 Symantec Client configuration settings: Access level settings

Setting	Description
User Type	Sets the permissions for a Symantec Client Firewall client. Administrator: All Symantec Client Firewall client product features and configuration options are available to users. Normal: Users have a limited subset of permissions that includes working with User rules, viewing firewall data, and modifying privacy control settings. Restricted: Users cannot configure rules or change settings. For the most part, the firewall is invisible to a user with this setting.

Global settings

Table 7-2 describes the Global client configuration settings.

Table 7-2 Symantec Client configuration settings: Global settings

Setting	Description
Symantec Client Firewall Protection	Enables or disables the firewall.
Ignore pRule Digest Values	Permitted applications are identified by name, version, date, and size. The Digest Value (computed application signature) that precisely identifies an application is ignored. If no other match criteria exist for an application associated with a pRule on a client with this setting, a rule for the application will be silently created. If other match criteria exist for the application, then those criteria will be applied.
Automatic Internet Access Control	When enabled, uses the pRule database to create new firewall rules for low-risk applications that it recognizes the first time that they are run. When disabled, new rules are not automatically configured.

Status settings

Table 7-3 describes the Status client configuration settings.

Table 7-3 Symantec Client configuration settings: Status settings

Setting	Description
Client Firewall	Enables or disables firewall rulebase inspection and intrusion detection. When disabled, the firewall still runs but is in a default-permit condition, disabling all client firewall settings. See Table 7-4, "Client firewall settings," on page 86.
Privacy Control	Enables or disables Privacy Control.

Table 7-3 Symantec Client configuration settings: Status settings

Setting	Description
Reporting Level	Minimal: Critical Internet events only. Notifies when Internet Access Control rules are created automatically, port scans occur, confidential information is blocked, and remote-access Trojan horse programs are encountered. Medium: Important Internet events. Same notification as Minimal and notifies when applications access the Internet. High: Complete program activities. Same notification as Medium and notifies when unused ports, cookies, and content are blocked.

Client firewall settings

Table 7-4 describes the client firewall settings. If the Client Firewall Status setting is disabled, these settings are not enforced.

See Table 7-3, “Symantec Client configuration settings: Status settings,” on page 85.

Table 7-4 Client firewall settings

Setting	Description
Custom Security Level: Client Firewall Level	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 are not specifically allowed. Firewall rules for every application that requests Internet access must be created. Rules are often created by a Symantec Client Firewall client application scan.
Custom Security Level: Java Applet Security	None: Lets all Java applets run. Medium: Prompts for permission each time that a Java applet attempts to run. Do not use the Medium setting if the client access level is set to Restricted. High: Prevents all Java applets from running.

Table 7-4 Client firewall settings

Setting	Description
Custom Security Level: ActiveX Control Security	None: Lets all ActiveX controls run. Medium: Prompts for permission each time that an ActiveX control attempts to run. If the client access level is Restricted, do not use the Medium setting. High: Prevents all ActiveX controls from running.
Custom Security Level: Access Control Alerts	Enable: Prompts to permit or block an application from accessing the Internet when no firewall rule exists for it. Disable: Blocks applications from accessing the network when there are no specific firewall rules in place for them. Make sure to disable Access Control Alerts if the user access setting is Restricted.
Custom Security Level: Unused port Access Alert	Enable: Alerts are generated when an attempt is made to access an unused port. Enabling this option significantly increases the number of alerts displayed. Disable: Alerts are not generated for unsolicited connection attempts.

Intrusion Detection settings

Table 7-5 describes the Intrusion Detection settings.

Table 7-5 Intrusion Detection settings

Setting	Description
Intrusion Detection	Enable: Monitors Internet communications for patterns that are typical of a hacker attack, for example, a port scan or attempts to connect to ports used by remote-access Trojan horse programs. Disable: Does not scan IP packets for intrusion behavior.

Table 7-5 Intrusion Detection settings

Setting	Description
Intrusion Detection: AutoBlock	Enable: Stops all inbound communications from attacking computers for 30 minutes. Disable: Does not use AutoBlock. In some cases, normal activity might be recognized 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, specified computers can be excluded from AutoBlock. 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.

Privacy control settings

Table 7-6 describes the Privacy control settings.

Table 7-6 Privacy control settings

Setting	Description
Confidential Information Level	High: Blocks all specified confidential information entered in a Web page from being sent to nonsecured (HTTP) Web sites. Medium: Prompts each time that specified confidential information entered in a Web page is sent to a nonsecured (HTTP) Web site. Do not use this setting if the user access level is set to Restricted. None: Disables the monitoring of confidential information sent to Web sites.
Cookie Blocking Level	High: Blocks all cookies. Medium: Prompts each time that a Web site requests a cookie. Do not use this setting if the user access level is set to Restricted. None: Allows all cookies.

Table 7-6 Privacy control settings

Setting	Description
Browser Privacy	Enable: Prevents a Web site from retrieving the user's email address or the address of the last Web site visited. Disable: Permits the sending of the user's email address or address of the last Web site visited.
Secure Connections	Enable: Permits communication via HTTPS protocol. If enabled, confidential information is sent. Disable: Blocks HTTPS communications, including most credit card and financial transactions.

General options settings

Table 7-7 describes the General options settings.

Table 7-7 General options settings

Setting	Description
Show Taskbar Icon	Yes: Displays the Symantec Client Firewall client icon in the system tray, which can be right-clicked to log on and off, exit the program, or perform other tasks. No: The Symantec Client Firewall client icon is not displayed in the system tray.
Show Alert Tracker	Yes: Displays the half-globe AlertTracker icon at the side of the screen to view recent messages. No: Does not display the half-globe AlertTracker icon.
Run at System Startup	Yes: The Symantec Client Firewall client runs when the computer is started. No: The Symantec Client Firewall client must be started manually.

Tray menu options settings

Table 7-8 describes the Tray menu options settings. These are menu selections that become available when a client user right-clicks the Symantec Client Firewall client icon in the Windows system tray.

Table 7-8 Tray menu options settings

Setting	Description
Display Options	Yes: Displays the Options selection on the Tray menu, which allows you to display the Symantec Client Firewall client Options dialog box for access to general settings, statistics, the Event Log, and Tray menu settings. No: Does not display the Options selection on the Tray menu.
Display Advanced Options	Yes: Displays the Advanced options selection on the Tray menu, which allows you to display the Symantec Client Firewall client Advanced Options dialog box to change security settings for individual Web sites as well as other miscellaneous settings. No: Does not display the Advanced options selection on the Tray menu.
Display View Event Log	Yes: Displays the View Event Log selection on the Tray menu, which allows you to view the Event Log. The Event Log contains information on content blocking, connections, firewall activity, and other events. No: Does not display the View Event Log selection on the Tray menu.
Display View Statistics	Yes: Displays the View Statistics selection on the Tray menu, which allows you to view realtime, detailed protection statistics. No: Does not display the View Statistics selection on the Tray menu.

Advanced options settings

Table 7-9 describes the Advanced options settings. For all of these settings, the client computer must be restarted before the setting will take effect.

Table 7-9 Advanced options settings

Setting	Description
HTTP Port List	Specifies the list of ports: HTTP ports to filter for Java and ActiveX blocking, script blocking, confidential information, and so on. Note that when this option is selected, any ports listed here will overwrite any ports listed on a client through the Symantec Client Firewall client user interface.
Block IGMP Protocol	Enable: Blocks the use of the Internet Group Management Protocol (IGMP), a standard for IP multicasting on the Internet. Attackers sometimes exploit this protocol to freeze a computer once they obtain its IP address. Disable: Does not block IGMP.
Stealth Block Ports	Enable: Blocked ports do not respond to inquiries from the Internet. Disable: Blocked ports respond that they are closed.
Block Fragmented IP Packets	Enable: Blocks IP packets that have severely fragmented headers and contain data areas that are too small to be useful for legitimate network communications. Disable: Does not block bad IP packets. IP packets of this type are used in system attacks.

Setting Symantec Client Firewall client user access levels

The extent of individual customization of the Symantec Client Firewall client and available information is determined by the client's user access level. As the firewall administrator, you set the user access level for firewalls in Symantec Client Firewall Administrator. The user access level setting is saved when you save the policy. The user access level setting is implemented for firewalls after the policy is rolled out.

The Symantec Client Firewall client user levels are listed and described in Table 7-10.

Table 7-10 Symantec Client Firewall client user access levels

User level	Description
Admin	Users with Admin access have the same access permissions as firewall administrators for their local Symantec Client Firewall client: ■ Adding, modifying, and deleting any Admin or User type rules ■ Changing all client settings, including enabling and disabling the firewall ■ Adding and deleting IP addresses to Trusted and Restricted Zones ■ Editing the Intrusion Detection Signature Exclusion list ■ Modifying privacy control settings ■ Running LiveUpdate
Normal	Users with Normal access rights have the following permissions: ■ Adding, modifying, and deleting User type rules; limited view ■ Viewing the Event Log; viewing statistics; deciding which data to view (in Statistics window only) ■ Enabling or disabling silent rule creation ■ Limited viewing of Zone IP addresses ■ Running application scans ■ Modifying Privacy Control settings and setting reporting level ■ Running LiveUpdate and using Help
Restricted	Users with Restricted access rights have limited access to the Symantec Client Firewall client: ■ Running LiveUpdate and using Help Once a user is classified as Restricted, that user will be unable to run any Internet applications unless there are specific rules permitting access to Internet applications in the same policy file.

When you assign an access level of Restricted, you need to configure other client configuration settings:

- Use a setting other than Medium for the Symantec Client Firewall client or Privacy Control settings.

  A setting of Medium means that the user will be prompted about allowing or blocking communication each time that there is a cookie, Java applet, ActiveX control, and so forth, on a Web site. Since Restricted users do not have permission to respond to alerts, and will not see the alerts, the Medium setting is not applicable.
- Disable the Access Control Alerts setting, because restricted users are neither able to receive nor respond to alerts.

To set Symantec Client Firewall client user access levels

- In Symantec Client Firewall Administrator, on the Client Settings tab, under Access Level, in the Value column, on the User Type row, select one of the following:
  - Admin
  - Normal
  - Restricted
  - Keep User Selection - Do Not Change

Enabling Automatic Internet Access Control

The Symantec Client Firewall client maintains a pRule database of Internet applications that are generally safe to use. The Automatic Internet Access Control works by allowing the pRule database to automatically create firewall rules for applications that it recognizes, the first time applications are run. When Internet applications are run that the pRule database does not recognize, the rules for the application cannot be generated in this fashion, and must either be manually configured at the client or handled by some other method (blocked or filtered).

When this setting is enabled, the amount of interaction between the client and the firewall software is minimized. The Enable selection is recommended in most situations.

Note: A client user must have a system account with access to the Windows registry to use Automatic Internet Acess Control.

Client settings and computer privileges

For client users to configure rules, they must have computer privileges that allow them to update the Windows registry. Without these privileges, their rules and settings changes in response to alerts will not be saved, and they will experience repetitions of the same alerts.

If users cannot have access to the Windows registry, you need to roll out a policy that has both Automatic Internet Access Control and Access Control Alerts disabled.

Chapter 8

Managing client log data

This chapter includes the following topics:

About logging

The Symantec Client Firewall client event logs contain information about activity permitted and blocked by the firewall for each client and data on various aspects of firewall functioning. You can examine the specifics of problem communications, or assess patterns of overall firewall activity.

Data for the Event Log is organized into categories. Table 8-1 lists the Event Log tabs and their descriptions.

Table 8-1 Event Log tabs

Tab	Information
Content Blocking	Details about Java applets and ActiveX controls blocked by the Symantec Client Firewall client.
Connections	A history of all TCP/IP network connections made with the Symantec Client Firewall client computer. Connections are logged when the connection is closed.
Firewall	Communications intercepted by the firewall, including rules that were processed, alerts displayed, unused ports blocked, and AutoBlock events.
Intrusion Detection	Whether Intrusion Detection is active, the attack signatures being monitored, and the number of intrusions blocked. Also lists any IDS attacks that occurred and were blocked.
Privacy	The cookies that have been permitted or blocked, including the name of the cookie and the Web site that requested the cookie. The information listed is dependent on the cookie settings.
System	Shows when the Symantec Client Firewall client has been enabled or disabled, connection activity, and administrator updates to rules, pRules, and IDS settings.
Web History	URLs visited by the Symantec Client Firewall client computer. This provides a history of Web activity.
Alerts	Shows all alert activity, including normal Internet Access Control alerts and security alerts triggered by possible attacks on the Symantec Client Firewall client computer.

Saving client log data to text files

There may be cases in which you want to save individual Symantec Client Firewall client Event Log data for later inclusion in spreadsheets and reports.

You can save firewall log data for any Symantec Client Firewall client Event Log category by using the Log Export command line utility. The Log Export utility (LogExprt.exe) is supplied with Symantec Client Firewall client and lets you create a delimited text file that contains log data from a single Event Log category. Each possible log corresponds to a tab in the Event Log dialog box (for example, System or Alerts).

By default, the Log Export (LogExprt.exe) application is located in the ...\Program Files\Symantec Client Firewall directory.

Log Export utility syntax

The Log Export (LogExprt.exe) command line utility has the following syntax:

LogExprt [-v] [-l<Log>] [-x<File>] [-d<Delimiter>] [-f + | -, Col, Data]

Each of the parameters and a description of its use is provided in Table 8-2.

Table 8-2 LogExprt.exe parameter descriptions

Parameter	Description and usage
-v	Used by itself, -v lists the names of the individual Symantec Client Firewall client Event Log files (ending with the file suffix .rel, one for each tab category). Using the -v parameter together with the -l parameter (and a .rel file name) returns the column names of the specified Event Log file.
-l<Log>	Used in conjunction with other parameters, identifies the Symantec Client Firewall client Event Log file (.rel file). Path names that contain spaces must be enclosed in double quotes.
-x<File>	Used with the -l parameter, exports the log data from the specified Symantec Client Firewall client Event Log file. If an export file name is not specified, the Event Log .rel file name is used, but with a file suffix of .txt. Path names that contain spaces must be enclosed in double quotes.

Table 8-2 LogExprt.exe parameter descriptions

Parameter	Description and usage
-d<Delimiter>	Specifies the single character to be used as a delimiter when exporting the Symantec Client Firewall client Event Log data to a text file. If this parameter is omitted, the default delimiter used is the comma character (,). The delimiter must be enclosed in double quotes.
-f + | -, Col, Data	Specifies data filtering. You can use multiple filters within a single LogExprt command. A plus (+) or minus (-) defines the filter type. ■ Plus (+) specifies that only Event Log entries will be exported that match the values specified for Col and Data. ■ The minus (-) character specifies that all Event Log entries will be exported except those that match the values specified for Col and Data. Col specifies the column in the event log file to which the filter applies. You may use wildcards. Col is not case-sensitive. Data specifies the values to search for in the specified column. This data must be matched for the filter to take effect. You may use wildcards. Data is not case-sensitive. Filter specifications that contain spaces must be enclosed in double quotes.

Using wildcard characters in filters with LogExprt.exe

You can use the wildcard characters shown in Table 8-3 when using filters with a LogExprt.exe command.

Table 8-3 Wildcard characters that can be used with LogExprt.exe

Wildcard	Description
*	Matches any sequence of characters (zero or more)
?	Matches any single character
\	Suppresses the syntactic significance of special characters
[SET]	Matches any character in the specified set
[!SET] or [^SET]	Matches any character that is not in the specified set

Log Export utility examples

The following command-line examples demonstrate typical LogExprt usage:

- LogExprt.exe -v -liamalert
  Lists the columns in the Alerts event log category.

- LogExprt.exe -x -liamalert
  Exports data from the Alerts event log file to a comma-delimited file named Iamalert.txt in the current directory.

- LogExprt.exe -x"c:\logs\log.txt" -liamalert
  Exports data from the Alerts event log file to a comma-delimited file named Log.txt in the c:\logs directory.

- LogExprt.exe -x -liamfw -d"~"
  Exports data from the Firewall event log file to a tilde-delimited file named Iamfw.txt in the current directory.

- LogExprt.exe -x -liamfw -f"+,Date,1/*/2002"
  Exports data from the Firewall event log file to a comma-delimited file named Iamfw.txt in the current directory. Only entries created during January, 2002 will be added to the file.

- LogExprt.exe -x -liamfw -f"+,Date,1/*/2002" -f"+,Message,*CONNECT*"
  Exports data from the Firewall event log file to a comma-delimited file named Iamfw.txt in the current directory. Only entries created during January, 2002 that contain the word CONNECT in the Message column will be added to the file.

Index