McAfee® Host Intrusion Prevention

version 7.0
COPYRIGHT
Copyright © 2007 McAfee, Inc. All Rights Reserved.
No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS
AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEE SECURITYALLYALLIANCE EXCHANGE), MCAFEE, MCAFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

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

License Attributions
Refer to the product Release Notes.
# Contents

1 **Introducing Host Intrusion Prevention** | 7
- What's new in this release ............................................. 8
- New features .................................................................. 8
- Using this guide ............................................................... 8
- Audience ....................................................................... 9
- Conventions .................................................................... 10
- Getting product information ............................................ 11
- Standard documentation .................................................. 11
- Contact information .......................................................... 12

2 **Basic Concepts** | 13
- IPS feature ................................................................. 13
  - Signature rules ........................................................ 13
  - Behavioral rules ........................................................ 14
  - Events ......................................................................... 14
  - Reactions .................................................................... 14
  - Exception rules .......................................................... 14
- Firewall feature ............................................................ 15
  - Firewall rules ............................................................ 15
  - Client firewall rules ..................................................... 15
- Application Blocking feature ........................................... 16
  - Client application blocking rules .................................. 16
- General feature ............................................................ 16
- Policy management .......................................................... 17
  - Policy enforcement ....................................................... 17
  - Policies and policy categories ....................................... 17
  - Policy inheritance and assignment ............................... 18
  - Policy ownership .......................................................... 18
  - Policy assignment locking ............................................ 18
- Deployment and management ........................................... 19
  - Preset protection ........................................................ 19
  - Adaptive and Learn mode ............................................ 19
  - Tuning ......................................................................... 20
  - Reports ........................................................................ 20

3 **Using ePolicy Orchestrator** | 21
- ePolicy Orchestrator operations used with Host Intrusion Prevention ........................................ 22
  - ePolicy Orchestrator console ....................................... 22
  - Policy management ....................................................... 23
  - Assigning owners to policies ......................................... 24
  - Generating notifications ............................................... 24
  - Generating reports ....................................................... 24
- Host Intrusion Prevention operations ................................ 24
  - Installing the Host Intrusion Prevention server .......... 24
  - Deploying Host Intrusion Prevention clients ............... 25
  - Viewing and working with client data ......................... 25
  - Placing clients in Adaptive or Learn mode .................. 26
  - Configuring policies ..................................................... 27
  - Fine-tuning ................................................................. 28
  - Using Help .................................................................. 29
4 IPS Policies 31
Overview ................................................................. 31
Host and network IPS signature rules ...................... 32
Preset IPS policies .................................................. 33
Quick access ......................................................... 34
Configuring the IPS Options policy .......................... 34
Configuring the IPS Protection policy ....................... 36
Configuring the IPS Rules policy ............................... 39
IPS Rules policy details ........................................... 40
Exception Rules ..................................................... 40
Signatures ............................................................. 44
Application Protection Rules ................................... 51
IPS Events ............................................................ 54
Viewing events ....................................................... 55
Configuring the event view ...................................... 56
Filtering events ...................................................... 56
Marking events ....................................................... 57
Marking similar events .......................................... 58
Viewing event details ............................................. 59
Creating event-based exceptions and trusted applications ..... 59
IPS Client Rules ...................................................... 61
Regular View ......................................................... 62
Aggregated View ................................................... 62
Search IPS Exception View .................................... 64
IPS Events ............................................................ 54
Viewing events ....................................................... 55
Configuring the event view ...................................... 56
Filtering events ...................................................... 56
Marking events ....................................................... 57
Marking similar events .......................................... 58
Viewing event details ............................................. 59
Creating event-based exceptions and trusted applications ..... 59
IPS Client Rules ...................................................... 61
Regular View ......................................................... 62
Aggregated View ................................................... 62
Search IPS Exception View .................................... 64
5 Firewall Policies 66
Overview ................................................................. 66
Rules ................................................................. 67
How firewall rules work ......................................... 68
How stateful filtering works ..................................... 69
How stateful packet inspection works ....................... 70
Firewall rule groups and connection-aware groups ........ 72
Isolating network connections ................................ 73
Firewall Learn and Adaptive modes ......................... 75
Quarantine policies and rules ................................... 76
Preset Firewall policies ........................................... 77
Configuring the Firewall Options policy ..................... 78
Configuring the Firewall Rules policy ........................ 79
Creating new Firewall Rules policies ....................... 80
Creating a new firewall rule or firewall group ............... 82
Filtering and aggregating firewall client rules .............. 85
Viewing and editing firewall rules .............................. 87
Deleting a firewall rule or group ............................... 87
Associating rules, groups and connection-aware groups ...... 87
Configuring the Quarantine Options policy ................ 88
Quarantine ............................................................. 89
Creating new Quarantine Rules policies .................... 90
Viewing and editing quarantine rules ........................ 91
Creating a new quarantine rule or group .................... 91
Deleting a quarantine rule or group .......................... 92
6 Application Blocking Policies 93
Overview ................................................................. 93
Application creation ............................................... 93
Application hooking .............................................. 94
Preset Application Blocking policies ....................... 94
Quick access ......................................................... 94
Configuring the Application Blocking Options policy .... 95
Configuring the Application Blocking Rules policy ....... 97
## General Policies

Overview ................................................. 102
Preset General policies ................................ 103
Configuring Enforce Policies .......................... 104
Configuring the Client UI policy ....................... 104
Creating and applying a Client UI policy .......... 105
Configuring the Trusted Networks policy .......... 110
Configuring the Trusted Applications policy . . 111
Creating and applying Trusted Applications policies 111
Creating trusted applications ....................... 112
Editing trusted applications ......................... 113
Enabling and disabling trusted applications .... 114
Deleting trusted applications ....................... 114

## Maintenance

Fine-tuning a deployment ........................... 115
Analyzing IPS events ................................ 115
Creating exception rules and trusted application rules 116
Working with client exception rules ............... 116
Creating and applying new policies ................ 116
Policy maintenance and tasks ....................... 117
Policies tab ........................................... 117
Policy Catalog ........................................ 119
Running server tasks ................................ 122
Directory Gateway ................................... 122
Event Archiver ........................................ 122
Property Translator .................................. 122
Setting up notifications for events ............... 123
How notifications work ................................ 123
Host Intrusion Prevention notifications ......... 124
Running reports ....................................... 125
Pre-defined reports .................................. 125
Host Intrusion Prevention reports ................ 126
Updating ............................................... 130
Checking in the update package ................. 130
Updating clients ...................................... 131

## Host Intrusion Prevention Client

Windows client ....................................... 132
System tray icon ...................................... 133
Client console ........................................ 133
Alerts ..................................................... 137
IPS Policy tab ......................................... 142
Firewall Policy tab .................................... 144
Application Policy tab ............................... 146
Blocked Hosts tab .................................... 148
Application Protection tab ......................... 150
Activity Log tab ...................................... 151
Solaris client .......................................... 153
Policy enforcement with the Solaris client .... 153
Troubleshooting ....................................... 153
Linux client ............................................. 156
Policy enforcement with the Linux client ....... 156
Notes about the Linux client ....................... 156
Troubleshooting ....................................... 157
McAfee® Host Intrusion Prevention is a host-based intrusion detection and prevention system that protects system resources and applications from external and internal attacks.

Host Intrusion Prevention protects against unauthorized viewing, copying, modifying, and deleting of information and the compromising of system and network resources and applications that store and deliver information. It accomplishes this through an innovative combination of host intrusion prevention system signatures (HIPS), network intrusion prevention system signatures (NIPS), behavioral rules, and firewall rules.

Host Intrusion Prevention is fully integrated with ePolicy Orchestrator and uses the ePolicy Orchestrator framework for delivering and enforcing policies. The division of Host Intrusion Prevention functionality into IPS, Firewall, Application Blocking, and General features provides greater control in delivering policy protections and protection levels to the users.

Protection is provided as soon as Host Intrusion Prevention is installed. The default protection settings require little or no tuning and allow for a rapid, large-scale deployment. For greater protection, edit and add policies to tune the deployment.

For basic information about using this product and this guide, see:

- What’s new in this release
- Using this guide
- Getting product information
- Contact information
What’s new in this release

Host Intrusion Prevention 7.00 provides support for 32-bit and 64-bit operating systems; Windows Vista; IPv6; ePolicy Orchestrator 4.0; improved time-based password support; Terminal Server; and protection of corporate network by isolation from non-corporate interfaces, quarantine during bootup. A command-line maintenance tool and a troubleshooting interface have been added.

New features

- New operating system support (32-bit and 64-bit)
  - Windows Vista.
  - Windows 2003 SP1 or later.
- Corporate network isolation:
  - Blocks all traffic that does not match the selected Connection Aware Group.
  - Protects from accidental security breach caused by opening other network interfaces while engaged with the corporate network.
- Application of quarantine rules during bootup until the firewall service starts up.
- Protection and local interface access for all terminal server/multiple user sessions.
- Network IPS and self-protection security enhancements.
- Troubleshooting enhancement: The Client UI policy page now includes a configurable Troubleshooting tab.
- ePolicy Orchestrator v4 Support: web-based interface; new workflows; dashboards.
- IPv6 Support in Firewall: where an IP address is required, the interface accepts both IPv4 and IPv6 addresses.
- Time-based passwords:
  - Can be applied to groups of devices.
  - Can be shorter, making them useful to help desk and end users.
- Command-line maintenance tool:
  - Leverages the new time-based passwords for easier maintenance.
  - Turns logs, engines on/off; exports activity log.
  - Works with third-party deployment tools

Using this guide

This guide provides the following information on configuring and using your product. For system requirements and installation instructions, refer to the Configuration Guide.
Introducing Host Intrusion Prevention
An overview of the product, including a description of new or changed features; an overview of this guide; McAfee contact information.

Basic Concepts
An explanation of the basic elements of Host Intrusion Prevention and how they work.

Using ePolicy Orchestrator
An explanation of how to use Host Intrusion Prevention and ePolicy Orchestrator.

IPS Policies
An explanation of how to work with IPS policies.

Firewall Policies
An explanation of how to work with firewall policies.

Application Blocking Policies
An explanation of how to work with application blocking policies.

General Policies
An explanation of how to work with general policies.

Maintenance
An explanation of how to maintain and update Host Intrusion Prevention.

Host Intrusion Prevention Client
An explanation of how to work with the client.

Frequently Asked Questions
Answers to frequently asked questions about Host Intrusion Prevention.

Writing Custom Signatures
Appendix on how to write custom signatures.

Glossary

Index

Audience
This information is intended for network or IT administrators who are responsible for their company’s host intrusion detection and prevention system.
Conventions

This guide uses the following conventions:

**Bold**
All words from the user interface, including options, menus, buttons, and dialog box names.

**Example:**
Type the *User* name and *Password* of the desired account.

**Condensed**
The path of a folder or program; text that represents something the user types exactly (for example, a command at the system prompt).

**Example:**
The default location for the program is:

```
C:\Program Files\McAfee\EPO\3.5.0
```

Run this command on the client computer:

```
C:\SETUP.EXE
```

**Courier**
For emphasis or when introducing a new term; for names of product documentation and topics (headings) within the material.

**Example:**
Refer to the *VirusScan Enterprise Product Guide* for more information.

**Italic**
A web address (URL) and/or a live link.

Visit the McAfee web site at:

[http://www.mcafee.com](http://www.mcafee.com)

<TERM> Angle brackets enclose a generic term.

**Example:**
In the console tree, right-click <SERVER>.

**Note:** Supplemental information; for example, an alternate method of executing the same command.

**Tip:** Suggestions for best practices and recommendations from McAfee for threat prevention, performance and efficiency.

**Caution:** Important advice to protect your computer system, enterprise, software installation, or data.

**Warning:** Important advice to protect a user from bodily harm when interacting with a hardware product.
Getting product information

Unless otherwise noted, the product documentation are Adobe Acrobat .PDF files available on the product CD or from the McAfee download site.

Standard documentation

**Installation Guide** — Procedures for deploying and managing supported products through the ePolicy Orchestrator management software.

**Product Guide** — Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures.

**Help** — High-level and detailed information accessed from the software application Help button.

**Quick Reference Card** — A handy card with information on basic product features, routine tasks that you perform often, and critical tasks that you perform occasionally. A printed card accompanies the product CD.

**Release Notes** — ReadMe. Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation. (A text file is included with the software application and on the product CD.)
Contact information

**Threat Center: McAfee Avert® Labs**  
Avert Labs Threat Library  
http://vil.nai.com  
Avert Labs WebImmune & Submit a Sample *(Logon credentials required)*  
https://www.webimmune.net/default.asp  
Avert Labs DAT Notification Service  
http://vil.nai.com/vil/signup_DAT_notification.aspx

**Download Site**  
**Product Upgrades** *(Valid grant number required)*  
**Security Updates** *(DATs, engine)*  
**HotFix and Patch Releases**  
- **For Security Vulnerabilities** *(Available to the public)*  
- **For Products** *(ServicePortal account and valid grant number required)*  
**Product Evaluation**  
**McAfee Beta Program**

**Technical Support**  
http://www.mcafee.com/us/support/  
**KnowledgeBase Search**  
http://knowledge.mcafee.com/  
**McAfee Technical Support ServicePortal** *(Logon credentials required)*  
https://mysupport.mcafee.com/eservice_enu/start.swe

**Customer Service**  
**Web**  
http://www.mcafee.com/us/about/contact/index.html  
**Phone** — US, Canada, and Latin America toll-free:  
+1-888-VIRUS NO or +1-888-847-8766  
Monday – Friday, 8 a.m. – 8 p.m., Central Time

**Professional Services**  
**Enterprise:**  
**Small and Medium Business:**  
McAfee® Host Intrusion Prevention is a host-based intrusion protection system. It protects against known and unknown attacks, including worms, Trojan horses, buffer overflow, critical system file modification, and privilege escalation. Host Intrusion Prevention management is delivered through the ePolicy Orchestrator console and provides the ability to set and apply host intrusion prevention, firewall, application blocking, and general policies. Host Intrusion Prevention clients are deployed to servers and desktops and function as independent protective units. They report their activity to ePolicy Orchestrator and retrieve updates for new attack definitions.

This section describes the four features of Host Intrusion Prevention and how it works with ePolicy Orchestrator, and includes the following topics:

- **IPS feature**
- **Firewall feature**
- **Application Blocking feature**
- **General feature**
- **Policy management**
- **Deployment and management**

**IPS feature**

The IPS (Intrusion Prevention System) feature monitors all system and API calls and blocks those that might result in malicious activity. Host Intrusion Prevention determines which process is using a call, the security context in which the process runs, and the resource being accessed. A kernel-level driver, which receives redirected entries in the user-mode system call table, monitors the system call chain. When calls are made, the driver compares the call request against a database of combined signatures and behavioral rules to determine whether to allow, block, or log an action.

**Signature rules**

Signature rules are patterns of characters than can be matched against a traffic stream. For example, a signature rule might look for a specific string in an HTTP request. If the string matches one in a known attack, action is taken. These rules provide protection against known attacks.
Signatures are designed for specific applications and for specific operating systems; for example, web servers such as Apache, IIS, and NES/iPlanet. The majority of signatures protect the entire operating system, while some protect specific applications.

**Behavioral rules**

Hard-coded behavioral rules define a profile of legitimate activity. Activity not matching the profile is considered suspicious and triggers a response. For example, a behavioral rule might state that only a web server process should access HTML files. If any other process attempts to access html files, action is taken. These rules provide protection against zero-day and buffer overflow attacks.

**Events**

IPS Events are generated when a client recognizes a signature or behavioral rule violation. Events are logged in the IPS Events tab of IPS Rules. Administrators can monitor these events to view and analyze system rule violations. They can then adjust event reactions or create exceptions or trusted application rules to reduce the number of events and fine-tune the protection settings.

**Reactions**

A reaction is what a client does when it recognizes a signature of a specific severity. A client reacts in one of three ways:

- **Ignore** — No reaction; the event is not logged and the process is not prevented.
- **Log** — The event is logged but the process is not prevented.
- **Prevent** — The event is logged and the process is prevented.

A security policy may state, for example, that when a client recognizes an Information level signature, it logs the occurrence of that signature and allows the process to be handled by the operating system; and when it recognizes a High level signature, it prevents the process.

> Logging can be enabled directly on each signature.

**Exception rules**

An exception is a rule for overriding blocked activity. In some cases, behavior that a signature defines as an attack may be part of a user’s normal work routine or an activity that is legal for a protected application. To override the signature, you can create an exception that allows legitimate activity. For example, an exception might state that for a particular client, a process is ignored.

You can create these exceptions manually, or place clients in Adaptive mode and allow them to create client exception rules. To ensure that some signatures are never overridden, edit the signature and disable the Allow Client Rules options. You can track the client exceptions in the ePolicy Orchestrator console, viewing them in a regular and aggregated view. Use these client rules to create new policies or add them to existing policies that you can apply to other clients.
Firewall feature

The Host Intrusion Prevention Firewall feature acts as a filter between a computer and the network or Internet it is connected to. The Firewall Rules policy uses static packet filtering with top-down rule matching. When a packet is analyzed and matched to a firewall rule, with criteria such as IP address, port number, and packet type, the packet is allowed or blocked. If no matching rule is found, the packet is dropped. The current version Firewall Rules policy uses both stateful packet filtering and stateful packet inspection.

Other features include:
- A Quarantine Mode into which client computers can be placed and to which you can apply a strict set of firewall rules that defines with whom quarantined clients can and cannot communicate.
- Connection Aware Groups that let you create specialized rule groups based on a specific connection type for each network adapter.

Firewall rules

You can create firewall rules as simple or complex as you need. Host Intrusion Prevention supports rules based on:
- Connection type (network or wireless).
- IP and non-IP protocols.
- Direction of the network traffic (incoming, outgoing, or both).
- Applications that generated the traffic.
- Service or port used by a computer (as the recipient or the sender).
- Service or port used by a remote computer (as the sender or the recipient).
- Source and destination IP addresses.
- Time of day or week that the packet was sent or received.

Client firewall rules

As with the IPS rules, a client in Adaptive or Learn mode can create client rules to allow blocked activity. You can track the client rules and view them in a regular and aggregated view. Use these client rules to create new policies or add them to existing policies that can be applied to other clients.
The Application Blocking feature monitors applications being used and either allows or blocks them.

Host Intrusion Prevention offers two types of application blocking:

- Application creation
- Application hooking

When Host Intrusion Prevention monitors application creation, it looks for programs that are trying to run. In most cases, there is no problem; but, there are some viruses, for example, that try to run programs that harm a system. You can prevent this by creating application rules, similar to firewall rules, which only allow programs to run that are permitted for a user.

When Host Intrusion Prevention monitors application hooking, it looks for programs that are trying to bind or “hook” themselves to other applications. Sometimes, this behavior is harmless, but sometimes this is suspicious behavior that can indicate a virus or other attack on your system.

You can configure Host Intrusion Prevention to monitor only application creation, only application hooking, or both.

The Application Blocking feature works like the Firewall feature. Create a list of application rules; one rule for each application you want to allow or block. Each time Host Intrusion Prevention detects an application trying to start or hook to another application, it checks its application rule list to determine whether to allow or block the application.

 Clients in Adaptive or Learn mode can create client rules to allow blocked application creation or hooking, which appear in both a regular and aggregated view. Use these client rules, just as you would with the IPS and firewall client rules, to create new policies or add them to existing policies that can be applied to other clients.

The Host Intrusion Prevention General feature provides access to policies that are general in nature and not specific to IPS, Firewall, or Application Blocking features. This includes:

- Enabling or disabling the enforcement of all policies.
- Determining how the client interface appears and is accessed.
- Creating and editing trusted network addresses and subnets.
- Creating and editing trusted applications to prevent triggering false positive events.
Policy management

A policy is a collection of Host Intrusion Prevention settings that you configure through the ePolicy Orchestrator console, then enforce on Host Intrusion Prevention clients. Policies allow you to ensure that the security software on managed systems is configured to meet the needs of your environment.

The ePolicy Orchestrator console allows you to configure Host Intrusion Prevention policies from a central location. Policies are a part of the Host Intrusion Prevention NAP file added to the master repository when you installed Host Intrusion Prevention.

Policy enforcement

When you change Host Intrusion Prevention policies in the ePolicy Orchestrator console, the changes take effect on the managed systems at the next agent-to-server communication interval (ASCI). This interval is set to occur once every 60 minutes by default.

Host Intrusion Prevention policies can be enforced immediately by running a wake-up call from the ePolicy Orchestrator console.

Policies and policy categories

Policy information for each product is grouped by category. Each policy category refers to a specific subset of policies. In the Policy Catalog, a product’s policy categories are displayed when you expand the product name.

Figure 2-1 Policy Catalog

A named policy is a configured set of policy definitions for a specific policy category. You can create, modify, or delete as many named policies as needed for each policy category. In the Policy Catalog, named policies for a specific category are displayed when you expand the category name.

Each policy category has a Global Default named policy. You cannot edit or delete this policy.
Two Host Intrusion Prevention policy categories, **IPS Rules** and **Trusted Applications**, enable you to assign more than one named policy instances and offer a profile of IPS and application policies that can be applied.

**Figure 2-2 A profile of two Trusted Application policy instance**

<table>
<thead>
<tr>
<th>Trusted Applications</th>
<th>Assign additional policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted applications are safe in any environment, have no known vulnerabilities, and are allowed to perform all operations except those that compromise the application. Use this section to create distinct policies based on client profiles. You can then assign a combination of these policies to configure appropriate protection for clients.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Created At</th>
<th>Inherited From</th>
<th>Inherited By</th>
<th>Delete</th>
<th>Lock</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee 1 Global Default</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>McAfee 2 (this node)</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Policy inheritance and assignment**

Policies are applied to any console Directory tree node by inheritance or assignment. *Inheritance* determines whether the policy settings for any node are taken from its parent. By default, inheritance is enabled throughout the Directory. You can break inheritance by direct policy *assignment*. Host Intrusion Prevention, as managed by ePolicy Orchestrator, enables you to create policies and assign them without regard to inheritance. When you break this inheritance by assigning a new policy anywhere in the Directory, all child nodes inherit the new policy.

**Policy ownership**

With all policies available, each policy is then required to have an assigned owner. By default, the owner of a policy is the global or site administrator who created it.

Ownership ensures that no one other than the global administrator or owner of the named policy can modify it. Any administrator can use any policy that exists in the catalog, but only the owner or global administrator can modify it.

If you assign a policy that you do not own to nodes of the Directory that you administer, and the owner of the policy modifies it, all systems to which this policy is assigned receive these modifications.

To use and control a policy owned by a different administrator, duplicate the policy and then assign the duplicate policy.

**Policy assignment locking**

A global administrator can lock the assignment of a policy at any location within the Directory. Policy assignment locking prevents other users from switching the assignment of one policy for another. It is inherited with the policy.

Policy assignment locking is useful if a global administrator configures and assigns a certain policy at the top of the Directory to ensure no other users replace it with a different named policy anywhere in the Directory.

Policy locking does not prevent the policy owner from making changes to the named policy’s settings. Therefore, if you intend to lock a policy assignment, be sure that you are the owner of the policy.
Deployment and management

The deployment and management of Host Intrusion Prevention clients are handled from ePolicy Orchestrator. In the ePO console tree you can group clients hierarchically by attributes. For example, you might group a first level by geographic location and a second level by operating system platform or IP address. We recommend grouping clients by Host Intrusion Prevention configuration criteria, including system type (server or desktop), use of major applications (web, database, or mail server), and strategic locations (DMZ or intranet). You can place clients that fit a common usage profile into a common group on the console tree. In fact, you might name a group after its usage profile, for example, Web Servers.

With computer grouped in the console tree according to type, function, or geographic location, you can easily divide administrative functions along the same lines. With Host Intrusion Prevention you can also divide administrative duties based on product features, such as IPS or firewall.

With this release of Host Intrusion Prevention and ePolicy Orchestrator, policies are independent entities that are shareable across multiple nodes. You assign one policy for each category in a feature of Host Intrusion Prevention. Some categories, such as IPS rules, allow for several policies, with some either inherited from a parent node or applied at the node itself. In this instance, Host Intrusion Prevention handles conflicts by applying the stricter rule first. Through inheritance in ePolicy Orchestrator, when you assign a group node the appropriate policies, every system under that node automatically inherits its parent’s configuration.

Deploying Host Intrusion Prevention clients to thousands of computers is easily managed because most clients fit into a few usage profiles. Managing a large deployment is reduced to maintaining a few policy rules. As a deployment grows, newly added systems should fit one or more existing profiles, and can be placed under the correct group node on the console tree.

Preset protection

Host Intrusion Prevention offers basic protection through the McAfee default policy settings. This “out-of-the-box” protection requires no tuning and generates few events. Clients can be initially deployed on a large scale, even before you tune the deployment. For many environments where the client is installed on workstations and laptops, this basic protection may be sufficient.

Advanced protection is also available from some preset IPS and firewall policies. A profile for servers, for example, needs stronger protection than that offered in basic workstation protection. Or you can use the preset advanced protection policies as a basis for creating custom policies.

Adaptive and Learn mode

To further tune protection settings, Host Intrusion Prevention clients can create client-side exception rules to server-mandated policies that block legitimate activity. The creation of client rules is permitted when clients are placed in Adaptive or Learn mode. In Adaptive mode, available for IPS, Firewall, and Application Blocking features, client rules are created without interaction from the user. In Learn mode, available for Firewall and Application Blocking features, the user must tell the system whether or not to create a client rule.
In both modes, events are first analyzed for the most malicious attacks, such as buffer overflow. If the activity is considered regular and necessary for business, Host Intrusion Prevention clients create client rules to allow operations that would otherwise be blocked. By placing clients in Adaptive or Learn mode, you can obtain a tuning configuration for them. Host Intrusion Prevention then allows you to take any, all, or none of the client rules and convert them to server-mandated policies. The Adaptive and Learn Modes can be turned off at any time to tighten the system’s intrusion prevention protection.

Often in a large organization, avoiding disruption to business takes priority over security concerns. For example, new applications may need to be installed periodically on some client computers, and you may not have the time or resources to immediately tune them. Host Intrusion Prevention enables you to place specific clients in Adaptive mode for IPS protection. Those computers will profile a newly installed application, and forward the resulting client rules to the server. The administrator can promote these client rules to an existing or new policy and then apply the policy to other computers to handle the new software.

### Tuning

As part of Host Intrusion Prevention deployment, you need to identify a small number of distinct usage profiles and create policies for them. The best way to achieve this is to set up a test deployment, then begin reducing the number of false positives and generated events. This process is called tuning.

Stronger IPS rules, for example, offer more signatures that target a wider range of violations, and generate many more events than in a basic environment. If you apply advanced protection, we recommend using the IPS Protection policy to stagger the impact. This entails mapping each of the severity levels (High, Medium, Low, and Information) to a reaction (Prevent, Log, Ignore). By initially setting all severity reactions except High to Ignore, only the High severity signatures will be applied. The other levels can be raised incrementally as tuning progresses.

You can reduce the number of false positives by creating exception rules, trusted applications, and firewall rules. Exception rules are mechanisms for overriding a security policy in specific circumstances. Trusted applications are application processes that are always permissible. Firewall rules determine whether traffic is permissible, and either allow or block packet transmission.

### Reports

Reports enable you to obtain data about a particular item and filter it for specific subsets of that data, for example high-level events reported by particular clients for a specified time period. Reports can be scheduled and sent as an email message.
You must use ePolicy Orchestrator to configure and manage Host Intrusion Prevention, which consists of these basic tasks:

- **Install/check in Host Intrusion Prevention server files and client package.**
  Use the Host Intrusion Prevention installer to check in the Host Intrusion Prevention server files, which include a NAP file, content with default signatures and rules, and reports to the ePolicy Orchestrator Repository. Check in the Host Intrusion Prevention client package to the ePolicy Orchestrator Repository. For details, see the *Host Intrusion Prevention 7.0 Installation Guide*.

- **Deploy Host Intrusion Prevention clients.**
  Use the ePolicy Orchestrator console to deploy Host Intrusion Prevention clients to computers in the Directory console tree. For details, see the *ePolicy Orchestrator 3.6 Product Guide*.

- **Configure Host Intrusion Prevention policies.**
  Configure the IPS, firewall, application blocking, and general policies to apply to the clients. The default settings in each policy provide basic protection, but for tighter security you need to tune the deployment and configure policies to fit your environment. See the appropriate chapters in this guide for details.

- **Assign owners to policies in the Policy Catalog.**
  Ownership is assigned in the Policy Catalog. For details see the *ePolicy Orchestrator 3.6 Product Guide*.

- **Send Host Intrusion Prevention policy update information to clients.**
  ePolicy Orchestrator sends updated information to Host Intrusion Prevention clients. The clients enforce the policies, collect event information, and transmit the information back to ePolicy Orchestrator. The interaction between client and server is determined by the ePolicy Orchestrator agent policy settings. For details, see the *ePolicy Orchestrator 3.6 Product Guide*.

- **Set up notifications in ePolicy Orchestrator for Host Intrusion Prevention events.**
  For details, see the *ePolicy Orchestrator 3.6 Product Guide*.

- **Run reports in ePolicy Orchestrator to view event and protection results.**
  Information on Host Intrusion Prevention client activity is sent to ePolicy Orchestrator and stored in its database. Use the console to run reports on Host Intrusion Prevention protection.
For more information on using Host Intrusion Prevention with ePolicy Orchestrator, see the following topics:

- ePolicy Orchestrator operations used with Host Intrusion Prevention
- Host Intrusion Prevention operations

### ePolicy Orchestrator operations used with Host Intrusion Prevention

Some basic functionality of Host Intrusion Prevention is carried out by ePolicy Orchestrator features. Details of using these features are found in ePolicy Orchestrator documentation. A brief overview, along with details for areas that are specific to Host Intrusion Prevention, is given in this document.

### ePolicy Orchestrator console

Use the ePolicy Orchestrator console to manage Host Intrusion Prevention. For details, see the ePolicy Orchestrator 3.6 Product Guide.

The ePolicy Orchestrator console is divided into two main sections: a console tree and a details pane.

The console tree is the navigation pane where you select ePolicy Orchestrator nodes (computers, groups, and sites) under the Directory and apply Host Intrusion Prevention policies. The tree also contains links to the other main features of the console interface, including the Policy Catalog, Notifications, and Reports.

The details pane displays the functionality settings of the node selected in the console tree.

![Figure 3-1 ePolicy Orchestrator console](image-url)
Policy management

A policy is a collection of software settings that you create, configure, and enforce. You can apply default policies or create and apply customized policies to any node of the Directory to which you have permissions. You can configure and assign policies before or after a product is deployed. Each policy category indicates whether the policy applies to a Windows client only (Windows) or to all Windows, Solaris, and Linux clients (All Platforms).

You can choose to enforce all or none of the policy selections on any node of the Directory.

In the Assign Policies page, which appears when you select a node, you can choose to enforce policies for products or product features.

**Figure 3-2 Assign Policies page**

In the Policy Catalog page, you can view policy assignments and owners.

**Figure 3-3 Policy Catalog**

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Owner</th>
<th>Assignments</th>
<th>Rename</th>
<th>Duplicate</th>
<th>Delete</th>
<th>Export</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive</td>
<td>Global Administrators</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load</td>
<td>Global Administrators</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Off (McAfee Default)</td>
<td>Global Administrators</td>
<td>1 assignment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On</td>
<td>Global Administrators</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Define new policy...

- IPT Firewall Rules (Windows)
- IPT Rules (Windows)
- Quarantine Options (Windows)
- 7.8 Firewall Rules (Windows)
- 7.8 quarantine Rules (Windows)
Assigning owners to policies

All policies for Host Intrusion Prevention to which you have permissions are available from the Policy Catalog page. To prevent any user from modifying other users’ policies, each policy is assigned an owner: the global or site administrator who created it.

Only a policy’s creator or a global administrator can modify or delete a policy. Any administrator can apply any policy in the Policy Catalog page, but only the owner or global administrator can modify it.

If you assign a policy that you do not own to segments of the Directory, be aware that if the policy owner modifies it, all nodes to which this policy is assigned receive these modifications. To use a policy owned by a different administrator, duplicate the policy, and then assign the duplicate to the node.

Generating notifications

E-mail, pager, and SNMP trap notifications can alert you to any events that occur on Host Intrusion Prevention clients or the server itself. You can configure rules to send messages, SNMP traps, or run external commands when specific Host Intrusion Prevention events are received and processed by the ePolicy Orchestrator server. The highly configurable notification feature enables you to specify the event categories that generate a notification message and the frequencies with which notifications are sent.

Generating reports

The Host Intrusion Prevention clients on the client systems send information to the server, which is stored in a reports database. It is against this stored information that you run reports and queries. There are eight pre-defined reports that fall into two main categories: IPS reports and firewall reports. For additional information, see Running reports on page 125.

Host Intrusion Prevention operations

A brief overview of all aspects of using Host Intrusion Prevention that are specific to the product follow. Details in using these features are found in this document.

Installing the Host Intrusion Prevention server

You must install the management server before you can deploy clients. For detailed instructions, refer to the Host Intrusion Prevention Installation Guide.
Deploying Host Intrusion Prevention clients

Clients are the element that provide protection in a Host Intrusion Prevention deployment. Ideally, every system in a working environment is protected by client software. We recommend a phased approach to deployment:

- **Determine your initial client rollout plan.** Although you will deploy Host Intrusion Prevention clients to every host (servers and desktops) in your company, we recommend that you start by installing clients on a limited number of representative systems and tuning their configuration. After you have fine-tuned the deployment, you can then deploy more clients and leverage the policies, exceptions, and client rules created in the initial rollout.

- **Establish a naming convention for your clients.** Clients are identified by name in the console tree, in certain reports, and in event data generated by activity on the client. Clients can take the names of the hosts on which they are installed, or you can assign a specific client name during installation. We recommend establishing a naming convention for clients that is easy to interpret by anyone working with the Host Intrusion Prevention deployment.

- **Install the clients.** Clients are installed with a default set of IPS, firewall, application blocking, and general rule policies. New policies with updated rules can later be pushed from the server.

- **Group the clients logically.** Clients can be grouped according to any criteria that fits in the console tree hierarchy. For example, you might group clients according to their geographic location, corporate function, or the characteristics of the system.

For detailed instructions, refer to the *Host Intrusion Prevention Installation Guide*.

Viewing and working with client data

After you have installed and grouped your clients, you have completed the deployment. You should begin to see events triggered by activity on the clients in violation of the set IPS security policy. If you have placed clients in Adaptive mode, you should see the client rules that indicate which client exception rules are being created. By analyzing this data, you begin to tune the deployment.

To analyze event data, view the IPS Event tab in the IPS Feature. You can drill down to the details of an event, such as which process triggered the event, when the event was generated, and which client generated the event. Analyze the event and take the appropriate action to tune the Host Intrusion Prevention deployment to provide better responses to attacks. The IPS Event tab displays default client-based and network-based intrusion prevention signatures as well as custom host-based signatures.

To analyze client rules, view the Client Rules tab. Client Rules also appear in the firewall and application blocking features. You can see which rules are being created, aggregate them to find the most prevalent common rules, and move the rule directly to a policy for application to other clients.

In addition, the Reporting feature provides detailed reports based on events, client rules, and the Host Intrusion Prevention configuration. Use these reports to communicate environment activity to other members of your team and management.
Placing clients in Adaptive or Learn mode

A major element in the tuning process placing Host Intrusion Prevention clients in Adaptive mode for IPS, firewall, and application blocking, or Learn mode for firewall and application blocking. These modes allow clients to create client exception rules to administrative policies. Adaptive mode does this automatically without user interaction, while Learn mode requires the user to tell the system what to do when an event is generated.

These modes analyze events first for the most malicious attacks, such as buffer overflow. If the activity is considered regular and necessary for business, client exception rules are created. By setting representative clients in Adaptive or Learn mode, you can obtain a tuning configuration for them. Host Intrusion Prevention then allows you to take any, all or none of the client rules and convert them to server-mandated policies. When tuning is complete, turn off the Adaptive or Learn modes to tighten the system’s intrusion prevention protection.

- Run clients in Adaptive or Learn mode for at least a week. This allows the clients time to encounter all the activity they would normally encounter. Try to do this during times of scheduled activity, such as backups or script processing.

- As each activity is encountered, IPS events are generated and exceptions are created. Exceptions are activities that are distinguished as legitimate behavior. For example, a policy might deem certain script processing as illegal behavior, but certain systems in your engineering groups need to perform such tasks. Allow exceptions to be created for those systems so they can continue to function normally while the policy continues to prevent this activity on other systems. Then make these exceptions part of a server-mandated policy to cover only the engineering group.

- You might have particular software applications that are required for normal business in some areas of the company, but are prevented in others. For example, you might allow Instant Messaging in your Engineering and Technical Support organizations, but prevent its use in your Finance and HR departments. You can establish the application as trusted on the systems in your Engineering and Technical Support organizations to allow users full access to it.

- The Firewall feature acts as a filter between a computer and the network or Internet. The firewall scans all incoming and outgoing traffic at the packet level. As it reviews each arriving or departing packet, the firewall checks its list of firewall rules, which is a set of criteria with associated actions. If a packet matches all the criteria in a rule, the firewall performs the action specified by the rule — either allowing the packet through the firewall, or blocking it.
Configuring policies

Policies are the rules you set for each computer in a network that Host Intrusion Prevention protects. The Host Intrusion Prevention client on the client systems receives these policy updates at regular intervals.

Select a node in the console tree under Directory and the features available in Host Intrusion Prevention appear in the details pane on the Policies tab. These include:

- General Policies
- IPS Policies
- Firewall Policies
- Application Blocking Policies

Click the down arrow to reveal the categories available for each feature. See the appropriate sections in this guide on each of these features for details.

Policy viewing alerts

When you view the details of a Host Intrusion Prevention policy, you may be asked to trust a signed Java applet that is needed to display the policy content. If this alert appears, click Yes (or Always) to display the details of the policy.

Figure 3-4 Java applet security warning
Some Firewall feature policies require an ActiveX control. In opening one of these policies, you may be asked to run the control that is needed to display the policy content. If this alert appears, click Yes to display the details of the policy.

**Figure 3-5 Active X control security warning**

![Security Warning]

---

**Fine-tuning**

After you install the Host Intrusion Prevention software, McAfee recommends that you configure it to provide the greatest amount of security while not conflicting with day-to-day activities. The default policies in Host Intrusion Prevention fit the broadest set of customer environments and may meet your needs. To fine-tune policies to fit your particular setting, we recommend the following practices:

- Carefully define your Host Intrusion Prevention security configuration. Evaluate who is responsible for configuring particular parts of the system and grant them appropriate access.

- Change the default IPS Protection or Firewall Rules policies, which provide increasing levels of preset protection.

- Modify severity levels of specific signatures. For example, when a signature is triggered by day-to-day work of users, adjust the severity level to a lower level. For more information, refer to Configuring the IPS Protection policy on page 36.

- Configure notifications, which alert specific individuals when particular events occur. For example, a notification can be sent when an activity that triggers a High severity event occurs on a particular server. For more information, refer to Setting up notifications for events on page 123.
Using Help

Both ePolicy Orchestrator and Host Intrusion Prevention provide online help. ePolicy Orchestrator help is called from the help button in ePolicy Orchestrator toolbar and the console details panes. Host Intrusion Prevention help is called from the help buttons in the Host Intrusion Prevention Policy Settings page and supporting dialog boxes.

The Host Intrusion Prevention Help window provides information about the policy or dialog box from which it was called. Related Topic links on the page take you to instructions on performing certain tasks. Additional information can be accessed with the table of contents, the index, or the search feature.

Help navigation procedures

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate back to page that initially appeared or from which you clicked a link</td>
<td>Click Back on the shortcut menu.</td>
</tr>
<tr>
<td>Note: Do not use the Previous or Next buttons. They are used to navigate through the linear order of pages in the table of contents.</td>
<td></td>
</tr>
<tr>
<td>View the table of contents, index, and search from a single help pane</td>
<td>Click Show Navigation.</td>
</tr>
<tr>
<td>Indicate where in the table of contents the page appears</td>
<td>Click Show in Contents.</td>
</tr>
<tr>
<td>Note: Some pages are help specific and do not appear in the table of contents.</td>
<td></td>
</tr>
<tr>
<td>Page through the Help as ordered in the table of contents</td>
<td>Click Previous and Next.</td>
</tr>
<tr>
<td>View related how-to topics</td>
<td>Click Related Links.</td>
</tr>
<tr>
<td>Locate an item alphabetically within the index</td>
<td>Click Index in the left pane.</td>
</tr>
<tr>
<td>Print a page</td>
<td>Click Print, or click Print on the shortcut menu.</td>
</tr>
<tr>
<td>Create a bookmark of a page for an HTML browser</td>
<td>Click Bookmark.</td>
</tr>
<tr>
<td>Conduct a search</td>
<td>Click Search in the navigation pane, enter the word or words to search on, and click Go.</td>
</tr>
<tr>
<td>Remove highlighted text on a page after a search</td>
<td>Click Refresh on the shortcut menu.</td>
</tr>
</tbody>
</table>
Help in the user interface

A brief description of what a tab or dialog box is used for appears on the tab or in the dialog box itself.

A description of each toolbar button appears when you place the mouse pointer over it. For icons in lists that represent information, consult the following table:

**Table 3-1 Host Intrusion Prevention icons**

<table>
<thead>
<tr>
<th>IPS Events/Signatures</th>
<th>Severity Level: Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Severity Level: Low</td>
</tr>
<tr>
<td></td>
<td>Severity Level: Medium</td>
</tr>
<tr>
<td></td>
<td>Severity Level: High</td>
</tr>
<tr>
<td></td>
<td>Severity Level: Disabled</td>
</tr>
</tbody>
</table>

**IPS Exception Rules**

|                                | Status: Enabled             |
|                                | Status: Disabled            |
|                                | Reaction: Permit            |
|                                | Reaction: Block             |
|                                | Note attached               |

**IPS Signature Rules**

|                                | Network Intrusion Protection |
|                                | Custom Host Intrusion Protection |

**Firewall/Quarantine/Application Blocking Rules**

|                                | Direction: Incoming         |
|                                | Direction: Outgoing         |
|                                | Direction: Incoming and Outgoing |
|                                | Action: Permit              |
|                                | Action: Block               |
|                                | Treat rule match as intrusion |
|                                | Restrict rule to defined time interval |
The IPS (Intrusion Prevention System) feature of Host Intrusion Prevention protects computers with host intrusion prevention technology. IPS policies turn IPS protection on and off, set the reaction level to events, and provide details on exceptions, signatures, application protection rules, events, and client-generated exceptions.

This section describes the IPS feature and includes the following topics:

- **Overview**
- **Configuring the IPS Options policy**
- **Configuring the IPS Protection policy**
- **Configuring the IPS Rules policy**
- **IPS Rules policy details**
- **IPS Events**
- **IPS Client Rules**
- **Search IPS Exception Rules**

### Overview

Host Intrusion Prevention clients have a database of IPS signature rules that determine whether activity on the client computer is benign or malicious. When malicious activity is detected, alerts known as events are sent to the ePO console and appear in the Host Intrusion Prevention IPS Rules policy.

The protection level set for signatures in the IPS Protection policy determines which action a client takes when an event occurs. Responses or reactions include ignore, log, or prevent the activity.

Events that are false positives arising from legitimate activity can be overridden by creating an exception to the signature rule or by qualifying applications as trusted. Clients in Adaptive mode automatically create exceptions, called client rules. Administrators can manually create exceptions at anytime.

Monitoring the events that occur and the client exception rules that are created helps determine how to tune the deployment for the best IPS protection.
Host and network IPS signature rules

Attacks can follow a signature pattern of characters. This signature can identify and prevent malicious activity. For example, a signature is set to look for the string `/` in a web URL. If the signature is enabled and the system encounters this string, an event is triggered.

A signature-based approach, with both host and network IPS signatures, accounts for the majority of detection schemes used in intrusion detection and is one mechanism that Host Intrusion Prevention uses. A database of signature rules is installed with every client and is updated as new attacks types are discovered.

Signatures are categorized by severity level and by description of the danger an attack poses. They are designed for specific applications and for specific operating systems. The majority protect the entire operating system, while some protect specific applications.

Host Intrusion Prevention offers mostly host IPS signatures with a few additional network IPS signatures.

HIPS

HIPS protection resides on individual systems such as servers, workstations or notebooks. The Host Intrusion Prevention client delivers protection by inspecting traffic flowing into or out of a system and examining the behavior of the applications and operating system for attacks. When an attack is detected, the client can block it at the network segment connection, or can issue commands to the application or operating system to stop the behavior initiated by the attack. For example, buffer overflow is prevented by blocking malicious programs inserted into the address space exploited by an attack. Installation of back door programs with applications like Internet Explorer is blocked by intercepting and denying the application’s “write file” command.

Benefits of Host IPS

- Protects against an attack as well as the results of an attack, such as blocking a program from writing a file.
- Protects laptops against attack when they are outside the protected network.
- Protects against local attacks introduced by CDs, memory sticks, or floppy disks. These attacks often focus on escalating the user’s privileges to “root” or “administrator” to compromise other systems in the network.
- Provides a last line of defense against attacks that have evaded other security tools.
- Prevents internal attack or misuse on devices located on the same network segment.
- Protects against attacks where the encrypted data stream terminates at the system being protected by examining the decrypted data and behavior.
- Independent of network architecture; allows for protection of systems on obsolete or unusual network architectures such as Token Ring or FDDI.
NIPS

NIPS protection also resides on individual systems. All data that flows between the protected system and the rest of the network is examined for an attack. When an attack is identified, the offending data is discarded or blocked from passing through the system.

Benefits of Network IPS

- Protects systems located downstream in a network segment.
- Protects servers and the systems that connect to them.
- Protects against network Denial-of-Service attacks and bandwidth-oriented attacks that deny or degrade network traffic.

Behavioral rules

Behavioral rules define a profile of legitimate activity. Activity that does not match the profile triggers an event. For example, you can set a rule stating that only a web server process should access web files. If another process attempts to access a web file, this behavioral rule triggers an event.

Host Intrusion Prevention combines the use of signature rules and hard-wired behavioral rules. This hybrid method of identifying attacks detects most known attacks as well as previously unknown or zero-day attacks.

Preset IPS policies

The Host Intrusion Prevention IPS feature contains three policy categories:

- **IPS Options**: This policy turns on or off both host and network IPS protection. Preset policies include On (McAfee Default), Off, Adaptive.
- **IPS Protection**: This policy sets the reaction to events. Preset policies include Basic (McAfee Default), Prepare for Enhanced, Enhanced, Prepare for Maximum, Maximum, Warning.
- **IPS Rules**: This policy can have one or more policy instances. The preset policy is the default policy (McAfee Default).
Quick access

The IPS feature provides links (*) for quick access to monitor and manage IPS Events, IPS Rules, and IPS Client Rules.

Figure 4-1 IPS feature

Configuring the IPS Options policy

The **IPS Options** policy is the basic on/off switch for IPS protection and the means for placing a client in Adaptive mode, which allows the client to retain the exceptions it creates, and automatically blocks network intrusions. Select one of the preset policies or create a new policy.

**To configure the IPS Options policy:**

1. Expand the **IPS** feature, and click **Edit** on the **IPS Options** category line.

2. To apply a preset policy, select it in the policy list. Click the policy name icon to view the settings:

<table>
<thead>
<tr>
<th>Select this policy...</th>
<th>For these options...</th>
</tr>
</thead>
<tbody>
<tr>
<td>(On (McAfee Default))</td>
<td>Enable Host IPS</td>
</tr>
<tr>
<td></td>
<td>Enable Network IPS</td>
</tr>
<tr>
<td></td>
<td>Automatically Block Network Intruders for 10 minutes</td>
</tr>
<tr>
<td></td>
<td>Retain Blocked Hosts</td>
</tr>
<tr>
<td></td>
<td>Retain Client Rules</td>
</tr>
</tbody>
</table>
To create a new IPS Options policy:
1 Click Edit on the IPS Options category line, and select New Policy in the policy list.

2 In the Create New Policy dialog box, select the policy to duplicate, type the name of the new policy, and then click OK.

3 Select the needed options:

<table>
<thead>
<tr>
<th>Select this policy...</th>
<th>For these options...</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Off)</td>
<td>Retain Blocked Hosts</td>
</tr>
<tr>
<td></td>
<td>Retain Client Rules</td>
</tr>
<tr>
<td>(Adaptive)</td>
<td>Enable Host IPS</td>
</tr>
<tr>
<td></td>
<td>Enable Network IPS</td>
</tr>
<tr>
<td></td>
<td>Retain Blocked Hosts</td>
</tr>
<tr>
<td></td>
<td>Enable Adaptive Mode</td>
</tr>
<tr>
<td></td>
<td>Retain Client Rules</td>
</tr>
</tbody>
</table>

Note: Create a new, duplicate policy when viewing the details of a preset policy by clicking Duplicate at the bottom of the policy dialog box. Type the name of the new policy and indicate whether to assign the policy immediately to the current node.
Configuring the IPS Protection policy

The IPS Protection policy sets the protective reaction for signature severity levels. These settings instruct clients what to do when an attack or suspicious behavior is detected. Each signature has one of four severity levels:

- **High** (Red) — Signature of clearly identifiable security threats or malicious actions. These signatures are specific to well-identified exploits and are mostly non-behavioral in nature. Prevent these signatures on every system.

- **Medium** (Orange) — Signature of behavioral activity where applications operate outside their envelope. Prevent these signatures on critical systems, as well as on web servers and SQL servers.

- **Low** (Yellow) — Signatures of behavioral activity where applications and system resources are locked and cannot be changed. Preventing these signatures increases the security of the underlying system, but additional fine-tuning is needed.

- **Information** (Blue) — Signature of behavioral activity where applications and system resources are modified and might indicate a benign security risk or an attempt to access sensitive system information. Events at this level occur during normal system activity and generally are not evidence of an attack.
These levels indicate potential danger to a system and enable you to define specific reactions for different levels of potential harm. You can modify the severity levels and reactions for all signatures. For example, when suspicious activity is unlikely to cause damage, you can select ignore as the reaction. When an activity is likely to be dangerous, you can set prevent as the reaction.

The IPS Protection policy has several preset policies from which to select. If the preset policies do not provide the selected option combination you want, create a new policy and select the required options. Selections in the IPS Protection policy dialog box vary depending on the selected policy.

**To configure the IPS Protection policy:**

1. Expand the IPS feature, and click Edit on the IPS Protection category line.

2. To apply a preset policy, select it in the policy list. Click the policy name icon to view the settings:

3. Click Apply.

**To create a new IPS Protection policy:**

1. Click Edit on the IPS Severity category line, and select New Policy in the policy list.

2. In the Create New Policy dialog box, select the policy to duplicate, type the name of the new policy, and then click OK.

Create a new, duplicate policy when viewing the details of a preset policy by clicking Duplicate at the bottom of the policy dialog box. Type the name of the new policy and indicate whether to assign the policy immediately to the current node.
The **IPS Protection** dialog box appears.

**Figure 4-3 IPS Protection**

3. Select the type of reaction for each severity level:

<table>
<thead>
<tr>
<th>For this item...</th>
<th>Select...</th>
</tr>
</thead>
</table>
| High             | Ignore to permit the event without logging it.  
                  | Log to permit the event and log it.  
                  | Prevent to prevent the event and log it. |
| Medium           | Ignore to permit the event without logging it.  
                  | Log to permit the event and log it.  
                  | Prevent to prevent the event and log it. |
| Low              | Ignore to permit the event without logging it.  
                  | Log to permit the event and log it.  
                  | Prevent to prevent the event and log it. |
| Information      | Ignore to permit the event without logging it.  
                  | Log to permit the event and log it. |

4. Click **Apply**, and then click **Close**.

5. Click **Apply** on the **IPS Protection** category line.

Policies can be deleted only in the ePolicy Orchestrator Policy Catalog page and only by global administrators.
Configuring the IPS Rules policy

Unlike most policy categories, the IPS Rules policy can have several policy profiles assigned. This expanded use of policies allows you to create several policies that profile a client’s usage, location, or type of system on which it is installed to more easily apply intrusion prevention safeguards. For example, for an IIS Server you might apply a general default policy, a server policy, and an IIS policy, the latter two configured to specifically target systems running as IIS servers. In addition to applying existing policies, you can also easily create new ones if the available policies do not meet your safeguard needs.

To assign IPS Rules policies:
1. Expand the IPS feature, and click Edit on the IPS Rules policy name line.
2. To apply an existing policy, select it in the policy list. Click the policy name to view details of the policy.
3. Click Apply.
4. To add another policy instance, click Assign Additional Policy at the top of the IPS Rules section.
   A new policy row appears.
5. Repeat steps 1 to 3.

To create a new IPS Rules policy:
1. Do one of the following:
   - Click Edit in an IPS Rules policy name row.
   - Click Assign additional policy at the top of the IPS Rules listing.
2. Select New Policy in the policy list
3. In the Create New Policy dialog box, select the policy to duplicate, type the name of the new policy, and then click OK.
4. In the IPS Rules tab edit, as appropriate:
   - Exceptions (See Exception Rules on page 40.)
   - Signatures (See Signatures on page 44.)
   - Application Protection Rules (See Signatures on page 44.)
5. Click Close to close the IPS Rules policy dialog box.
6. Click Apply in the IPS Rules policy name row.

Policies can be deleted only in the ePolicy Orchestrator Policy Catalog page and only by global administrators.
IPS Rules policy details

The IPS Rules policy allows you to create and apply one or more policies that define IPS settings. Policies should be based on common usage, location, or access rights and privileges. For example, you might assign an IIS Server a Global Policy, a Server Client Policy, and an IIS Policy.

Each policy details:

- Exception Rules
- Signatures
- Application Protection Rules

All available IPS policies are in the Policies list in the IPS Rules Policy Settings dialog box. Policies applied to the selected node appear in bold. Click Effective Policy to view a union of all exception rules, signatures, and include/exclude rules that apply to the selected node.

The IPS Rules Policy Settings dialog box also provides access to the following IPS policy-related features:

- IPS Events
- IPS Client Rules
- Search IPS Exception Rules

Exception Rules

Sometimes behavior that would be interpreted as an attack can actually be a normal part of a user’s work routine. This is called a false positive alert. To prevent false positives, create an exception for that behavior.

The exceptions feature enables you to weed out false positive alerts, minimizes needless data flowing to the console, and ensures that the alerts are legitimate security threats.

For example, during the process of testing clients, a client recognizes the Outlook Envelope - Suspicious Executable Mod. signature. This signature signals that the Outlook e-mail application is attempting to modify an application outside the envelope of usual resources for Outlook. Thus, an event triggered by this signature is cause for alarm, because Outlook may be modifying an application not normally associated with e-mail, for example, Notepad.exe. In this instance, you might reasonably suspect that a Trojan horse has been planted. But, if the process initiating the event is normally responsible for sending e-mail, for example, saving a file with Outlook.exe, you need to create an exception that allows this action.

You can view a list of exceptions, and create and modify them on the Exceptions tab in the IPS Rules dialog box.
Creating exception rules

When creating an exception rule, you need to define the exception and indicate the signature to which the exception applies. You can create an entirely new exception, one based on a duplicate of an existing exception, or one based on an event.

**To create an exception:**

1. Do one of the following:
   - On the Exception Rules tab, click Create on the shortcut menu or toolbar. A blank New Exception dialog box appears.
   - On the Exception Rules tab, select an existing exception and click Duplicate on the shortcut menu or toolbar. A prefilled Duplicate Exception dialog box appears.
   - On the IPS Events tab, select the event for which you want to create an exception and click Create Exception on the shortcut menu or the toolbar. Select the policy in which to create the exception, and click OK. A prefilled New Exception dialog box appears.
Enter the appropriate data on each of the tabs, and click one of the following buttons:

- **OK** to save the changes and close the dialog box.
- **Apply** to save the changes and keep the dialog box open to create another exception rule.
- **Cancel** to delete changes and close the dialog box.
- **Help** for details.

**Editing exception rules**

You can view and edit details of an existing exception.

**To edit an exception rule:**

1. Select an exception and click **Properties** on the shortcut menu or toolbar; or, double-click an exception.

   The **Exception Properties** dialog box appears.

2. Modify any data on each of the tabs, and then click **OK**. Click **Help** in the dialog box for details.
Enabling and disabling exception rules
Instead of deleting exceptions not in use, you can disable them temporarily and later enable them to put them into effect.

To disable/enable an exception:
- On the Exception Rules tab, select a rule and click Disable/Enable on the shortcut menu or toolbar.
  
  The status of the selected exception changes accordingly.

Deleting exception rules
To permanently delete an exception, select it on the Exception Rules tab, and then click Delete on the shortcut menu or toolbar. The exception is removed from the Exceptions tab.

Moving exception rules to another policy
You can easily move an exception from one policy to another from the Exception Rules tab.

To move an exception rule to another policy:
1. Select the exception rule you want to move and click Move to Another Policy on the shortcut menu or the toolbar.

2. In the Select Policy list, select the policy and click OK.

   A copy of the exception rule appears in the selected policy.
Signatures

Signatures describe security threats, attack methodologies, and network intrusions. Each signature has a default severity level, which describes the potential danger of an attack:

- **High** (red) — Signatures that protect against clearly identifiable security threats or malicious actions. Most of these signatures are specific to well-identified exploits and are mostly non-behavioral in nature. They should be prevented on every host.

- **Medium** (orange) — Signatures that are behavioral in nature and deal with preventing applications from operating outside of their environment (relevant for clients protecting web servers and Microsoft SQL Server 2000). On critical servers, you may want to prevent those signatures after fine-tuning.

- **Low** (yellow) — Signatures that are behavioral in nature and shield applications. Shielding means locking down application and system resources so that they cannot be changed. Preventing yellow signatures increases the security of the underlying system, but requires additional fine-tuning.

- **Information** (blue) — Indicates a modification to the system configuration that might create a benign security risk or an attempt to access sensitive system information. Events at this level occur during normal system activity and generally are not evidence of an attack.

Types of signatures

The IPS Rules policy can contain three type of signatures:

- **Host signatures** — Default Host Intrusions Prevention Signatures (HIPS).

- **Custom host signatures** — Custom HIPS that you create.

- **Network signatures** — Default Network Intrusion Prevention Signatures (NIPS).

**Host signatures**

Host-based intrusion prevention signatures (HIPS) detect and prevent system operations activity attacks, and includes *File, Registry, Service, and HTTP* type rules. They are developed by the Host Intrusion Prevention security experts and are delivered with the product.

Each signature has a description and a default severity level. With appropriate privilege levels, an administrator can modify the severity level of a signature or disable a signature for client groups.

When triggered, host-based signatures generate an IPS event that appears in the **IPS Events** tab.

**Custom host signatures**

Custom signatures are host-based signatures that you can create for additional protection to suit your needs. For example, when you create a new directory with important files, you can create a custom signature to protect it.

**Network signatures**

Network-based intrusion prevention signatures (NIPS) detect and prevent known network-based attacks that arrive on the host system.
Network-based signatures appear in the console in the same list of signatures as the host-based signatures. They have their own icon in the Type column and are designated as Network IPS in the Signature Properties General dialog box.

Each signature has a description and a default severity level. With appropriate privilege levels, an administrator can modify the severity level of a signature or disable a signature.

Every network-based signature has an option to turn logging off, even if the signature is associated with a log or prevent reaction due to the effective policy. However, in case of a prevent reaction, the operation is prevented, even if no event is logged.

You can create exceptions for network-based signatures; however, you cannot specify any additional parameter attributes such as operating system user and process name. Advanced details contains network specific parameters, for example IP addresses, which you can specify.

Events generated by network-based signatures are displayed along with the host-based events in the IPS Events tab and exhibit the same behavior as host-based events.

Viewing signatures
Host Intrusion Prevention provides three views of signatures on the Signatures tab. The default listing includes only active signatures. You can also view only disabled signatures, or a combination of active and disabled signatures.

Figure 4-6 IPS Rules—Signatures tab
To modify the view of signatures:
- Right-click in the signature list and select the desired view:

<table>
<thead>
<tr>
<th>Select…</th>
<th>To view…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Active Signatures</td>
<td>Only the signatures that are active for the IPS Rules policy. This is the default view.</td>
</tr>
<tr>
<td>Show Disabled Signatures</td>
<td>Only the signatures whose severity level is set to disabled.</td>
</tr>
<tr>
<td>Show All Signatures</td>
<td>A combination of active and disabled signatures.</td>
</tr>
</tbody>
</table>

Modifying host and network signatures
You can view and modify default signatures on the Signatures tab of the IPS Rules policy. This enables you to change the severity level of the signature if the signature is causing false positives.

To modify default signatures:
1. Double-click the signature you want to modify.

   The Signature Properties dialog box appears.

2. On the General tab, modify the Severity Level, Allow Client Exceptions, or Log Status settings, and enter notes in the Note box to document the change.

3. On the Description tab, review what the signature is protecting and what it provides. If there is a link, click it to open a browser page and view more information on the security threat.

4. Click OK.

   You can modify the severity level of several signatures at one time by selecting the signatures and clicking Modify the Severity Level. In the dialog box that appears, select Modified and the new severity level to be applied to the signatures, or select Default to return the signatures to their default severity level. Click OK to save the changes. Severity Level settings include High, Medium, Low, Information, and Disabled.

Creating custom signatures
Host Intrusion Prevention gives you the flexibility to create and manage your own signatures and share them between policies. Creating custom signatures, which is recommended only for advanced users, provides additional flexibility for your environment. Refer to Writing Custom Signatures on page 160 for details.

You can use two methods to create signatures:
- Signature Creation Wizard — This is the simplest method, but you cannot change operations that the signature is protecting.
- Standard Mode — This is the more advanced method that enables you to add or delete operations that the signature is protecting.
Using the wizard to create signatures

The signature creation wizard is the recommended method if you are new to creating signatures. The wizard offers two dialog boxes where you enter the necessary information for the signature, but it does not offer any flexibility for the operations that the signature is protecting because you cannot change, add, or delete operations.

To create signatures using the wizard:

1. On the Signature toolbar, click Signature Creation Wizard.

2. In the Signature Creation Wizard - Step 1 of 2 dialog box, enter a name and a description, select the platform and severity level, and then click Next.

3. In the Signature Creation Wizard - Step 2 of 2 dialog box, select the item to protect against modifications, enter details, and then click Finish.
The new signature appears in the list with a custom signature icon.

**Using the standard mode to create signatures**

Use this method only if you are an advanced user. It offers the flexibility to select the operations that the signature is protecting, including changing, adding, and deleting operations. You can create an entirely new signature, one based on an existing custom signature, or one based on a duplicate of an existing custom signature.

**To create a signature with the standard mode:**

1. Do one of the following:
   - On the Signatures tab, click Create on the shortcut menu or toolbar. A blank New Custom Signature dialog box appears.
   - On the Signatures tab, select a custom signature and click Duplicate on the shortcut menu or toolbar. A prefilled Duplicate Custom Signature dialog box appears.

2. On the General tab, enter a name and select the platform, severity level, log status, and whether to allow the creation of client rules.
On the **Description** tab, type a description of what the signature is protecting. This description appears in the **IPS Event** dialog box when the signature is triggered.

On the **Sub-Rule** tab, select either **Standard Method** or **Expert Method** to create the rule.
To use Standard Method:  

The Standard Method limits the number of types you can include in the signature rule.

1. Click **Add**. The New Standard Rule dialog box appears.
2. On the **General** tab, enter a name for the signature and choose a type.
3. On the **Operations** tab, specify the operations that trigger the selected rule.
4. On the **Parameters** tab, include or exclude particular parameters in the rule.
5. On the **Rule Syntax** tab, view the rule syntax that was generated for the signature you are creating.
6. Click **OK**. The rule is compiled and the syntax is verified. If there is an error and the rule fails verification, a dialog box describing the error appears. You can then fix the error and verify the rule again.

To use Expert Method:

The Expert Method, recommended only for advanced users, enables you to provide the rule syntax without limiting the number of types you can include in the signature rule. Before writing a rule, make sure you understand rule syntax. Refer to Writing Custom Signatures on page 160.

1. On the Rules tab of the Custom Signature dialog box, select **Expert** and:
2. Click **Add**. The New Expert Rule dialog box appears.
3. On the **General** tab, type a name for the rule in the Rule Name box and any notes in the Note box.
4. On the **Rule Syntax** tab, type the rule. Rules are written in ANSI format and TCL syntax. See Writing Custom Signatures on page 160 for details.
5. Click **OK**. The rule is compiled and the syntax is verified. If there is an error and the rule(s) fails verification, a dialog box describing the error appears. You can then fix the error and verify the rule again.

5. Click **Apply** to apply the new settings, and then **OK**.

---

You can include multiple rules in a signature.

---

**Editing custom signatures**

You can edit custom signatures to add, remove, or modify rules or other data contained within the signature.

**To edit a custom signature:**

1. On the **Signature** tab, double-click the custom signature you want to edit.

   The Custom Signature Properties dialog box appears.

2. Make changes on each tab as needed. Click **Help** in the dialog box for details.

3. Click **OK** to save the changes.

---

**Deleting custom signatures**

In addition to creating and editing custom signatures, you can also delete them. When you delete a custom signature, all existing events that were triggered by this signature will have the signature ID appended to its name in the **IPS Events** tab.

**To delete a custom signature:**

1. On the **Signature** tab, select the custom signature you want to delete and click **Delete** on the shortcut menu or the toolbar.

2. In the dialog box that appears asking to confirm the deletion, click **OK**.
Application Protection Rules

Application Protection Rules alleviate compatibility and stability issues involving process hooking. It permits or blocks user-level API hooking for defined and generated lists of processes. Kernel-level file and registry hooking are not affected.

Host Intrusion Prevention provides a static list of processes that are permitted or blocked. This list is updated with content update releases. In addition, processes that are permitted to hook can be added dynamically to the list when process analysis is enabled. This analysis is performed:

- Each time the client is started and running processes are enumerated.
- Each time a process starts.
- Each time the process monitoring list is updated by the ePolicy Orchestrator server.
- Each time the list of processes that listen on a network port is updated.

This analysis involves checking first if the process is in the blocked list. If not, the permitted list is checked. If not in that list, the process is analyzed to see if it listens on a network port or runs as a service. If not, it is blocked; if it listens on a port or runs as a service, it is permitted to hook.

Figure 4-11 Application Protection Rules analysis
The IPS component maintains an information cache on running processes, which tracks hooking information. The firewall component determines if a process listens on a network port, calls an API exported by the IPS component, and passes the information to the API to be added to the monitored list. When the API is called, the IPS component locates the corresponding entry in its running processes list. A process that is not already hooked and is not part of the static block list is then hooked. The firewall provides the PID (Process ID), which is the key for the cache lookup of a process.

The API exported by the IPS component also allows the client UI to retrieve the list of currently hooked processes, which is updated whenever a process is hooked or unhooked. A hooked process will be unhooked if the console sends an updated process list that specifies that the already hooked process should no longer be hooked. When the process hooking list is updated, every process listed in the information cache of running processes is compared against the updated list. If the list indicates that a process should be hooked and it is not already hooked, that process will be hooked. If the lists indicate that a process should not be hooked and it is already hooked, that process will be unhooked.

The process hooking lists can be viewed and edited on the Application Protection Rules tab. The client user interface, unlike the view on the IPS Rules policy, shows a list of all hooked application processes.

Figure 4-12 IPS Rules—Application Protection Rules

To create an application protection rule:
1. Do one of the following:
   - On the Application Protection Rules tab, click Create on the toolbar or the shortcut menu. The New Application Protection Rules dialog box appears.
   - On the Application Protection Rules tab, select an application and click Duplicate on the toolbar or the shortcut menu. A prefilled Duplicate IPS Application Protection Rules dialog box appears.
2. On the General tab, enter the name, status, and whether the application is included. For details, click Help.

**Figure 4-13 New Trusted Application dialog box—General tab**

3. On the Processes tab, indicate the processes to which you want to apply the rule. For details, click Help.

**Figure 4-14 New Trusted Application dialog box—Processes tab**

4. Click OK.
Editing Application Protection Rules
You can view and edit the properties of an existing application rule, changing its inclusion status from include to exclude and vice versa.

To edit application rule properties:
1. On the Application Protection Rules tab, select an application and click Properties on the toolbar or shortcut menu; or, double-click the selected trusted application.
   - The Application Protection Rules Properties dialog box appears.
2. Modify any data on the two tabs, and then click OK.

Enabling and disabling Application Protection Rules
Instead of deleting application rules not in use, you can disable them temporarily, and later enable them to put them into effect.

To disable/enable an application rule:
1. On the Application Protection Rules tab, select the enabled rule you want to disable or the disabled one you want to enable.
2. Click Disable or Enable on the toolbar or shortcut menu.
   - The status of the application on the Application Protection Rules tab changes accordingly.

Deleting Application Protection Rules
To permanently delete an application protection rule, select it on the Application Protection Rules tab, and then click Delete on the toolbar or the shortcut menu. The rule is removed from the tab.

IPS Events
An IPS event is triggered when a security violation, as defined by a signature, is detected. For example, Host Intrusion Prevention compares the start of any application against a signature for that operation, which may represent an attack. If a match occurs, an event is generated. If not, perhaps because of an exception to the signature or if the application has been designated as trusted, no event is generated.

When Host Intrusion Prevention recognizes an IPS event, it flags it on the IPS Events tab with one of four severity level criteria: High, Medium, Low, and Information.

When two events are triggered by the same operation, the highest reaction is taken.
From the list of events generated, you can determine which events are allowable and which indicate suspicious behavior. To allow events, configure the system with the following:

- **Exceptions** — which are rules that override a signature rule. To create an exception specific to the event, see [Creating and applying Trusted Applications policies on page 111](#).

- **Trusted Applications** — which allow internal applications whose operations may be blocked by a signature. To create a trusted application specific to the event, see [Creating and applying Trusted Applications policies on page 111](#).

This fine-tuning process keeps the events that do appear to a minimum, providing more time for analysis of the serious events that occur.

### Viewing events

To analyze IPS events, Host Intrusion Prevention enables you to mark the events in one of three states (Unread, Read, Hidden), and then filter these events in one of several displays.

#### To view IPS events:

1. In the console tree, select the node for which you want to view IPS events.

2. Click the **IPS Events** quick access link at the top of the IPS feature in the policy pane; or, if the IPS Management window is open, click the **IPS Events** tab.

A list containing all the events associated with the client appears. By default, not all events are displayed. For details on configuring the event view, see [Configuring the event view on page 56](#).
Configuring the event view

By default, not all events are displayed. By default, only events for the 30 days appear. You can set the view to display events for a certain number of days or events that occurred before a certain date and time.

To change the event view:

1. On the IPS Events tab, click Configure Event View on the toolbar or the shortcut menu.

The Configure Event View dialog box appears.

2. Enter the number of days of events to display.

3. Select Events before (date) and enter a date and time to display events that occurred before the date and time indicate.

4. Click OK.

Filtering events

The events you see are determined by which display you select. Select the appropriate command from the shortcut menu:

- **Show All Events** — This display shows all events. Read events appear in normal type, unread events appear in bold type, hidden events appear in gray type, and hidden aggregated events appear in light blue type.

- **Show Read and Unread Events** — This display shows all events that are either in the read or unread state, but does not show hidden events.

- **Show Unread Events** — This display shows all events that are unread. These events appear in bold type. Read and hidden events are not included in this view.

- **Show Read Events** — This display shows all events that are in the read state. These events appear in normal type. Unread and hidden events are not included in this view.

- **Show Hidden Events** — This display shows all events that are in the hidden state. These events appear in gray type.
Marking events

Events are marked in one of three states to help filter the display:

- **Unread** — The default setting for all events. This indicates the event has not been reviewed. It appears in **bold** type.

- **Read** — The event has been reviewed and marked as **Read**. It appears in normal type.

- **Hidden** — These events are removed from the normal event view. They appear in gray only in the **Hidden Events** or **All Events** view display, unless marked as **Read** or **Unread**.

When you mark events, they are marked for all users connected to the same management server.

**To mark an event as read:**
1. On the **IPS Events** tab, select the events you want to mark as read.
2. Click the **Mark as Read** button on the shortcut menu or toolbar.
   The typeface of the event changes from bold to normal.

**To mark an event as unread:**
1. On the **IPS Events** tab, select the events you want to mark as unread.
2. Click **Mark as Unread** on the shortcut menu or toolbar.
   The typeface of the event changes from normal to bold.

**To hide an event:**
1. On the **IPS Events** tab, select the events you want to hide.
2. Click **Hide (Mark as Hidden)** on the shortcut menu or toolbar.
   The selected events are removed from the current view.
3. To view the hidden events, click **Show Hidden Events** on the shortcut menu or toolbar.

**To remove events from the hidden view:**
1. Click **Show Hidden Events** on the shortcut menu or toolbar.
   The hidden events are displayed.
2. Select the events you want to remove from the hidden view.
3. Click **Mark as Read** or **Mark as Unread**.
   The selected events are removed from the **Hidden** state.
4. Click **Show Read and Unread Events** or **Show All Events** on the shortcut menu.
Marking similar events

With the large number of IPS events that can appear, you should limit the number of events displayed or how they appear. You can do this by marking particular events as read, unread, or hidden one by one; however, this can be a cumbersome process.

The Mark Similar Event as Read / Unread / Hidden option allows you to mark in one operation all existing similar events that match a set of criteria. New events triggered after performing this operation, however, are not automatically marked.

The matching criteria you establish are based on the attributes associated with events, and include any or all of the following:
- Agent
- Signatures
- User
- Process
- Severity Level

To mark similar events:

1. Select an event and click Mark Similar Events on the shortcut menu or Mark Similar Events on the toolbar.

   The Mark Similar Events dialog box appears.

   **Figure 4-17  Mark Similar Events dialog box**

2. In the Mark events as list, select one of three states for the events: Unread, Read, or Hidden.

3. Select the checkbox next to each attribute you want to use as criteria for marking the events.

   The parameter value next to the checkbox is automatically selected. To select another parameter, click Select. In the Selection List dialog box that appears, select the parameter and click OK.
4. After you return to the original dialog box, click OK. Any events that match the selected criteria are changed to the selected state.

If you do not select specific criteria, all events are affected when you click OK.

Viewing event details

The **IPS Event Properties** dialog box displays information about a selected event. Viewing this data can be useful to fine-tune the system, allowing you to create an exception or trusted application or to search for existing exceptions based on the event.

To view event details:
- Double-click the event, or select the event and click **Properties** on the shortcut menu or the toolbar.

The **IPS Event Properties** dialog box appears with four tabs: **General**, **Description**, **Advanced Details**, and **Summary**. Click the **Help** in the dialog box for details.

Figure 4-18 IPS Event dialog box—General tab

Creating event-based exceptions and trusted applications

Under certain circumstances, behavior that is interpreted as an attack can be a normal part of a user’s work routine. When this occurs, you can create an exception rule or create a trusted application rule for that behavior.
You can create event-based exceptions or trusted applications directly from an event to prevent the event from reoccurring, or you can create exceptions or trusted application without reference to any particular event. For the latter, refer to Exception Rules on page 40 and Creating and applying Trusted Applications policies on page 111.

Creating exceptions and trusted applications allows you to weed out false positive alerts, and ensures that the notifications you receive are meaningful communications.

**Example**

For example, during the process of testing clients, you may find clients recognizing the signature E-mail access. Under certain circumstances, an event triggered by this signature is cause for alarm. Hackers may install trojan applications that use TCP/IP Port 25 typically reserved for e-mail applications, and this action would be detected by the TCP/IP Port 25 Activity (SMTP) signature. On the other hand, normal e-mail traffic might also match this signature. When you see this signature, investigate the process that initiated the event. If the process is one that is not normally associated with e-mail, like Notepad.exe, you might reasonably suspect that a trojan was planted. If the process initiating the event is normally responsible for sending e-mail (Eudora, Netscape, Outlook) create an exception to that event.

You may also find, for example, that a number of clients are triggering the signature startup programs, which indicates either the modification or creation of a value under the registry keys:

```
HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Run
HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/RunOnce
```

As the values stored under these keys indicate programs that are started when the computer boots, recognition of this signature may indicate that someone is attempting to tamper with the system. Or it might indicate something as benign as one of your employees installing RealAudio on their computer. The installation of RealAudio adds the value RealTray to the Run registry key.

To eliminate the triggering of events every time someone installs authorized software, you create exceptions to these events. The client will no longer generate events to this authorized installation.

**To create an event-based exception:**

1. Select an event and click Create Exception on the shortcut menu or the toolbar.

   A prefilled New Exception dialog box appears.

2. Follow the directions for creating an exception in Exception Rules on page 40.

**To create an event-based trusted application:**

1. Select an event and click Create Trusted Application on the shortcut menu or the toolbar.

   A prefilled New Trusted Application dialog box appears.

2. Follow the directions for creating a trusted application in Creating and applying Trusted Applications policies on page 111.
Searching for related exceptions

An event may be a false positive, which is a legitimate operation that incorrectly appears as an intrusion. For false positives you can create an exception and prevent logging future identical events; however, you may have already created several exceptions for similar events. Instead of creating a new exception, you might be able to edit an existing exception to make it apply to the false positive event. Keeping exceptions organized and few in number makes them easier to manage.

The Search for Related Exceptions feature enables you to search for existing exceptions that match one or more attributes that belong to an event. For example, you can search for exceptions matching the event’s signature or process or both. Alternatively, you can search for exceptions that are already deployed on the client on which the event occurred or perhaps those applied to the user associated with the event.

To search for a related exception:
1. Select an event on the IPS Events tab for which you want to find related exceptions, and click Search for Related Exceptions or the toolbar or the shortcut menu.

   The Search IPS Exception Rules search criteria dialog box appears with prefilled process, signature, and user information.

2. Select the checkbox for each criterion you want to apply. You can edit the values by clicking Edit.

3. Click OK.

   The Search IPS Exceptions tab displays the results of the search. See Search IPS Exception Rules on page 64 for more details on using this search feature.

IPS Client Rules

When clients are in Adaptive mode, client exception rules are created automatically to allow operations that would otherwise be blocked by administrator-mandated policies. Client rules can also be created manually, provided the Client UI policy option to allow manual creation of client rules is enabled. Both automatic and manually-created client rules appear on the IPS Client Rules tab. Some or all of the client exception rules generated on a representative client can be promoted to the general Exception Rules tab of a particular IPS Rules policy, allowing for ease in tuning a deployment.
Regular View

Client exception rules appear in a Regular View and an Aggregated View. In the Regular View you can sort and filter the list of rules to find specific exceptions and see their details. You can also migrate client rules to server-side exception rules of an IPS Rules policy.

To migrate client rules to an IPS Rules policy:
1. Select a client exception rule on the Regular View tab and click Create Exception Rule.
2. Select the policy to which you want to migrate the client rule and click OK.
3. In the prefilled Exception Rule dialog box, verify or edit the information and click OK.

The new exception rule appears on the Exception Rules tab of the IPS Rules policy selected in the migration process.

For more details, see Exception Rules on page 40.

Aggregated View

In the Aggregated View, you can aggregate client rule exceptions based on signature, user, process, status, reaction, and node to determine the frequency of similar exception rules created on all clients.

Manage exceptions that appear on the IPS Client Rules tab with the Aggregated View feature. This view enables you to combine exceptions that have the same attributes, so that only one aggregated exception appears, while keeping track of the number of times the exceptions occur. This information enables you to fine-tune a deployment, possibly transferring some of the client exception rules to administrator-mandated exception rules to reduce false positives for a particular system environment.

Aggregated exceptions appear in blue text and have a number in the Count column. To aggregate exceptions you select aggregation criteria while viewing exceptions.
To aggregate client rules:

1. Click the **Aggregate View** tab on the **IPS Client Rules** tab.

2. In the **Aggregate Client Rules** dialog box, select the criteria for aggregating the client rule exceptions. Options include: **Signature**, **User**, **Process**, **Enabled**, **Reaction**, and **Node**.

3. Click **OK**.

   A list of signatures and the number of exception rules created for each appears.

4. Select a row and click **Show Individual Rules** to see details of each exception rule associated with the selection.

   Your are returned to the **Regular View** tab with details on each rule in the aggregated set.
Search IPS Exception Rules

You can search for exceptions in any IPS Rules policy on the Search IPS Exception Rules tab. This search function enables you to determine if an exception is required for a signature rule. It also enables you to manage exceptions by deleting duplicate exception rules or creating trusted applications to allow a blocked process. Search criteria include the processes that triggered an event, the signatures that caused the event to be triggered, and the users affected by the exception rule. After you have found the related exception rules you are searching for, you are advised to manage this list to keep the number of overall exceptions to a minimum. You can do this by deleting ones that are not needed because exceptions already exist for a particular processes or signature, or by duplicating and editing an exception to replace several similar exceptions. The Search IPS Exceptions tab also enables you to disable exceptions instead of permanently deleting them, and to find exceptions that match a profile to copy to other IPS policies.

To search for exceptions and manage the list of exceptions:

1. On the Search IPS Exception Rules tab, click Search.

   The Search IPS Exception Rules dialog box appears.

   Figure 4-21  Search IPS Exception Rules

   Select the appropriate search criteria checkboxes, and then select the All or Specific option. When you select the Specific option, click Edit to indicate which specific items to include in the search.

2. Select the appropriate criteria and do one of the following:

   - select All (the default) for all processes.
   - select Specific and click Edit to indicate specific processes. In the Search for Specific Criteria dialog box, move items from the available list to the selected list and click OK.
3 Click OK.

The list of exceptions matching the search criteria appears.

**Figure 4-22 Search IPS Exception Rules tab**

When you select several criteria, the results that appear matches any of the criteria you selected, not all the criteria. For example, if you select two specific processes, the exceptions that appear match either of the two processes; what does not appear are exceptions that match both processes only.

4 Select an exception in the list and use commands on the shortcut menu or the toolbar to enable/disable it, move it from one policy to another, create a new exception by duplicating it, or delete it. For more details, see *Exception Rules* on page 40.
Firewall Policies

The firewall feature performs stateful packet filtering and stateful packet inspection, allowing it to identify packets for different types of connections, and hold in memory the attributes of network connections from start-to-finish of transmission. By applying policies set or customized by the administrator, the firewall permits transmission of packets that match a known connection state, and blocks all others.

This section describes the Firewall feature and includes these topics:

- Overview
- Configuring the Firewall Options policy
- Configuring the Firewall Rules policy
- Configuring the Quarantine Options policy
- Quarantine

Overview

The Host Intrusion Prevention firewall protects a networked computer from intrusions that compromise data, applications, or the operating system. It provides this protection by working at several layers of the network architecture, where different criteria are used to restrict network traffic. This network architecture is built on the seven-layer Open System Interconnection (OSI) model, where each layer handles specific network protocols.
Rules

The firewall in Host Intrusion Prevention 7.0 includes both stateful packet filtering and stateful packet inspection.

When using IPv6, stateful functionality is available on Vista only.

Stateful packet filtering
Stateful packet filtering is the stateful tracking of TCP/UDP/ICMP protocol information at Transport Layer 4 and lower of the OSI network stack. Each packet is examined and if the inspected packet matches an existing firewall rule, it is allowed and an entry is made in a state table. The state table dynamically tracks connections previously matched against a static rule set, and reflects the current connection state of the TCP/UDP/ICMP protocols. If an inspected packet matches an existing entry in the state table, the packet is allowed without further scrutiny. When a connection is closed or times out, the corresponding entry is removed from the state table.

Stateful packet inspection
Stateful packet inspection is the process of stateful packet filtering and tracking commands at Application Layer 7 of the network stack. This combination offers a strong definition of the computer’s connection state. Access to the application level commands provides error-free inspection and securing of FTP and DHCP protocols.
State table

A feature of a stateful firewall is a state table that dynamically stores information about active connections created by allow rules. Each entry in the table defines a connection based on:

- **Protocol**—The predefined way one service talks with another; includes TCP, UDP and ICMP protocols.

- **Local and remote computer IP addresses**—Each computer is assigned a unique IP address. IPv4 permits addresses up to 32 bits long, whereas IPv6 permits addresses up to 128 bits long. IPv6 is supported by some operating systems, such as Windows Vista and several Linux distributions. Host Intrusion Prevention supports both standards.

- **Local and remote computer port numbers**—A computer sends and receives services using numbered ports. For example, HTTP service typically is available on port 80, and FTP services on port 21. Port numbers range from 0 to 65535.

- **Process ID (PID)**—A unique identifier for the process associated with a connection’s traffic.

- **Timestamp**—The time of the last incoming or outgoing packet associated with the connection.

- **Timeout**—The time limit (in seconds), set with the Firewall Options policy, after which the entry is removed from the table if no packet matching the connection is received. The timeout for TCP connections is enforced only when the connection is not established.

- **Direction**—The direction (incoming or outgoing) of the traffic that triggered the entry. After a connection is established, bidirectional traffic is allowed even with unidirectional rules, provided the entry matches the connection’s parameters in the state table.

**State table functionality**

- If firewall rule sets change, all active connections are checked against the new rule set. If no matching rule is found, the connection entry is discarded from the state table.

- If an adapter obtains a new IP address, the firewall recognizes the new IP configuration and drops all entries in the state table with an invalid local IP address.

- All entries in the state table associated with a process are deleted when the process ends.

**How firewall rules work**

Firewall rules determine how to handle network traffic. Each rule provides a set of conditions that traffic has to meet and has an action associated with it: allow or block traffic. When Host Intrusion Prevention finds traffic that matches a rule’s conditions, it performs the associated action.

Host Intrusion Prevention uses precedence to apply rules: the rule at the top of the firewall rules list is applied first. If the traffic meets this rule’s conditions, Host Intrusion Prevention allows or blocks the traffic. It does not try to apply any other rules in its rule list.
If, however, the traffic does not meet the first rule’s conditions, Host Intrusion Prevention looks at the next rule in its list. It works its way down through the list until it finds a rule that the traffic matches. If no rule matches, the firewall automatically blocks the traffic. If Learn mode is activated, it prompts for an action to be taken; if Adaptive mode is activated, it creates an allow rule for the traffic.

Sometimes the intercepted traffic matches more than one rule in the list. If so, precedence means that Host Intrusion Prevention applies only the first matching rule in the list.

**Ordering the firewall rule list**

When you create or customize a firewall rules policy, place the most specific rules at the top of the list and more general rules at the bottom. This ensures that Host Intrusion Prevention filters traffic appropriately and does not miss rules based on exceptions to other, more general rules.

For example, to block all HTTP requests except those from IP address 10.10.10.1, you need to create two rules:

- **Allow Rule:** Allow HTTP traffic from IP address 10.10.10.1. This rule is the most specific.
- **Block Rule:** Block all traffic using the HTTP service. This rule is more general.

You must place the more specific Allow Rule higher in the firewall rule list than the more general Block Rule. This ensures that when the firewall intercepts an HTTP request from address 10.10.10.1, the first matching rule it finds is the one that allows this traffic through the firewall.

If you placed the more general Block Rule higher than the more specific Allow Rule, Host Intrusion Prevention would match the HTTP request from 10.10.10.1 against the Block Rule before it found the exception. It would block the traffic, even though you really wanted to allow HTTP requests from this address.

---

The functionality that permits moving rules from one position in the rules list to another also permits moving rules into connection-aware groups, in which rules are processed only when certain criteria are met. See [Firewall rule groups and connection-aware groups](#) on page 72 and [Associating rules, groups and connection-aware groups](#) on page 87.

---

**How stateful filtering works**

Stateful filtering involves processing a packet against two rule sets, a configurable firewall rule set and a dynamic firewall rule set or state table.

The configurable rules have two possible actions:

- **Allow**—The packet is permitted and an entry is made in the state table.
- **Block**—The packet is blocked and no entry is made in the state table.

The state table entries result from network activity and reflect the state of the network stack. Each rule in the state table has only one action, **Allow**, so any packet matched to a rule in the state table is automatically permitted.

The filtering process includes these steps:
1 The firewall compares an incoming packet against entries in the state table. If the packet matches any entry in the table, the packet is immediately allowed. If not, the configurable firewall rules list is examined.

- A state table entry is considered a match if the Protocol, Local Address, Local Port, Remote Address and Remote Port match those of the packet.

2 If the packet matches an allow rule, it is allowed and an entry is created in the state table.

3 If the packet matches a block rule, it is blocked.

4 If the packet does not match any configurable rule, it is blocked.

**How stateful packet inspection works**

Stateful packet inspection combines stateful filtering with access to application-level commands, securing protocols such as FTP.

FTP involves two connections: control for commands and data for the information. When a client connects to an FTP server, the control channel is established, arriving on FTP destination port 21, and an entry is made in the state table. When the firewall encounters a connection opened on port 21, it knows to perform stateful packet inspection on the packets coming through the FTP control channel, if the option for FTP inspection has been set with the Firewall Options policy.

With the control channel open, the client communicates with the FTP server. The firewall parses the PORT command in the packet sent over the connection and creates a second entry in the state table to allow the data connection.
When the FTP server is in active mode, the server opens the data connection; in passive mode, the client initiates the connection. When the server receives the first data transfer command (LIST), it opens the data connection to the client and transfers the data. The data channel is closed after the transmission is completed.

The combination of the control connection and one or more data connections is called a session, and FTP dynamic rules are sometimes referred to as session rules. The session remains established until its control channel entry is deleted from the state table. During the periodic cleanup of the table, if a session’s control channel has been deleted, all data connections are subsequently deleted.

**Stateful protocol tracking**

The following is a summary of the types of connections monitored by the stateful firewall and how they are handled.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description of handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>A UDP connection is added to the state table when a matching static rule is found and the action from the rule is Allow. Generic UDP connections, which carry Application-Level protocols unknown to the firewall, remain in the state table as long as the connection is not idle longer than the specified timeout period.</td>
</tr>
<tr>
<td>ICMP</td>
<td>Only ICMP Echo Request and Echo Reply message types are tracked. Other ICMP connections are managed like generic UDP connections. <strong>Note:</strong> In contrast to the reliable, connection-oriented TCP protocol, UDP and ICMP are less reliable, connectionless protocols. To secure these protocols, the firewall considers generic UDP and ICMP connections to be virtual connections, held only as long as the connection is not idle longer than the timeout period specified for the connection. The timeout for virtual connections is set with the Firewall Options policy.</td>
</tr>
<tr>
<td>TCP</td>
<td>TCP protocol works on the “3-way handshake.” When a client computer initiates a new connection, it sends a packet to its target with a SYN bit that is set, indicating a new connection. The target responds by sending a packet to the client with a SYN-ACK bit set. The client responds then by sending a packet with an ACK bit set and the stateful connection is established. All outgoing packets are allowed, but only incoming packets that are part of the established connection are allowed. An exception is when the firewall first queries the TCP protocol and adds all pre-existing connections that match the static rules. Pre-existing connections without a matching static rule are blocked. The TCP connection timeout, which is set with the Firewall Options policy, is enforced only when the connection is not established. A second or forced TCP timeout applies to established TCP connections only. This timeout is controlled by a registry setting and has a default value of one hour. Every four minutes the firewall queries the TCP stack and discards connections that are not reported by TCP.</td>
</tr>
</tbody>
</table>
| DNS      | There is query/response matching to ensure DNS responses are only allowed to the local port that originated the query and only from a remote IP address that has been queried within the UDP Virtual Connection Timeout interval. Incoming DNS responses are allowed if:  
  - The connection in the state table has not expired.  
  - The response comes from the same remote IP address and port where the request was sent. |
Firewall Policies

Overview

Firewall rule groups and connection-aware groups

You can group rules for easier management. Normal rule groups do not affect the way Host Intrusion Prevention handles the rules within them; they are still processed from top to bottom.

Host Intrusion Prevention also supports a type of rule group that does affect how rules are handled. These groups are called connection-aware groups (CAGs). Rules within connection-aware groups are processed only when certain criteria are met.

Connection-aware groups let you manage rules that apply only when you connect to a network using a wired connection, a wireless connection, or a non-specific connection with particular parameters. Multiple CAGs may apply simultaneously. Thus you can have one CAG for wired connections and a different CAG for wireless connections. In addition, these groups are network adapter-aware, so that computers with multiple network interfaces can have rules apply that are adapter specific. Parameters for allowed connections can include any or all of the following for each network adapter:

- IP address
- DNS suffix
- Default Gateway IP/MAC pair
- DHCP Server IP/MAC pair
- DNS server queried to resolve URLs
- Primary WINS server used
- Secondary WINS server used

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description of handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>There is query/response matching to ensure that return packets are allowed only for legitimate queries. Thus incoming DHCP responses are allowed if:</td>
</tr>
<tr>
<td></td>
<td>- The connection in the state table has not expired.</td>
</tr>
<tr>
<td></td>
<td>- The response transaction ID matches the one from the request.</td>
</tr>
<tr>
<td>FTP</td>
<td>The firewall performs stateful packet inspection on TCP connections opened on port 21. Inspection occurs only on the control channel, the first connection opened on this port.</td>
</tr>
<tr>
<td></td>
<td>FTP inspection is performed only on the packets that carry new information. Retransmitted packets are ignored.</td>
</tr>
<tr>
<td></td>
<td>Dynamic rules are created depending on direction (client/server) and mode (active/passive):</td>
</tr>
<tr>
<td></td>
<td>-- Client FTP Active Mode: the firewall creates a dynamic incoming rule after parsing the incoming port command, provided the port command RFC 959 compliant. The rule is deleted when the server initiates the data connection or the rule expires.</td>
</tr>
<tr>
<td></td>
<td>-- Server FTP Active Mode: the firewall creates a dynamic outgoing rule after parsing the incoming port command.</td>
</tr>
<tr>
<td></td>
<td>-- Client FTP Passive Mode: the firewall creates a dynamic outgoing rule when it reads the PASV command response sent by the FTP server, provided it has previously seen the PASV command from the FTP client and the PASV command is RFC 959 compliant. The rule is deleted when the client initiates the data connection or the rule expires.</td>
</tr>
<tr>
<td></td>
<td>-- Server FTP Passive Mode: the firewall creates a dynamic incoming rule.</td>
</tr>
</tbody>
</table>
If two connection-aware groups apply to a connection, Host Intrusion Prevention uses normal precedence and processes the first applicable connection-aware group in its rule list. If no rule in the first connection-aware group matches, rule processing continues and may match a rule in the next group.

When Host Intrusion Prevention matches a connection-aware group’s parameters to an active connection, it applies the rules within the connection group. It treats the rules as a small rule set and uses normal precedence. If some rules do not match the intercepted traffic, the firewall ignores them.

A connection is allowed when all of the following conditions apply to a network adapter:

- If Connection type is **LAN**.
  - or
  - If Connection type is **Wireless (802.11)**.
  - or
  - If Connection type is **Any** and the DNS suffix list or the IP Address List is populated.

- If **IP Address** is selected, the IP address of the adapter must match one of the list entries.

- If **DNS Suffix** is selected, the DNS suffix of the adapter must match one of the list entries.

- If **Default Gateway** is selected, the default adapter Gateway IP/MAC pair must match at least one of the list entries.

- If **DHCP Server** is selected, the adapter DHCP server IP/MAC pair must match at least one of the list entries.
  
  **Note:** The MAC address is optional and used only when specified.

- If **DNS Server** is selected, the adapter DNS server IP address must match any of the list entries.

- If **Primary WINS Server** is selected, the adapter primary WINS server IP address must match at least one of the list entries.

- If **Secondary WINS Server** is selected, the adapter secondary WINS server IP address must match at least one of the list entries.

### Isolating network connections

Connection isolation prevents undesirable traffic from accessing a designated network via other active network interfaces on a computer, such as a wireless adapter connected to a Wi-Fi hotspot. When the **Isolate this connection** option is selected for a CAG, and a Network Interface Card (NIC) matching the CAG criteria is active, the only traffic allowed is traffic matching rules above the CAG in the firewall policy or traffic passing through the network interface identified by the CAG criteria. All other traffic is blocked by the firewall.

- The firewall processes traffic against its list of rules until a Connection-Aware Group (CAG) is encountered. At the CAG:
  - If the traffic through a NIC matches the CAG’s criteria, the firewall evaluates the CAG’s rules for a match.
- If the traffic through a NIC **does not match** the CAG’s criteria, and the connection isolation option **is not** enabled, the firewall skips the CAG and continues analyzing against the rules that follow the CAG.
- If the traffic through a NIC **does not match** the CAG criteria, and the connection isolation option **is** enabled, the traffic is blocked.

**Figure 5-3 Network Connection Isolation**

**Examples of connection isolation**

As examples of using the connection isolation option, consider two settings: a corporate environment and a hotel. The active firewall rules list contains rules and groups in this order:
1 Rules for basic connection
2 VPN connection rules
3 CAG with corporate LAN connection rules
4 CAG with VPN connection rules.

**Connection isolation on the corporate network**
Connection rules are processed until the Connection-Aware Group with corporate LAN connection rules is encountered. This CAG contains these settings:

- **Connection type** = LAN
- **Domain** = mycompany.com
- **Isolate this Connection** = yes

The computer has both LAN and wireless network adapters and connects to the corporate network with a wired connection, but the wireless interface is still active, so it connects to a hotspot outside the office. The computer connects to both networks because the rules for basic access are at the top of the firewall rules list. The wired LAN connection is active and meets the criteria of the corporate LAN CAG. The firewall processes the traffic through the LAN but because connection isolation is enabled, all other traffic not through the LAN is blocked.

**Connection Isolation at a hotel**
Connection rules are processed until the Connection-Aware Group with VPN connection rules is encountered. This CAG contains these settings:

- **Connection type** = Any
- **Domain** = vpn.mycompany.com
- **IP Address** = an address in a range specific to the VPN concentrator
- **Isolate this Connection** = yes

General connection rules allow the set-up of a timed account at the hotel to gain internet access. The VPN connection rules allow connection and use of the VPN tunnel. After the tunnel is established, the VPN client creates a virtual adapter that matches the criteria of the VPN CAG. The only traffic the firewall allows is inside the VPN tunnel and the basic traffic on the actual adapter. Attempts by other hotel guests to access the computer over the network, either wired or wireless, are blocked.

**Firewall Learn and Adaptive modes**
When you enable the firewall feature, Host Intrusion Prevention continually monitors the network traffic that a computer sends and receives. It allows or blocks traffic based on the Firewall Rules policy. If the traffic cannot be matched against an existing rule, it is automatically blocked unless the firewall’s Learn mode or Adaptive mode is enabled.

You can enable Learn mode for incoming communication only, for outgoing communication only, or both.
In Learn mode, Host Intrusion Prevention displays a Learn mode alert when it intercepts unknown network traffic. This alert prompts the user to Allow or Block any traffic that does not match an existing rule, and automatically creates corresponding dynamic rules for the non-matching traffic.

In Adaptive mode, Host Intrusion Prevention automatically creates an Allow rule to allow all traffic that does not match any existing Block rule, and automatically creates dynamic Allow rules for non-matching traffic.

For security reasons, however, in both the Learn mode and Adaptive mode, incoming pings are blocked unless an explicit Allow rule is created for incoming ICMP traffic. In addition, incoming traffic to a port that is not open on the host is blocked unless an explicit Allow rule is created for the traffic. For example, if the host has not started telnet service, incoming TCP traffic to port 23 (telnet) is blocked even when there is no explicit rule to block this traffic. You can create an explicit Allow rule for any desired traffic.

Host Intrusion Prevention displays all the rules created on clients through Learn Mode or Adaptive Mode, and allows these rules to be saved and migrated to administrative rules.

Stateful filtering
If Adaptive or Learn mode is applied with the stateful firewall, the filtering process changes slightly to allow the adaptive creation of a new rule to handle the incoming packet. This filtering process proceeds like this:

1. The firewall compares an incoming packet against entries in the state table and finds no match, then examines the static rule list and finds no match.
2. No entry is made in the state table, but if this is a TCP packet, it is put in a pending list. If not, the packet is discarded.
3. If new rules are permitted, a unidirectional static allow rule is created. If this is a TCP packet, an entry is made in the state table.
4. If a new rule is not permitted, the packet is dropped.

Quarantine policies and rules
When a client returns to the network after a prolonged absence, the quarantine policies restrict a client’s ability to communicate with the network until ePolicy Orchestrator verifies that the client has all the latest policies, software updates, and DAT files.

Out-of-date policies and files can create security holes and leave systems vulnerable to attacks. By quarantining users until ePolicy Orchestrator updates them, unnecessary security risks are avoided. For example, a quarantine policy is useful for laptops whose policies and files may become out of date when they are away from the corporate network for a few days.
When you enable the Quarantine Options policy, both ePolicy Orchestrator and Host Intrusion Prevention participate. ePolicy Orchestrator detects whether a user has all the latest information they need. Host Intrusion Prevention enforces the quarantine until the client has all the necessary policies and files.

If your user connects to the network using VPN software, be sure the quarantine rules allow any traffic required to both connect and authenticate over the VPN.

When you configure the Quarantine Options policy, you specify a list of quarantined IP addresses and subnets. Any user assigned one of these addresses is quarantined by Host Intrusion Prevention upon returning to the network.

When the Quarantine Options policy is applied to a client, Host Intrusion Prevention uses the ePolicy Orchestrator agent to determine if the client has the most recent policies and files. This involves checking if all ePolicy Orchestrator tasks have run properly.

If the user is up-to-date, Host Intrusion Prevention immediately releases the client from quarantine.

If one or more ePolicy Orchestrator tasks have not run, however, the user is not up-to-date and Host Intrusion Prevention does not automatically release the quarantine. The client could remain quarantined for a few minutes while the ePolicy Orchestrator agent updates policies and files. Host Intrusion Prevention can continue or stop the quarantine, as determined by settings in the Quarantine Options policy. If you configure Host Intrusion Prevention to continue enforcing the quarantine, clients could remain quarantined for a prolonged period.

With the quarantine policy, Host Intrusion Prevention enforces a strict set of firewall quarantine rules that define with whom quarantined clients can communicate.

Quarantine mode requires Firewall be enabled. Even if the Quarantine mode is enabled, the quarantine does not take effect unless Firewall is also enabled.

### Preset Firewall policies

The Host Intrusion Prevention Firewall feature contains four policy categories:

- **Firewall Options**: Turns firewall protection on or off. Preset policies include Off (McAfee Default), On, Adaptive, Learn.

- **Firewall Rules**: Defines firewall rules. Preset policies include Minimal (McAfee Default), Learning Starter, Client High, Client Medium, Server High, Server Medium.

- **Quarantine Options**: Turns quarantine mode on or off. The preset policy is Disabled (McAfee Default).

- **Quarantine Rules**: Defines firewall rules applied during quarantine. The preset policy is the default policy (McAfee Default).
Configuring the Firewall Options policy

The Firewall Options policy enables or disables the firewall, and applies Adaptive or Learn mode for clients. You can choose from four preconfigured policies, or you can create and apply a new policy.

To configure the Firewall Options policy:
1. In the console tree, select the group or computer to apply the policy.
2. On the Policies tab, expand the Host Intrusion Prevention Firewall feature.
3. In the Firewall Options line, click Edit.
   The policy name list becomes active.
4. Do one of the following:
   - Select a preconfigured policy in the list, and click Apply.
   - Select New Policy.
     The Create New Policy dialog box appears.

<table>
<thead>
<tr>
<th>Select...</th>
<th>For these settings...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off (McAfee Default)</td>
<td>All are disabled</td>
</tr>
<tr>
<td>On</td>
<td>- Enable Firewall</td>
</tr>
<tr>
<td></td>
<td>- Enable regular protection</td>
</tr>
<tr>
<td></td>
<td>- Retain client rules</td>
</tr>
<tr>
<td>Adaptive</td>
<td>- Enable Firewall</td>
</tr>
<tr>
<td></td>
<td>- Enable Adaptive mode</td>
</tr>
<tr>
<td></td>
<td>- Retain client rules</td>
</tr>
<tr>
<td>Learn</td>
<td>- Enable Firewall</td>
</tr>
<tr>
<td></td>
<td>- Enable Learn mode, Incoming and Outgoing</td>
</tr>
<tr>
<td></td>
<td>- Retain client rules</td>
</tr>
</tbody>
</table>

- Select New Policy.

The Create New Policy dialog box appears.

You can create a new, duplicate policy when viewing the details of a preset policy by clicking Duplicate at the bottom of the policy dialog box. Type the name of the new policy and indicate whether to assign the policy immediately to the current node.

5. Select the policy to duplicate, type a name for the new policy, and click OK.
   The Firewall Options dialog box appears.
6 Select the appropriate settings. For details, click Help.

7 Click Apply and close the dialog box.

The name of the new policy appears in the policy list.

8 Click Apply.

Configuring the Firewall Rules policy

Firewall rules determine how a system operates when it intercepts network traffic, permitting or blocking it. You create and manage firewall rules by applying a Firewall Rules policy with the appropriate settings.

The Firewall Rules policy provides access for:

- Creating new Firewall Rules policies
- Viewing and editing firewall rules
- Creating a new firewall rule or firewall group
- Deleting a firewall rule or group
- Viewing and editing firewall rules
Creating new Firewall Rules policies

To add a new policy that is not specific to a node, create a policy in the Policy Catalog. See Policy Catalog on page 119 for details. To add a new policy specific to a node, follow the instructions in this section.

To create a Firewall Rules policy:
1. In the console tree, select the group or computer to which you want to apply the policy.
2. On the Policies tab, expand the Firewall feature.
3. In the Firewall Rules line, click Edit.
   The policy name list becomes active.
4. Do one of the following:
   - Select one of the preconfigured policies in the list and click Apply.

<table>
<thead>
<tr>
<th>Select this policy...</th>
<th>For this protection...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal (Default)</td>
<td>Blocks any incoming ICMP traffic that an attacker could use to gather information about your computer. Host Intrusion Prevention allows all other ICMP traffic.</td>
</tr>
<tr>
<td></td>
<td>Allows Windows file sharing requests from computers in the same subnet, and blocks file sharing requests from anyone else. (The Trusted Networks policy must have Include Local Subnet Automatically selected.)</td>
</tr>
<tr>
<td></td>
<td>Allows you to browse Windows domains, workgroups, and computers.</td>
</tr>
<tr>
<td></td>
<td>Allows all high incoming and outgoing UDP traffic.</td>
</tr>
<tr>
<td></td>
<td>Allows traffic that uses BOOTP, DNS, and Net Time UDP ports.</td>
</tr>
<tr>
<td>Learning Starter</td>
<td>Blocks incoming ICMP traffic that an attacker could use to gather information about your computer. Host Intrusion Prevention allows all other ICMP traffic.</td>
</tr>
<tr>
<td></td>
<td>Allows Windows file sharing requests from computers in the same subnet, and blocks file sharing requests from anyone else. (The Trusted Networks policy must have Include Local Subnet Automatically selected.)</td>
</tr>
<tr>
<td></td>
<td>Allows you to browse Windows domains, workgroups, and computers.</td>
</tr>
<tr>
<td></td>
<td>Allows traffic that uses BOOTP, DNS, and Net Time UDP ports.</td>
</tr>
<tr>
<td>Client Medium</td>
<td>Allows only ICMP traffic needed for IP networking (including outgoing pings, trace routes, and incoming ICMP messages). Host Intrusion Prevention blocks all other ICMP traffic.</td>
</tr>
<tr>
<td></td>
<td>Allows UDP traffic necessary for accessing IP information (such as your own IP address, or the network time). This protection level also allows traffic on high UDP ports (1024 or higher).</td>
</tr>
<tr>
<td></td>
<td>Allows Windows file sharing, but only for a local subnet. You cannot browse outside your local subnet, and this protection blocks anyone outside your subnet from accessing files on your computer. (The Trusted Networks policy must have Include Local Subnet Automatically selected.)</td>
</tr>
</tbody>
</table>
Select this policy... | For this protection...
---|---
Client High | Use this protection level if you are under attack or at high risk of an attack. This protection level allows only minimal traffic in and out of your system.
- Allows only ICMP traffic necessary for proper networking. This protection blocks both incoming and outgoing pings.
- Allows only UDP traffic necessary for accessing IP information (such as your own IP address or the network time).
- Blocks Windows file sharing.
Server Medium | Use this protection level for a network server.
- Allows ICMP traffic that facilitates communication between the server and its clients. This protection blocks all other ICMP traffic.
- Allows UDP traffic necessary for accessing IP information. This protection also allows traffic on high UDP ports (1024 or higher).
Server High | Use this protection level for a server connected directly to the Internet, at a high risk of attack. Use this protection level as a basis for creating your own, customized rule set.
- Allows specific ICMP traffic — that which facilitates communications between the server and its clients. Host Intrusion Prevention blocks all other ICMP traffic.
- Allows UDP traffic necessary for accessing IP information. Host Intrusion Prevention blocks all other UDP traffic.

5 Select New Policy to create a new policy.

The Create New Policy dialog box appears.

**Figure 5-5 Create New Policy dialog box**

Select the policy to duplicate, type a name for the new policy, and click OK.

The Firewall Rules dialog box appears listing the rules and groups that comprise the new policy.

Groups can be identified by the right arrow preceding the name of the group. When the arrow points down, the group is open; its contents are visible; rules can be added, edited or deleted. Using the Move Up and Move Down buttons, rules can be added to the group. Click the arrow to toggle between closed and open.
Use the buttons at the bottom of the Firewall Rules tab to do any of the following:

- Add rules or groups (see Creating a new firewall rule or firewall group).
- Create a duplicate of the rule (see Duplicating a firewall rule).
- Edit rules (see Viewing and editing firewall rules).
- Remove rules (see Deleting a firewall rule or group).
- Reorder the list of rules (see Ordering the firewall rule list on page 69).
- Associate rules with connection-aware groups (see Associating rules, groups and connection-aware groups on page 87).

Creating a new firewall rule or firewall group

You can add a new rule by creating it or by duplicating an existing rule and editing it. You can also create a group for a set of rules, a connection-aware group, or add predefined rules. Create new rules and groups on the Firewall Rules tab in the Firewall Rules policy.

Fields in the dialog box that are marked with * are required.

To create a firewall rule:
1. On the Firewall Rules tab in the Firewall Rules policy dialog box, click Add Rule. The rule configuration dialog box appears.
2 Select the appropriate settings.

3 Click OK.

You can also create rules by adding predefined rules and rule groups to the policy. See To add predefined rules: on page 86.

To create a new rule group:
1 On the Firewall Rules tab in the Firewall Rules policy dialog box, click Add Rule. The New Firewall Rule Group dialog box appears.

2 In the Name field, type a name for this group.

3 Click OK to add the group.

You can now create new rules within this group, or move existing rules into it from the firewall rule list.

To create a connection-aware group:
1 On the Firewall Rules tab in the Firewall Rules policy dialog box, click Add Connection Aware Group. The New Connection Aware Group dialog box appears.
2 Type a name for this group in the Name field.

3 In Connection type, select the type of connection (Any, LAN or Wireless) to apply the rules in this group.

4 From the drop-down box in New Criterion, select a category of criterion to apply to the rule. Click Add Criterion to display an addition to the dialog box in which to type the new matching criterion.

   - If you select Any as the connection type, you are required to select either IP Address or DNS Suffix and edit the corresponding list.
   - Specify a DHCP server MAC address only for DHCP servers on the same subnet as the client. Identify remote DHCP servers only by their IP address.

5 Click Add to append more criteria in the same category. Click Remove or Remove All to eliminate one or all of the previously added criteria in the selected category.

6 Click OK. The connection-aware group appears in blue on the Firewall Rules tab.
For more information on Connection Aware Groups, see Firewall rule groups and connection-aware groups on page 72 and Associating rules, groups and connection-aware groups on page 87.

**To view or add client rules:**
The Client Rules tab displays all firewall rules created on client systems. The default view displays all rules, including duplicates. Rules can be aggregated into sets that share similar characteristics specified by selecting one or more of the checkboxes near the top of the display.


2. Select a rule and click View to see the rule. Click Add to include the rule in the selected policy.

3. To modify the view, do any of the following:

### Filtering and aggregating firewall client rules

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View details of a rule</td>
<td>Select the rule and click View.</td>
</tr>
<tr>
<td>Move a rule to a policy</td>
<td>Select the rule and click Add to Policy.</td>
</tr>
<tr>
<td>Scroll through the list of rules</td>
<td>Click the navigation buttons on the toolbar.</td>
</tr>
<tr>
<td>Filter the list of rules by selected criteria</td>
<td>Click Set Filter, then select the criteria on which to filter and their values.</td>
</tr>
<tr>
<td>Aggregate the rules by selected criteria</td>
<td>Select the checkbox for each criterion on required for a rule to be included in the aggregation.</td>
</tr>
</tbody>
</table>

Client rules can be sorted by distinguishing characteristics to help analyze patterns or trends in the way client users employ their rule-setting privileges.

**Filtering**
Applying filters to the client rules generates a list of rules that satisfies all of the variables (criteria) selected and defined on the Set Filter Criteria dialog box. The result is a list of rules that include all of the criteria.

1. Click Set Filter. The Add Filter Criteria dialog appears.
2 From the drop-down list, select a filtering criterion to be applied, then click **Add Criterion**. The dialog box expands to include additional fields to define value(s) appropriate to the selected criterion. When finished adding filtering criteria, click **OK**.

**Aggregating**

Aggregating client rules generates a list of rules grouped by the value associated with each of the variables (criterion) selected on the Client Rules tab. The result is a list of rules, displayed in groups and sorted by the value associated with the selected variables, (e.g., all rules where the selected action is **allow**, followed by all rules where the selected action is **block**).

1 Select the **Firewall Client Rules** tab in the Firewall Rules policy, (see Figure 5-10 on page 85).

2 Select the criteria for aggregating rules by selecting one or more of the checkboxes displayed near the top of the page. The rules sort themselves based on the selected criteria. To view details of an aggregated firewall rule select the rule, and click **View**.

**To add predefined rules:**

1 On the **Firewall Rules Policy** page, select the **Predefined Rules** tab.

2 Select one or more rule or groups and select **Add to Policy**. You may need to scroll to the bottom of the list to locate the **Add to Policy** button.

**Duplicating a firewall rule**

You can make a copy of a rule and use it as the basis for developing a new rule.

To duplicate a firewall rule:

1 On the **Firewall Rules** tab, select a rule and click **Duplicate**. The duplicated rule appears on the **Firewall Rules** tab.
2 Select the duplicated rule and click Edit to rename it and make any other changes that distinguish the new rule from the earlier rule. For details, click Help.

3 Click Apply to save any changes.

Viewing and editing firewall rules

You can view the details of a rule or edit it to change options. View and edit rules on the Firewall Rules tab in the Firewall Rules policy.

To view and edit a firewall rule:
1 On the Firewall Rules tab, select a rule and click Edit. The Firewall Rule dialog box appears.
2 Change any of this rule's settings. For details, click Help.
3 Click Apply to save any changes.

Deleting a firewall rule or group

Delete rules and groups on the Firewall Rules tab in the Firewall Rules policy.

To delete a firewall rule or group:
1 Select the Firewall Rules tab in the Firewall Rules policy, and select the rules or groups to delete.
2 Click Delete.

Caution
Clicking Delete removes the selected rule without any further request for confirmation.

Note
Groups are displayed in black type. Connection-aware groups are displayed in blue type. Click the arrow to change its direction.

Associating rules, groups and connection-aware groups

Incorporate a rule listed on the Firewall Rules tab into an existing group or connection-aware group.

To incorporate a rule into a group or connection-aware group:
1 Select the target group or connection-aware group and ensure that the arrow, which appears between the Status field and the Name field, points downward,

Groups are displayed in black type. Connection-aware groups are displayed in blue type. Click the arrow to change its direction.

2 Select the rule to include in the target.
3 Click Move Up or Move Down to relocate the rule or group until it enters the target and its name is indented under the name of the group or connection-aware group.
4 Click Apply to save changes.

To incorporate a group into a connection-aware group:
Proceed as above except substitute a group for a rule in Step 2.
Configuring the Quarantine Options policy

The Quarantine Options policy allows you to enable or disable quarantine mode; create a quarantine notification message; define quarantined networks; configure fail options; and apply quarantine rules until the firewall service starts up (generally referred to as “boot-time quarantine).

To configure the Quarantine Options policy:
1. In the console tree, select the group or computer where you want to apply the policy.
2. Expand the Firewall feature, and in the Quarantine Options line, click Edit.
   The policy name list becomes active.
   The Create New Policy dialog box appears.
   You can create a new, duplicate policy when viewing the details of a preset policy by clicking Duplicate at the bottom of the policy dialog box. Type the name of the new policy and indicate whether to assign the policy immediately to the current node.
4. Select the policy to duplicate, type the name of the new policy, and click OK. The Quarantine Options dialog box appears.

   ![Figure 5-13 Quarantine Options]

Select the appropriate settings.
5 Click **Apply** and close the dialog box. The name of the new policy appears in the policy list.

---

**Quarantine**

The Quarantine function protects designated networks from unauthorized access by computers seeking to join them. The protected networks are defined by IP address, subnet, or range.

When both Firewall and Quarantine Mode are enabled, computers attempting to access the network from an IP address that matches a protected IP address are subject to quarantine. In addition, when boot-time quarantine is enabled, computers in the process of booting-up are subject to quarantine from the moment the network stack comes up until the moment the firewall services start, at which time their IP address is examined to determine if there is a match with a protected network.

Quarantine Rules are defined by the administrator. Usually, these are restrictive rules that limit the actions that can be performed by the access-seeking computer until it is identified as qualified for admission to the network by the McAfee Agent (sometimes referred to as Common Management Agent, ePolicy Orchestrator Agent, or simply the Agent.)

To be qualified, the computer must satisfy certain conditions relating to prior use of ePolicy Orchestrator, including successful connection; collection and transmission of properties; policy enforcement; and creating a scheduled task. If the computer fails, it is subject to the pre-selected configuration options of continued quarantine or, alternatively, removing quarantine and subjecting the computer to the Firewall Rules currently in force.

*If users connect to the network using VPN software, ensure that quarantine rules allow any traffic required to connect and authenticate over the VPN.*

You can use the regular Firewall feature to determine which VPN-related rules you need for **Quarantine mode**. Enable the firewall’s Learn mode or Adaptive mode, and then connect using VPN software. Host Intrusion Prevention automatically generates relevant VPN rules, which you can then reproduce in your quarantine rules.

The **Quarantine Rules** policy provides access for:

- Creating new Quarantine Rules policies
- Viewing and editing quarantine rules
- Creating a new quarantine rule or group
- Deleting a quarantine rule or group

---

Select **Apply quarantine rule list until service has started** to enable boot-time quarantine.
Creating new Quarantine Rules policies

To add a new policy that is not specific to a node, create a policy in the Policy Catalog. See Policy Catalog on page 119 for details. To add a new policy specific to a node, follow the instructions in this section.

To create a Quarantine Rules policy:

1. In the console tree, select the group or computer in the console tree where you want to apply the policy.

2. Expand the Firewall feature, and in the Quarantine Rules line, click Edit.

   The policy name list becomes active.

3. Do one of the following:

   - Select one of the preconfigured policies in the list, and click Apply
   - Select New Policy to create a new policy,

   The Create New Policy dialog box appears.

4. Select the policy to duplicate, type a name for the new policy, and click OK.

   The Quarantine Rules dialog box appears with the new policy selected in the policy list pane.

Figure 5-14 Quarantine Rules dialog box

5. Do any of the following:

   - Add rules (see Creating a new quarantine rule or group).
   - Edit rules (see Viewing and editing quarantine rules).
   - Remove rules (see Deleting a quarantine rule or group).

6. Click Close to close the dialog box.

   The name of the new policy appears in the policy list.

7. Click Apply.

   You can also create a new policy from within the Quarantine Rules dialog box by clicking Add Policy or Duplicate Policy.
Viewing and editing quarantine rules

You can view the details of a rule or edit a rule’s options. View and edit rules in the Quarantine Rules dialog box.

To view and edit a quarantine rule:
1. Select a policy in the Policies list, and in the details pane select the rule you want to view or edit.
2. Click Properties.
   The Quarantine Rule dialog box appears.
3. Change any of this rule’s settings.
4. Click OK to save any changes.

Creating a new quarantine rule or group

You can add a new rule by creating it or by duplicating an existing rule and editing it. You can also create a group for a set of rules or add predefined rules. You create new rules and groups in the Quarantine Rules dialog box.

To create a quarantine rule:
1. On the Quarantine Rules tab of the Quarantine Rules policy, click Add, then New Rule.
   The Quarantine Firewall Rule dialog box appears.
2. Select the appropriate settings.
3. Click OK.

To create a new rule group:
1. On the Quarantine Rules tab of the Quarantine Rules policy, click Add and then New Group.
   The Quarantine Firewall Rule Group dialog box appears.
2. In the Name field, type a name for this group.
3. Click OK to add the group.
   You can now create new rules within this group, or move existing rules into it from the quarantine firewall rule list.

To add predefined rules:
1. On the Quarantine Rules tab of the Quarantine Rules policy, click Add and then Predefined Rules.
   The Select Predefined Rules dialog box appears.
2. Select one or more groups or rules within a group.
3. Click OK to add the selected groups and rules.
Deleting a quarantine rule or group

You delete rules and groups in the Quarantine Rules dialog box.

To delete a quarantine rule or group:
1. On the Quarantine Rules tab of the Quarantine Rules policy, select the rules or groups you want to delete.
2. Click Delete.
3. Click Yes in the confirmation dialog box to remove the items from the list.
The Application Blocking feature of Host Intrusion Prevention manages a set of applications that you allow to run (known as application creation) or bind (known as application hooking) with other applications.

This section describes the Application Blocking feature and includes the following topics:

- Overview
- Configuring the Application Blocking Options policy
- Configuring the Application Blocking Rules policy

**Overview**

The Application Blocking feature enables or disables application blocking and configures application blocking rules. With application blocking you can set application creation blocking, application hooking blocking, or both. You can also indicate whether to keep application blocking rules created on clients manually or through the Adaptive or Learn modes.

**Application creation**

Block application creation when you want to prevent specific or unknown programs from running. For example, some Trojan horse attacks can run malicious applications on computers without the knowledge of the user. If you block application creation, you can prevent these attacks from succeeding by allowing only specific, legitimate applications to run. You can also enable automatic Adaptive mode or interactive Learn mode to dynamically build a set of allowed applications.
Application hooking

Block application hooking to prevent unknown applications from binding themselves to other programs. This type of hooking, which occurs at the kernel level of the API, is needed by some legitimate applications, but can also indicate an attack. For example, a malicious application might try to e-mail itself by hooking to the e-mail application. You can prevent these attacks by blocking application hooking or configure it so that only specific applications bind themselves to other programs. You can also enable automatic Adaptive mode or interactive Learn mode to handle unknown applications trying to hook other applications.

Preset Application Blocking policies

The Application Blocking feature contains two policy categories:

- **Application Blocking Options**: Turns application creation and hooking blocking on or off. Preset policies include Off (McAfee Default), On, Adaptive, Learn.

- **Application Blocking Rules**: Defines application blocking settings. The preset policy is the default (McAfee Default).

Quick access

The Application Blocking feature provides links (*) for quick access to monitor and manage Application Blocking Rules and Application Blocking Client Rules.

![Figure 6-1 Application Blocking feature](image_url)
Configuring the Application Blocking Options policy

The Application Blocking Options policy has four preconfigured policies from which to choose. Alternatively, you can create a new policy and apply it.

To apply an Application Blocking Options policy:

1. In the console tree, select the group or computer where you want to apply the policy.

2. Expand the Application Blocking feature, and click Edit in the Application Blocking Options line.

   The policy name list becomes active.

3. Do one of the following:
   - Select one of the preconfigured policies in the list and click Apply:

     | Select this policy... | For these settings... |
     |-----------------------|-----------------------|
     | Off (McAfee Default)  | All settings are disabled. |
     | On                   | Application Creation Blocking, Regular Protection |
     |                       | Application Hooking Blocking, Regular Protection |
     | Adaptive             | Application Creation Blocking, Adaptive mode |
     |                       | Application Hooking Blocking, Adaptive mode |
     | Learn                | Application Creation Blocking, Learn mode |
     |                       | Application Hooking Blocking, Learn mode |

   - Select New Policy.

      The Create New Policy dialog box appears.

   You can create a new, duplicate policy when viewing the details of a preset policy by clicking Duplicate at the bottom of the policy dialog box. Type the name of the new policy and indicate whether to assign the policy immediately to the current node.

4. Select the policy to duplicate, type a name for the new policy, and click OK.

   The Application Blocking Options dialog box appears.
5 Select the appropriate settings.

6 Click Apply and close the dialog box.

The name of the new policy appears in the policy list.

7 Click Apply.
Configuring the Application Blocking Rules policy

Rules determine how the application blocking feature treats different applications. Create and manage rules by applying an Application Blocking Rules policy with the appropriate settings.

The Application Blocking Rules policy provides access for:

- Creating new Application Blocking Rules policies
- Viewing and editing Application Blocking Rules
- Creating new Application Blocking Rules
- Deleting an application blocking rule
- Viewing application client rules

Creating new Application Blocking Rules policies

To add a new policy that is not specific to a node, create a policy in the Policy Catalog. See Policies tab on page 117 for details. To add a new policy specific to a node, follow the instructions in this section.

To create an Application Blocking Rules policy:

1. In the console tree, select the group or computer where you want to apply the policy.

2. Expand the Application Blocking feature, and click Edit in the Application Blocking Rules line.

   The policy name list becomes active.


   The Create New Policy dialog box appears.

   Figure 6-3  Create New Policy dialog box

4. Select the policy to duplicate, type the name of the new policy, and click OK.

   The Application Blocking Rules dialog box appears with the new policy selected in the policy list pane.
Figure 6-4 Application Blocking Rules dialog box

5 Do any of the following:

- Add rules (see Creating new Application Blocking Rules).
- Edit rules (see Viewing and editing Application Blocking Rules).
- Remove rules (see Deleting an application blocking rule).

6 Click Close to close the dialog box.

The name of the new policy appears in the policy list.

7 Click Apply.

You can also create a new policy from within the Application Blocking Rules dialog box with the Add Policy or Duplicate Policy buttons.

Viewing and editing Application Blocking Rules

You can view the details of a rule or edit a rule to disable it, customize it, and change application options. View and edit rules on the Application Blocking Rules tab in the Application Blocking Rules policy.

To view and edit an application blocking rule:

1 On the Application Blocking Rules tab, select a policy in the Policies list, and then in the details pane select the rule you want to view or edit.

2 Click Properties.

The Application Rule dialog box appears.

3 Change any of this rule’s settings. See Creating new Application Blocking Rules for details on each setting:

4 Click OK to save any changes.
Creating new Application Blocking Rules

You can create a new rule from scratch or by duplicating an existing rule and editing it. You create new rules on the Application Rules tab in the Application Blocking Rules dialog box.

To create a new application blocking rule:
1 On the Application Blocking Rules tab in the Application Blocking Rules policy, click Add.

The Application Rule dialog box appears.

Figure 6-5 Application Rule dialog box

2 Select the application to apply this rule to from the Application list. If the application does not appear in this list, click Browse and navigate to the application’s executable file.

3 Click Customize to configure how the rule’s application is matched and select one of the following:
   - **Application Fingerprint**: Calculates a hash of the application on the server that will match only if the client’s application is the same version of the application referenced on the server.
   - **The path when matched first, but then the fingerprint**: When the application is launched for the first time, it will be matched based on the path specified by the user. If it matches, the fingerprint will be calculated at the client. From that point on, the rule will match based only on the fingerprint of the application.
   - **The path always, and not the fingerprint**: When the application is launched, it will be matched based only on the path specified by the user.

   ■ Clicking Browse allows you to navigate to applications on the ePO server. In most instances, you need to click Customize and select the appropriate options to ensure that the correct application on the client system is applied.

4 Select the Application Options:

<table>
<thead>
<tr>
<th>Select this option...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application rule is Active</td>
<td>Enable this rule.</td>
</tr>
</tbody>
</table>
5 Click OK to add the new rule to the Application Rules list.

### Deleting an application blocking rule

Delete rules on the Application Blocking Rules tab in the Application Blocking Rules policy.

**To delete an application blocking rule:**

1. On the Application Blocking Rules tab in the Application Blocking Rules policy, select one or more rules to delete.
2. Click Delete.
3. Click Yes in the confirmation dialog box to remove the rule(s) from the list.

> When you delete a rule, you remove it permanently. We recommend editing the rule and deselecting Active to disable the rule.

### Viewing application client rules

The Application Blocking Client Rules tab displays all rules created on client systems that allow or block applications. The Regular View displays all rules, including duplicates. The Aggregated View displays rules in groups of similar characteristics.

**To view all client application rules:**

1. Click the Application Blocking Client Rules tab in the Application Blocking Rules policy, and click the Regular View tab.

#### Figure 6-6  Regular View tab
2. To modify the view, do any of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View details of a rule</td>
<td>Select the rule and click Properties.</td>
</tr>
<tr>
<td>Move a rule to a policy</td>
<td>Select the rule and click Add to Policy.</td>
</tr>
<tr>
<td>Scroll through the list of rules</td>
<td>Click the navigation buttons on the toolbar.</td>
</tr>
<tr>
<td>Filter the list of rules</td>
<td>Click Set Filter. In the Set Application Filter dialog box, select one or more checkboxes and enter a value in the corresponding field to set a filter.</td>
</tr>
</tbody>
</table>

To view aggregated client application rules:

1. Click the Application Blocking Client Rules tab in the Application Blocking Rules policy, and click the Aggregated View tab.

2. Click Select Column to display the Aggregate Application Rule dialog box if it is not already displayed.

Figure 6-7  Aggregated View tab

3. Select one or more options to determine the criteria for aggregating the client rules, and click OK.

To view details of an aggregated client application rule:

- On the Aggregated View tab, select an aggregated rule and click Show Individual Rules on the shortcut menu or the toolbar.

All individual rules in the aggregated rule appear on the Regular View tab.
General Policies

The General feature of Host Intrusion Prevention provides access to policies that are general in nature and not specific to one feature.

This section describes the General feature and includes the following topics:

- Overview
- Configuring Enforce Policies
- Configuring the Client UI policy
- Configuring the Trusted Networks policy
- Configuring the Trusted Applications policy

Overview

General policies apply to IPS and firewall settings and take precedence over settings in individual IPS and firewall policies.

The Enforce Policies policy is the basic on/off switch for enforcing Host Intrusion Prevention administrative policies on the client.

The Client UI policy determines which options are available to a client computer with a Host Intrusion Prevention client, including whether the client icon appears in the system tray, types of intrusion alerts, and passwords for access to the client interface.

The Trusted Networks policy lists IP addresses and subnets that are safe for communication. Trusted networks can include subnets, individual IP addresses, or ranges of IP addresses. Marking networks as trusted eliminates or reduces the need for IPS exceptions and additional firewall rules.

The Trusted Applications Rules policy lists applications that are safe, have no known vulnerabilities, and are allowed to perform any operation. Marking applications as trusted eliminates or reduces the need for IPS exceptions and additional firewall and application blocking rules. Like the IPS Rules policy (see Configuring the IPS Rules policy on page 39), this policy category can contain multiple policy instances.

Settings for Trusted Networks and Trusted Applications policies can reduce or eliminate false positives, which aids in tuning a deployment.
Preset General policies

The General feature contains four policy categories:

- **Enforce Policies**: Turns administrative policy enforcement on or off. Preset policies include Yes (McAfee Default), No.

- **Client UI**: Defines access to the Host Intrusion Prevention client user interface. The preset policy is the default policy (McAfee Default).

- **Trusted Networks**: Sets trusted networks. The preset policy is the default policy (McAfee Default).

- **Trusted Applications**: Defines trusted applications. The preset policy is the default policy (McAfee Default).
Configuring Enforce Policies

This policy is the basic on/off switch for enforcing policies. This policy cannot be deleted or edited and no new policies can be created.

To change the policy setting:
1. In the console tree, select the group or computer where you want to apply the policy.

2. Expand the General feature and click Edit in the Enforce Policies line.
   The policy name list becomes active.

3. Select No or Yes.
   The default Yes allows administrative policies to be enforced on clients; No prevents administrative policies from being enforced.

   Selecting No does not disable the client and its protection of its host; it simply prevents policy updates from being enforced on the client.

4. Click Apply.

Configuring the Client UI policy

The Client UI policy determines what options are available to a Windows client computer protected with Host Intrusion Prevention. These include icon display settings, intrusion event reactions, and administrator and client user access. The options with this policy make it possible to meet the demands of three typical user roles:

Regular User
This is the average user who has the Host Intrusion Prevention client installed on a desktop or laptop. The Client UI policy enables this user to:

- View the Host Intrusion Prevention client icon in the system tray and launch the client user interface.
- Get pop-up intrusion alerts or disable the pop-ups after they start to appear.
- Create additional IPS, firewall, and application blocking rules.
Disconnected User
This is a user, perhaps with a laptop, who is disconnected from the Host Intrusion Prevention server for a period of time. The user might have technical problems with Host Intrusion Prevention or need to perform operations without interaction with it. The Client UI policy enables this user to obtain a computer-specific, time-based password to perform administrative tasks, or to turn on or off protection features.

Administrator User
This is an IT administrator for all computers who needs to perform special operations on a client computer, overriding any administrator-mandated policies. The Client UI policy enables this user to obtain a non-expiring administrator password to perform administrative tasks.

Administrative tasks for both disconnected and administrator users include:
- Enabling or disabling IPS, Firewall, and Application Blocking Options policies.
- Creating additional IPS, Firewall, and Application Blocking rules if certain legitimate activity is blocked.

Creating and applying a Client UI policy
If the default Client UI policy does not have the settings you want, create a new policy and select the appropriate options. You can then apply the policy to one or a group of computers.

To configure a Client UI policy:
1 In the console tree, select the group or computer where you want to apply the new policy.
2 Expand the General feature and click Edit in the Client UI line.
   The policy name list becomes active.
3 Select New Policy.
   The Create New Policy dialog box appears.

Create a new, duplicate policy when viewing the details of a preset policy by clicking Duplicate at the bottom of the policy dialog box. Type the name of the new policy and indicate whether to assign the policy immediately to the current node.

4 Select the policy to duplicate, type the name of the new policy, and click OK.
   The Client UI dialog box appears.
Change any of this settings as needed. For general details, click Help. For details on passwords, see Setting passwords on page 106; for details on tray-icon control, see Tray icon control on page 109.

Click OK to save any changes.

For details on working with the client interface, see Host Intrusion Prevention Client on page 132.

Setting passwords

The Client UI policy is where you create the password required to unlock the client UI if it appears on a client computer. When this policy is applied to the client, the password is activated.

Two types of passwords are available:

- An administrator password, which an administrator can configure and is valid as long as the policy is applied to the client. The client UI remains unlocked until it is closed. To reopen the client UI, reenter the administrator password. To create and apply an administrator password, select any site, group, or computer in the directory tree.

- A time-based password, which is automatically generated, applies only to a particular computer, and has an expiration date and time. The client UI remains unlocked, even if closed, as long as the time-based password is valid. To create and apply a time-based password, select a single computer in the directory tree.

Policies are enforced on the client only when the client is closed, regardless of whether the client is locked or unlocked.
For details on using a password to unlock the Client UI, see *Unlocking the client interface* on page 134.

**To create an administrator password:**

1. Click the **Advanced Options** tab in the Client UI policy.

**Figure 7-4  Client UI—Advanced Options tab**

2. Type a password in the **Password** text box. It must have at least ten characters.

3. Retype the password in the **Confirm Password** text box.

4. Click **Apply**.

When you use the administrator password on the client, always select the **Admin Password** checkbox.
To create a time-based password:
1. Click the Advanced Options tab in the Client UI policy dialog box.
2. Select Enable Time-Based Password.
3. Click Compute Time-Based Password. The Time-Based Password dialog box appears.

![Time-Based Password dialog box](image)

4. Enter the date and time when the password expires, and then click Compute Password.

A coded password appears in the Password text box.

Troubleshooting options
Use the Troubleshooting tab to designate message types that trigger logging of IPS and Firewall events on the selected client computer; and to disable IPS Engines during troubleshooting.

![Client UI—Troubleshooting Options tab](image)

To set up a troubleshooting configuration, follow these steps:
1 From the **IPS Log Level** drop-down box, select the message type that represents the lowest caution level that logs IPS events:

- **Debug**—All cautionary messages are logged.
- **Information**—Information, Warning and Error cautionary messages are logged.
- **Warning**—Warning and Error cautionary messages are logged.
- **Error**—Error cautionary messages are logged.
- **Disabled**—No cautionary messages are logged.

On Windows Vista the path of the HipShield.log file is: Program Data\McAfee\Host Intrusion Prevention\. On all other supported Windows platforms the path is: Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention\. 

2 Select **Log Security Violations** to include them in the log.

3 Select the **Firewall Log Level** message type that represents the lowest caution level that logs Firewall events.

On Windows Vista the path of the FireSvc.log file is: Program Data\McAfee\Host Intrusion Prevention\. On all other supported Windows platforms the path is: Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention\. 

4 Use the **Enable these IPS Engines** checkboxes to disable IPS Engines during troubleshooting. Enable Engines when resuming normal activities after troubleshooting.

**Tray icon control**

If there are users who on occasion need to temporarily turn off a Host Intrusion Prevention feature to access a legitimate but blocked application or network site, for example, they can use the Host Intrusion Prevention tray icon to disable a feature without opening the client UI, which requires a password.

For details on using the tray icon menu, see *System tray icon on page 133.*

**To provide tray icon control of Windows UI:**

1 Select **Show tray icon** on the **Display Options** tab.

2 Select **Allow disabling of features from the tray icon** on the **Advanced Options** tab, then select any or all of the features to be disabled.

After the policy is applied to the client, the Host Intrusion Prevention icon appears in the system tray, and its menu expands to include feature disabling and restoring options. The disabled feature remains disabled until restored by the menu command or a new policy with the feature enabled is pushed to the client.

**Note the following:**

- Disabling IPS disables both host IPS and network IPS protection.
- Disabling App Blocking disables both Application creation blocking and Application hooking blocking protection.
- If the Client UI is open, the menu commands have no effect.
Configuring the Trusted Networks policy

The Trusted Networks policy enables you to maintain a list of network addresses and subnets, which you can tag as trusted. The policy lets you:

- Set up trusted network options.
- Add or delete addresses or subnets in the trusted list.

If one trusted network trusts a specific IP address for Network IPS and another trusted network does not trust the same IP address for Network IPS, like firewall rules, the entry listed first takes precedence.

To configure trusted network options:

1. In the console tree, select the group or computer where you want to apply the policy.
2. Expand the General feature, and click Edit in the Trusted Network line. The policy name list becomes active.
4. Select the policy to duplicate, type a name for the new policy, and click OK. The Trusted Networks dialog box appears.

Create a new, duplicate policy when viewing the details of a preset policy by clicking Duplicate at the bottom of the policy dialog box. Type the name of the new policy and indicate whether to assign the policy immediately to the current node.

Generate a new, duplicate policy when viewing the details of a preset policy by clicking Duplicate at the bottom of the policy dialog box. Type the name of the new policy and indicate whether to assign the policy immediately to the current node.

**Figure 7-7 Trusted Networks**
5 Do any of the following:

<table>
<thead>
<tr>
<th>Select...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a trusted network address to the list. Select the address type (single, range, subnet), enter the appropriate address, and select whether to mark as trusted for Network IPS.</td>
</tr>
<tr>
<td>Edit</td>
<td>Change the data in a selected trusted network address.</td>
</tr>
<tr>
<td>Remove</td>
<td>Remove a selected trusted network address.</td>
</tr>
<tr>
<td>Include Local Subnet</td>
<td>Automatically treat all users on the same subnet as trusted, even those not in the list.</td>
</tr>
<tr>
<td>Automatically</td>
<td></td>
</tr>
<tr>
<td>Do not include Local Subnet</td>
<td>Treat only users in the list as trusted even if they are all on the same trusted subnet.</td>
</tr>
</tbody>
</table>

6 Click Apply and close the dialog box.

The name of the new policy appears in the policy list.

7 Click Apply.

---

**Configuring the Trusted Applications policy**

The Trusted Applications policy enables you to create a list of trusted applications. Enforce one or more profile-based policies with these application settings to reduce or eliminate most false positives.

**Creating and applying Trusted Applications policies**

Create and apply a Trusted Applications policy that defines trusted applications. You can create an entirely new policy, or one based on an existing policy.

**To create a new policy:**

1 Expand the General feature, and click Edit in the Application Rules line.

   The policy name list becomes active.

2 Select New Policy.

   The Create New Policy dialog box appears.

3 Select the policy to duplicate, type the name of the new policy, and click OK.

   The Trusted Application tab appears.
Configuring the Trusted Applications policy

Change any of the settings as needed. For details, click Help.

Click Close to save any changes.

Creating trusted applications

In tuning a deployment, creating IPS exception rules is one way to reduce false positives. This is not always practical when dealing with several thousand clients or having limited time and resources. A better solution is to create a list of trusted applications, which are applications known to be safe in a particular environment. For example, when you run a backup application, many false positive events can be triggered. To avoid this, make the backup application a trusted application.

A trusted application is susceptible to common vulnerabilities such as buffer overflow and illegal use. Therefore, a trusted application is still monitored and can trigger events to prevent exploits.

To create a trusted application:

1. Do one of the following On the Trusted Application tab:
   - Click Create on the toolbar or the shortcut menu. The New Trusted Application dialog box appears.
   - Select an application in the list and click Duplicate on the toolbar or the shortcut menu. A prefilled Duplicate Trusted Application dialog box appears.

   You can also create trusted applications based on an event. For details, see Creating event-based exceptions and trusted applications on page 59.

2. On the General tab, enter the name, status, and whether the application is trusted for IPS, firewall and application hooking. For details, click Help.
3 On the **Processes** tab, select the processes to apply the trusted application. For details, click **Help**.

**Figure 7-10  New Trusted Application dialog box—Processes tab**

4 Click **OK**.

**Editing trusted applications**

You can view and edit the properties of an existing trusted application.
To edit trusted application properties:
1. On the Trusted Application tab, double-click a trusted application.

   The Trusted Application Properties dialog box appears.

2. Modify any of the data on the General and Process tabs, and then click OK.

Enabling and disabling trusted applications
Instead of deleting trusted applications not in use, you can disable them temporarily, and later enable them.

To disable/enable a trusted application:
1. On the Trusted Application tab, select the trusted application to disable or enable.

2. Click Disable or Enable on the toolbar or shortcut menu.

   The status of the application on the Trusted Application tab changes accordingly.

Deleting trusted applications
To permanently delete a trusted application, select it on the Trusted Application tab, and then click Delete on the toolbar or the shortcut menu.
This section describes the activities used to maintain and fine-tune a Host Intrusion Prevention deployment and includes the following topics:

- Fine-tuning a deployment
- Policy maintenance and tasks
- Running server tasks
- Setting up notifications for events
- Running reports
- Updating

Fine-tuning a deployment

After you have deployed clients with default settings, you can fine-tune and tighten security for optimum protection. Fine-tuning a deployment involves:

- Analyzing IPS events.
- Creating exception rules and trusted application rules.
- Working with client exception rules.
- Creating and applying new policies.

Analyzing IPS events

An IPS event is triggered when a security violation, as defined by a signature, is detected. It appears on the IPS Events tab with a severity level of High, Medium, Low, or Information, which maps to a reaction.

When single operation triggers two events, the event with the stronger reaction is taken.
From the list of generated events, determine which indicate no risk and which indicate suspicious behavior. To allow events, configure the system with the following:

- **Exceptions** — allow or block rules that override a signature rule.
- **Trusted Applications** — allow internal applications whose operations may be blocked by a signature.

This fine-tuning process keeps false positives to a minimum, providing more time for analysis of serious events. For more details, see *IPS Events* on page 54.

**Creating exception rules and trusted application rules**

After analyzing the list of IPS events, you can create exception rules or trusted application rules for each false positive event per user profile. This keeps the list of events to a minimum, allows for better understanding of malicious attacks, and ensures that systems are protected against such attacks.

From the **IPS Events** tab, you can create an exception or a trusted application based on a particular event. For details, see *Creating event-based exceptions and trusted applications* on page 59.

**Working with client exception rules**

An easy approach to creating exceptions is to place clients in Adaptive mode, and allow the clients to automatically create client exception rules to allow non-malicious behavior. All client rules appear on the **Client Rules** tab of the **IPS Rules** policy. The **Firewall Rules** and the **Application Blocking Rules** policies also display client rules created through Adaptive or Learn mode.

To obtain the most frequently generated rules, use the aggregated view of client rules, which group similar rules. The rules could then be moved to administrative policies.

For details on working with client rules, see:

- *IPS Client Rules* on page 61.
- *Configuring the Firewall Rules policy* on page 79.
- *Configuring the Application Blocking Rules policy* on page 97.

**Creating and applying new policies**

After creating new exception rules and trusted applications, add these to existing policies where appropriate. You can also create new IPS and Trusted Application policies based on the one that required the creation of exceptions and trusted applications.

For details on creating and applying new policies, see:

- *Configuring the IPS Rules policy* on page 39.
- *Configuring the Firewall Rules policy* on page 79.
- *Configuring the Application Blocking Rules policy* on page 97.
Policy maintenance and tasks

ePolicy Orchestrator provides two locations on the console tree to view and manage Host Intrusion Prevention policies and tasks:

- **Policies tab** of a selected node in the console tree
- **Policy Catalog** page.

Policies tab

Use the Policies tab to view, modify, or create the policy information relating to a selected node. For details, see:

- **IPS Policies** on page 31
- **Firewall Policies** on page 66
- **Application Blocking Policies** on page 93
- **General Policies** on page 102.

Policy inheritance and assignment

The Policies tab enables you to lock or unlock policy inheritance, view and reset broken inheritance, and copy policy assignments from one node to another.

To lock the assignment of a custom policy:

1. In the console tree, select a group or computer and click the Policies tab.
2. Expand a Host Intrusion Prevention feature to display the policies assigned to the node.
3. Click Edit for a custom policy.
4. Select Lock, and then click Apply.

Only administrators can lock a named policy.

To view and reset broken inheritance below a specific node:

1. In the console tree, select a group or computer and click the Policies tab.
2. Expand a Host Intrusion Prevention feature to display the policies assigned to the node.

![Figure 8-1 Policy inheritance](image.png)
Under **Inherited By** is the number of nodes to which this policy’s inheritance is broken.

This number is the number of nodes where the policy is broken, not the number of systems which do not inherit the policy. For example, if only one particular group node does not inherit the policy, this is represented by **1 doesn’t inherit**, regardless of the number of systems within the group.

3 Click the blue text indicating the number of child nodes that do not inherit.

The **View broken inheritance** page appears and list node names.

**Figure 8-2  View broken inheritance page**

4 To reset the inheritance of any of these nodes, select the checkbox next to the node name, and then click **Reset Inheritance**.

**To copy and paste policy assignments of a node:**

1 In the console tree, select a group or computer from which you want to copy policy assignments and click the **Policies** tab.

2 Click **Copy policy assignments**.

3 Select the features whose policy assignments you want to copy and click **OK**.

4 In the console tree, select a group or computer and click **Paste policy assignments**.

5 Click **OK** to confirm the replacement of assignments.
Policy Catalog

Use the Policy Catalog node of the console tree to view, create, and edit policies without reference to a particular node.

Viewing policy information

The Policy Catalog enables you to view all Host Intrusion Prevention policies, their assignments, and owners.

To view all policies that have been created:
1. In the console tree, select Policy Catalog.
2. Expand Host Intrusion Prevention to expose the policy categories.

To view nodes where a policy is assigned:
1. On the Policy Catalog page, expand Host Intrusion Prevention, and then expand a policy category.
2. Under Assignments on the row of the desired named policy, click the blue text that indicates the number of nodes to which the policy is assigned (for example, 1 assignments).
On the View assignments page, each node with the policy assigned appears with its **Node Name** and **Node Type**. This list shows the assignment points only, not the nodes where the policy is inherited.

**Figure 8-5 View assignments for a policy**

<table>
<thead>
<tr>
<th>Node Name</th>
<th>Node Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory: \Srv1\FS-91</td>
<td>computer</td>
</tr>
</tbody>
</table>

3 Click the node name to see the Assign Policies page for that node.

**To view the settings and owner of a policy:**

1 On the Policy Catalog page, expand Host Intrusion Prevention, and then expand a policy category.

   The owner of the named policy is displayed under Owner.

2 Click the policy name to view its settings.

**To view assignments where policy enforcement is disabled:**

1 On the Policy Catalog page, click the blue text next to Enforcement, which indicates the number of assignments where enforcement is disabled.

   The View assignments where policy enforcement is disabled page appears.

2 Click any nodes in the list to open the Assign Policies page for that node.

**Editing policy information**

From the Policy Catalog page you can create new named policies, which by default are not assigned to any particular nodes.
To edit a policy:

1. On the Policy Catalog page, expand Host Intrusion Prevention, and then expand a policy category.

2. Do any of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a policy</td>
<td>Click Define new policy, name it, and edit the settings.</td>
</tr>
<tr>
<td>Rename a policy</td>
<td>Click Rename and change the name of the policy. (Not available for the default policy.)</td>
</tr>
<tr>
<td>Duplicate a policy</td>
<td>Click Duplicate, change the name of the policy, and edit the settings.</td>
</tr>
<tr>
<td>Delete a policy</td>
<td>Click Delete. (Not available for the default policy.) Note: When you delete a policy, all nodes to which it is currently applied inherit the policy of this category from their parent nodes. Before deleting a policy, look at all of the nodes to which it is assigned, and assign a different policy if you don’t want the policy to inherit from the parent node. If you delete a policy that is applied at the Directory level, the default policy of this category is applied.</td>
</tr>
<tr>
<td>Assign a policy owner</td>
<td>Click the owner of the policy and select another owner from a list. (Not available for the default policy.)</td>
</tr>
<tr>
<td>Export a policy</td>
<td>Click Export, then name and save the policy (an XML file) to the desired location.</td>
</tr>
<tr>
<td>Export all policies</td>
<td>Click Export all policies, then name and save the policy XML file to the desired location</td>
</tr>
<tr>
<td>Import policies</td>
<td>Click Import Policy at the top of the Policy Catalog page, select the policy XML file, and then click OK</td>
</tr>
</tbody>
</table>

For details on any of these features, refer to the ePolicy Orchestrator Product Guide or the online help.
Running server tasks

Host Intrusion Prevention provides server tasks manage and maintain the security level of clients. These include:

- Updating user domain lists (*Directory Gateway*)
- Archiving and removing events from the database (*Event Archiver*)
- Translating client properties to facilitate management (*Property Translator*)

For more information running server tasks, see the ePolicy Orchestrator online help or product guide.

Directory Gateway

The Directory Gateway server task updates the list of domains where a client runs. This updated list is needed during IPS exception rule creation, because exception rules are enforced only on the domains listed in the database. Over time, domains are added and removed, so the list needs to be update periodically to ensure proper application of exceptions.

For this task, select a domain in the list that appears on which to run the update and enter the required domain user name and password credentials. The appropriate directory servers are then queried for domain updates. This task can be scheduled on a daily or weekly interval depending on the size of the environment, with larger deployments requiring more frequent updates.

Event Archiver

The Event Archiver server task archives events from the database for optimum database performance. Over time, Host Intrusion Prevention generates thousands of events, greatly increasing the size of the database. Periodically archive and remove older events to control database size ensuring the proper functioning of the application.

For this task, enter the directory path location for the archive file and the minimum age in days of the events to be archived. A zipped XML file named with the current date is created in the location indicated and the events are removed from the database.

Property Translator

The Property Translator server task translates Host Intrusion Prevention data that is stored in the ePolicy Orchestrator database to handle Host Intrusion Prevention sorting, grouping, and filtering of data. This task, which runs automatically every 15 minutes, should not be edited; however, you can disable this task if necessary.

To change the frequency to other than 15 minutes, disable the original task and create a new server task with a new frequency.
Setting up notifications for events

The Notifications feature can alert you to any events that occur on Host Intrusion Prevention clients or the server itself. You can configure rules to send e-mail, SMS, text pager messages, or SNMP traps, or run external commands when specific events are received and processed by the ePolicy Orchestrator server. You can specify the event categories that generate a notification message and the frequency that notifications are sent. For complete details, see the ePolicy Orchestrator online help or product guide.

How notifications work

In the Host Intrusion Prevention environment, when events occur they are delivered to the ePolicy Orchestrator server. Notification rules are associated with the group or site that contains the affected systems, and are applied to the events. If the conditions of a rule are met, a notification message is sent, or an external command is run, as specified by the rule.

You can configure independent rules at different levels of the Directory. You can also configure when notification messages are sent by setting thresholds that are based on aggregation and throttling.

ePolicy Orchestrator provides default rules that you can enable for immediate use. Before enabling any of the default rules:

1. Specify the e-mail server from which the notification messages are sent.
2. Check that the recipient e-mail address is the one you want to receive e-mail messages.

Creating rules

You can create rules for a variety of event categories. These include:

- Access Protection rule violation detected and blocked
- Access Protection rule violation detected and NOT blocked
- Computer placed in quarantine mode
- E-mail content filtered or blocked
- Intrusion detected
- Non-compliant computer detected
- Normal operation
- Policy enforcement failed
- Repository update or replication failed
- Software deployment failed
- Software deployment succeeded
- Software failure or error
- Unknown category
- Update/upgrade failed
- Update/upgrade succeeded

All rules are created in the same basic manner by:

1. Describing the rule.
2. Setting filters for the rule.
3. Setting thresholds for the rule.
4. Creating the message to be sent and the type of delivery.
Host Intrusion Prevention notifications

Host Intrusion Prevention supports the following product-specific notification categories:

- Host Intrusion detected and handled
- Network Intrusion detected and handled
- Application blocked
- Computer placed in quarantine mode

Notifications can be configured only for all or none of the Host (or Network) IPS signatures. Entercept 5.x supported notifications based on sets of signature IDs or individual severity levels. Host Intrusion Prevention supports the specification of a single IPS signature ID as the Threat Name or Rule Name field in the notification rule configuration. By internally mapping the signature ID attribute of an event to the threat name, a rule is created to uniquely identify an IPS signature.

The specific mappings of Host Intrusion Prevention parameters allowed in the subject/body of a message include:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Host and Network IPS Events Values</th>
<th>Blocked Application Event Values</th>
<th>Quarantine Event Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReceivedThreatNames</td>
<td>SignatureID</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>SourceComputers</td>
<td>Remote IP address</td>
<td>computer name</td>
<td>computer name</td>
</tr>
<tr>
<td>AffectedObjects</td>
<td>Process Name</td>
<td>Application name</td>
<td>IP address of computer</td>
</tr>
<tr>
<td>EventTimestamp</td>
<td>Incident time</td>
<td>Incident time</td>
<td>Incident time</td>
</tr>
<tr>
<td>EventID</td>
<td>ePO mapping of event ID</td>
<td>ePO mapping of event ID</td>
<td>ePO mapping of event ID</td>
</tr>
<tr>
<td>AdditionalInformation</td>
<td>Localized Signature Name (from client computer)</td>
<td>Application full path</td>
<td>none</td>
</tr>
</tbody>
</table>
Running reports

The Host Intrusion Prevention software includes reporting functionality through ePolicy Orchestrator. You can produce several useful reports and queries from events and properties that are sent by the client to the server and stored in the database.

The Host Intrusion Prevention software includes predefined report and query templates, which are stored in the report repository and query repository under Reporting in the console tree. For information, see ePolicy Orchestrator 3.6 Reporting Guide.

You can produce reports and queries for a group of selected client systems, or limit report results by product or system criteria. You can export reports into a variety of file formats, including HTML and Microsoft Excel.

You can:

- Set a directory filter to gather only selected information. Choose which Directory segment to include in the report.
- Set a data filter using logical operators, to define precise filters on the data returned by the report.
- Generate graphical reports from the information in the database, and filter the reports as needed. You can print the reports and export them to other software.
- Conduct queries of computers, events, and installations.

Pre-defined reports

The Host Intrusion Prevention clients on the client systems send the server information that is stored in a reports database. You run reports and queries against this stored data.

There are eight pre-defined Host Intrusion Prevention reports that fall into two main categories: IPS reports and firewall reports. You can also create your own report templates using Crystal Reports 8.5.

Report repository

The report repository contains the pre-defined reports and queries from Host Intrusion Prevention and any custom reports and queries you create.

You can organize and maintain the report repository to suit your needs. For example, you can add reports that you exported as report templates, for example, to save custom selections made when generating a report, or add custom report templates. You can also organize report templates in logical groupings. For example, you can group reports that you run daily, weekly, and monthly under report groups with the same name.
Summary information and details

After a report is generated, you view summary information, as determined by the filter, if any, that you have set. From the summary information you can drill down to one or two levels for detailed information, all in the same report.

Report content control

You can control how much report information is visible to different users; for example, global administrators or site administrators. Site administrators and site reviewers can only report on those client systems in sites where they have permissions. Report information is also controlled by applying filters.

Host Intrusion Prevention reports

The Host Intrusion Prevention report templates include:

<table>
<thead>
<tr>
<th>IPS Reports</th>
<th>Firewall Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Events Summary by Signature</td>
<td>Blocked Application Summary</td>
</tr>
<tr>
<td>IPS Event Summary by Target</td>
<td>Top 10 Blocked Applications</td>
</tr>
<tr>
<td>Network Intrusion Summary by Source IP</td>
<td>Failed Quarantine Updates</td>
</tr>
<tr>
<td>Top 10 Attacked Nodes for IPS</td>
<td></td>
</tr>
<tr>
<td>Top 10 Triggered Signatures</td>
<td></td>
</tr>
</tbody>
</table>

**IPS Events Summary by Signature**

Use this report to view IPS events per signature. Details include:

<table>
<thead>
<tr>
<th>Initial View</th>
<th>Level 1 Drill Down</th>
<th>Level 2 Drill Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Name &gt; Signature Name</td>
<td>OS User</td>
<td></td>
</tr>
<tr>
<td>Event Count</td>
<td>Process &gt;</td>
<td>Reaction</td>
</tr>
<tr>
<td></td>
<td>Count</td>
<td>Node name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recording Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severity Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event description</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced details</td>
</tr>
</tbody>
</table>

Filters on signature, recording time, severity level, OS user, reaction, process, and source IP.
IPS Event Summary by Target

Use this report to view IPS events per host. Details include:

<table>
<thead>
<tr>
<th>Initial View</th>
<th>Level 1 Drill Down</th>
<th>Level 2 Drill Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name &gt;</td>
<td>Host Name</td>
<td>OS User</td>
</tr>
<tr>
<td>Event Count</td>
<td>Signature &gt;</td>
<td>Reaction</td>
</tr>
<tr>
<td></td>
<td>Count</td>
<td>Process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recording Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severity Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event description</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced details</td>
</tr>
</tbody>
</table>

Filters on signature, recording time, severity level, OS user, reaction, process, and source IP.

Network Intrusion Summary by Source IP

Use this report to view network intrusion events per source IP. Details include:

<table>
<thead>
<tr>
<th>Initial View</th>
<th>Level 1 Drill Down</th>
<th>Level 2 Drill Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP &gt;</td>
<td>Source IP</td>
<td>OS User</td>
</tr>
<tr>
<td>Event Count</td>
<td>Signature Name &gt;</td>
<td>Reaction</td>
</tr>
<tr>
<td></td>
<td>Count</td>
<td>Process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Node name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recording Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severity Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event description</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced details</td>
</tr>
</tbody>
</table>

Filters on source IP, signature, OS user, reaction, recording time, severity level, and host name.
Top 10 Attacked Nodes for IPS
Use this report to view a bar chart of the top 10 hosts where IPS events are triggered. Details include:

<table>
<thead>
<tr>
<th>Initial View</th>
<th>Level 1 Drill Down</th>
<th>Level 2 Drill Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name &gt;</td>
<td>Host Name</td>
<td>OS User</td>
</tr>
<tr>
<td>Event Count</td>
<td>Signature &gt;</td>
<td>Reaction</td>
</tr>
<tr>
<td></td>
<td>Count</td>
<td>Process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recording Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severity Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event description</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced details</td>
</tr>
</tbody>
</table>

Filters on platform and signature type.

Top 10 Triggered Signatures
Use this report to view a bar chart of the 10 most triggered IPS signatures. Details include:

<table>
<thead>
<tr>
<th>Initial View</th>
<th>Level 1 Drill Down</th>
<th>Level 2 Drill Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Name &gt;</td>
<td>Signature Name</td>
<td>OS User</td>
</tr>
<tr>
<td>Event Count</td>
<td>Process &gt;</td>
<td>Reaction</td>
</tr>
<tr>
<td></td>
<td>Count</td>
<td>Node name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recording Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severity Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event description</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced details</td>
</tr>
</tbody>
</table>

Filters on platform and signature type.

Blocked Application Summary
Use this report to view a summary of blocked application events per application. Details include:

<table>
<thead>
<tr>
<th>Initial View</th>
<th>Drill Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Description &gt;</td>
<td>Host Name</td>
</tr>
<tr>
<td>Event Count</td>
<td>Host IP</td>
</tr>
<tr>
<td></td>
<td>Event time</td>
</tr>
<tr>
<td></td>
<td>Process name</td>
</tr>
<tr>
<td></td>
<td>Application path</td>
</tr>
<tr>
<td></td>
<td>Application version</td>
</tr>
<tr>
<td></td>
<td>Application hash</td>
</tr>
</tbody>
</table>

Filters on application description and event time.
Top 10 Blocked Applications
Use this report to view a bar chart of the 10 most blocked applications. Details include:

<table>
<thead>
<tr>
<th>Initial View</th>
<th>Drill Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Description &gt;</td>
<td>Host Name</td>
</tr>
<tr>
<td>Event Count</td>
<td>Host IP</td>
</tr>
<tr>
<td></td>
<td>Event time</td>
</tr>
<tr>
<td></td>
<td>Process name</td>
</tr>
<tr>
<td></td>
<td>Application path</td>
</tr>
<tr>
<td></td>
<td>Application version</td>
</tr>
<tr>
<td></td>
<td>Application hash</td>
</tr>
</tbody>
</table>

Filters on application description, host name, and event time.

Failed Quarantine Updates
Use this report to view failed quarantine updates per host. Details include:

<table>
<thead>
<tr>
<th>Initial View</th>
<th>Drill Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name &gt;</td>
<td>Host Name</td>
</tr>
<tr>
<td>Event Count</td>
<td>Host IP</td>
</tr>
<tr>
<td></td>
<td>Event time</td>
</tr>
</tbody>
</table>

Filters on application host name, host IP, and event time.
Updating

The ePO database contains Host Intrusion Prevention security content data, such as signatures, which is displayed in Host intrusion Prevention policies. Host Intrusion Prevention supports multiple versions of client content and code, with the latest available content appearing in the ePO console. New content is always supported in subsequent versions, so content updates contain mostly new information or minor modifications to existing information.

Updates are handled by a content update package. This package contains content version information and updating scripts. Upon check-in, the package version is compared to the version of the most recent content information in the database. If the package is newer, the scripts from this package are extracted and executed. This new content information is then passed to clients at the next agent-server communication.

> Host Intrusion Prevention content updates must be checked into the ePO Repository for distribution to clients. Host Intrusion Prevention clients should obtain updates only through communication with the ePO server, and not directly through FTP or HTTP protocols.

The basic process includes checking in the update package to the ePO Repository, and then sending the updated information to the clients.

Checking in the update package

You can create an ePO server task that automatically checks in content update packages to the ePO Repository, or you can download an update package and check it in manually.

To add update packages automatically:
1. Select the ePO server name in the ePO console tree, and click the Scheduled Tasks tab.
2. Click Create task.
3. In the Configure New Task pane, type a name for the task, for example, HIP Content Updates.
4. From the Task type list, select Repository Pull.
5. From the Schedule type list, select a frequency.
6. Click Next.
7. Select the source repository (McAfeeHttp or McAfeeFtp) and any other available options.
8. Click Finish.

This task downloads the content update package directly from McAfee at the indicated frequency and adds it to the Repository, updating the database with new Host Intrusion Prevention content.
To add update packages manually:
1 Select the Repository in the ePO console tree and click Check in package.
2 Click Next, and then select Products or updates.
3 Click Next, and then enter the full path for the PkgCatalog.z file.
4 Click Next, and then click Finish.

Updating clients

After the update package is checked in to the Repository, you can send the updates to the client either by running an update task or by sending an agent wakeup call. A client can also request updates.

To run an update task:
1 Select the computer, group, or site in the ePO console tree to which you want to send content updates, and select the Tasks tab.
2 Select Schedule Task from the shortcut menu.
3 Type the name of the task, select ePolicy Orchestrator Agent Update, and click OK.
4 Right-click the task and select Edit Task.
5 In the ePolicy Orchestrator Scheduler dialog box, click Settings.
6 In the dialog box that appears, select HIP Content and click OK. (This option is available only if a content package is checked in to the Repository.)
7 In the ePolicy Orchestrator Scheduler dialog box, click the Schedule tab, and set the task to run immediately.
8 On the Task tab, deselect Inherit and select Enable.
9 Click Apply and then OK.

To send an agent wakeup call:
1 Right-click the site, group, or computer in the ePO console tree where you want to send content updates, and select Agent Wakeup Call.
2 Set the randomization to 0 minutes, and click OK.

The content updates are sent and applied to the client.

To have a client request an update:
(Valid only if an ePO agent icon appears in the system tray)

- Right-click the ePO icon in the system tray and select Update Now.

The McAfee Autoupdate progress dialog box appears. The content updates are pulled and applied to the client.
The Host Intrusion Prevention client can be installed on Windows, Solaris, and Linux platforms. Only the Windows version of the client has an interface, but all versions have troubleshooting functionality. This section describes the basic features of each client version.

- **Windows client**
- **Solaris client**
- **Linux client**

### Windows client

Direct client-side management of the Host Intrusion Prevention Windows client is available through a client interface. To display the client console, double-click the client icon in the system tray, or, on the **Start** menu, select **Programs | McAfee | Host Intrusion Prevention**.

When the client console first appears, most options are locked. When the console is in the locked mode, you can only view current settings and manually create client rules if the Client UI policy has manual creation of client rules enabled. For complete control of all settings in the console, unlock the interface with a password created in the applied Client UI policy. For details on these Client UI policy settings, see *Creating and applying a Client UI policy on page 105*. 
System tray icon

If the Host Intrusion Prevention icons appears in the system tray, it provides access to the client console and indicates the status of the client.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Host Intrusion Prevention status</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Working properly</td>
</tr>
<tr>
<td>![Icon]</td>
<td>A potential attack was detected</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Turned off, or not working properly</td>
</tr>
</tbody>
</table>

A description of the status appears when you place the mouse pointer over the icon. Right-click the icon to access the shortcut menu:

<table>
<thead>
<tr>
<th>Click...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure</td>
<td>Open the Host Intrusion Prevention client console.</td>
</tr>
<tr>
<td>About...</td>
<td>Open the About Host Intrusion Prevention dialog box, which displays the version number and other product information.</td>
</tr>
</tbody>
</table>

If the Allow disabling of features from the tray icon option is applied to the client, some or all of these additional commands are available:

<table>
<thead>
<tr>
<th>Click...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Settings</td>
<td>Enable all disabled features. Available only if one or more features have been disabled.</td>
</tr>
<tr>
<td>Disable All</td>
<td>Disable IPS, Firewall, Application Blocking features. Available only if all the features are enabled.</td>
</tr>
<tr>
<td>Disable IPS</td>
<td>Disable the IPS feature. This includes both Host IPS and Network IPS functionality. Available only if the feature is enabled.</td>
</tr>
<tr>
<td>Disable Firewall</td>
<td>Disable the Firewall feature. Available only if the feature is enabled.</td>
</tr>
<tr>
<td>Disable App Blocking</td>
<td>Disable the Application Blocking feature. This includes both Application Creation Blocking and Application Hooking Blocking. Available only if the feature is enabled.</td>
</tr>
</tbody>
</table>

Client console

The Host Intrusion Prevention client console gives you access to several configuration options. To open the console, do one of the following:

- Double-click the icon in the system tray.
- Right-click the icon and select Configure.
- On the Start menu select Programs | McAfee | Host Intrusion Prevention.
The console lets you configure and view information about Host Intrusion Prevention features. It contains several tabs, which correspond to a specific Host Intrusion Prevention feature. For details, see:

- **IPS Policy tab on page 142**
- **Firewall Policy tab on page 144**
- **Application Policy tab on page 146**
- **Blocked Hosts tab on page 148**
- **Application Protection tab on page 150**
- **Activity Log tab on page 151**

### Unlocking the client interface

An administrator remotely managing Host Intrusion Prevention using ePolicy Orchestrator can password protect the interface to prevent accidental changes. With a time-based and computer-specific password, an administrator or user can temporarily unlock the interface and make changes.

**To unlock the Host Intrusion Prevention interface:**

1. Obtain a password from the Host Intrusion Prevention administrator.

   For details on creating a password, see *Setting passwords on page 106.*

2. On the **Task** menu, select **Unlock User Interface.**

   The **Login** dialog box appears.

3. Type the password and click **OK.** If the password is an administrator password, and not a timed password, select **Administrator password** before clicking **OK.**

### Setting options

The Host Intrusion Prevention client console provides access to some settings delivered by the Client UI policy and enables you to customize them for the individual client.

**To customize client options:**

1. On the **Edit** menu click **Options.**

   The **Host Intrusion Prevention Options** dialog box appears.

2. Select and deselect options as needed.

<table>
<thead>
<tr>
<th>Select...</th>
<th>For this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display pop-up alert</td>
<td>An alert dialog box appears when an attack occurs. For details, see <em>Alerts.</em></td>
</tr>
<tr>
<td>Play sound</td>
<td>A sound plays when an attack occurs.</td>
</tr>
<tr>
<td>Flash tray icon</td>
<td>The icon toggles between regular status and attack status when an attack occurs.</td>
</tr>
</tbody>
</table>
Error Reporting

Host Intrusion Prevention includes an error reporting utility that tracks and logs software failures. When enabled, it prompts the user to forward detected problem data to McAfee technical support, where it can be used to open a support case, if appropriate.

To use the error reporting utility, a computer must have Internet access and a web browser that is Java Script enabled.

If McAfee Alert Manager is installed on the network where a computer failed, it informs the network administrator that a problem was detected. The network administrator can guide the user on how to handle the problem.

When the utility detects a failure, the user selects an option:

- **Submit Data** — This connects to the McAfee technical support web site and submits the data.
- **Ignore Error** — No connection is made.

When submitting data to the McAfee technical support web site, the user may be asked for additional information. If the problem has a known cause, the user may be directed to a web page that provides information about the problem and how to deal with it.

Troubleshooting

Host Intrusion Prevention includes a **Troubleshooting** option on the Help menu, which is available when the interface is unlocked. Options include enabling IPS and firewall logging and disabling system engines.

Logging

As part of troubleshooting you can create IPS and firewall activity logs that can be analyzed on the system or sent to McAfee support to help resolve problems.
To set IPS logging options:
1. Select the IPS Enable Logging checkbox.
2. Select the message type (All or a combination of Information, Warning, Debug, Error, Security Violations).
   
   At a minimum, you must select Error and Security Violations.
3. Click OK.

   The information is written to the CSlog.txt file in the Program Files\McAfee\Host Intrusion Prevention folder.

To set Firewall logging options:
1. Select the Firewall Enable Logging checkbox.
2. Select the message type (All or a combination of Information, Warning, Error, Kernel).
3. Click OK.

   The information is written to the FireSvc.dbg file in the Program Files\McAfee\Host Intrusion Prevention folder.

Host IPS engines
As part of troubleshooting, you can also disable engines that protect a client. McAfee recommends that only administrators in communication with McAfee support use this troubleshooting procedure.

For access, click Functionality in the Troubleshooting Options dialog box. In the HIPS Engines dialog box that appears, disable one or more client system engines by deselecting the checkbox next to the engine. After the problem has been resolved, and to return to a normal operating environment, be sure all engines are selected.
A user can encounter several types of alert messages and needs to react to them. These include intrusion detection, firewall, quarantine, application blocking, and spoof detection alerts. Firewall and application blocking alerts appear only when the client is in Learn mode for these features.

### Intrusion alerts

If you enable IPS protection and the **Display pop-up alert** option, this alert automatically appears when Host Intrusion Prevention detects a potential attack. If the client is in Adaptive mode, this alert appears only if the **Allow Client Rules** option is disabled for the signature that caused the event to occur.

The **Intrusion Information** tab displays details about the attack that generated the alert, including a description of the attack, the user/client computer where the attack occurred, the process involved in the attack, and the time and date when Host Intrusion Prevention intercepted it. In addition, a generic administrator-specified message can appear.

---

**Figure 9-2** HIPS Engines

**Figure 9-3** Intrusion Detected Alert dialog box
You can ignore the event by clicking Ignore, or create an exception rule for the event by clicking Create Exception. The Create Exception button is active only if the Allow Client Rules option is enabled for the signature that caused the event to occur.

If the alert is the result of a HIP signature, the exception rule dialog box is prefilled with the name of the process, user, and signature. You can select All Signatures or All Processes, but not both. The user name will always be included in the exception.

If the alert is the result of a NIP signature, the exception rule dialog box is prefilled with the signature name and the host IP address. You can optionally select All Hosts.

In addition, you can click Notify Admin to send information about the event to the Host Intrusion Prevention administrator. This button is active only if the Allow user to notify administrator option is enabled in the applied Client UI policy.

Select Do not show any alerts for IPS Events to stop displaying IPS Event alerts. To have the alerts reappear after selecting this option, select Display pop-up alert in the Options dialog box.

This intrusion alert also appears for firewall intrusions if a firewall rule is matched that has the Treat rule match as an intrusion option selected.

**Firewall alerts**

If you enable firewall protection and the Learn mode for either incoming or outgoing traffic, a firewall alert appears. The Application Information tab displays information about the application attempting network access, including application name, path, and version. The Connection Information tab displays information about the traffic protocol, address, and ports.

**To respond to a firewall Learn Mode alert**

1. On the Application Information tab of the alert dialog box, do one of the following:
   - Click Deny to block this and all similar traffic.
   - Click Allow to permit this and all similar traffic through the firewall

2. Optional: On the Connection Information tab, select possible options for the new firewall rule:

<table>
<thead>
<tr>
<th>Select...</th>
<th>To do this...</th>
</tr>
</thead>
</table>
| Create a firewall application rule for all ports and services | Create a rule to allow or block an application’s traffic over any port or service. If you do not select this option, the new firewall rule allows or blocks only specific ports:  
  - If the intercepted traffic uses a port lower than 1024, the new rule allows or blocks only that specific port.  
  - If the traffic uses port 1024 or higher, the new rule allows or blocks the range of ports from 1024 to 65535. |
| Remove this rule when the application terminates             | Create a temporary allow or block rule that is deleted when the application is closed. If you do not select this option, the new firewall rule is created as a permanent client rule. |
Host Intrusion Prevention creates a new firewall rule based on the options selected, adds it to the Firewall Rules list, and automatically allows or blocks similar traffic.

**Figure 9-4 Firewall alert—Application Information and Connection Information tabs**

![Image](image_url)

**Application Blocking alerts**

When application creation or application hooking is enabled in the Application Blocking Options policy, Host Intrusion Prevention monitors application activities and allows or blocks them based on the rules in the Application Blocking Rules policy.

If you enabled Learn mode for either creation blocking or hooking blocking, Host Intrusion Prevention displays an Application Creation Alert or Application Hook Alert whenever it detects an unknown application trying to run or bind to another program.

The Application Information tab displays information about the application attempting to run (creation) or to hook (hook) to another process, including application name, path, and version.

Use this dialog box to select an action:

- **Click Allow** to let the application complete its action:
  - For an Application Creation Alert, clicking Allow lets the application run.
  - For an Application Hook Alert, clicking Allow lets the application bind itself to another program.

- **Click Deny** to block the application:
  - For an Application Creation Alert, clicking Deny prevents the application from running.
  - For an Application Hook Alert, clicking Deny blocks the application from binding itself to another program.

When you click Allow or Deny, Host Intrusion Prevention creates a new application rule based on your choice. After collecting client properties, this rule is added to the to the Application Client Rule tab of the Application Rules policy. The application is then allowed or blocked automatically.
Quarantine alerts

If you enable Quarantine mode and include the IP address of the client for quarantine enforcement in the Quarantine Options policy, a quarantine alert appears in the following situations:

- Changing the client computer’s IP address
- Disconnecting and then reconnecting the client Ethernet connection
- Restarting the client

Spoof Detected alerts

If you enable the IPS feature, this alert automatically appears if Host Intrusion Prevention detects an application on your computer sending out spoofed network traffic. This means that the application is trying to make it seem like traffic from your computer actually comes from a different computer. It does this by changing the IP address in the outgoing packets. Spoofing is always suspicious activity. If you see this dialog box, immediately investigate the application that sent the spoofed traffic.

The Spoof Detected Alert dialog box appears only if you select the Display pop-up alert option. If you do not select this option, Host Intrusion Prevention automatically blocks the spoofed traffic without notifying you.

The Spoof Detected Alert dialog box is very similar to the firewall feature’s Learn Mode alert. It displays information about the intercepted traffic on two tabs — the Application Information tab, and the Connection Information tab.

The Application Information tab displays:

- The IP address that the traffic pretends to come from.
- Information about the program that generated the spoofed traffic.
- The time and date when Host Intrusion Prevention intercepted the traffic.

The **Connection Information** tab provides further networking information. In particular, **Local Address** shows the IP address that the application is pretending to have, while **Remote Address** shows your actual IP address.

**Figure 9-7 IP Spoof Detected Alert dialog box**

When Host Intrusion Prevention detects spoofed network traffic, it tries to block both the traffic and the application that generated it. It does this by adding a new rule to the end of the firewall rule list. This **Block spoofing attacker** rule specifically blocks all traffic created by the suspicious application, unless another rule in the rule list overrides it.
IPS Policy tab

Use the IPS Policy tab to configure the IPS feature, which protects against host intrusion attacks based on signature and behavioral rules. From this tab you can enable or disable functionality and configure client exception rules. For more details on IPS policies, see Chapter 4, IPS Policies.

Figure 9-8 IPS Policy tab

IPS Policy options

Options at the top of the tab control settings delivered by the server-side IPS policies after the client interface is unlocked.

To customize IPS Policy options:
1. Click the IPS Policy tab.
2. Select or deselect an option as needed.

<table>
<thead>
<tr>
<th>Select...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Host IPS</td>
<td>Enable host intrusion prevention protection.</td>
</tr>
<tr>
<td>Enable Network IPS</td>
<td>Enable network intrusion prevention protection.</td>
</tr>
<tr>
<td>Enable Adaptive Mode</td>
<td>Enable Adaptive mode to automatically create exceptions to intrusion prevention signatures.</td>
</tr>
<tr>
<td>Automatically block attackers</td>
<td>Block network intrusion attacks automatically for a set period of time. Select Until removed to block an attack until it is removed, or select for X min. to block an attack for set a number of minutes, with the default at 30.</td>
</tr>
</tbody>
</table>
IPS Policy exception rules
The IPS exception rules list displays client exception rules that you can view and edit.

To edit the exception rules:
1. Click Add to add a rule.

   The Exception Rule dialog box appears.

2. Type a description for the rule.

3. Select the application the rule applies to from the application list, or click Browse to locate the application.

4. Select Exception rule is Active to make the rule active.

   Exception applies to all signatures, which is not enabled and selected by default, applies the exception to all signatures.

5. Click OK.

   The new rule appears in the list.

6. For other edits, do one of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the details</td>
<td>Double-click a rule, or select a rule and click Properties. The Exception</td>
</tr>
<tr>
<td>of a rule or edit a</td>
<td>Rule dialog box appears displaying rule information that can be edited.</td>
</tr>
<tr>
<td>rule</td>
<td></td>
</tr>
<tr>
<td>Make a rule active/inactive</td>
<td>Select or clear the Exception rule is Active checkbox in the Exception</td>
</tr>
<tr>
<td></td>
<td>Rule dialog box. You can also select or clear the checkbox next to the rule</td>
</tr>
<tr>
<td></td>
<td>icon in the list.</td>
</tr>
<tr>
<td>Delete a rule</td>
<td>Select a rule and click Remove.</td>
</tr>
</tbody>
</table>

Exception rules list
The exception rules list displays exception rules relevant to the client and provides summary and detailed information for each rule.

<table>
<thead>
<tr>
<th>This column...</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exception</td>
<td>The name of the exception.</td>
</tr>
<tr>
<td>Signature</td>
<td>The name of the signature against which the exception is created.</td>
</tr>
<tr>
<td>Application</td>
<td>The application that this rule applies to, including the program name</td>
</tr>
<tr>
<td></td>
<td>and executable file name.</td>
</tr>
</tbody>
</table>
Firewall Policy tab

Use the Firewall Policy tab to configure the Firewall feature, which allows or blocks network communication based on rules that you define. From this tab you can enable or disable functionality and configure client firewall rules. For more details on firewall policies, see Chapter 5, Firewall Policies.

Figure 9-9 Firewall Policy tab

Firewall Policy options

Options at the top of the tab control settings delivered by the server-side firewall policies.

To customize Firewall Policy options:

1. Click the Firewall Policy tab.
2. Select or deselect an option as needed.

<table>
<thead>
<tr>
<th>Select...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Firewall</td>
<td>Enable firewall policy protection.</td>
</tr>
<tr>
<td>Learn Mode</td>
<td>Enable Learn mode for incoming traffic.</td>
</tr>
<tr>
<td>Incoming Enabled</td>
<td></td>
</tr>
<tr>
<td>Learn Mode</td>
<td>Enable Learn mode for outgoing traffic</td>
</tr>
<tr>
<td>Outgoing Enabled</td>
<td></td>
</tr>
<tr>
<td>Adaptive Mode</td>
<td>Enable Adaptive Mode.</td>
</tr>
<tr>
<td>Trusted...</td>
<td>Create trusted networks. For details, see Configuring the Trusted Networks policy on page 110.</td>
</tr>
</tbody>
</table>

For a discussion of Learn mode versus Adaptive mode, see Placing clients in Adaptive or Learn mode on page 26.
Firewall Policy Rules
The Firewall rules list displays client rules that you can view and edit. For details on working with firewall rules, see:

- Viewing and editing firewall rules on page 87.
- Creating a new firewall rule or firewall group on page 82.
- Deleting a firewall rule or group on page 87.

Note
You cannot add firewall connection-aware groups from the client. This functionality is available only in the Firewall Rules policy managed at the ePolicy Orchestrator console.

Firewall rules list
The firewall rules list displays rules and rule groups relevant to the client and provides summary and detailed information for each rule.

<table>
<thead>
<tr>
<th>This column...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The purpose of this rule or rule group.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Which protocol(s) the rule applies to (TCP, UDP, ICMP). Whether the rule permits traffic, or blocks it:</td>
</tr>
<tr>
<td></td>
<td>Permits traffic.</td>
</tr>
<tr>
<td></td>
<td>Blocks traffic.</td>
</tr>
<tr>
<td></td>
<td>Whether the rule applies to incoming traffic, outgoing traffic, or both:</td>
</tr>
<tr>
<td></td>
<td>Incoming traffic.</td>
</tr>
<tr>
<td></td>
<td>Outgoing traffic.</td>
</tr>
<tr>
<td></td>
<td>Both directions.</td>
</tr>
<tr>
<td></td>
<td>Whether Host Intrusion Prevention treats traffic that matches this rule as an intrusion (an attack) on your system.</td>
</tr>
<tr>
<td></td>
<td>Whether this rule only applies at specific times.</td>
</tr>
<tr>
<td>Service (L)</td>
<td>Services on your computer where this rule applies. When possible, this column shows associated port numbers. You can define an individual service, a range of services, a list of specific services, or specify all (Any) or no services (N/A).</td>
</tr>
<tr>
<td>Service (R)</td>
<td>Services where this rule applies on the computer you are sending traffic to, or receiving traffic from. When possible, this column shows associated port numbers. You can define an individual service, a range of services, a list of specific services, or specify all (Any) or no services (N/A).</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address, subnet, domain, or other specific identifier that this rule applies to.</td>
</tr>
<tr>
<td>Application</td>
<td>The application that this rule applies to, including the program name and executable file name.</td>
</tr>
</tbody>
</table>
Application Policy tab

Use the Application Policy tab to configure the Application Blocking feature. You can specify whether an application can run (known as application creation), or whether it can bind itself to other programs (known as application hooking), whether to enable Learn mode for application creation and hooking, and configure client application rules. For more details on application blocking, see Chapter 6, Application Blocking Policies.

Figure 9-10  Application Policy tab

Application Policy options

Options at the top of the tab control settings delivered by the server-side application policies.

To customize Application Policy options:

1. Click the Application Policy tab.
2. Select or deselect an option as needed.

<table>
<thead>
<tr>
<th>Select...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Application Creation Blocking</td>
<td>Enable application creation blocking. The Enable Learn Mode Application Creation options is enabled.</td>
</tr>
<tr>
<td>Enable Application Hooking Blocking</td>
<td>Enable application hooking blocking. The Enable Learn Mode Application Hooking options is enabled.</td>
</tr>
<tr>
<td>Enable Learn Mode Application Creation</td>
<td>Enable Learn mode for application creation, where the user is prompted to allow or block application creation.</td>
</tr>
<tr>
<td>Enable Learn Mode Application Hooking</td>
<td>Enable Learn mode for application hooking, where the user is prompted to allow or block application hooking.</td>
</tr>
</tbody>
</table>
Application Policy rules

The application policy rules list displays client rules you can view and edit. For details on working with application blocking rules, see:

- Viewing and editing Application Blocking Rules on page 98.
- Deleting an application blocking rule on page 100.

Application rules list

The application rules list displays rules relevant to the client and provides summary and detailed information for each rule.

<table>
<thead>
<tr>
<th>This column...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The purpose of this rule.</td>
</tr>
<tr>
<td>Create</td>
<td>Permits application to run.</td>
</tr>
<tr>
<td></td>
<td>Blocks application from running.</td>
</tr>
<tr>
<td>Hook</td>
<td>Permits application to hook other programs.</td>
</tr>
<tr>
<td></td>
<td>Blocks application from hooking other programs.</td>
</tr>
<tr>
<td>Application</td>
<td>The file name and path of the application that this rule applies to.</td>
</tr>
</tbody>
</table>
Blocked Hosts tab

Use the Blocked Hosts tab to monitor a list of blocked hosts (IP addresses) that is automatically created when Network IPS (NIPS) protection is enabled (see IPS Policy options on page 142). If Create Client Rules is selected in the IPS Options policy in the ePolicy Orchestrator console, you can add to and edit the list of blocked hosts.

Figure 9-11 Blocked Hosts tab

Blocked Hosts list

You can view and edit the list of blocked addresses. Edits include adding, removing, editing blocked hosts, and viewing blocked host details.

The blocked hosts list shows all hosts currently blocked by Host Intrusion Prevention. Each line represents a single host. You can get more information on individual hosts by reading the information in each column.

<table>
<thead>
<tr>
<th>Column</th>
<th>What it shows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The IP address that Host Intrusion Prevention is blocking.</td>
</tr>
<tr>
<td>Blocked Reason</td>
<td>An explanation of why Host Intrusion Prevention is blocking this address.</td>
</tr>
<tr>
<td></td>
<td>If Host Intrusion Prevention added this address to the list because of an attempted attack on your system, this column describes the type of attack.</td>
</tr>
<tr>
<td></td>
<td>If Host Intrusion Prevention added this address because one of its firewall rules used the Treat rule match as intrusion option, this column lists the name of the relevant firewall rule.</td>
</tr>
<tr>
<td></td>
<td>If you added this address manually, this column lists only the IP address that you blocked.</td>
</tr>
</tbody>
</table>
To edit the Blocked Hosts list:

1. Click Add to add a host. The Blocked Host dialog box appears.
2. Enter the IP address you want to block. To search for an IPS address by domain name, click DNS Lookup.
3. Determine how long to block the IP address:
   - Select Until Removed to keep the host blocked until deleted.
   - Select For and type the number of minutes, up to 60, to keep the host blocked for a fixed period of time.
4. Click OK. The new blocked host appears in the list.

   After you create a blocked address, Host Intrusion Prevention adds a new entry to the list on the Application Protection tab. It blocks any communication attempt from that IP address until you remove it from the blocked addresses list, or a set period of time expires.

5. For other edits, do one of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the details of or edit a blocked host</td>
<td>Double-click a host entry, or select a host and click Properties. The Blocked Host dialog box displays information that can be edited.</td>
</tr>
<tr>
<td>Delete a blocked host</td>
<td>Select a host and click Remove.</td>
</tr>
</tbody>
</table>
Application Protection tab

The Application Protection tab displays a list of applications protected on the client. This is a view-only list populated by administrative policy and a client-specific application list created heuristically. For details, see Application Protection Rules on page 51.

Figure 9-12 Application Protection List tab

Application Protection list

This list shows all monitored processes on the client.

<table>
<thead>
<tr>
<th>Column</th>
<th>What it shows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>The application process.</td>
</tr>
<tr>
<td>PID</td>
<td>The process ID, which is the key for the cache lookup of a process.</td>
</tr>
<tr>
<td>Process Full Path</td>
<td>The full path name of the application process.</td>
</tr>
</tbody>
</table>
Activity Log tab

Use the Activity Log tab to configure the logging feature and track Host Intrusion Prevention actions.

Figure 9-13 Activity Log tab

Activity Log options

Options at the top of the tab control what items to log and display.

To customize Activity Log options:
1. Click the Activity Log tab.
2. Select or deselect an option as needed.

Select... | To do this...
--- | ---
Traffic Logging - Log All Blocked | Log all blocked firewall traffic.
Traffic Logging - Log All Allowed | Log all allowed firewall traffic.
Filter Options - Traffic | Filter the data to display blocked and allowed firewall traffic.
Filter Options - Applications | Filter the data to display events caused by applications.
Filter Options - Intrusions | Filter the data to display intrusions.

Note: You can enable and disable logging for the firewall traffic, but not for the IPS or application blocking features. However, you can choose to hide these events in the log by filtering them out.
Activity Log list

The Activity Log contains a running log of activity. Most recent activity appears at the bottom of the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>What it shows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The date and time of the Host Intrusion Prevention action.</td>
</tr>
<tr>
<td>Event</td>
<td>The feature that performed the action.</td>
</tr>
<tr>
<td></td>
<td>- Traffic indicates a firewall action.</td>
</tr>
<tr>
<td></td>
<td>- Application indicates an application blocking action.</td>
</tr>
<tr>
<td></td>
<td>- Intrusion indicates an IPS action.</td>
</tr>
<tr>
<td></td>
<td>- System indicates an event relating to the software’s internal components.</td>
</tr>
<tr>
<td></td>
<td>- Service indicates an event relating to the software’s service or drivers.</td>
</tr>
<tr>
<td>Source</td>
<td>The remote address that this communication was either sent to, or sent from.</td>
</tr>
<tr>
<td>Intrusion Data</td>
<td>An icon indicating that Host Intrusion Prevention saved the packet data</td>
</tr>
<tr>
<td></td>
<td>associated with this attack. (This icon only appears for IPS log entries.)</td>
</tr>
<tr>
<td>Note:</td>
<td>This column only appears if you select Create Sniffer Capture... in the</td>
</tr>
<tr>
<td></td>
<td>McAfee Host Intrusion Prevention Options dialog box.</td>
</tr>
<tr>
<td>Application</td>
<td>The program that caused the action.</td>
</tr>
<tr>
<td>Message</td>
<td>A description of the action, with as much detail as possible.</td>
</tr>
</tbody>
</table>

You can clear the list either by deleting the log contents or saving it to a .txt file.

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permanently delete the contents of the log</td>
<td>Click Clear.</td>
</tr>
<tr>
<td>Save the contents of the log and delete the list from the tab</td>
<td>Click Save. In the Save Log File To dialog box that appears, name and save the .txt file.</td>
</tr>
</tbody>
</table>
Solaris client

The Host Intrusion Prevention 7.0 Solaris client identifies and prevents potentially harmful attempts to compromise a Solaris server’s files and applications. It protects the server’s operating system along with Apache and Sun web servers, with an emphasis on preventing buffer overflow attacks.

Policy enforcement with the Solaris client

Not all policies that protect a Windows client are available for the Solaris client. In brief, Host Intrusion Prevention protects the host server from harmful attacks but does not offer firewall protection. The valid policies are listed here.

<table>
<thead>
<tr>
<th>With this policy...</th>
<th>These options are available...</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIP 7.0 GENERAL:</td>
<td></td>
</tr>
<tr>
<td>Client UI</td>
<td>None except admin or time-based password to allow use of the troubleshooting tool.</td>
</tr>
<tr>
<td>Trusted Networks</td>
<td>None</td>
</tr>
<tr>
<td>Trusted Applications</td>
<td>Only Mark as trusted for IPS and New Process Name to add trusted applications.</td>
</tr>
<tr>
<td>HIP 7.0 IPS:</td>
<td></td>
</tr>
<tr>
<td>IPS Options</td>
<td>Enable HIPS</td>
</tr>
<tr>
<td></td>
<td>Enable Adaptive Mode</td>
</tr>
<tr>
<td></td>
<td>Retain existing Client Rules</td>
</tr>
<tr>
<td>IPS Protection</td>
<td>All</td>
</tr>
<tr>
<td>IPS Rules</td>
<td>Exception Rules</td>
</tr>
<tr>
<td></td>
<td>Signatures (default and custom HIPS rules only)</td>
</tr>
<tr>
<td>Note: NIPS signatures and Application Protection Rules are not available.</td>
<td></td>
</tr>
<tr>
<td>IPS Events</td>
<td>All</td>
</tr>
<tr>
<td>IPS Client Rules</td>
<td>All</td>
</tr>
<tr>
<td>Search IPS Exception Rules</td>
<td>All</td>
</tr>
<tr>
<td>HIP 7.0 FIREWALL</td>
<td>None</td>
</tr>
<tr>
<td>HIP 7.0 APPLICATION BLOCKING</td>
<td>None</td>
</tr>
</tbody>
</table>

Troubleshooting

After the Solaris client is installed and started, it protects its host. However, you may need to troubleshoot installation or operation issues.

Client installation issues

If a problem was caused while installing or uninstalling the client, there are several things to investigate. These can include ensuring that all required files were installed in the correct directory, uninstalling and then reinstalling the client, and checking process logs.
Verifying installation files
After an installation, check that all the files were installed in the appropriate directory on the client. The /opt/McAfee/hip directory should contain these essential files and directories:

<table>
<thead>
<tr>
<th>File/Directory Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HipClient</td>
<td>Solaris client</td>
</tr>
<tr>
<td>HipClient-bin</td>
<td></td>
</tr>
<tr>
<td>HipClientPolicy.xml</td>
<td>Policy rules</td>
</tr>
<tr>
<td>hipts</td>
<td>Troubleshooting tool</td>
</tr>
<tr>
<td>hipts-bin</td>
<td></td>
</tr>
<tr>
<td>*.so</td>
<td>Host Intrusion Prevention and ePO agent shared object modules</td>
</tr>
<tr>
<td>log directory</td>
<td>Contains log files: HIPShield.log and HIPClient.log</td>
</tr>
</tbody>
</table>

Installation history is written to /opt/McAfee/etc/hip-install.log. Refer to this file for any questions about the installation or removal process of the Host Intrusion Prevention client.

Verifying client is running
The client might be installed correctly, but you might encounter problems with its operation. If the client does not appear in the ePO console, for example, check that it is running, using either of these commands:

- /etc/rc2.d/S99hip status
- ps -ef | grep hip.

Client operations issues
The Solaris client has no user interface to troubleshoot operation issues. It does offer a command-line troubleshooting tool, hipts, located in the /opt/McAfee/hip directory. To use this tool, you must provide a Host Intrusion Prevention client password. Use the default password that ships with the client (abcde12345), or send a Client UI policy to the client with either an administrator’s password or a time-based password set with the policy, and use this password.

Use the troubleshooting tool to:

- Indicate the logging settings and engine status for the client.
- Turn message logging on and off.
- Turn engines on and off.

Log on as root and run the following commands to aid in troubleshooting:

<table>
<thead>
<tr>
<th>Run this command...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>hipts status</td>
<td>Obtain the current status of the client indicating which type of logging is enabled, and which engines are running.</td>
</tr>
<tr>
<td>hipts logging on</td>
<td>Turn on logging of specific messages types.</td>
</tr>
<tr>
<td>hipts logging off</td>
<td>Turn off logging of all message types. Logging is off by default.</td>
</tr>
</tbody>
</table>
## Starting and stopping the client

You may need to stop a running client and restart it as part of troubleshooting.

### To stop a Solaris client:

1. Disable IPS protection. Use one of these procedures:
   - Set **IPS Options** to **Off** in the ePO console and apply the policy to the client.
   - Run the command: `hipts engines MISC:off`.

2. Run the command: `/etc/rc2.d/S99hip stop`.

### To restart a Solaris client:

1. Run the command: `/etc/rc2.d/S99hip restart`.

2. Enable IPS protection. Use one of these procedures, depending on which you used to stop the client:
   - Set **IPS Options** to **On** in the ePO console and apply the policy to the client.
   - Run the command: `hipts engines MISC:on`.

---

### Run this command... | To do this...
--- | ---
`hipts message <message name>:on` | Display the message type indicated when logging is set to “on.” Messages include:
- error
- warning
- debug
- info
- violations

`hipts message <message name>:off` | Hide the message type indicated when logging is set to “on.” Message error is off by default.

`hipts message all:on` | Display all message types when logging is set to “on.”

`hipts message all:off` | Hide all message types when logging is set to “on.”

`hipts engines <engine name>:on` | Turn on the engine indicated. Engine is on by default. Engines include:
- MISC
- FILES
- GUID
- MMAP
- BO
- ENV
- HTTP

`hipts engines <engine name>:off` | Turn off the engine indicated.

`hipts engines all:on` | Turn on all engines.

`hipts engines all:off` | Turn off all engines.

---

In addition to using the troubleshooting tool, consult the HIPShield.log and HIPClient.log files in the `/opt/McAfee/hip/log` directory to verify operations or track issues.
Linux client

The Host Intrusion Prevention 7.0 Linux client identifies and prevents potentially harmful attempts to compromise a Linux server’s files and applications. It leverages the native SELinux protection mechanism, translating IPS policies into SELinux rules and SELinux events back to IPS events, and provides easy management from the ePO console.

Policy enforcement with the Linux client

Not all policies that protect a Windows client are available for the Linux client. In brief, Host Intrusion Prevention protects the host server from harmful attacks but does not offer network intrusion protection, including buffer overflow. The policies that are valid are listed here.

<table>
<thead>
<tr>
<th>With this policy...</th>
<th>These options are available...</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIP 7.0 GENERAL:</td>
<td></td>
</tr>
<tr>
<td>Client UI</td>
<td>None except admin or time-based password to allow use of the troubleshooting tool.</td>
</tr>
<tr>
<td>Trusted Networks</td>
<td>None</td>
</tr>
<tr>
<td>Trusted Applications</td>
<td>Only Mark as trusted for IPS and New Process Name to add trusted applications.</td>
</tr>
<tr>
<td>HIP 7.0 IPS:</td>
<td></td>
</tr>
<tr>
<td>IPS Options</td>
<td>Enable HIPS</td>
</tr>
<tr>
<td></td>
<td>Enable Adaptive Mode</td>
</tr>
<tr>
<td></td>
<td>Retain existing Client Rules</td>
</tr>
<tr>
<td>IPS Protection</td>
<td>All</td>
</tr>
<tr>
<td>IPS Rules</td>
<td>Exception Rules</td>
</tr>
<tr>
<td></td>
<td>Signatures (default and custom HIPS rules only)</td>
</tr>
<tr>
<td></td>
<td>Note: NIPS signatures and Application Protection Rules are not available.</td>
</tr>
<tr>
<td>IPS Events</td>
<td>All</td>
</tr>
<tr>
<td>IPS Client Rules</td>
<td>All</td>
</tr>
<tr>
<td>Search IPS Exception Rules</td>
<td>All</td>
</tr>
<tr>
<td>HIP 7.0 FIREWALL</td>
<td>None</td>
</tr>
<tr>
<td>HIP 7.0 APPLICATION BLOCKING</td>
<td>None</td>
</tr>
</tbody>
</table>

Notes about the Linux client

- If you have an existing SELinux policy in place or are using default protection settings, installing a Linux client replaces the policy with a default McAfee Host Intrusion Prevention policy. Uninstalling the Linux client restores the previous SELinux policy.

- The Linux client requires that SELinux be installed and enabled (set to enforce or permissive). If it is installed but disabled, enable it, set it to targeted policy, and restart the computer before installing the Linux client.

- Linux controls file attribute changes with a single SELinux permission (file:setattr). It does not have individual control of chdir or symlink, control of changing directory, or control of creating a symbolic link.
SELinux uses a mandatory access control mechanism implemented in the Linux kernel with the Linux Security Modules (LSM) framework. This framework checks for allowed operations after standard Linux discretionary access controls are checked. Because the Linux client uses LSM, any other application that uses LSM will not work unless stacking is implemented.

Troubleshooting

After the Linux client is installed and started, it protects its host. However, you may need to troubleshoot installation or operation issues.

Client installation issues

If a problem was caused while installing or uninstalling the client, there are several things to investigate. These can include ensuring that all required files were installed in the correct directory, uninstalling and then reinstalling the client, and checking process logs.

Verifying installation files

After an installation, check to see that all the files were installed in the appropriate directory on the client. The `opt/McAfee/hip` directory should contain these essential files and directories:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HipClient</td>
<td>Linux client</td>
</tr>
<tr>
<td>HipClient-bin</td>
<td></td>
</tr>
<tr>
<td>HipClientPolicy.xml</td>
<td>Policy rules</td>
</tr>
<tr>
<td>hipts</td>
<td>Troubleshooting tool</td>
</tr>
<tr>
<td>hipts-bin</td>
<td></td>
</tr>
<tr>
<td>*.so</td>
<td>Host Intrusion Prevention and ePO agent shared object modules</td>
</tr>
<tr>
<td>log directory</td>
<td>Contains log files: HIPShield.log and HIPClient.log</td>
</tr>
</tbody>
</table>

Installation history is written to `/opt/McAfee/etc/hip-install.log`. Refer to this file for any questions about the installation or removal process of the Host Intrusion Prevention client.

Verifying the client is running

If the client does not appear in the ePO console, for example, check that the client is running. To do this, run this command:

```
ps -ef | grep hip
```

Client operations issues

The client might be installed correctly, but you might encounter problems with the operation of the client. You can check whether the client is running, and stop and restart the client.
Troubleshooting tool

The Linux client has no user interface for troubleshooting operation issues. It does offer a command-line troubleshooting tool, `hipts`, located in the `opt/McAfee/hip` directory. To use this tool, you must provide a Host Intrusion Prevention client password. Use the default password that ships with the client (abcde12345), or send a Client UI policy to the client with either an administrator’s password or a time-based password set with the policy, and use this password.

Use the troubleshooting tool to:

- Indicate the logging settings and engine status for the client.
- Turn message logging on and off.
- Turn engines on and off.

Log on as root and run the following commands to aid in troubleshooting:

<table>
<thead>
<tr>
<th>Run this command...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hipts status</code></td>
<td>Obtain the current status of the client indicating which type of logging is enabled, and which engines are running.</td>
</tr>
<tr>
<td><code>hipts logging on</code></td>
<td>Turn on logging of specific messages types.</td>
</tr>
<tr>
<td><code>hipts logging off</code></td>
<td>Turn off logging of all message types. Logging is off by default.</td>
</tr>
</tbody>
</table>
| `hipts message <message name>:on` | Display the message type indicated when logging is set to “on.” Messages include:  
  - error  
  - warning  
  - debug  
  - info  
  - violations |
| `hipts message <message name>:off` | Hide the message type indicated when logging is set to “on.” Message error is off by default. |
| `hipts message all:on` | Display all message types when logging is set to “on.” |
| `hipts message all:off` | Hide all message types when logging is set to “on.” |
| `hipts engines <engine name>:on` | Turn on the engine indicated. Engine is on by default. Engines include:  
  - MISC  
  - FILES |
| `hipts engines <engine name>:off` | Turn off the engine indicated. |
| `hipts engines all:on` | Turn on all engines. |
| `hipts engines all:off` | Turn off all engines. |

Tip

In addition to using the troubleshooting tool, consult the HIPShield.log and HIPClient.log files in the McAfee/hip/log directory to verify operations or track issues.
Starting and stopping the client

You may need to stop a running client and restart it as part of troubleshooting.

To stop a Linux client:
1. Disable IPS protection. Use one of these procedures:
   - Set **IPS Options** to **Off** in the ePO console and apply the policy to the client.
   - Run the command: `hipts engines MISC:off`.
2. Run the command: `hipts agent off`.

To restart a Linux client:
1. Run the command: `hipts agent on`.
2. Enable IPS protection. Use one of these procedures, depending on which you used to stop the client:
   - Set **IPS Options** to **On** in the ePO console and apply the policy to the client.
   - Run the command: `hipts engines MISC:on`.
This section describes the structure of custom signatures and provides information on how to write custom signatures for the various client platforms. Topics include:

- Rule Structure
- Windows Custom Signatures
- Solaris Custom Signatures
- Linux Custom Signatures

## Rule Structure

Every signature contains one or more rules written in ANSI Tool Command Language (TCL) syntax. Each rule contains mandatory and optional sections, with one section per line. Optional sections vary according to the operating system and the class of the rule. Each section defines a rule category and its value. One section always identifies the class of the rule, which defines the rule’s overall behavior.

The basic structure of a rule is the following:

```tcl
Rule {
    SectionA value
    SectionB value
    SectionC value
    ...
}
```

Be sure to review the rules for writing strings and escape sequences in TCL before attempting to write custom rules. A quick review of any standard reference on TCL should ensure that you enter proper values correctly.
A rule to prevent a request to the web server that has “subject” in the http request query has the following format:

```
Rule {
    Class Isapi
    Id 4001
    level 4
    query { Include "*subject*" }
    method { Include "GET" }
    time { Include "*" }
    application { Include "*" }
    user_name { Include "*" }
    directives -c -d isapi:request
}
```

See Windows Custom Signatures for an explanation of the various sections and values.

**Mandatory common sections**

A rule’s mandatory sections and their values include the items below. For mandatory sections relevant to the class section that is selected, see the class section under Windows, Unix, and Linux Custom Signatures. The keywords Include and Exclude are used for all sections except for Id, level, and directives. Include means that the section works on the value indicated, and Exclude means that the section works on all values except the one indicated.

<table>
<thead>
<tr>
<th>Section Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Depends on operating system.</td>
<td>Indicates the class this rule applies to. See: Windows Custom Signatures, Solaris Custom Signatures, Linux Custom Signatures</td>
</tr>
<tr>
<td>Id</td>
<td>4000 - 7999</td>
<td>The unique ID number of the signature. The numbers are the ones available for custom rules.</td>
</tr>
<tr>
<td>level</td>
<td>0</td>
<td>The security level of the signature: 0=Disabled, 1=White, 2=Yellow, 3= Orange, 4= Red</td>
</tr>
<tr>
<td>time</td>
<td>(Include &quot;*&quot; )</td>
<td>This section has this one value only.</td>
</tr>
</tbody>
</table>
Use of Include and Exclude

When you mark a section value as *Include*, the section works on the value indicated; when you mark a section value as *Exclude*, the section works on all values except the one indicated. When you use these keywords, they are enclosed in brackets \{ ... \} and their value in quotes “ ... “.

### Writing Custom Signatures

#### Rule Structure

#### Use of Include and Exclude

When you mark a section value as *Include*, the section works on the value indicated; when you mark a section value as *Exclude*, the section works on all values except the one indicated. When you use these keywords, they are enclosed in brackets \{ ... \} and their value in quotes “ ... “.

<table>
<thead>
<tr>
<th>Section Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_name</td>
<td>{Include/Exclude “user or system account”}</td>
<td>The users to whom the rule applies. Specify particular users or all users. Remarks for Windows: For local user: use &lt;machine name&gt;/&lt;local user name&gt;. For domain user: use &lt;domain name&gt;/&lt;domain user name&gt;. For local system: use Local/System; this is equivalent to NT Authority/System in Windows NT, and &lt;domain&gt;/&lt;machine&gt; in Windows 2000. Some remotely initiated actions do not report the ID of the remote user, but use the local service and its user context instead. You need to plan accordingly when developing rules. When a process occurs in the context of a Null Session, the user and domain are ‘Anonymous’. If a rule applies to all users, use *. On Solaris this section is case sensitive.</td>
</tr>
<tr>
<td>application</td>
<td>{Include/Exclude “path and application name”}</td>
<td>The full path of the process that performed the operation that created the instance. When the operation is remote, the application is the local service/server that handles the operation. Some local operations are handled as if they were remote. For example, for Windows the application name will be the local service/server that handles the operation. If a rule applies to all applications, use *. On Solaris this section is case sensitive.</td>
</tr>
<tr>
<td>directives -c -d</td>
<td>operation type</td>
<td>The operation types are class dependent, and are listed for each class in the later sections. Note that the switches –c and –d must be used.</td>
</tr>
</tbody>
</table>

Note

You can create a signature with multiple rules by simply adding one rule after another. Keep in mind that each rule in the same signature must have the same value for its *id* and *level* sections.
For example, to monitor all the text files in C:\test:

```
files { Include "C:\test\*.txt" }
```

and to monitor all the files except the text files in C:\test:

```
files { Exclude "C:\test\*.txt" }
```

Combine the keywords to exclude values from a set of included values. To monitor all the text files in folder C:\test except file abc.txt:

```
files { Include "C:\test\*.txt" }
files { Exclude "C:\test\acb.txt" }
```

Each time you add the same section with the same keyword, you add an operation. To monitor any text file in folder C:\test whose name starts with the string “abc”:

```
files { Include "C:\test\*.txt" }
files { Include "C:\test\acb*" }
```

## Optional common sections

A rule’s common optional sections and their values include the item below. For optional sections relevant to the class section that is selected, see the class section under Windows, Unix, and Linux Custom Signatures. The keywords Include and Exclude are used for both dependencies and attributes. Include means that the section works on the value indicated, and Exclude means that the section works on all values except the one indicated.

<table>
<thead>
<tr>
<th>Section</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dependencies</td>
<td>-c -d</td>
<td>(Include/Exclude &quot;id of a rule&quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defines dependencies between rules and prevents the triggering of dependent rules. Only switches –c and –d are used.</td>
</tr>
</tbody>
</table>

## Use of the dependencies section

Add the optional section dependencies to prevent a more general rule from being triggering along with a more specific rule. For example, if there is one rule to monitor for a single text file in C:\test

```
files { Include "C:\test\abc.txt" }
```

as well as a rule to monitor all the text files in C:\test

```
files { Include "C:\test\*.txt" }
```

Add the section dependencies to the more specific rule, basically telling the system not to trigger the more general rule if the specific rule is triggered.

```
files { Include "C:\test\abc.txt" }
dependencies –c –d "the general rule"
```

## Section value variables

Wildcards, meta-symbols, and predefined variables can be used as the value in the available sections.
Use of wildcards

You can use wildcards for some of the section values.

<table>
<thead>
<tr>
<th>Character</th>
<th>What is represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (question mark)</td>
<td>A single character.</td>
</tr>
<tr>
<td>* (asterisk)</td>
<td>Multiple characters.</td>
</tr>
<tr>
<td>&amp; (ampersand)</td>
<td>Multiple characters except / and . Use to match the root-level contents of a folder but not any subfolders.</td>
</tr>
<tr>
<td>! (exclamation mark)</td>
<td>Wildcard escape.</td>
</tr>
</tbody>
</table>

Use of environment variables

Use environment variables, the iEnv command with one parameter (the variable name), as a shorthand to specify Windows file and directory path names.

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>What is represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>iEnv SystemRoot</td>
<td>C:<code>\winnt</code>, where C is the drive that contains the Windows System folder. For example:</td>
</tr>
<tr>
<td>iEnv SystemDrive</td>
<td>C:<code>\</code> where C is the drive that contains the Windows System folder. For example:</td>
</tr>
</tbody>
</table>

Use of predefined variables

Host Intrusion Prevention provides pre-defined variables for rule writing. These variables, are preceded by “$,” and are listed below.

Windows IIS Web Server

<table>
<thead>
<tr>
<th>Variable</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIS_BinDir</td>
<td>Directory where inetinfo.exe is located</td>
</tr>
<tr>
<td>IIS_Computer</td>
<td>Machine name that IIS runs on</td>
</tr>
<tr>
<td>IIS_Envelope</td>
<td>Includes all files that IIS is allowed to access</td>
</tr>
<tr>
<td>IIS_Exe_Dirs</td>
<td>Virtual directories that allow file execution including system root and IIS root”</td>
</tr>
<tr>
<td>IIS_Ftp_Dir</td>
<td>FTP site root directories</td>
</tr>
<tr>
<td>IIS_FTP_USR</td>
<td>Local ftp Anonymous user account name</td>
</tr>
<tr>
<td>IIS_FtpLogDir</td>
<td>FTP log files directory</td>
</tr>
<tr>
<td>IIS_IUSR</td>
<td>Local web anonymous user account name</td>
</tr>
</tbody>
</table>
### Writing Custom Signatures

#### Rule Structure

- **IIS_IUSR**: Domain web anonymous user account name
- **IIS_IWAM**: The IIS Web Application Manager user account name
- **IIS_LogFileDir**: Web log files directory
- **IIS_LVirt_Root**: All IIS virtual directories
- **IIS_Processes**: Processes with access rights to IIS resources
- **IIS_Services**: All the services needed for IIS to work properly

### MS SQL Database Server

<table>
<thead>
<tr>
<th>Variable</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSSQL_Allowed_Access_Paths</td>
<td>Directories like \WINNT and \WINNT\System32 that are accessible</td>
</tr>
<tr>
<td>MSSQL_Allowed_Execution_Paths</td>
<td>Directories like \WINNT and \WINNT\System32 that are executable</td>
</tr>
<tr>
<td>MSSQL_Allowed_Modification_Paths</td>
<td>Directories like \WINNT\Temp that are modifiable</td>
</tr>
<tr>
<td>MSSQL_Auxiliary_Services</td>
<td>The auxiliary MS SQL services found on the system</td>
</tr>
<tr>
<td>MSSQL_Core_Services</td>
<td>The core MS SQL services found on the system</td>
</tr>
<tr>
<td>MSSQL_Data_Paths</td>
<td>All other data files associated with MS SQL that may be outside of the MSSQL_DataRoot_Path directory</td>
</tr>
<tr>
<td>MSSQL_DataRoot_Paths</td>
<td>The path to the MS SQL data files for each instance</td>
</tr>
<tr>
<td>MSSQL_Instances</td>
<td>The name of each installed MS SQL instance</td>
</tr>
<tr>
<td>MSSQL_Registry_Paths</td>
<td>All registry locations associated with MS SQL</td>
</tr>
</tbody>
</table>

### Solaris Apache and iPlanet

<table>
<thead>
<tr>
<th>Variable</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAPACHE_Bins</td>
<td>Path to Apache binaries</td>
</tr>
<tr>
<td>UAPACHE_CgiRoots</td>
<td>Path to CGI roots</td>
</tr>
<tr>
<td>UAPACHE_ConfDirs</td>
<td>Directories containing Apache configuration files</td>
</tr>
<tr>
<td>UAPACHE_DocRoots</td>
<td>Path to document roots</td>
</tr>
<tr>
<td>UAPACHE_Logs</td>
<td>Apache log files</td>
</tr>
<tr>
<td>UAPACHE_Logs_dir</td>
<td>Log file directory</td>
</tr>
<tr>
<td>UAPACHE_Roots</td>
<td>Apache web roots</td>
</tr>
<tr>
<td>UAPACHE_Users</td>
<td>Users that Apache runs as</td>
</tr>
<tr>
<td>UAPACHE_VcgiRoots</td>
<td>Path to CGI roots of virtual servers</td>
</tr>
<tr>
<td>UAPACHE_VdocRoots</td>
<td>Virtual document roots</td>
</tr>
<tr>
<td>UAPACHE_Vlogs</td>
<td>Log files of virtual servers</td>
</tr>
<tr>
<td>UAPACHE_Vlogs_dir</td>
<td>Directories for the log files of virtual servers</td>
</tr>
<tr>
<td>UIPLANET_BinDirs</td>
<td>Path to iPlanet binaries</td>
</tr>
<tr>
<td>UIPLANET_CgiDirs</td>
<td>Path to CGI directories</td>
</tr>
<tr>
<td>UIPLANET_DocDirs</td>
<td>Paths to document directories</td>
</tr>
<tr>
<td>UIPLANET_Process</td>
<td>Path to iPlanet ns-httpd binary</td>
</tr>
<tr>
<td>UIPLANET_Roots</td>
<td>Path to iPlanet root</td>
</tr>
</tbody>
</table>
Windows Custom Signatures

This topic describes how to write Windows custom signatures.

Rules in the Windows class Files use double slashes and rules in the Solaris Class UNIX_Files use a single slash.

The class section value depends on the nature of the security issue and on the protection the rules can offer. For Windows these value are available:

<table>
<thead>
<tr>
<th>Class</th>
<th>When to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files</td>
<td>For file or directory operations. See Class Files.</td>
</tr>
<tr>
<td>Isapi</td>
<td>For monitoring request to IIS. See Class Isapi.</td>
</tr>
<tr>
<td>Registry</td>
<td>For Registry key and value operations. See Class Registry.</td>
</tr>
<tr>
<td>Services</td>
<td>For Services operations. See Class Services.</td>
</tr>
</tbody>
</table>

Class Files

The following table lists the possible sections of the class Files.

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Files</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>4000 - 7999</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td>0, 1, 2, 3, 4</td>
<td></td>
</tr>
<tr>
<td>time</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>user-name</td>
<td>user of system account</td>
<td></td>
</tr>
<tr>
<td>application</td>
<td>path + application name</td>
<td></td>
</tr>
<tr>
<td>files</td>
<td>File or folders involved in the operation</td>
<td>See Note 1, 2</td>
</tr>
<tr>
<td>dest_file</td>
<td>Destination file, if the operation involves source and destination files</td>
<td>This section is optional. See Note 1, 2</td>
</tr>
<tr>
<td>directives</td>
<td>files:create</td>
<td>Create file directly, or move file into directory</td>
</tr>
<tr>
<td></td>
<td>files:read</td>
<td>Open the file in Read mode</td>
</tr>
<tr>
<td></td>
<td>files:write</td>
<td>Open the file in Write mode</td>
</tr>
<tr>
<td></td>
<td>files:execute</td>
<td>Execute file (executing a directory means that this directory will become the current directory)</td>
</tr>
<tr>
<td></td>
<td>files:delete</td>
<td>Delete file from a directory, or move it to another directory</td>
</tr>
<tr>
<td></td>
<td>files:rename</td>
<td>Rename a file in the same directory; see Note 2</td>
</tr>
<tr>
<td></td>
<td>files:attribute</td>
<td>Change the file attributes. Monitored attributes are “Read-only”, “Hidden”, “Archive” and “System”. The Windows 2000 only attributes “Index”, “Compress” and “Encrypt” are not monitored.</td>
</tr>
</tbody>
</table>
Note 1
If the section `files` is used, the path to a monitored folder or file can either be the full path or a wildcard. For example, the following are valid path representations:

```plaintext
files { Include "C:\test\abc.txt" }
files { Include "*\test\abc.txt" }
files { Include "*\abc.txt" }
```

If the section `dest_file` is used, the absolute path cannot be used and a wildcard must be present in the beginning of the path to represent the drive. For example, the following are valid path representations:

```plaintext
dest_file { Include "*\test\abc.txt" }
dest_file { Include "*\abc.txt" }
```

Note 2
The directive `files:rename` has a different meaning when combined with section `files` and section `dest_file`.

- When combined with section `files`, it means that renaming of the file in the section `files` is monitored. For example, the following rule monitors renaming of file `C:\test\abc.txt` to any other name:

  ```plaintext
  Rule {
  Class Files
  Id 4001
  level 1
  files { Include "C:\test\abc.txt" }
  time { Include "*" }
  application { Include "*"}
  user_name { Include "*"}
  directives -c -d files:rename
  }
  ```

- Combined with section `dest_file`, it means that no file can be renamed to the file in the section `dest_file`. For example, the following rule monitors renaming of any file to `C:\test\abc.txt`:

  ```plaintext
  Rule {
  Class Files
  Id 4001
  level 1
  dest_file { Include "*\test\abc.txt" }
  time { Include "*" }
  application { Include "*"}
  user_name { Include "*"}
  directives -c -d files:rename
  }
  ```

The section `files` is not mandatory when the section `dest_file` is used. If section `files` is used, both sections `files` and `dest_file` need to match.
Advanced Details

Some or all of the following parameters appear in the Advanced Details tab of security events for the class Files. The values of these parameters can help you understand why a signature is triggered.

<table>
<thead>
<tr>
<th>GUI name</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>files</td>
<td>Name of the file that was accessed</td>
</tr>
<tr>
<td>dest file</td>
<td>Only applicable for renaming files: new name that the file was changed to</td>
</tr>
</tbody>
</table>

The following rule would prevent anybody and any process from creating the file ‘abc.txt’ in the folder C:\test\.

```
Rule {
    Class Files
    Id 4001
    level 4
    files { Include "C:\test\abc.txt" }
    time { Include "***" }
    application { Include "***" }
    user_name { Include "***" }
    directives -c -d files:create
}
```

The various sections of this rule have the following meaning:

- **Class Files**: indicates that this rule relates to file operations class.
- **id 4001**: Assigns the ID 4001 to this rule. If the custom signature had multiple rules, every one of these rules would need to use the same ID.
- **level 4**: Assigns the Security Level ‘high’ to this rule. If the custom signature had multiple rules, every one of these rules would need to use the same level.
- **files { Include "C:\test\abc.txt" }**: Indicates that the rule covers the specific file and path C:\test\abc.txt. If the rule were to cover multiple files, you would add them in this section in different lines. For example when monitoring for files C:\test\abc.txt and C:\test\xyz.txt the section changes to: files { Include "C:\test\abc.txt" "C:\test\xyz.txt" }.
- **time { Include "***" }**: This section is currently not used, but must be included in this way in the rule.
- **application { Include "***" }**: Indicates that this rule is valid for all processes. If you’d want to limit your rule to specific processes, you would spell them out here, complete with their path name.
- **user_name { Include "***" }**: Indicates that this rule is valid for all users (or more precisely, the security context in which a process runs). If you’d want to limit your rule to specific user contexts, you would spell them out here in the form Local/user or Domain/user. See paragraph “Mandatory Common Sections” for details.
- **directives -c -d files:create**: Indicates that this rule covers the creation of a file. The switches –c and –d must always be used in the directives section.
Class Isapi

The following table lists the possible sections of the class *Isapi*.

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td><em>Isapi</em></td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>4000 - 7999</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td>0, 1, 2, 3, 4</td>
<td></td>
</tr>
<tr>
<td>time</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td>user or system account</td>
<td></td>
</tr>
<tr>
<td>application</td>
<td>path + application name</td>
<td></td>
</tr>
<tr>
<td>url</td>
<td>This section is optional. It is section is matched against the url part of an incoming request; see notes 1, 2, 3, 4.</td>
<td></td>
</tr>
<tr>
<td>query</td>
<td>This section is optional. It is matched against the query part of an incoming request; see notes 1, 2, 3, 4.</td>
<td></td>
</tr>
<tr>
<td>method</td>
<td>“GET”, “POST”, “INDEX” and all other allowed http methods</td>
<td>This section is optional. See note 4.</td>
</tr>
<tr>
<td>directives</td>
<td>-c -d isapi:request</td>
<td></td>
</tr>
</tbody>
</table>

**Note 1**

An incoming http request can be represented as: `http://www.myserver.com/ {url}?{query}`. In this document, we refer to `{url}` as the “url” part of the http request and `{query}` as the “query” part of the http request. Using this naming convention, we can say that the section “url” will be matched against `{url}` and the section “query” will be matched against `{query}`.

For example the following rule would be triggered if the http request `http://www.myserver.com/search/abc.exe?subject=wildlife&environment=ocean` would be received by IIS:

```
Rule {
    Class Isapi
    Id 4001
    level 1
    url ( Include "*abc*" )
    time ( Include "***" )
    application ( Include "***" )
    user_name ( Include "***" )
    directives -c -d isapi:request
}
```

This rule is triggered because `{url}`=/search/abc.exe, which matches the value of the section “url” (i.e. abc).

**Note 2**

Before matching is done, sections “url” and “query” are decoded and normalized so that requests cannot be filled with encoding or escape sequences.
Note 3
A maximum length restriction can be defined for the sections “url” and “query”. By adding “;number-of-chars” to the value of these sections, the rule can only match if the (url) or (query) have more characters than “number-of-chars”. For example, the following rule will match if the url part of the request contains “abc” and the url part of the request has over 500 characters:

Rule {
    Class Isapi
    Id 4001
    level 1
    url { Include "*abc*;500" }
    time { Include "*" }
    application { Include "*" }
    user_name { Include "*" }
    directives -c -d isapi:request
}

Note 4
A rule needs to contain at least one of the optional sections url, query, method.

Advanced Details
Some or all of the following parameters appear in the Advanced Details tab of security events for the class /isapi. The values of these parameters can help you understand why a signature is triggered.

<table>
<thead>
<tr>
<th>GUI name</th>
<th>explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>Decoded and normalized location part of an incoming HTTP request (the part before the '?').</td>
</tr>
<tr>
<td>query</td>
<td>Decoded and normalized query part of an incoming HTTP request (the part after the first '?').</td>
</tr>
<tr>
<td>web server type</td>
<td>Type and version of the Web server application used.</td>
</tr>
<tr>
<td>method</td>
<td>Method of the incoming HTTP request (such as Get, Put, Post, Query, etc.).</td>
</tr>
<tr>
<td>local file</td>
<td>Physical name of the file that is retrieved or attempted to be retrieved by the request. Decoded and normalized under IIS.</td>
</tr>
<tr>
<td>raw url</td>
<td>“Raw” (undecoded and not normalized) Request Line of the incoming HTTP request. Request Line is “&lt;method&gt; &lt;location[?query]&gt; &lt;http version&gt; CRLF”.</td>
</tr>
<tr>
<td>user</td>
<td>User name of the client making the request; only available if the request is authenticated.</td>
</tr>
<tr>
<td>source</td>
<td>Client name or IP address of the computer where the HTTP request originated.</td>
</tr>
<tr>
<td>server</td>
<td>Information about the Web server where the event is created (that’s the machine where the client is installed) in the manner &lt;host name&gt;:&lt;IP address&gt;:&lt;port&gt;. The host name is the host variable from the HTTP header; it is left blank if not available.</td>
</tr>
<tr>
<td>content len</td>
<td>Number of bytes in the body of the message part of the query.</td>
</tr>
</tbody>
</table>

The following rule would prevent a request to the web server that has “subject” in the query part of the http request:
Rule {
    Class Isapi
    Id 4001
    level 4
    query { Include "*subject*" }
    method { Include "GET" }
    time { Include "*" }
    application { Include "*" }
    user_name { Include "*" }
    directives -c -d isapi:request
}

For example, the GET request `http://www.myserver.com/test/abc.exe?subject=wildlife&environment=ocean` would be prevented by this rule.

The various sections of this rule have the following meaning:

- **Class Isapi**: indicates that this rule relates to the Isapi operations class.
- **Id 4001**: Assigns the ID 4001 to this rule. If the custom signature had multiple rules, every one of these rules would need to use the same ID.
- **level 4**: Assigns the Security Level ‘high’ to this rule. If the custom signature had multiple rules, every one of these rules would need to use the same level.
- **query { Include "*subject*" }**: Indicates that the rule matches any (GET) request that contains the string “subject” in the query part of the http request. If the rule were to cover multiple query parts files, you would add them in this section in different lines.
- **method { Include "GET" }**: Indicates that the rule can only match GET requests
- **time { Include "*" }**: This section is currently not used, but must be included in this way in the rule.
- **application { Include "*" }**: Indicates that this rule is valid for all processes. If you’d want to limit your rule to specific processes, you would spell them out here, complete with their path name.
- **user_name { Include "*" }**: Indicates that this rule is valid for all users (or more precisely, the security context in which a process runs). If you’d want to limit your rule to specific user contexts, you would spell them out here in the form Local/user or Domain/user. See paragraph “Mandatory Common Sections” for details.
- **directives -c -d isapi:request**: Indicates that this rule covers an http request. The switches –c and –d must always be used in the directives section.
Class Registry

The following table lists the possible sections of the class Registry.

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Registry</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>4000 - 7999</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td>0, 1, 2, 3, 4</td>
<td></td>
</tr>
<tr>
<td>time</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td>user or system account</td>
<td></td>
</tr>
<tr>
<td>application</td>
<td>path + application name</td>
<td></td>
</tr>
<tr>
<td>keys or values</td>
<td>registry key or value</td>
<td>See Note 1</td>
</tr>
<tr>
<td>old data</td>
<td>Previous data of the value</td>
<td>This section is optional. It is only for &lt;directive&gt; Modify; see Note 2.</td>
</tr>
<tr>
<td>new data</td>
<td>New data of the value</td>
<td>This section is optional. It is only for &lt;directive&gt; Modify or Create; see Note 2.</td>
</tr>
<tr>
<td>directives -c</td>
<td>registry:delete</td>
<td>Deletion of a registry key/value</td>
</tr>
<tr>
<td></td>
<td>registry:modify</td>
<td>Modification of the content of a registry value or the modification of the info of a registry key</td>
</tr>
<tr>
<td></td>
<td>registry:permissions</td>
<td>Modification of the permissions of a registry key.</td>
</tr>
<tr>
<td></td>
<td>registry:read</td>
<td>Obtaining registry key information (number of subkeys, etc), or, getting the content of a registry value.</td>
</tr>
<tr>
<td></td>
<td>registry:enumerate</td>
<td>Enumeration of a registry key, that is, getting the list of all the key’s subkeys and values.</td>
</tr>
</tbody>
</table>

Note 1
HKEY_LOCAL_MACHINE in a registry path is replaced by REGISTRY_MACHINE\ and CurrentControlSet is replaced by ControlSet. For example the registry value “abc” under registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa is represented as \REGISTRY\MACHINE\SYSTEM\ControlSet\Control\Lsa\abc.

Note 2
The data of the sections old data and new data must be in hexadecimal. For example, the data ‘def’ of registry value “\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\abc” must be represented as old_data { Include “%64%65%66”}.

Note 3
Not all registry directives are universally supported. The following is a list of which registry directives are supported on which platforms:

<table>
<thead>
<tr>
<th>Registry directive</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>registry:create</td>
<td>Win2k, Win XP x32, Win XP x64, Win 2003 x32 (before SP1), Win 2003 x32 (SP1 and up), Win 2003 x32, and Vista x64. Applies to keys and values.</td>
</tr>
<tr>
<td>registry:read</td>
<td>Win2k, Win XP x32, Win XP x64, Win 2003 x32 (before SP1), Win 2003 x32 (SP1 and higher), Win 2003 x32, Vista x64, and Vista x64. Applies to keys and values.</td>
</tr>
<tr>
<td>registry:delete</td>
<td>Win2k, Win XP x32, Win XP x64, Win 2003 x32 (before SP1), Win 2003 x32 (SP1 and higher), Win 2003 x32, Vista x64, and Vista x64. Applies to keys and values.</td>
</tr>
</tbody>
</table>
Advanced Details

Some or all of the following parameters appear in the Advanced Details tab of security events for the class Registry. The values of these parameters can help you understand why a signature is triggered.

<table>
<thead>
<tr>
<th>GUI Name</th>
<th>explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Key</td>
<td>Name of the registry key affected, including the path name. The prefix \REGISTRY\MACHINE\ stands for HKEY_LOCAL_MACHINE\ and \REGISTRY\CURRENT_USER\ stands for HKEY_USER.</td>
</tr>
<tr>
<td>Registry Value(s)</td>
<td>Name of the registry value concatenated with the full name of its key.</td>
</tr>
</tbody>
</table>

**registry:modify**

- Win2k, Win XP x32, Win XP x64, Win 2003 x32 (before SP1), Win 2003 x32 (SP1 and higher), Win 2003 x64, Vista x32, and Vista x64.
- Applies to values only.

**registry:permissions**

- Win2k, Win XP x32, Win 2003 x32 (before SP1), and Vista x32.
- Applies only to setting permissions on a key.

**registry:enumerate**

- Win2k, Win XP x32, Win XP x64, Win 2003 x32 (before SP1), Win 2003 x32 (SP1 and higher), Win 2003 x64, Vista x32, and Vista x64.
- Applies to keys only.

**registry:monitor**

- Win2k, Win XP x32, Win 2003 x32 (before SP1), and Vista x32.
- Applies only to RegNotifyChangeKeyValue advapi32.dll API.

**registry:restore**

- Win2k, Win XP x32, Win 2003 x32 (before SP1), and Vista x32.
- Applies only to RegRestoreKey advapi32.dll API.

**registry:replace**

- Win2k, Win XP x32, Win 2003 x32 (before SP1), and Vista x32.
- Applies only to RegReplaceKey advapi32.dll API.

**registry:load**

- Win2k, Win XP x32, Win 2003 x32 (before SP1), and Vista x32.
- Applies only to RegLoadKey advapi32.dll API.

**registry:open_existing_key**

- Win2k, Win XP x32, Win XP x64, Win 2003 x32 (before SP1), Win 2003 x32 (SP1 and higher), Win 2003 x64, Vista x32, and Vista x64.
- Applies to keys only.

**registry:rename**

- Vista x32 and Vista x64.
- Applies to keys only.

Example

The following rule would prevent anybody and any process from deleting the registry value “abc” under registry key “\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa”

```
Rule {
    Class Registry
    Id 4001
    level 4
```
The various sections of this rule have the following meaning:

- **Class Registry**: indicates that this rule relates to requests sent to IIS.

- **Id 4001**: Assigns the ID 4001 to this rule. If the custom signature had multiple rules, every one of these rules would need to use the same ID.

- **level 4**: Assigns the Security Level ‘high’ to this rule. If the custom signature had multiple rules, every one of these rules would need to use the same level.

- **values**: Indicates that the rule monitors registry value abc under registry key `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`. If the rule were to cover multiple values, you would add them in this section in different lines.

- **time**: This section is currently not used, but must be included in this way in the rule.

- **application**: Indicates that this rule is valid for all processes. If you’d want to limit your rule to specific processes, you would spell them out here, complete with their path name.

- **user_name**: Indicates that this rule is valid for all users (or more precisely, the security context in which a process runs). If you’d want to limit your rule to specific user contexts, you would spell them out here in the form Local/user or Domain/user. See paragraph “Mandatory Common Sections” for details.

- **directives -c -d registry:delete**: Indicates that this rule covers deletion of a registry key or value. The switches –c and –d must always be used in the directives section.

### Class Services

The following table lists the possible sections of the class **Services**.

<table>
<thead>
<tr>
<th>section</th>
<th>values</th>
<th>meaning/remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Services</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>4000 - 7999</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td>0, 1, 2, 3, 4</td>
<td></td>
</tr>
<tr>
<td>time</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td>user or system account</td>
<td></td>
</tr>
<tr>
<td>application</td>
<td>path + application name</td>
<td></td>
</tr>
<tr>
<td>services</td>
<td>name of the service which is the subject of the operation creating the instance</td>
<td>either section “services” or “display_names” must be used; the name of a service is found in the registry under HKLM\SYSTEM\CurrentControlSet\Services; see Note 1</td>
</tr>
<tr>
<td>display_names</td>
<td>display name of the service</td>
<td>this name is shown in Services Control Panel; see Note 1</td>
</tr>
</tbody>
</table>
For directive -c -d services:delete,
Deletion of a Service

For directive -c -d services:create,
Creation of a Service

For directive -c -d services:start,
Giving a start command to a service

For directive -c -d services:stop,
Giving a stop command to a service

For directive -c -d services:pause,
Giving a pause command to a service

For directive -c -d services:continue,
Giving a continue command to a service

For directive -c -d services:startup,
Modifying the startup mode of a service

For directive -c -d services:profile_enable,
Enabling a Hardware profile

For directive -c -d services:profile_disable,
Disabling a Hardware profile

For directive -c -d services:logon,
Modifying the logon information of a service

**Note 1**
The section `service` must contain the name of the service of the corresponding registry key under HKLM_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.

The section `display_names` must contain the display name of the service, the name shown in the Services Control Panel, which is found in registry value HKLM_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<name-of-service>\DisplayName.

**Advanced Details**
Some or all of the following parameters appear in the Advanced Details tab of security events for the class `Services`. The values of these parameters can help you understand why a signature is triggered.

<table>
<thead>
<tr>
<th>GUI Name</th>
<th>Explanation</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>display names</td>
<td>Name of the Windows service as it is displayed in the Services Manager control panel.</td>
<td></td>
</tr>
<tr>
<td>services</td>
<td>System name of the Windows service (shown in HKLM\CurrentControlSet\Services); this may be different from the name displayed in the Services Manager control panel.</td>
<td></td>
</tr>
<tr>
<td>params</td>
<td>Only applicable for starting a service: parameters passed to the service upon activation.</td>
<td></td>
</tr>
<tr>
<td>old startup</td>
<td>Only applicable for creating or changing the startup mode of a service: indicates the startup mode before it was changed or attempted to be changed.</td>
<td>Boot, System, Automatic, Manual, Disabled</td>
</tr>
</tbody>
</table>
The following rule would prevent deactivation of the Alerter service.

```
Rule {
  Class Services
  Id 4001
  level 4
  Service { Include "Alerter" }
  time { Include "*" }
  application { Include "*" }
  user_name { Include "*" }
  directives -c -d service:stop
}
```

The various sections of this rule have the following meaning:

- **Class Services**: indicates that this rule relates to file operations class.

- **Id 4001**: Assigns the ID 4001 to this rule. If the custom signature had multiple rules, every one of these rules would need to use the same ID.

- **level 4**: Assigns the Security Level ‘high’ to this rule. If the custom signature had multiple rules, every one of these rules would need to use the same level.

- **Service { Include “Alerter” }**: Indicates that the rule covers the service with name “Alerter”. If the rule were to cover multiple services, you would add them in this section in different lines.

- **time { Include “*” }**: This section is currently not used, but must be included in this way in the rule.

- **application { Include “*” }**: Indicates that this rule is valid for all processes. If you’d want to limit your rule to specific processes, you would spell them out here, complete with their path name.

- **user_name { Include “*” }**: Indicates that this rule is valid for all users (or more precisely, the security context in which a process runs). If you’d want to limit your rule to specific user contexts, you would spell them out here in the form Local/user or Domain/user. See paragraph “Mandatory Common Sections” for details.

- **directives -c -d service:stop**: Indicates that this rule covers deactivation of a service. The switches –c and –d must always be used in the directives section.

---

### GUI Name | Explanation | Possible Values
--- | --- | ---
new startup | Only applicable for changing the startup mode of a service: indicates the startup mode that a service has after it was changed, or that it would have if the change went through. | Boot, System, Automatic, Manual, Disabled |
logon | Only applicable for changes in the logon mode of a service: logon information (system or user account) used by the service. |
Solaris Custom Signatures

This topic describes how to write Solaris custom signatures.

Rules in the Windows class Files use double slashes and rules in the Solaris Class UNIX_Files use a single slash.

The class of the signature depends on the nature of the security issue and on the protection the rules can offer. The table below lists the available Solaris classes:

<table>
<thead>
<tr>
<th>class</th>
<th>meaning / remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIX_file</td>
<td>Used for file or directory operations. See Class UNIX_file.</td>
</tr>
<tr>
<td>UNIX_apache</td>
<td>Used for http operations. See Class UNIX_apache.</td>
</tr>
</tbody>
</table>

Class UNIX_file

The following table lists the possible sections of the class Files.

<table>
<thead>
<tr>
<th>section</th>
<th>values</th>
<th>meaning/remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>UNIX_file</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>4000 - 7999</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td>0, 1, 2, 3, 4</td>
<td></td>
</tr>
<tr>
<td>time</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td>user or system account</td>
<td></td>
</tr>
<tr>
<td>application</td>
<td>user or system account path + application name</td>
<td></td>
</tr>
<tr>
<td>files</td>
<td>source file(s)</td>
<td>Files to look for. This is optional if section source is used; see Note 1.</td>
</tr>
<tr>
<td>source</td>
<td>target file names</td>
<td>This is optional. See Note 1.</td>
</tr>
<tr>
<td>file permission</td>
<td>list of permissions of source file names</td>
<td>This is optional. See Note 2.</td>
</tr>
<tr>
<td>new permission</td>
<td>permission mode of newly created file or modified permission</td>
<td>This is optional. See Note 2.</td>
</tr>
<tr>
<td>directives</td>
<td>unixfile:symlink</td>
<td>Creating a symbolic link.</td>
</tr>
<tr>
<td></td>
<td>unixfile:link</td>
<td>Creating a hard link. See Note 3.</td>
</tr>
<tr>
<td></td>
<td>unixfile:read</td>
<td>Opening the file in Read mode.</td>
</tr>
<tr>
<td></td>
<td>unixfile:write</td>
<td>Opening the file in Write mode.</td>
</tr>
<tr>
<td></td>
<td>unixfile:unlink</td>
<td>Deleting a file from a directory or deleting the directory.</td>
</tr>
<tr>
<td></td>
<td>unixfile:rename</td>
<td>Renaming the file. See Note 4.</td>
</tr>
<tr>
<td></td>
<td>unixfile:chmod</td>
<td>Changing the permissions on the directory or file.</td>
</tr>
<tr>
<td></td>
<td>unixfile:chown</td>
<td>Changing the file ownership of the directory or file.</td>
</tr>
<tr>
<td></td>
<td>unixfile:create</td>
<td>Creating a file.</td>
</tr>
<tr>
<td></td>
<td>unixfile:mkdir</td>
<td>Creating a directory.</td>
</tr>
<tr>
<td></td>
<td>unixfile:rmdir</td>
<td>Removing a directory.</td>
</tr>
<tr>
<td></td>
<td>unixfile:chdir</td>
<td>Changing the working directory</td>
</tr>
</tbody>
</table>
Note 1
Relevant (X) directives per section:

<table>
<thead>
<tr>
<th>directive</th>
<th>file</th>
<th>source</th>
<th>file permission</th>
<th>new permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>symlink</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>read</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>write</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>unlink</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>rename</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>chmod</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>chown</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>create</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mkdir</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>rmdir</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>chdir</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Note 2
The value of the sections file permissions and new permissions corresponds to the Access Control List (acl). These can have values of “SUID” or “SGID” only.

Note 3
The directive Unixfile:link has a different meaning when combined with section files and section source:

- Combined with section files, it means that creating a link to the file in the section files is monitored.
- Combined with section source, it means that no link can be created with the name as specified in the section source.

Note 4
The directive Unixfile:rename has a different meaning when combined with section files and section source:

- Combined with section files, it means that renaming of the file in the section files is monitored.
- Combined with section source, it means that no file can be renamed to the file in the section source.
Advanced Details

Some or all of the following parameters appear in the Advanced Details tab of security events for the class UNIX_Files. The values of these parameters can help you understand why a signature is triggered.

<table>
<thead>
<tr>
<th>GUI name</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>files</td>
<td>Names of the file that was accessed or attempted to be accessed.</td>
</tr>
<tr>
<td>source</td>
<td>Only applicable when operation is the creation of a symbolic link between files: name of the new link; or when operation is the renaming of a file: new name of the file.</td>
</tr>
<tr>
<td>file permission</td>
<td>Permissions of the file.</td>
</tr>
<tr>
<td>source permission</td>
<td>Only applicable when operation is the creation of a symbolic link between files: permissions of the target file (the file to which the link points).</td>
</tr>
<tr>
<td>new permission</td>
<td>Only applicable when creating a new file or when doing a chmod operation: permissions of the new file.</td>
</tr>
</tbody>
</table>

Class UNIX_apache

The following table lists the possible sections of the class Unix_apache. This class can be used for the Apache, iPlanet and Netscape Enterprise Web Servers.

<table>
<thead>
<tr>
<th>section</th>
<th>values</th>
<th>meaning/remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>UNIX_apache</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>4000 – 7999</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td>0, 1, 2, 3, 4</td>
<td></td>
</tr>
<tr>
<td>time</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td>user or system account</td>
<td></td>
</tr>
<tr>
<td>application</td>
<td>path + application name</td>
<td></td>
</tr>
<tr>
<td>url</td>
<td>This section is optional. It is matched against the url part of an incoming request; see Notes 1, 2, 3, 4.</td>
<td></td>
</tr>
<tr>
<td>query</td>
<td>This section is optional. It is matched against the query part of an incoming request; see Notes 1, 2, 3, 4.</td>
<td></td>
</tr>
<tr>
<td>method</td>
<td>“GET”, “POST”, “INDEX” and the other http methods</td>
<td>This section is optional. See Note 4.</td>
</tr>
<tr>
<td>directives</td>
<td>-c -d apacherequest</td>
<td></td>
</tr>
</tbody>
</table>

Note 1
An incoming http request can be represented as: http://www.myserver.com/{url}?{query}. In this document, we refer to {url} as the “url” part of the http request and {query} as the “query” part of the http request. Using this naming convention, we can say that the section “url” will be matched against {url} and the section “query” will be matched against {query}. 
For example the following rule would be triggered if the http request http://www.myserver.com/search/abc.exe?subject=wildlife&environment=ocean would be received by IIS:

```
Rule {
    Class UNIX_apache
    Id 4001
    level 1
    url { Include "*abc*" }
    time { Include "*" }
    application { Include "*" }
    user_name { Include "*" }
    directives -c -d apache:request
}
```

This rule is triggered because {url}=/search/abc.exe, which matches the value of the section “url” (namely. abc).

**Note 2**
Before matching is done, sections “url” and “query” are decoded and normalized so that requests cannot be filled with encoding or escape sequences.

**Note 3**
A maximum length restriction can be defined for the sections “url” and “query”. By adding ";number-of-chars" to the value of these sections, the rule can only match if the (url) or (query) have more characters than “number-of-chars”. For example, the following rule will match if the url part of the request contains “abc” and the url part of the request has over 500 characters:

```
Rule {
    Class UNIX_Apache
    Id 4001
    level 1
    url { Include "*abc*:500" }
    time { Include "*" }
    application { Include "*" }
    user_name { Include "*" }
    directives -c -d apache:request
}
```

**Note 4**
A rule needs to contain at least one of the optional sections url, query, method.
Linux Custom Signatures

This topic describes how to write Linux custom signatures.

The class of the signature depends on the nature of the security issue and on the protection the rules offer. The table below lists the available Linux classes:

<table>
<thead>
<tr>
<th>class</th>
<th>meaning / remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIX_file</td>
<td>Used for file or directory operations. See Class UNIX_file.</td>
</tr>
</tbody>
</table>

Class UNIX_file

The following table lists the possible sections of the class Files.

<table>
<thead>
<tr>
<th>section</th>
<th>values</th>
<th>meaning/remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>UNIX_file</td>
<td></td>
</tr>
<tr>
<td>id</td>
<td>4000 - 7999</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td>0, 1, 2, 3, 4</td>
<td></td>
</tr>
<tr>
<td>time</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td>user or system account</td>
<td></td>
</tr>
<tr>
<td>application</td>
<td>user or system account path + application name</td>
<td></td>
</tr>
<tr>
<td>files</td>
<td>source file(s)</td>
<td>Files to look for. This is optional if section source is used; see Note 1.</td>
</tr>
<tr>
<td>directives</td>
<td>unixfile:link</td>
<td>Creating hard links.</td>
</tr>
<tr>
<td></td>
<td>unixfile:read</td>
<td>Opening the file in Read mode.</td>
</tr>
<tr>
<td></td>
<td>unixfile:write</td>
<td>Opening the file in Write mode.</td>
</tr>
<tr>
<td></td>
<td>unixfile:unlink</td>
<td>Deleting a file from a directory or deleting the directory.</td>
</tr>
<tr>
<td></td>
<td>unixfile:rename</td>
<td>Renaming the file.</td>
</tr>
<tr>
<td></td>
<td>unixfile:setattr</td>
<td>Changing the permissions and file ownership of the directory or file.</td>
</tr>
<tr>
<td></td>
<td>unixfile:create</td>
<td>Creating a file.</td>
</tr>
<tr>
<td></td>
<td>unixfile:mkdir</td>
<td>Creating a directory.</td>
</tr>
<tr>
<td></td>
<td>unixfile:rmdir</td>
<td>Removing a directory.</td>
</tr>
</tbody>
</table>
Summary of parameters and directives

The following is a summary of parameters and directives according to type.

List of parameters according to type

<table>
<thead>
<tr>
<th>Type</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files, Windows Platform</td>
<td>Application, Destination File, Files, User Name</td>
</tr>
<tr>
<td>HTTP, Windows Platform</td>
<td>Application, Method, Query, URL, User Name</td>
</tr>
<tr>
<td>Files, Solaris and Linux Platform</td>
<td>Application, Source, Files, User Name</td>
</tr>
<tr>
<td>Registry</td>
<td>Application, Registry Key, User Name, Registry Value</td>
</tr>
<tr>
<td>Services</td>
<td>Application, Display Name, Service, User Name</td>
</tr>
<tr>
<td>Apache, Solaris Platform</td>
<td>Application, URL, Query, Method, User Name</td>
</tr>
</tbody>
</table>

List of directives according to type

<table>
<thead>
<tr>
<th>Type</th>
<th>Directives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files, Windows Platform</td>
<td>create, read, write, execute, delete, rename, attribute</td>
</tr>
<tr>
<td>HTTP, Windows Platform</td>
<td>request</td>
</tr>
<tr>
<td>Files, Solaris Platform</td>
<td>create, symlink, link, chown, chmod, write, rmdir, chdir, read, unlink, mkdir, rename</td>
</tr>
<tr>
<td>Files, Linux Platform</td>
<td>create, link, setattr, write, rmdir, read, unlink, mkdir, rename</td>
</tr>
<tr>
<td>Registry</td>
<td>create, read, delete, modify, permissions, enumerate, monitor, restore, replace, load</td>
</tr>
<tr>
<td>Services</td>
<td>start, stop, pause, continue, startup, profile_enable, profile_disable, logon, create, delete</td>
</tr>
<tr>
<td>Apache, Solaris Platform</td>
<td>request</td>
</tr>
</tbody>
</table>
Frequently Asked Questions

This section answers some practical questions that can arise when using Host Intrusion Prevention 7.0.

- **What is a policy?**
- **What is the McAfee Default policy?**
- **What happens to the nodes of the Directory under a node where I assigned a new policy?**
- **How are the nodes to which a policy is applied affected when the policy is modified?**
- **Why isn’t the new Host Intrusion Prevention policy I assigned being enforced?**
- **Can I delegate administration of IPS and firewall policies to different administrators in different geographic locations?**
- **Can I apply the same security configuration to different systems?**
- **Can I view or edit the policies applicable to a specific node or client?**
- **How do I view all available policies and the nodes they are assigned to?**
- **How do I view IPS events triggered by clients?**
- **How do I create an exception based on an IPS Event?**
- **How do I refine IPS Rules policies with automated tuning mechanisms?**
- **How do I create custom signatures for an IPS Policy?**
- **How do I reorganize existing exceptions and custom signatures into a new policy?**
- **How do I find existing policies that match a given profile?**

**What is a policy?**
A policy is a customized subset of product settings corresponding to a policy category. You can create, modify, or delete as many named policies as needed for each policy category.

**What is the McAfee Default policy?**
Upon installation, each policy category contains at least one named policy, McAfee Default. The McAfee Default policies cannot be edited, renamed, or deleted.
What happens to the nodes of the Directory under a node where I assigned a new policy?
All nodes with inheritance enabled for the specific policy category inherit the policy applied to a parent node.

How are the nodes to which a policy is applied affected when the policy is modified?
All nodes to which a policy is applied receive any modification made to the policy at the next agent-server communication or by running an agent wake-up call. The policy is then enforced at each policy enforcement interval.

Why isn't the new Host Intrusion Prevention policy I assigned being enforced?
New policy assignments are not enforced until the next agent-server communication or by running an agent wake-up call after the assignment has been made. Also, if the client UI is unlocked with a password, no new policy assignments are enforced.

Can I delegate administration of IPS and firewall policies to different administrators in different geographic locations?
Yes. Host Intrusion Prevention enables you to delegate responsibility for all or individual product features such as IPS or Firewall. Finer granularity of roles within the feature, for example, client management and exception creation, is not supported.

Assign user rights at the site level, one level below the root directory, and the rights are inherited by all nodes under that site. Explicit user permission on nodes below the site level is not supported. To delegate administration by geographic location, designate a geographic location at a site node, and then apply the appropriate user rights.

Can I apply the same security configuration to different systems?
The console tree organizes nodes hierarchically. You assign policies at nodes, so the site-level nodes typically denote profile-based groupings, such as All Servers, All Desktops, IIS Servers, or SQL Servers. This group pattern can be replicated under each site node.

ePolicy Orchestrator enables the creation of policies that are independent of any node, yet shareable across all nodes. When you assign a policy to a node, it is automatically inherited by its children, unless overridden by another policy. You can create a policy matching each profile, such as IIS Server Policy, and apply it to each of the corresponding node groups, such as IIS Servers.

Place a computer with a new Host Intrusion Prevention client in the appropriate profile group to be assigned the correct security policies. If this is not possible, you can set the policy for an individual client by modifying the policies at the individual node level. Most inherited policies can be overridden, unless a policy has forced inheritance assigned.

If the ePolicy Orchestrator tree nodes have already been organized to support products whose organization does not suit Host Intrusion Prevention, it may be difficult to reorganize the tree. Because reorganization might break existing policy assignments, knowledge of and permissions over all applicable products is required.
Can I view or edit the policies applicable to a specific node or client?
Yes. Host Intrusion Prevention policies have specific categories, such as IPS Rules and IPS Protection, each providing specific settings. Under each Host Intrusion Prevention features, you can see the categories for the selected node on the Policies tab. Each category displays the name of its assigned policy (or policies). Most categories, like IPS Protection, display a single policy, while the IPS Rules and Trusted Applications categories display one or more policy instances. To view the details of each policy, click the name of the policy.

How do I view all available policies and the nodes they are assigned to?
The ePolicy Orchestrator tree has a Policy Catalog node, which displays the list of all policies in each category with a count of their assignments. Click the count value to display a list of all nodes where the policy is directly assigned. The count does not include nodes where the policy has been inherited.

How do I view IPS events triggered by clients?
ePolicy Orchestrator does not have its own event viewer, so events are handled by the Host Intrusion Prevention IPS Events tab within the IPS Rules policy. To view the list of events associated with a selected node, click the Policies tab, and then click the IPS Events link. The IPS Events tab displays the combined set of IPS events generated by clients under the selected node for a specific number of days. The view automatically refreshes as new events are triggered, and offers these operations:

- Sorting events on a single attribute and filtering on various attributes.
- Viewing event details.
- Marking events as read or hidden, and displaying the events in combinations of read, unread, and hidden events.
- Creating exceptions or trusted application based on events.

How do I create an exception based on an IPS Event?
Select a single event in the IPS Events tab and click Create Exception. A pre-filled New Exception dialog box based on the original event appears. A tab in the New Exception dialog box displays a list of target IPS Rules Policy instances into which you will place this Exception upon creation.

The new exception can only be placed in an existing policy that can be edited.

Apply an exception to a specific client or to multiple clients - the target policy for an exception can be a specific client policy, or one that fits a common profile. However, all policies are shareable by default, and appear in the assignment list for each node. It is recommended that a small number of policies be carefully created and maintained, so that they can collectively satisfy the needs of all clients.

Instead of creating a new exception, you can search for and edit an existing exception with similar attributes in an existing policy with the Search Related Exceptions functionality.

How do I refine IPS Rules policies with automated tuning mechanisms?
Host Intrusion Prevention provides an adaptive mode option, which allows clients to automatically and silently create client rules that allow blocked but non malicious activity to occur. After clients have been in adaptive mode for a time, an administrator can do the following:
- View the list of client rules created on a set of clients having a similar profile, and create a new policy based on the information. This new policy can then be applied to a larger set of clients with the same profile.

- Determine that specific client rules represent security violations and block these rules as part of the IPS Rules policy.

- View an aggregated list of exceptions to obtain an idea of the prevalence of the same operation on different clients with the same profile.

- Move a client exception rule to the list of policy exceptions.

- Search existing policy exceptions to find an exception similar to a client exception that can be edited.

**How do I create custom signatures for an IPS Policy?**

Custom signatures are part of the IPS Rules policy and can be created to meet a profile’s specific security needs. A custom signature wizard is available for simple signatures, while custom signature Standard and Expert modes are available for advanced users.

**How do I reorganize existing exceptions and custom signatures into a new policy?**

As administrator you have identified some false-positive on a few clients and created exceptions for them. Given that these false-positive events seemed isolated, you initially placed these into various policies. Taking a second look at the exceptions, you see a new pattern – one that can be isolated into its own policy.

To reorganize these exceptions into a new policy, create a new IPS Rules policy and add it to the list of IPS Rules policy for the appropriate node. View the list of all exceptions from the various policies assigned to that node. Select one or more of the appropriate exceptions, and move them to the new policy.

This new policy can then be applied to other clients that fit the newly identified profile, either individually or as a group.

**How do I find existing policies that match a given profile?**

Typically, an organization will have multiple IPS Rules policies, one per client profile, such as IIS Server and SQL Server. Given that multiple administrators typically manage different parts of the system, sometimes working in different shifts, it is essential to have a small number well-maintained policies. This will help you as an administrator to quickly understand the current organization of policies and find what you are searching for.

You can use the IPS Exception Search to search for exceptions based on their attributes, and locate their parent policy in the process. The search allows you to:

- Find policies that contain an exception for an application.

- Find exceptions created for a signature.

- Find policies that contain exceptions matching one or more attributes of a false positive event.
agent host
See client computer.

agent wakeup call
The ability to initiate agent-to-server communication from the serverside.
See also SuperAgent wakeup call.

agent-to-server communication
Any communication that occurs between ePolicy Orchestrator agents and the ePolicy Orchestrator server where agents and server exchange data. Typically, the agent initiates all communication with the server.

agent-to-server communications interval (ASCI)
The time period between predefined agent-to-server communication.

aggregated view
A view of identical items grouped into a single entity.

alert
See also event.

ASCI
See agent-to-server communication interval.

attack
An attempted breach of system security. Attacks range in severity from low, someone having an unauthorized view of data on your system, to high, someone destroying or stealing data or shutting down your system.

Adaptive mode
The protection setting for a HIP client where rules are learned and added automatically without user intervention. This mode is applicable to IPS, firewall, and application blocking rules.

application blocking
A feature that allows or blocks certain applications. Two types of application blocking are available: application creation and application hooking.

back orifice
A remote administration tool that can provide unwanted access to and control of a computer by way of its Internet link. It runs on Windows 95, Windows 98, and Windows NT.

backdoor
A planned security breach in an application that can allow unauthorized access to data.
behavioral rule
IPS rule that defines a profile of legitimate activity. Activity that does not match the profile triggers an event.
See also signature.

blocked host
A specific host from which Host Intrusion Prevention allows you to block communication; it attempts to trace the source of the packets received from the blocked host.

branch
Locations on the master repository that allow you to store and distribute different versions of selected updates.
See also selective updating.

brute force
A hacking method used to find passwords or encryption keys by trying every possible combination of characters until the code is broken.

buffer overflow attack
The method of overfilling a software buffer to insert and execute some other code with elevated privileges, often a shell from which further commands can be issued.

camping out
A hacking technique of breaking into a system, and then finding a safe place from which to monitor the system, store information, or re-enter the system at a later time.

category
A division of an Host Intrusion Prevention feature to which you can assign a policy. For example, the IPS feature includes an IPS Options, IPS Protection, and IPS Rules category.

check in, checking in
The process of adding files to the master repository.

client computer
A computer on which the ePolicy Orchestrator agent and Host Intrusion Prevention client is installed.

client rules
An IPS, Firewall, or Application Blocking rule created on a client to allow legitimate activity that is otherwise blocked. Client rules are not part of a server-side policy but can be moved to a policy for application to other clients.

common framework
The architecture that allows different McAfee products to share the common components and code, which are the Scheduler, AutoUpdate, and the ePolicy Orchestrator agent.

complete properties
The entire set of properties being exchanged during agent-to-server communication.
See also incremental properties.

computers
In the console tree, the physical computers on the network managed by ePolicy Orchestrator. Computers can be added under existing sites or groups in the Directory.

configuration settings
See policy.

console tree item
The individual icons in the console tree of the ePolicy Orchestrator console.
**console tree**  
The contents of the **Tree** tab in the left pane of the ePolicy Orchestrator console; it shows the items that are available in the console.

**custom agent installation package**  
An agent installation package that uses the user credentials you provide to perform the installation, instead of those of the currently logged on user.

**DAT files**  
Detection definition files, sometimes referred to as signature files.  
See also **EXTRA.DAT file**, **incremental DAT files**, and **SuperDAT**.

**denial of service**  
An attack method whereby a computer is overwhelmed with bogus requests, causing it to crash or keeping it from honoring legitimate requests.

**denial-of-service attack (DoS)**  
A means of attack, an intrusion, against a computer, server or network that disrupts the ability to respond to legitimate connection requests. A denial-of-service attack overloads its target with false connection requests, so that the target ignores legitimate requests.

**deploy, deployment**  
The act of distributing and installing and configuring client computers from a central location.

**details pane**  
The right pane of the ePolicy Orchestrator console, which shows details of the currently selected console tree item.

**Directory**  
In the console tree, the list of all computers to be managed via ePolicy Orchestrator; the link to the primary interfaces for managing these computers.

**distributed software repositories**  
A collection of web sites or computers located across the network in such a way as to provide bandwidth-efficient access to client computers. Distributed software repositories store the files that client computers need to install supported products and updates to these products.  
See also **fallback repository**, **global distributed repository**, **local distributed repository**, **master repository**, **mirror distributed repository**, **source repository**, and **SuperAgent distributed repository**.

**download site**  
The McAfee web site from which you retrieve product or DAT updates.  
See also **update site**.

**effective policy**  
A union of all IPS Rules and Trusted Application Rules policies that apply to client computers.

**enforce, enforcement**  
The act of applying predefined settings on client computers at predetermined intervals.

**ePolicy Orchestrator agent**  
A program that performs background tasks on managed computers, mediates all requests between the ePolicy Orchestrator server and the anti-virus and security products on these computers, and reports back to the server to indicate the status of these tasks.

**ePolicy Orchestrator console**  
The user interface of the ePolicy Orchestrator software that is used to remotely control and monitor managed computers.  
See also **ePolicy Orchestrator remote console**.
**ePolicy Orchestrator database server**
The computer that hosts the ePolicy Orchestrator database. This can be the same computer on which the ePolicy Orchestrator server is installed or a separate computer.

**ePolicy Orchestrator database**
The database that stores all data received by the ePolicy Orchestrator server from ePolicy Orchestrator agents and all settings made on the server itself.
See also *ePolicy Orchestrator database server*.

**ePolicy Orchestrator remote console**
The ePolicy Orchestrator user interface when it is installed on a separate computer from the ePolicy Orchestrator server.
See also *ePolicy Orchestrator console*.

**ePolicy Orchestrator server**
The back-end component of the ePolicy Orchestrator software.
See also *ePolicy Orchestrator agent* and *ePolicy Orchestrator console*.

**error reporting utility**
A utility specifically designed to track and log failures in the McAfee software on your system. The information that is obtained can be used to analyze problems.

**event**
An alert triggered when a security violation as defined by a signature occurs. All events triggered on a selected host appear in the list of IPS events.
See also *Signature*.

**exception rule**
A permit rule allowing legitimate activity that is otherwise blocked by a signature.

**EXTRA.DAT file**
Supplemental virus definition file that is created in response to an outbreak of a new virus or a new variant of an existing virus.
See also *DAT files*, *incremental DAT files*, and *SUPERDAT*.

**fallback repository**
A type of distributed software repository used in the event that client computers cannot contact any of their predefined distributed repositories. Typically, another source repository is defined as the fallback repository.
See also *replicate*, *replication*.

**false positive**
An event triggered by a legitimate operation of a benign process rather than an intrusion.

**feature**
A functional division of a product. Host Intrusion Prevention features include IPS, Firewall, Application Blocking, and General.

**firewall**
A filter between a computer and network connections that allows or blocks traffic based on firewall rules. With stateful filtering the state of connections is tracked, and with stateful inspection the tracking of commands higher in the network stack are examined, both allowing for greater control and security of connections.

**force install, force uninstall**
See *product deployment client task*.

**FRAMEPKG.EXE**
See *agent installation package*.
full properties
All properties that can be exchanged during agent-to-server communication.
See also minimal properties.

global/McAfee default policy
The base policy settings for a category that provide out-of-the-box protection.

global administrator
A user account with read, write, and delete permissions, as well as rights to all operations; specifically, operations that affect the entire installation, and are reserved for use by only the global administrator.
Compare to global reviewer, site administrator, site reviewer.

global blacklist
A list of e-mail addresses or domains that the administrator creates as a company-wide standard. Any e-mail messages from the addresses or domains on the global blacklist will always be treated as spam.
Compare to global whitelist; see also blacklist.

global distributed repository
A distributed software repository that can be automatically kept current with the contents of the master repository.
See also replicate, replication.

global policy
The default McAfee policy for a category.

global reviewer
A user account with read-only permissions, that can view all settings in the software for an entire installation, but cannot change any settings.
Compare to global administrator, site administrator, site reviewer.

global updating
A method for deploying product updates as soon as the files are checked into the master repository without user intervention. Files are immediately replicated to all SuperAgent and global distributed repositories; the ePolicy Orchestrator server sends a wakeup call to all SuperAgents; SuperAgents send a broadcast wakeup call to all agents in the same subnet; then all client computers retrieve the updated files from the nearest repository.

group
In the console tree, a logical collection of entities assembled for ease of management. Groups can contain other groups or computers, and can be assigned IP address ranges or IP subnet masks to allow sorting computers by IP address. If you create a group by importing a Windows NT domain, you can automatically send the agent installation package to all imported computers in the domain.

high-risk application
Under Application Protection Rules, an application that is open to having code injected into its memory space or dynamic library and thus requiring protection.

host, host computer
See client computer.

host IPS (HIPS)
Host protection rules that monitor and prevent attacks on the operating system and applications of a host system.

Host Intrusion Prevention (HIP) client
The Host Intrusion Prevention module that is installed on each host system in your network. The client serves as a protective layer surrounding a computer’s operating system and applications, identifying and preventing suspected breaches of security and malicious attacks.
HotFix releases (now Patches)
Intermediate releases of the product that fix specific issues.

inactive agent
Any agent that has not communicated with the ePolicy Orchestrator server within a specified time period.

inherit, inheritance
The act of applying the settings defined for an item within a hierarchy from the item above it.

item
See console tree item.

Learn mode
The Host Intrusion Prevention protection setting-wheres rules are learned and added after a user responds to a prompt to allow or block an action. This mode is applicable to the Firewall and Application Blocking features.

local distributed repository
A type of distributed software repository whose content is manually updated.

Lost&Found group
A group used to temporarily store computers whose appropriate location in the Directory cannot be determined.

managed products
A security product like Host Intrusion Prevention that is managed from ePolicy Orchestrator.

master repository
A type of distributed software repository whose contents acts as the standard for all other distributed repositories. Typically, the master repository contents are defined from a combination of the source repository contents and additional files added to the master repository manually.
See also pull, replicate, replication.

.NAP file
The file extension used to designate McAfee software program files that are installed in the software repository for ePolicy Orchestrator to manage.

network IPS (NIPS)
Network protection rules that monitor and prevent network attacks.

node
See console tree item.

package catalog file
A file that contains details about each update package, including the name of the product for which the update is intended, language version, and any installation dependencies.

ping attack
The method of overwhelming a network with ping commands.

ping of death
A hacking technique used to cause a denial of service by sending a large ICMP packet to a target. As the target attempts to reassemble the packet, the size of the packet overflows the buffer and can cause the target to reboot or hang.

policy
A group of settings assigned to a category of a product feature. For most categories, only one named policy for each category is permitted. The exceptions are IPS Rules and Application Rules, where one or more named policies can be applied.
**policy enforcement interval**
The time period during which the agent enforces the settings it has received from the ePolicy Orchestrator server. Because these settings are enforced locally, this interval does not require any bandwidth.

**policy files**
Set of policy settings for one or more products that are saved to the local drive of the ePolicy Orchestrator server, but cannot be accessed by a remote console.
See also policy templates.

**policy pages**
Part of the ePolicy Orchestrator console; they allow you to set policies and create scheduled tasks for products, and are stored on individual ePolicy Orchestrator servers (they are not added to the master repository).

**port scanning**
A hacking technique used to check TCP/IP ports to reveal which services are available in order to plan an exploit involving those services, and to determine the operating system of a particular computer.

**product deployment client task**
A scheduled task for deploying all products currently checked into the master repository at once. It enables you to schedule product installation and removal during off-peak hours or during the policy enforcement interval.

**profile**
A grouping of policies based on common use of applications, network location, or access rights and privileges.

**properties**
Data exchanged during agent-to-server communication that includes information about each managed computer (for example, hardware and software) and its managed products (for example, specific policy settings and the product version number).

**pull**
The act of copying files from a source or fallback repository to the master repository. Because additional files can be added to the master repository manually, only those files on the source or fallback repository are overwritten.

**quarantine mode**
Enforced isolation of a computer until action can be taken to update protection policies.

**reaction**
The response by a client when intercepting a signature. Three possible reactions can occur: Ignore (ignores the operation), Log (logs the operation in the database as an intrusion), and Prevent (prevents the specific illegal operation from taking place and logs it).

**remote console**
See ePolicy Orchestrator remote console.

**Repository**
The location that stores policy pages used to manage products.

**selective updating**
The ability to specify which version of updates you want client computers to retrieve from distributed software repositories.
See also branch.

**server tasks**
Tasks that can be executed on the server-side of the software.
severity level
One of four levels of risk assigned to signatures:

Information (blue) – a modification to the system configuration or an attempt to access sensitive system components, but which are not generally evidence of an attack.

Low (yellow) – a modification to the system configuration or an attempt to access sensitive system components, but are not identified as known attacks and are indicative of suspicious behavior on the part of a user or application.

Medium (orange) – a known attack with low to medium risk, or highly suspicious behavior by a user or an application.

High (red) – attack that poses a serious threat to security.

signature
The set of rules that describes security threats and instructions to a host or network. Each of the three types of IPS signatures, host (HIPS), custom (HIPS), and network (NIPS), has an associated severity level indicating the danger of the potential attack.

See also behavioral rule.

signature files
See DAT files.

silent installation
An installation method that installs a software package onto a computer silently, without need for user intervention.

site
In the console tree, a logical collection of entities assembled for ease of management. Sites can contain groups or computers, and can be organized by IP address range, IP subnet mask, location, department, and others.

site administrator
A user account with read, write, and delete permissions, as well as rights to all operations for the specified site (except those restricted to the global administrator), and for all groups and computers under it on the console tree.

Compare to global reviewer, global administrator, site reviewer.

site reviewer
A user account with read-only permissions, that can view all settings in the software for the specified site, but cannot change any settings.

Compare to global administrator, global reviewer, site administrator.

smurf attack
A denial-of-service attack that floods its target with replies to ICMP echo (ping) requests. A smurf attack sends ping requests to Internet broadcast addresses, which forward the ping requests to as many as 255 hosts on a subnet. The return address of the ping request is spoofed to be the address of the attack target. All hosts receiving ping requests reply to the attack target, flooding the target with replies.

snooping
Passively observing a network.

spoofing
Forging something, such as an IP address, to hide one’s location and identity.

state
Describes the manner in which a client is actually functioning (current state), or is functioning after its next communication with the server (requested state). The console recognizes four different state: Normal, Uninstalling, No connection, No license.

Status Monitor
See Agent Monitor.
**SYN flood**
A hacking technique used to cause a denial of service. SYN packets are sent from a client with a spoofed IP address and are sent at a rate faster than the TCP stack on the host can handle. As the client address is spoofed, the client sends no SYN-ACK, but continues to flood the host with SYN packets, tying up the resources of the host.

**task**
See *client tasks*, *server tasks*.

**Trojan horse**
A program that either pretends to have, or is described as having, a set of useful or desirable features, but actually contains a damaging payload. Trojan horses are not technically viruses, because they do not replicate.

**trusted application**
An application that is known to be safe in an environment, has no known vulnerabilities, and is allowed to perform any operation.

**tuning**
The process of identifying a few profiles and creating policies for them in an effort to reduce the number of false positives and prevent generating events.

**update package**
 Package files from McAfee that provide updates to a product. All packages are considered product updates with the exception of the product binary (Setup) files.

**updating**
The process of installing updates to existing products or upgrading to new versions of products.

**zero-day attack**
Exploit that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.
Index

A
Adaptive mode, 19, 26
application blocking, 26, 95
firewall, 26, 75
IPS, 26, 34
alerts
Active X, 27
application blocking, 139
firewall, 138
intrusion, 137
Java applet, 27
policy viewing, 27
quarantine, 140
Spoof Detected, 140
Application Blocking
client rules, 16
configuring Options, 95
overview, 93
quick access, 94
application blocking
creation, 67, 93
hooking, 94
preset policies, 94
application blocking client rules
Aggregated View, 100
Regular View, 100
viewing, 100
Application Blocking Options policy
configuring, 95
application blocking rules, 98
creating, 99
deleting, 100
Application Blocking Rules policy
configuring, 97
creating, 97, 99
application protection rules, 51
creating, 52
deleting, 54
disabling, 54
editing, 54
enabling, 54
overview, 51
audience for manual, 9
Avert Labs Threat Center, 12
Avert Labs Threat Library, 12
B
behavioral rules, 33
beta program website, 12
boot-time quarantine, 89, 196
C
client rules
application blocking, 100
firewall, 15
IPS, 62
Client UI policy
applying, 105
configuring, 104
creating, 106
passwords, 106
connection isolation, 8, 73 to 75
corporate network isolation, 8, 73 to 75
custom
host signatures, 44
signatures, additional information, 50
customer service, contacting, 12
D
DAT files
Avert Labs notification service for updates, 12
updates, website, 12
definition of terms (See Glossary)
deployment
fine-tuning, 115
tuning, 20, 28, 115, 185
download website, 12
E
Enforce Policies policy
configuring, 104
ePO
console, 22
notifications, 24
operations used with Host Intrusion Prevention, 22
policy management, 23
policy owners, 24
reports, 24
evaluating McAfee products, 12
download website, 12
exception rules, 14
creating, 41
creating based on an event, 59
deleting, 43
disabling, 43
editing, 42
enabling, 43
moving to another policy, 43, 64
searching, 64
searching for related, 61
F
features
Application Blocking, 16, 93
Firewall, 15
General, 16
IPS, 13, 31
firewall
Adaptive mode, 75
connection aware groups, 72
connection aware rules, 72
connection isolation, 73 to 75
isolation of network connection, 73 to 75
Learn mode, 75
network connection isolation, 73 to 75
packet filtering, 67
packet inspection, 67
preset policies, 77
quarantine rules, 76
Quarantine Rules policy, 89
rule groups, 72
rules, 15
state table, 68
firewall client rules
aggregated view, 85
aggregating, 85
quick access, 80
Firewall Options policy
configuring, 78
preset policies, 78
firewall rule group
creating, 82
deleting, 87
firewall rules, 69
adding, 82
client, 15
creating, 82
deleting, 87
eriting, 87
how they work, 68
order, 69
quick access, 80
stateful filtering, 69
stateful inspection, 70
stateful protocol tracking, 71
viewing, 87
Firewall Rules policy
configuring, 79
creating, 80
preset policies, 80

G
General feature
overview, 102
preset policies, 103
glossary, 187 to 195
guide conventions
typeface and symbols, 10
guide resources
product documentation, 11

H
help
icon explanation, 30
in UI, 30
navigation procedures, 29
using, 29
Host Intrusion Prevention
configuring, 21
deploying clients, 25
deployment, 19
help, 29
installing, 24
maintenance, 19
tuning, 28
using ePO, 21 to 22
working with clients, 25
host signatures, 44
HotFix and Patch releases (for
products and security vulnerabilities), 12

IPS
client exception rules, 15
events, 14
events, analyzing, 115
exception rules, 14
feature, 13
feature overview, 31
reactions, 14
signatures, 13
IPS client rules, 61
aggregated view, 62
aggregating, 63
migrating to a policy, 62
overview, 61
regular view, 62
IPS events, 54
analyzing, 115
configuring view, 56
creating exceptions, 59, 185
creating trusted applications, 59
filtering view, 56
hiding, 57
marking, 57
marking as read, 57
marking as unread, 57
marking similar, 58
overview, 54
showing hidden, 57
viewing, 55, 185
details, 59
IPS Options policy
configuring, 34
creating, 35
preset policies, 34
IPS Protection policy
preset policies, 37
IPS Rules policy
application protection rules, 51
assigning, 39
configuring, 39
creating, 39
details, 40
exception rules, 40
signatures, 44
isolation of network connection, 73 to 75

K
KnowledgeBase search, 12

L
Learn mode, 19, 26
application blocking, 26, 139
firewall, 26, 75
Linux client
notes, 156
overview, 156
policy enforcement, 156
troubleshooting, 157

M
migrating
client rules to server-side IPS
exception rules, 62
policies from earlier versions
of McAfee software
application blocking, 98
Host IPS, 62

N
network
collection isolation, 44, 73 to 75
signatures, 44
new features, 8
notifications
generating, 24
types, 124
usage, 123

P
packet
packet inspection, 15
packet filtering, 67
packet inspection, firewall, 67
passwords
administrator, 107
for client UI, 106
time-based, 108
policies
administrators, 184
assigning owners, 24
assignment, 18, 117, 184
assignment locking, 18
categories, 17
configuring, 27
disabled enforcement, 120
editing information, 120
enforcement, 17, 184
inheritance, 18, 117
maintenance, 117
management, 17, 23
matching a profile, 186
ownership, 18
preset protection, 19
tasks, 117
using policies tab, 117
using Policy Catalog, 119
viewing info, 119
upating
checking in update, 130
content, 130
process, 130
upate website, 12
using this guide, 8

V
Virus Information Library (See Avert Labs Threat Library)

W
WebImmune, Avert Labs Threat Center, 12
Windows client
Activity Log tab, 151
Activity Log tab list, 152
Activity Log tab options, 151
alerts, 137
Application policy tab, 146
Application policy tab options, 146
Application policy tab rules, 147
Application policy tab rules list, 147
Application Protection tab, 150
Application Protection tab list, 150
Blocked Hosts list, 148
Blocked Hosts tab, 148
console, 133
error reporting, 135
Firewall policy tab, 144
Firewall policy tab options, 144
Firewall policy tab rules, 145
Firewall policy tab rules list, 145
IPS Policy tab, 142
IPS Policy tab options, 142
IPS Policy tab rules, 143
IPS Policy tab rules list, 143
overview, 132
setting options, 134
system tray icon, 109, 133
troubleshooting, 135
troubleshooting, IPS engines, 136
troubleshooting, logging, 135
unlocking UI, 134
Windows client alerts
application blocking, 139
firewall, 138
intrusion, 137
quarantine, 140
spoof detected, 140
Windows client UI control tray icon, 109
with IPv6 on Vista, 67