# Contents

**Introducing Host Intrusion Prevention** ................................................................. 7  
  Host IPS protection ................................................................. 7  
  Host IPS policies ................................................................. 8  
  Host IPS policy management .................................................. 9  
  Host IPS policy tracking and tuning .......................................... 10  

**Managing Your Protection** ................................................................. 12  
  Information management .......................................................... 12  
    Host IPS dashboards ........................................................... 12  
    Host IPS queries ............................................................... 13  
  Policy management ............................................................... 16  
    Where to find policies ......................................................... 16  
    Configuring policies .......................................................... 17  
    Default protection and tuning .............................................. 18  
    Host IPS policy migration .................................................. 22  
  System management ............................................................... 23  
    Host IPS permission sets ..................................................... 23  
    Host IPS server tasks ......................................................... 25  
    Host IPS event responses ................................................... 26  
    Host IPS protection updates ............................................... 27  

**Configuring IPS Policies** ................................................................. 29  
  Overview of IPS policies ...................................................... 29  
    Methods for delivery of IPS protection .................................. 30  
    Signatures ................................................................. 31  
    Behavioral rules ............................................................. 32  
    Reactions ................................................................. 32  
    Exceptions ................................................................. 32  
    Application protection rules .............................................. 33  
    Events ................................................................. 33  
    Enable IPS protection ...................................................... 33  
    Configuring the IPS Options policy ..................................... 34  
    Set the reaction for IPS signatures ...................................... 35
## Configuring the IPS Protection policy
- Define IPS protection: 36
- Configuring the IPS Rules policy: 37
- Assigning multiple instances of the policy: 37
- FAQ — Multiple-instance policies: 38
- How IPS signatures work: 39
- How IPS application protection rules work: 43
- How IPS exceptions work: 46

## Monitor IPS events
- Managing IPS events: 48
- Creating an exception from an event: 49
- Creating a trusted application from an event: 50

## Configuring Firewall Policies
- Overview of Firewall policies: 52
- How firewall rules work: 53
- How firewall rule groups work: 55
- How the Host IPS catalog works: 58
- Firewall stateful packet filtering and inspection: 59
- How learn and adaptive modes affect the firewall: 63
- Firewall client rules: 64

## Configuring General Policies
- Overview of General policies: 73
- Define client functionality: 74
Configuring a Client UI policy .................................................. 74
Setting Client UI general options ............................................. 75
Setting Client UI advanced options and passwords ..................... 75
Setting Client UI troubleshooting options .................................. 76
Define trusted networks .......................................................... 77
Configuring a Trusted Networks policy ..................................... 78
Define trusted applications ..................................................... 78
Configuring a Trusted Applications policy ................................. 79
Creating and editing Trusted Application rules ............................ 79
Assigning multiple instances of the policy ............................... 80

Working with Host Intrusion Prevention Clients .............................. 81
Overview of the Windows client ................................................ 81
System tray icon menu ......................................................... 81
Client console for Windows clients .......................................... 83
Unlocking the Windows client interface .................................... 83
Setting client UI options ....................................................... 83
Troubleshooting the Windows client ....................................... 84
Windows client alerts ........................................................... 86
About the IPS Policy tab ......................................................... 88
About the Firewall Policy tab ................................................ 89
About the Blocked Hosts tab .................................................. 91
Editing the Blocked Hosts list ................................................ 92
About the Application Protection List tab ................................. 92
About the Activity Log tab ..................................................... 93
Overview of the Solaris client .................................................. 94
Policy enforcement with the Solaris client .................................. 94
Troubleshooting the Solaris client .......................................... 95
Overview of the Linux client ................................................... 97
Policy enforcement with the Linux client ................................. 97
Notes about the Linux client ................................................ 97
Troubleshooting the Linux client ........................................... 98

Appendix A — Writing Custom Signatures and Exceptions ............. 101
Rule structure ....................................................................... 101
Common sections ............................................................... 102
Optional common sections ................................................... 104
Wildcards and variables ....................................................... 104
Windows custom signatures ................................................ 107
Contents

Windows class Buffer Overflow......................................................... 107
Windows class Files................................................................. 108
Windows class Hook................................................................. 111
Windows class Illegal Host IPS API Use....................................... 112
Windows class Illegal Use......................................................... 113
Windows class Isapi (HTTP)........................................................ 113
Windows class Program............................................................. 116
Windows class Registry............................................................. 117
Windows class Services............................................................. 120
Windows class SQL................................................................. 122
Classes and directives per Windows platform................................. 123
Non-Windows custom signatures..................................................... 127
Solaris/Linux class UNIX_file...................................................... 127
Solaris/Linux class UNIX_apache (HTTP)....................................... 130
Solaris/Linux class UNIX_Misc..................................................... 131
Solaris class UNIX_bo.............................................................. 132
Solaris class UNIX_map.............................................................. 133
Solaris class UNIX_GUID.......................................................... 133
Classes and directives per UNIX platform...................................... 134

Appendix B — Troubleshooting....................................................... 136
General issues............................................................................. 136
Host IPS logs.............................................................................. 141
Clientcontrol.exe utility............................................................ 144
Introducing Host Intrusion Prevention

McAfee® Host Intrusion Prevention is a host-based intrusion detection and prevention system that protects system resources and applications from external and internal attacks. It provides a manageable and scalable intrusion prevention solution for workstations, notebooks, and critical servers, including web and database servers. Its patented technology blocks zero-day and known attacks.

Host Intrusion Prevention (sometimes abbreviated in the product as Host IPS or HIP) can protect information and prevent the compromising of system and network resources and applications that store and deliver information. It accomplishes this with an end-point firewall feature and an intrusion prevention system (IPS) feature. The IPS feature has monthly content updates, which reduces the urgency of patches for new threats. The Host Intrusion Prevention firewall feature is purchased separately or in combination with the Host Intrusion Prevention IPS feature.

Host Intrusion Prevention is fully integrated with ePolicy Orchestrator and uses its framework to deliver and enforce policies. This approach provides a single management solution that allows for mass deployment of up to 100,000 systems in multiple languages across an entire enterprise for true global coverage.

Contents
- Host IPS protection
- Host IPS policies
- Host IPS policy management
- Host IPS policy tracking and tuning

Host IPS protection

After all the required components for Host Intrusion Prevention are installed and communicating, you are ready to apply protection, monitor events, and update policies and content as needed.

Basic protection

Host Intrusion Prevention ships with a set of default settings that provide basic protection for your environment. These settings include:

- For IPS protection:
  - High severity signatures are prevented and all other signatures are ignored
  - McAfee applications are listed as trusted applications for all rules except IPS self-protection rules
  - Predefined applications and processes are protected
- For firewall protection:
• Basic network connectivity is allowed

**NOTE:** When Host Intrusion Prevention 8.0 is first installed no protection is enabled. You must enable protection in the IPS Options or Firewall Options policy and apply the policy to the client.

**Advanced protection**

For advanced protection, switch from the default settings to stronger preset settings, or create custom settings.

Start with a sample deployment to monitor and tune the new settings. Tuning involves balancing intrusion prevention protection and access to required information and applications per group type.

**Host IPS policies**

A policy is a collection of settings that you configure and enforce through the ePolicy Orchestrator console. Applying policies ensures that your security needs on managed systems are met. Host Intrusion Prevention provides three policy features, each with a set of security options. These are: **IPS**, **Firewall**, and **General**. IPS and firewall features contain a “rules” policy with rules that define behavior, and an “options” policy that enables or disables the rules.

Ownership of policies is assigned in the **Policy Catalog**. After a policy is created, it can be edited or deleted only by the creator of the policy, the person associated as an owner of the policy, or the global administrator. Deleting a policy can be done only in the **Policy Catalog**.

**IPS policies**

The IPS feature contains three policies that protect both Windows and non-Windows computers. It details exceptions, signatures, application protection rules, events, and client-generated exceptions.

• **IPS Options** (All platforms). Turns on or off IPS protection and application of adaptive mode for tuning.

• **IPS Protection** (All platforms). Defines the protection reaction to events that signatures generate.

• **IPS Rules** (All platforms). Defines signatures, exceptions, and application protection rules. This policy is a multiple instance policy, which allows for several IPS Rules policies, instead of a single policy, to be assigned to a system. The effective policy is then the result of the merged contents of the policies. If there are conflicting settings, the most protective explicit setting is applied.

**Firewall policies**

The Firewall feature contains three policies that protect Windows computers only. It filters network traffic, allowing legitimate traffic through the firewall and blocking the rest.

• **Firewall Options** (Windows only). Turns on or off firewall protection and application of adaptive or learn mode for tuning.

• **Firewall Rules** (Windows only). Defines firewall rules.

• **Firewall DNS Blocking** (Windows only). Defines the domain name servers that are to be blocked.
General policies

The General feature contains three policies that can apply to both the IPS and Firewall features.

- **Client UI** (Windows only). Defines access to the Host Intrusion Prevention user interface on Windows client systems, including troubleshooting options. Also provides password-protection on all non-Windows client systems.
- **Trusted Networks** (Windows only). Lists IP addresses and networks that are safe for communication. Used with the IPS and Firewall features.
- **Trusted Applications** (All platforms). Lists applications that are trusted to perform most operations. Used with the IPS feature. This policy is also a multiple instance policy, which allows for several Trusted Applications policies, instead of a single policy, to be assigned to a system. The effective policy is the result of the merged contents of the policies. If there are conflicting settings, the most protective setting is applied.

Host IPS policy management

The ePolicy Orchestrator console allows you to configure Host Intrusion Prevention policies from a central location.

How policies are enforced

When you change Host Intrusion Prevention policies in the ePolicy Orchestrator console, the changes take effect on the managed systems at the next agent-server communication. This interval is set to occur once every 60 minutes by default. To enforce policies immediately, you can send an agent wake-up call from the ePolicy Orchestrator console.

Policies and their categories

Policy information for Host Intrusion Prevention is grouped by feature and category. Each policy category refers to a specific subset of policies.

A policy is a configured group of settings for a specific purpose. You can create, modify, or delete as many policies as needed.

Each policy has a preconfigured McAfee Default policy, which cannot be edited or deleted. Except for IPS Rules and Trusted Applications, all policies also have an editable My Default policy based on the default policy. Some policy categories include several read-only preconfigured policies. If these preconfigured policies meet your needs, you can apply any one of them. These read-only policies, like all policies, can be duplicated and the duplicate customized, if needed.

IPS Rules and Trusted Applications policies are multiple-instance policies because you can assign multiple policy instances under a single policy. The policy instances are automatically combined into one effective policy.

**TIP:** The McAfee Default policies for IPS Rules and Trusted Applications are automatically updated as part of the content update process. McAfee recommends always assigning these policies to all clients and creating additional policy instances to customize the behavior of these two policies.

How policies are applied

Policies are applied to any System Tree group or system by inheritance or assignment. *Inheritance* determines whether the policy settings for any system are taken from its parent. By default, inheritance is enabled throughout the System Tree. 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, all groups and systems below inherit the new policy.

**Policy ownership**

Each policy is required to have an assigned owner. Ownership ensures that no one can modify the policy other than the global administrator, the creator of the policy, or the person associated as the policy owner. Any administrator can use any policy that exists in the catalog, but only the creator, owner, or global administrator can modify it.

**TIP:** Rather than use a policy owned by a different administrator, we recommend that you duplicate the policy, then assign the duplicate. Otherwise, if you assign a policy that you do not own to System Tree groups that you administer, and the owner of the policy modifies it, all systems to which this policy is assigned receive these modifications.

### Host IPS policy tracking and tuning

The deployment and management of Host Intrusion Prevention clients are handled from ePolicy Orchestrator. In the ePO System Tree you can group systems 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. McAfee recommends grouping systems by Host Intrusion Prevention 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 systems that fit a common usage profile into a common group on the System Tree. In fact, you might name a group after its usage profile, for example, *Web Servers*.

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

Deploying Host Intrusion Prevention to thousands of computers is easily managed because most computers 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 be placed under the correct group on the System Tree.

**Preset protection**

Host Intrusion Prevention offers two types of protection:

- Basic protection is available through the McAfee Default policy settings. This protection requires little or no tuning and generates few events. For many environments this basic protection might be sufficient.

- Advanced protection is also available from some preconfigured IPS and firewall policies or by creating custom policies. Servers, for example, need stronger protection than that offered in basic protection.

Both scenarios require some tuning of protection settings for actual working environments is required.

**Adaptive mode**

To help tune protection settings, Host Intrusion Prevention clients can create client-side rules to server-mandated policies that block legitimate activity. The automatic creation of client rules
is permitted when clients are placed in *adaptive* mode. In adaptive mode, client rules are created without interaction from the user. After client rules are created, you need to carefully analyze them and decide which to convert to server-mandated policies.

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

Systems in adaptive mode have virtually no protection, so the adaptive mode should be used only for tuning an environment and eventually turned off to tighten the system’s protection.

**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 target a wider range of violations and generate more events than in a basic environment. If you apply advanced protection, McAfee recommends 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 are 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 an IPS signature in specific circumstances.
- Trusted applications are application processes that ignore all IPS or Firewall rules.
- Firewall rules determine whether traffic is permissible, and block packet reception or allow or block packet transmission.

**Dashboards and queries**

Dashboards enable you to track your environment by displaying several queries at once. These queries can be constantly refreshed or run at a specified frequency.

Queries enable you to obtain data about a particular item and filter the data 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.
Managing Your Protection

Management of a Host Intrusion Prevention deployment includes monitoring, analyzing, and reacting to activities; changing and updating policies; and performing system tasks.

Contents

- Information management
- Policy management
- System management

Information management

After you have installed Host Intrusion Prevention, you can track and report on security issues that arise in your environment. Use the dashboards for a daily view of the security situation or to run queries for detailed information on particular issues.

Host IPS dashboards

Dashboards are a collection of monitors that are an essential tool for managing your environment. Monitors can be anything from a chart-based query to a small web-application, like the MyAvert Threat Service. You can create and edit multiple dashboards if you have the permissions. Use any chart-based query as a dashboard that refreshes at a specified frequency, so you can put your most useful queries on a live dashboard.

Host Intrusion Prevention provides two default dashboards with these monitors:

Table 1: Host IPS dashboards and monitors

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Monitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IPS</td>
<td>• Firewall Status</td>
</tr>
<tr>
<td></td>
<td>• Host IPS Status</td>
</tr>
<tr>
<td></td>
<td>• Service Status</td>
</tr>
<tr>
<td></td>
<td>• Count of IPS Client Rules</td>
</tr>
<tr>
<td></td>
<td>• Content Versions</td>
</tr>
<tr>
<td></td>
<td>• Top 10 NIPS Events by Source IP</td>
</tr>
<tr>
<td>Host IPS Triggered Signatures</td>
<td>• Desktop High Triggered Signatures</td>
</tr>
<tr>
<td></td>
<td>• Desktop Medium Triggered Signatures</td>
</tr>
<tr>
<td></td>
<td>• Desktop Low Triggered Signatures</td>
</tr>
<tr>
<td></td>
<td>• Server High Triggered Signatures</td>
</tr>
<tr>
<td></td>
<td>• Server Medium Triggered Signatures</td>
</tr>
<tr>
<td></td>
<td>• Server Low Triggered Signatures</td>
</tr>
</tbody>
</table>
For more information about creating and using dashboards, see the ePolicy Orchestrator documentation.

**Host IPS queries**

Host Intrusion Prevention includes query functionality through ePolicy Orchestrator. You can create useful queries from events and properties stored in the ePO database or use predefined queries.

You can produce 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.

Query options:
- Setting a filter to gather only selected information. Choose which group or tags to include in the report.
- Setting a data filter using logical operators, to define precise filters on the data returned by the report.
- Generating graphical reports from the information in the database, filtering the reports as needed, printing the reports, and exporting them to other software.
- Running queries of computers, events, and installations.

**Predefined and custom queries to analyze your protection**

The reporting feature contains predefined queries from Host Intrusion Prevention and allows you to create custom queries.

Organize and maintain custom queries to suit your needs. For example, if you customize settings for a report, export these settings as a template. After creating custom templates, organize them in logical groupings so that you can run them as needed on a daily, weekly, or monthly basis.

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 drill down to one or two levels for detailed information, all in the same report.

You control how much report information is visible to different users; for example, global administrators versus other users. Some users view reports only on systems in sites where they have permissions. Report information is also controlled by applying filters.

**Custom queries**

You can create four specific Host IPS queries with the Query Builder under **Others**: Host IPS 8.0 Firewall Client Rules, Host IPS 8.0 Firewall Client Rule Executables, Host IPS 8.0 IPS Client Rules, and Host IPS 8.0 IPS Exceptions.

Parameters for these queries include:

**Table 2: Host IPS queries and parameters**

<table>
<thead>
<tr>
<th>Query</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IPS 8.0 Catalog Firewall Rules and Firewall Client Rules</td>
<td>• Action</td>
</tr>
<tr>
<td></td>
<td>• Direction</td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Last Modified</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This query returns IPS Catalog firewall rules, IPS Catalog firewall groups, and firewall client rules. Possible action values are <strong>allow</strong>, <strong>block</strong>, and <strong>jump</strong>, with jump the action for groups, which</td>
<td><strong>Last Modifying User</strong></td>
</tr>
<tr>
<td>Query</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| have no allow/block action. IPS Catalog rules and groups have the `leafNodeId` filter value set to 0, so to view firewall client rules only, set the `leafNodeId` filter value to > 0. | • Leaf Node ID  
• Local Services  
• Log Status  
• IP Protocol  
• Match Intrusion  
• Media Type  
• Name  
• Note  
• Remote Services  
• Rule ID  
• Schedule End  
• Schedule Start  
• Switch When Expired  
• Transport Protocol |
| Host IPS 8.0 Firewall Client Rule Executables | • Fingerprint  
• Name  
• Note  
• Path  
• Rule ID  
• Signer Name |
| Host IPS 8.0 IPS Client Rules | • Creation Date  
• Description  
• Executable Name  
• Executable Path  
• Fingerprint  
• Full Executable Name  
• Include All Executables  
• Include All Signatures  
• Include All Users  
• Last Modified Date  
• Local Version  
• Reaction  
• Signature ID  
• Signer Name  
• Status  
• User Name |
| Host IPS 8.0 IPS Exceptions | • IPS Exception Rule  
• IPS Rules Policy |

**Common Host IPS properties**

The Host IPS custom queries and some of the other custom queries allow you to include these Host IPS properties:

- Agent type
- IPS Adaptive Mode Status
• Blocked Attackers
• Client Version
• Content Version
• Firewall Adaptive Mode Status
• Firewall Fault (Errors)
• Firewall Inbound Learn Mode Status
• Firewall Outbound Learn Mode Status
• Firewall Rule Count
• Firewall Status
• Host IPS Fault (Errors)
• Host IPS Status
• Install Directory
• Language
• Local Exception Rule Count
• Network IPS Status
• Pending Reboot
• Plug-in Version
• Product Status
• Service Running
• Hotfix/Patch Version
• Product Version
• Service Pack
• Host IPS Event Info (Hidden, Read)
• Signature Name

**Pre-defined queries**

In addition to custom queries, you can use several pre-defined queries as is, or edit them to obtain just the information you need. Select from these Host IPS predefined queries:

<table>
<thead>
<tr>
<th>HIP Query</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Rules By Process</td>
<td>Displays firewall client rules listed by process.</td>
</tr>
<tr>
<td>Client Rules By Process/Port Range</td>
<td>Displays firewall client rules listed by process and port range.</td>
</tr>
<tr>
<td>Client Rules By Process/User</td>
<td>Displays firewall client rules listed by process and user.</td>
</tr>
<tr>
<td>Client Rules By Protocol/System Name</td>
<td>Displays firewall client rules listed by protocol and system name.</td>
</tr>
<tr>
<td>Client Rules By Protocol/Port Range</td>
<td>Displays firewall client rules listed by protocol and port range.</td>
</tr>
<tr>
<td>Client Rules by Protocol/Process</td>
<td>Displays firewall client rules listed by protocol and process.</td>
</tr>
<tr>
<td>Client Versions</td>
<td>Displays top three client versions with a single category for all other versions.</td>
</tr>
<tr>
<td>Clients Pending Restart</td>
<td>Displays managed systems where Host IPS is deployed and the installer needs to restart the system.</td>
</tr>
<tr>
<td>Content Versions</td>
<td>Displays top three content versions with a single category for all other versions.</td>
</tr>
<tr>
<td>Count of FW Client Rules</td>
<td>Displays the number of Firewall client rules created over time.</td>
</tr>
<tr>
<td>Count of IPS Client Rules</td>
<td>Displays the number of IPS client rules created over time.</td>
</tr>
<tr>
<td>Desktop High Triggered Signatures</td>
<td>Displays the top 10 most triggered IPS signatures of High Severity (Critical).</td>
</tr>
<tr>
<td>Desktop Medium Triggered Signatures</td>
<td>Displays the top 10 most triggered IPS signatures of Medium Severity (Warning).</td>
</tr>
<tr>
<td>Desktop Low Triggered Signatures</td>
<td>Displays the top 10 most triggered IPS signatures of Low Severity (Notice).</td>
</tr>
<tr>
<td>Events From Host IPS Trusted Networks</td>
<td>Displays events generated by systems within Host IPS trusted networks.</td>
</tr>
</tbody>
</table>
### HIP Query

<table>
<thead>
<tr>
<th>HIP Query</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Errors</td>
<td>Displays managed systems where the Firewall feature is enabled by policy but didn't start successfully.</td>
</tr>
<tr>
<td>Firewall Status</td>
<td>Displays where Firewall protection is enabled or disabled on managed systems.</td>
</tr>
<tr>
<td>Host IPS Errors</td>
<td>Displays managed systems where the IPS feature is enabled by policy but didn't start successfully.</td>
</tr>
<tr>
<td>Host IPS Status</td>
<td>Displays where IPS protection is enabled or disabled on managed systems.</td>
</tr>
<tr>
<td>IPS Exceptions Report</td>
<td>Displays IPS Rule policies that use IPS exceptions.</td>
</tr>
<tr>
<td>Server High Triggered Signatures</td>
<td>Displays the top 10 most triggered IPS signatures of High Severity (Critical).</td>
</tr>
<tr>
<td>Server Medium Triggered Signatures</td>
<td>Displays the top 10 most triggered IPS signatures of Medium Severity (Warning).</td>
</tr>
<tr>
<td>Server Low Triggered Signatures</td>
<td>Displays the top 10 most triggered IPS signatures of Low Severity (Notice).</td>
</tr>
<tr>
<td>Service Status</td>
<td>Displays where Host IPS is installed and whether it is running or not on managed systems.</td>
</tr>
<tr>
<td>Top 10 IPS Events by Target</td>
<td>Displays the top 10 systems with the most IPS events.</td>
</tr>
<tr>
<td>Top 10 NIPS By Source IP</td>
<td>Displays the top 10 network intrusion events by source IP addresses for the past three months.</td>
</tr>
<tr>
<td>Top 10 Triggered Signatures</td>
<td>Displays the top 10 triggered IPS signatures.</td>
</tr>
</tbody>
</table>

### Policy management

Management of policies involves configuring and applying policies and the tuning of protection for system resources and applications. Part of this process requires an analysis of events and client rules.

### Where to find policies

ePolicy Orchestrator provides two locations to view and manage Host Intrusion Prevention policies: the Assigned Policies tab (`Systems` | `System Tree` | `Assigned Policies` tab for a selected group in the System Tree) and the Policy Catalog tab (`Systems` | `Policy Catalog`).

For a selected group or system, use the `Assigned Policies` tab to:
- View the available policies of a particular feature of the product
- View details of the policy
- View inheritance information
- Edit policy assignment
- Edit custom policies

Use the `Policy Catalog` to:
- Create policies
- View and edit policy information
- View where a policy is assigned
• View the settings and owner of a policy
• View assignments where policy enforcement is disabled

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a policy</td>
<td>Click New Policy, name it, and edit the settings.</td>
</tr>
<tr>
<td>Edit a policy</td>
<td>Click Edit (only available for My Default or custom policies).</td>
</tr>
<tr>
<td>View a policy</td>
<td>Click View (only available for McAfee Default or preconfigured policies).</td>
</tr>
<tr>
<td>Rename a policy</td>
<td>Click Rename and change the name of the policy (not available for default</td>
</tr>
<tr>
<td></td>
<td>or preconfigured policies).</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 default or preconfigured policies).</td>
</tr>
<tr>
<td>Assign a policy owner</td>
<td>Click the owner of the policy and select another owner from a list (not</td>
</tr>
<tr>
<td></td>
<td>available for default or preconfigured policies).</td>
</tr>
<tr>
<td>Export a policy</td>
<td>Click Export, then name and save the policy (an XML file) to the desired</td>
</tr>
<tr>
<td></td>
<td>location.</td>
</tr>
<tr>
<td>Export all policies</td>
<td>Click Export all policies, then name and save the policy XML file to the</td>
</tr>
<tr>
<td></td>
<td>desired location.</td>
</tr>
<tr>
<td>Import policies</td>
<td>Click Import at the top of the Policy Catalog page, select the policy XML</td>
</tr>
<tr>
<td></td>
<td>file, then click OK.</td>
</tr>
</tbody>
</table>

For details on any of these features, see the ePolicy Orchestrator documentation.

**Configuring polices**

After you install the Host Intrusion Prevention software, McAfee recommends that you configure policies to provide the greatest amount of security without conflicting with day-to-day activities. The default policies in Host Intrusion Prevention fit the broadest set of customer environments and might meet your needs. To tune policies to fit your particular setting, we recommend the following:

• Carefully define your Host Intrusion Prevention security configuration. Evaluate who is responsible for configuring particular parts of the system and grant them appropriate permissions.
• 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 the day-to-day work of users, adjust the severity to a lower level.
• Configure dashboards for a quick overview of compliance and issues.
• Configure automatic responses to 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.
Creating a new policy
To create a new policy, you copy of an existing one and name the new copy. You can do this either in the Policy Catalog or from a Policy page.

Task
For option definitions, click ? in the interface.
• Do one of the following from the Policy Catalog:
  • Click the New Policy button. Select the policy you want to make a copy of, type the name of the new policy, and click OK.
  • Click the Duplicate link for a policy. Type the name of the new policy, and click OK.
  • Click the View or Edit link for a policy, then on the Policy page, click the Duplicate button. Type the name of the new policy, and click OK. The duplicated policy appears. Edit the policy and click Save.

Changing policy assignment
Use this task to change the Host Intrusion Prevention policy assignment for a group or a single system in the ePolicy Orchestrator System Tree.

Task
For option definitions, click ? in the interface.
• Do one of the following:
  • For a group, go to Systems | System Tree, select a group, and then on the Assigned Policies tab click Edit Assignment.
  • For a system go to Systems | System Tree, select a group that contains the system, and then on the System tab, select the system and select Actions | Agents | Modify Policies on a Single System.

Default protection and tuning
Host Intrusion Prevention works with default policies for basic protection. It allows greater protection through custom settings obtained through manual or automatic tuning.

Default protection
Host Intrusion Prevention ships with a set of default policies that provide basic protection for your environment. Both IPS and firewall protection are off by default and must enabled to allow default rules policies to be enforced.
For advanced protection, switch from the default IPS policies to stronger preset policies, or create custom policies.
Start with a sample deployment to monitor and tune the new settings. Tuning involves balancing intrusion prevention protection and access to required information and applications per group type.

Manual tuning
Manual tuning requires direct monitoring for a set period of time of events and client rules that are created.
• For IPS protection, monitor events for false positives and create exceptions or trusted applications to prevent these events from reoccurring.
• For firewall protection, monitor network traffic and add trusted networks to allow appropriate network traffic.
• Monitor the effects of the new exceptions, trusted applications, and trusted networks.
• If these rules succeed in preventing false positives, keeping network traffic to a minimum, and allowing legitimate activity, make them part of a new or existing policy.
• Apply the new policy to a set of computers and monitor the results.
• Repeat this process with each production group type.

**Automatic tuning**

Automatic tuning removes the need to constantly monitor all events and activities for all users.

• Apply adaptive mode for IPS and Firewall policies.
• In adaptive mode, IPS events are not triggered and activity is not blocked, except for malicious exploits. Client rules are created automatically to allow legitimate activity.
• Review the lists of client rules.
• Promote appropriate client rules to administrative policy rules.
• After a few weeks, turn off the adaptive mode.
• Monitor the test group for a few days to be sure the policy settings are appropriate and offer the desired protection.
• Repeat this process with each production group type.

**Clients and planning your deployment**

The Host Intrusion Prevention client is the essential component providing protection. When deploying clients, we recommend a phased approach:

• **Determine your initial client rollout plan.** Although you can deploy Host Intrusion Prevention clients to every host (servers, desktops, and laptops) in your company, McAfee recommends 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 System Tree, in certain reports, and in event data generated by activity on the client. Clients can take the names of the hosts where they are installed, or you can assign a specific client name during installation. McAfee recommends establishing a naming convention for clients that is easy to interpret by anyone working with the Host Intrusion Prevention deployment.

• **Install the clients.** Clients can be installed with a default set of IPS and firewall 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 System Tree hierarchy. For example, you might group clients according to their geographic location, corporate function, or the characteristics of the system.

**Client data and what it tells you**

After you install and group your clients, the deployment is complete. You should begin to see events triggered by activity on the clients. 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 Events tab of the Host IPS tab under Reporting. 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 Events tab displays all Host IPS events, including NIPS, Firewall intrusions, and TrustedSource block events.

To analyze client rules, view the IPS Client Rules and Firewall Client Rules tabs. You can see which rules are being created, aggregate them to find the most prevalent common rules, and move the rules directly to a policy for application to other clients.

In addition, the ePolicy Orchestrator Reporting module provides detailed reports based on events, client rules, and the Host Intrusion Prevention configuration. Use these queries to communicate environment activity to other members of your team and management.

**Adaptive mode**

A major element in the tuning process includes placing Host Intrusion Prevention clients in adaptive mode for IPS and Firewall. This mode allows computers to create client exception rules to administrative policies. Adaptive mode does this automatically without user interaction.

This mode analyzes 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 mode, you can create 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 adaptive mode to tighten the system’s intrusion prevention protection.

- Run clients in adaptive 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 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 require software applications for normal business in some areas of the company, but not in others. For example, you might allow Instant Messaging in your Technical Support organization, but prevent its use in your Finance department. You can establish the application as trusted on the systems in Technical Support to allow users full access to it.

- The Firewall feature acts as a filter between a computer and the network or the 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 — which allows the packet through the firewall, or blocks it.
FAQ — Adaptive mode

Adaptive mode is a setting you can apply to the IPS and firewall features when testing rollouts of new policies. It allows the Host Intrusion Prevention client to automatically create rules to allow activity while preserving minimum protection from vulnerabilities. The following questions and answers should help you in using this feature.

How do you turn on adaptive mode?

You turn on adaptive mode by enabling this option in the IPS Options or Firewall Options policy and applying this policy to the Host Intrusion Prevention client.

How does adaptive mode work differently with IPS and Firewall?

With IPS, the adaptive mode creates client-side rules that are exceptions to existing IPS signatures. With the firewall, the adaptive mode creates client-side rules to allow network packets not covered by existing firewall rules.

IPS client exceptions are created on a per-user, per-process, per-signature basis and are path-based only. Firewall client rules are created on a per-process basis and the processes associated with firewall client rules are based on path, file description, digital signature, and MD5 hash.

When is a rule not created automatically with adaptive mode?

With IPS:

- The signature in the effective IPS Rules policy does not allow a client rule to be created. (This setting is standard for most high-severity IPS signatures. These signatures are tuned to detect and prevent the most severe threats to your systems, so it is unlikely that normal business activity would require an automated exception.)
- The reaction to the signature is "Ignore."
- The associated action triggers a network IPS signature.
- A user attempts to stop the McAfee Host IPS service, regardless of the client rule setting for service self-protection in signature 1000.
- There is already an exception, which excludes the operation in question, in an applied IPS Rules policy.
- The process associated with the action is trusted for IPS in an applied Trusted Applications policy, and the signature is not excluded from Trusted Applications.

With the firewall:

- There is no application associated with the packet when examined in the client activity log. Some of the most common examples include:
  - Incoming requests for services that are not running, such as file transfer protocol (FTP) or Telnet.
  - Incoming Internet Control Message Protocol (ICMP), such as an echo request.
  - Incoming or outgoing ICMP on the Microsoft Windows Vista operating system.
  - Transmission Control Protocol (TCP) packets to port 139 (NetBIOS SSN) or 445 (MSDS), which might be required for Windows file sharing.
  - Internet Protocol Security (IPsec) packets associated with virtual private network (VPN) client solutions.
- There is already a rule in the applied Firewall Rules policy that blocks or allows the packet.
• The applied Firewall Rules policy has a location-aware group with connection isolation enabled, an active network interface card (NIC) matches the group, and the packet is sent or received on a NIC that does not match the group.
• The packet is not TCP, user datagram protocol (UDP), or ICMP.
• More than one user is logged on to the system, or no user is logged on to the system.

Are there other limitations?
• IPS might fail to detect the user associated with some client rules (displayed as "domain unknown/user unknown" in the client rule on ePolicy Orchestrator). Exceptions can still be created with these client rules, but they apply to all users.
• Some incoming TCP connections such as remote desktop or Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) might require multiple attempts to create a firewall rule.

Host IPS policy migration
You cannot use McAfee Host Intrusion Prevention version 6.1 or 7.0 policies with version 8.0 clients without first migrating version 6.1 or 7.0 policies to version 8.0 format. Host Intrusion Prevention 8.0 provides an easy means to migrate policies with the ePolicy Orchestrator Host IPS Policy Migration feature under Automation. This migration involves translating and moving policies. After the policy is migrated it appears under the Policy Catalog’s corresponding Host IPS 8.0 product feature and category with [6.1] or [7.0] following the name of the policy.

All policies are translated and migrated to corresponding version 8.0 policies, except for the following:
• Application Blocking Options policies are not migrated (these policies were removed in version 8.0).
• Application Blocking Rules policies are migrated into IPS Rules policies named Application Hooking and Invocation Protection <name> [6.1 or 7.0] (these policies were removed in version 8.0). After these policies are migrated into IPS Rules policies, their Application Protection Rules list is blank, and the Exceptions list contains exceptions for all default trusted application set to "Trusted for Application Hooking." To use this migrated policy you must also assign the My Default IPS Rules policy in a multiple-policy instance setting, as it contains the latest application protection list through content updates.

NOTE: Applications for which hooking is blocked in Application Blocking Rules policies are not migrated and need to be manually added to the Application Protection Rules in the IPS Rules policy after migration. Also, if you migrate a Trusted Applications policy with applications marked "Trusted for application hooking" to version 8.0, you must create an exception for that application in signature 6010 (Generic Application Hooking Protection) in a Host IPS Rules policy to preserve the application hooking protection.

• Firewall Quarantine Options policies are not migrated (these policies were removed in version 8.0).
• Firewall Quarantine Rules policies are not migrated (these policies were removed in version 8.0).
• IPS Client Rules and Firewall Client Rules are not migrated.

NOTE: Policy assignments are carried over during migration. If inheritance is broken at a particular location in the System Tree, the assignment is not overwritten, but inheritance may be broken at other points of the System Tree, as migrated assignments are merged. Always review policy assignment after migrating policies.
**Migrating policies directly**

After installing the Host Intrusion Prevention 8.0 extension, the easiest way to migrate all existing policies is to migrate policies directly.

1. Click **Automation | Host IPS Policy Migration**.
2. Under Action for Host IPS 6.1 or 7.0 policies in the ePO policy catalog, click **Migrate**.
3. When policy migration is complete, click **Close**.

All version 6.1/7.0 IPS, Firewall, and General feature policies are converted to version 8.0 and appear with [6.1] or [7.0] after their name.

**NOTE:** Running the policy migration a second time overwrites any policies of the same name that were migrated previously. This process is not selective, as all existing 6.1 or 7.0 policies are migrated. If you want to selectively migrate policies, you migrate using the xml file process.

**Migrating policies through an xml file**

If the Host Intrusion Prevention 6.1/7.0 extension is not installed and you have previously exported selected single policies to an xml file, or if you want to selectively migrate version 6.1/7.0 policies instead of all policies at once, you do this by migrating through an xml file. The process involves first exporting single Host Intrusion Prevention 6.1/7.0 policies to xml format, converting the contents of the xml file to Host Intrusion Prevention 8.0 policy versions, and later importing the migrated xml file into the ePO Policy Catalog.

1. Click **Automation | Host IPS Policy Migration**.
2. Under Action for Host IPS 6.1 or 7.0 policies in an xml file, click **Migrate**.
3. Select the Host IPS 6.1 or 7.0 version xml file previously exported, then click **OK**. The xml file is converted to policy version 8.0 format.
4. Right-click the link to the converted MigratedPolicies.xml file and save it for importing.
5. Import the xml file in to the ePO Policy Catalog.

**System management**

As part of managing the Host Intrusion Prevention deployment, you need to perform occasional system tasks. These include setting up user permissions, server tasks, notifications, and content updating.

**Host IPS permission sets**

A permission set is a group of permissions granted to a user account for specific products or features of a product. One or more permission sets can be assigned. All permissions to all products and features are automatically assigned to global administrators. Permission sets only grant permissions — they never remove a permission.

Global administrators can assign existing permission sets when creating or editing user accounts and when creating or editing permission sets.

The Host Intrusion Prevention extension adds a Host Intrusion Prevention section to the permission sets without applying any permissions. The global administrators must grant Host IPS permissions to existing permission sets or create new permission sets and add them there.

With Host Intrusion Prevention, permissions are granted for access to each feature of the product and whether the user has read or read/write permission. This applies to the Host
Intrusion Prevention policy pages and the Host Intrusion Prevention event and client rules pages under Reporting.

For this Host IPS feature... | These permissions are available...
--- | ---
IPS | None, view settings only, or view and change settings.
Firewall | None, view settings only, or view and change settings.
General | None, view settings only, or view and change settings.

The global administrator also needs to give ePolicy Orchestrator permissions to handle other areas that work with Host Intrusion Prevention, including queries and dashboards. For example, to analyze and manage firewall client rules found on the Host IPS pages under Reporting, a user needs view permissions for Event Log, view permissions for Systems, view permissions for System Tree access, and view and change permission for the Host Intrusion Prevention Firewall feature.

Table 3: Permissions required for working with various features

<table>
<thead>
<tr>
<th>For these Host IPS features</th>
<th>These permission sets are required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IPS dashboards</td>
<td>Dashboards, Queries</td>
</tr>
<tr>
<td>Host IPS queries</td>
<td>Queries</td>
</tr>
<tr>
<td>Host IPS client events and client rules</td>
<td>Systems, System Tree access, Threat Event Log</td>
</tr>
<tr>
<td>Host IPS server tasks</td>
<td>Server Tasks</td>
</tr>
<tr>
<td>Host IPS packages in repository</td>
<td>Software</td>
</tr>
<tr>
<td>Host IPS automatic responses</td>
<td>Automatic Responses, Event Notifications, Client Events</td>
</tr>
</tbody>
</table>

For more information on permission sets, see the ePolicy Orchestrator documentation.

Assigning permission sets

Use this task to assign permissions to Host Intrusion Prevention features on the ePO server.

Before you begin

Determine the Host Intrusion Prevention features to which you want to give access and the additional permission sets that must be assigned to access all aspects of that Host Intrusion Prevention feature. For example, to view Firewall Client rules, the user must have permission to the Firewall feature in the Host Intrusion Prevention permission set, as well as to Event log, Systems, and System Tree access permission sets.

Task

For option definitions, click ? in the interface.

1. Click Menu | User Management | Permission Sets.
2. Next to Host Intrusion Prevention, click Edit.
3. Select the desired permission for each feature:
   - None
   - View settings only
   - View and change settings
4. Click Save.
Assign other permission sets as required:

<table>
<thead>
<tr>
<th>For this Host IPS feature</th>
<th>Assign this permission set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IPS events</td>
<td>Host Intrusion Prevention — IPS, Event log, Systems, System Tree access</td>
</tr>
<tr>
<td>Host IPS client IPS rules</td>
<td>Host Intrusion Prevention — IPS, Event log, Systems, System Tree access</td>
</tr>
<tr>
<td>Host IPS client firewall rules</td>
<td>Host Intrusion Prevention — Firewall, Event log, Systems, System Tree access</td>
</tr>
<tr>
<td>Host IPS dashboards</td>
<td>Dashboard, Queries</td>
</tr>
<tr>
<td>Host IPS queries</td>
<td>Queries</td>
</tr>
</tbody>
</table>

**Host IPS server tasks**

Host Intrusion Prevention provides several preconfigured and configurable server tasks that you can set to run on a specified schedule or immediately as part of Host Intrusion Prevention protection maintenance. You can create custom Host Intrusion Prevention server tasks by clicking New Task and selecting one or more Host IPS properties on the Actions tab of the Server Task Builder. For more information on using and creating server tasks, see the ePolicy Orchestrator documentation.

To work with an existing server task, click **Menu | Automation | Server Tasks**, then click the appropriate command under Actions. To create a custom server task, click **New Task** and follow the steps in the Server Task Builder wizard.

**Table 4: Preconfigured and custom server tasks**

<table>
<thead>
<tr>
<th>Server Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IPS Property Translator (Preconfigured)</td>
<td>This server task translates Host Intrusion Prevention client rules that are stored in the ePolicy Orchestrator database to handle Host Intrusion Prevention sorting, grouping, and filtering of data. This task runs automatically every 15 minutes and requires no user interaction. You can, however, run it manually if you need to see immediate feedback from actions on the client.</td>
</tr>
<tr>
<td>Repository Pull (Custom)</td>
<td>This server task allows you to create a custom task to retrieve packages from the source site and place them in the master repository. Select the Host IPS Content as a package type to retrieve content updates automatically.</td>
</tr>
<tr>
<td>Run Query (Custom)</td>
<td>This server task allows you to create a custom task to run Host Intrusion Prevention preconfigured queries at a specified time and schedule.</td>
</tr>
<tr>
<td>Purge Threat Event Log (Custom)</td>
<td>This server task allows you to create a custom task to purge threat event logs based on a Host Intrusion Prevention query. Select a Host IPS Events query to purge from the log.</td>
</tr>
<tr>
<td>Export Policies (Custom)</td>
<td>This server task allows you to download an xml file that contains the associated Host Intrusion Prevention policy.</td>
</tr>
<tr>
<td>Export Queries (Custom)</td>
<td>This server task allows you to create a Host Intrusion Prevention query output file that can be saved or emailed.</td>
</tr>
</tbody>
</table>
Host IPS event responses

Automatic responses can alert you to any events that occur on Host Intrusion Prevention client systems. You can configure responses when specific events are received and processed by the ePolicy Orchestrator server. Configured responses are:

- Create issues
- Execute scheduled tasks
- Run external commands
- Send SNMP traps
- Send email

You can specify the event properties specific to Host Intrusion Prevention that generate a response and the frequency that responses are sent. For complete details, see the ePolicy Orchestrator 4.5 documentation.

Preparing to create Automatic Responses

When creating Automatic Responses, be sure to do the following:

1. Understand Automatic Responses and how it works with the System Tree and your network.
2. Plan your implementation, keeping in mind that certain users need to know about certain events.
3. Prepare the components and permissions used with Automatic Responses, including:
   - Automatic Responses permissions — Create or edit permission sets and ensure that they are assigned to the appropriate ePO users.
   - Email server — Configure the email (SMTP) server at Server Settings.
   - Email contacts list — Specify the list from which you select recipients of notification messages at Contacts.
   - Registered executables — Specify a list of registered executables to run when the conditions of a rule are met.
   - Server tasks — Create server tasks for use as actions to be carried out as a result of a response rule.
   - SNMP servers — Specify a list of SNMP servers to use while creating rules. You can configure rules to send SNMP traps to SNMP servers when the conditions are met to initiate a notification message.

Tips on using automatic responses

The areas that are specific to Host Intrusion Prevention information, the Host IPS Advanced Properties, are involved in setting filters, aggregating events, and configuring the action for the rule. To use these properties, set the event group to ePO Notification Events and the event type to Threat.

Table 5: Host IPS Advanced Properties

<table>
<thead>
<tr>
<th>Properties</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Name</td>
<td>Name of the monitored API that triggered an event</td>
</tr>
<tr>
<td>Direction</td>
<td>In/Out/ Either</td>
</tr>
<tr>
<td>Host IPS Event Description</td>
<td>Detailed description of the event</td>
</tr>
<tr>
<td>Local IP Address</td>
<td>Local IP address of the system involved in the event</td>
</tr>
</tbody>
</table>
### Host IPS protection updates

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.

Updates include data associated with the IPS Rules policy (IPS signatures and application protection rules) and the Trusted Applications policy (trusted applications). As these updates occur in the McAfee default policy, these policies must be assigned for both IPS Rules and Trusted Applications to take advantage of the updated protection.

The basic process includes checking in the update package to the ePO master repository, then sending the updated information to the clients. Clients obtain updates only through communication with the ePO server, and not directly through FTP or HTTP protocols.

**TIP:** Always assign the McAfee Default IPS Rules policy and McAfee Default Trusted Applications policy to benefit from any content updates. If you modify these default policies, the modification is not overwritten with an update because modified settings in these policies take precedence over default settings.

### Checking in update packages

You can create an ePO pull task that automatically checks in content update packages to the master repository. This task downloads the content update package directly from McAfee at the indicated frequency and adds it to the master repository, updating the database with new Host Intrusion Prevention content.

**Task**

1. Click **Menu | Software | Master Repository**, then click **Actions | Schedule Pull**.
2. Name the task, for example, **HIP Content Updates**, then click **Next**.
3. Select **Repository Pull** as the task type, the source of the package (**McAfeeHttp** or **McAfeeFtp**), the branch to receive the package (**Current, Previous, Evaluation**), and a selected package (**Host Intrusion Prevention Content**), then click **Next**.
4. Schedule the task as needed, then click **Next**.
5. Verify the information, then click **Save**.

<table>
<thead>
<tr>
<th>Properties</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process ID</td>
<td>Path of a threat source executable</td>
</tr>
<tr>
<td>Protocol</td>
<td>IP protocol (UDP, TCP, ICMP)</td>
</tr>
<tr>
<td>Remote IP Address</td>
<td>Remote IP address of the system involved in the event</td>
</tr>
<tr>
<td>Workstation Name</td>
<td>Name of the system involved in the event</td>
</tr>
</tbody>
</table>
Checking in packages manually

This task downloads the content update package directly from McAfee at the indicated frequency and adds it to the master repository, updating the database with new Host Intrusion Prevention content.

You can download an update package and check it in manually if you do not want to use an automatic pull task.

**Task**

1. Go to **Systems | System Tree | Client Tasks**, select the group where you want to send content updates, and click **New Task**.
2. Name the task, select **Product Update** as the type of task, then click **Next**.
3. Select **Selected packages**, select **Host Intrusion Prevention Content**, then click **Next**.
4. Schedule the task as desired, then click **Next**.
5. Review the details, then click **Save**.

Updating content from the client

A client can also request updates on demand if a McAfee Agent icon appears in the client computer’s system tray.

**Task**

- Right-click the McAfee Agent icon in the system tray and select **Update Now**. The McAfee AutoUpdate progress dialog box appears and content updates are pulled and applied to the client.
Configuring IPS Policies

IPS policies turn host intrusion prevention protection on and off, set the reaction level to events, and provide protection through the application of exceptions, signatures, and application protection rules. IPS protection is kept up-to-date with monthly content updates that contain new and revised signatures and application protection rules.

Contents
- Overview of IPS policies
- Enable IPS protection
- Set the reaction for IPS signatures
- Define IPS protection
- Monitor IPS events
- Monitor IPS client rules

Overview of IPS policies

The IPS (Intrusion Prevention System) feature monitors all system (kernel-level) and API (user-level) 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. This hybrid method detects most known attacks as well as previously unknown or zero-day attacks.

Protection also comes from exceptions, which override signatures that block legitimate activity, and application protection rules, which describe which processes to protect.

Available policies

There are three IPS policies:
- **IPS Options** — Enables IPS protection by turning on and off host and network IPS protection and applying options specific to Windows systems.
- **IPS Protection** — Tells the system how to react (block, ignore, log) when signatures of a specific severity (high, medium, low) are triggered.
- **IPS Rules** — Defines IPS protection by applying signatures and behavioral analysis to protect against known and zero-day attacks. Exceptions, which override signatures that block legitimate activity, and application protection rules, which indicate which processes to protect, complement the signatures. Like the **Trusted Applications** policy, this policy category can contain multiple policy instances. Content updates provide new and updated signatures and application protection rules to keep protection current.
Methods for delivery of IPS protection

Shielding and enveloping, system call interception, and installation of specific engines and drivers are the methods used to deliver IPS protection.

Enveloping and shielding

Host Intrusion Prevention uses enveloping and shielding signatures to protect against attacks. The enveloping strategy works to prevent applications from accessing files, data, registry settings, and services outside their own application envelope. The shielding strategy works to prevent application files, data, registry settings, and services from being accessed by an exploit from outside their own application envelope.

System call interception

Host Intrusion Prevention monitors all system and API calls and blocks malicious activity. It determines which process is using a call, the security context in which the process runs, and the resource being accessed. A Host Intrusion Prevention kernel-level driver, which receives redirected entries in the user-level 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.

User-level programs use the functionality provided by the kernel to access disk drives, network connections, and shared memory. Because the processor prevents direct access to kernel-level functions, user-level programs use system calls, which permit communication between user and kernel modes. System calls expose all kernel functionality that user-level programs require and are implemented inside the operating system using a system call table. Host Intrusion Prevention inserts itself into the system call chain by installing a kernel-level driver and redirecting the entries in the system call table. When an application requests a file, it is directed to the Host Intrusion Prevention driver, which checks the request against its set of signatures and behavioral rules to determine whether to allow or block the request.

HTTP engine for web servers

Host Intrusion Prevention gives protection against attacks directed at web applications and systems with its HTTP protection engine. It protects by parsing the HTTP stream coming in to an application and matching patterns on incoming HTTP requests. The HTTP Protection engine installs between the web server's SSL decryption and decoding element that turns requests into plain text and the web server's engine. This guarantees that the Host Intrusion Prevention engine sees requests in plain text and blocks malicious requests before they are processed. HTTP signatures prevent directory traversal and Unicode attacks, web defacement, data theft, and server hacking.

SQL engine for SQL servers

Host Intrusion Prevention protects against attacks on database servers with its SQL inspection engine, which installs between database network libraries and the database engine. It examines all SQL requests and blocks any that could trigger an event. SQL protection rules, which differentiate on user, query origination location, query validity, and other parameters.

SQL database signatures build on the core protection provided by standard signatures and add specific database interception and protection rules. The Host IPS SQL engine intercepts incoming database queries before they are processed by the database engine. Each query is examined to see whether it matches any known attack signatures, if it is well formed, and if there are tell-tale signs of SQL injection.
SQL database signatures implement database shielding to protect the database's data files, services, and resources. In addition, they implement database enveloping to ensure that the database operates within its well-defined, behavioral profile.

**Signatures**

Signatures are collections of intrusion prevention rules that can be matched against a traffic stream. For example, a signature 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 specific operating systems; for example, web servers such as Apache and IIS. The majority of signatures protect the entire operating system, while some protect specific applications.

**Host IPS signatures**

Host Intrusion Prevention protection resides on individual systems such as servers, workstations, or laptop. The Host Intrusion Prevention client inspects traffic flowing into or out of a system and examines 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 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.

These signatures:

- Protect against an attack and the results of an attack, such as preventing a program from writing a file.
- Protect laptops when they are outside the protected network.
- Protect against local attacks introduced by CDs or USB devices. These attacks often focus on escalating the user's privileges to “root” or “administrator” to compromise other systems in the network.
- Provide a last line of defense against attacks that have evaded other security tools.
- Prevent internal attack or misuse of devices located on the same network segment.
- Protect against attacks where the encrypted data stream terminates at the system being protected by examining the decrypted data and behavior.
- Protect systems on obsolete or unusual network architectures such as Token Ring or FDDI.

Host Intrusion Prevention contains a large default list of host IPS signatures for all platforms. You can edit the severity level, log status, and client rule creation setting of these signatures, or add custom signatures to the list. The list of signatures is updated if needed whenever you install a content update.

**Network IPS signatures**

Network IPS 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.

These signatures:

- Protect systems located downstream in a network segment.
- Protect servers and the systems that connect to them.
• Protect against network denial-of-service attacks and bandwidth-oriented attacks that deny or degrade network traffic.

Host Intrusion Prevention contains a default list of a small number of network IPS signatures for Windows platforms. You can edit the severity level, log status, and client rule creation setting of these signatures, but you cannot presently add custom network signatures. The list of signatures is updated if needed whenever you install a content update.

Behavioral rules

Behavioral rules block zero-day attacks and enforce proper operating system and application behavior. Heuristic behavioral rules define a profile of legitimate activity. Activity not matching these rules is considered suspicious and triggers a response. For example, a behavioral rule might state that only a web server process can access HTML files. If any other process attempts to access HTML files, action is taken. This type of protection, called application shielding and enveloping, prevents compromise of applications and their data and prevents applications from being used to attack other applications.

In addition, behavioral rules block buffer overflow exploits, preventing code execution resulting from a buffer overflow attack, one of the most common methods of attacking servers and desktops.

Reactions

A reaction is what the Host Intrusion Prevention client does when a signature of a specific severity is triggered.

The client reacts in one of three ways:

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

A security policy might state, for example, that when a client recognizes a low-severity signature, it logs the occurrence of that signature and allows the operation to occur; and when it recognizes a high-severity signature, it prevents the operation.

**NOTE:** Logging can be enabled directly on each signature. The IPS Protection policy automatically sets the reaction for signatures depending on severity level.

Exceptions

An exception overrides an activity blocked by the reaction to a signature.

In some cases, behavior that a signature defines as an attack might 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, an operation 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, filtered, and aggregated views. Use these client rules to create new policies or add them to existing policies that you can apply to other clients.
Host Intrusion Prevention clients contain a set 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 server and appear in the Host IPS tab under Reporting.

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

Events from legitimate activity that are false positives 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 any time.

Monitoring events and client exception rules helps determine how to tune the deployment for the most effective IPS protection.

Application protection rules

Application protection rules provide protection for defined and generated lists of processes against buffer overflow by permitting or blocking user-level API hooking.

Buffer overflow protection is generic for Host Intrusion Prevention and is applicable to any process that is hooked. The IPS policy contains a default list of application protection rules for Windows platforms. This list is updated, as needed, whenever you install a content update. You can add network facing and service-based applications to this list automatically if you have enabled the "Automatically include network-facing and service based applications" option in the IPS Options policy.

Events

IPS events are generated when a client reacts to a triggered signature.

Events are logged in the Events tab of the Host IPS tab under Reporting. Administrators can view and monitor these events to 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.

NOTE: The Host Intrusion Prevention client aggregates events so not all events are sent to the ePO server. This prevents numerous events that happen within 20 seconds of each other from being repeatedly sent to the server. If an event reoccurs after 20 seconds, an additional event is reported. Administrators can view all events on the Host IPS tab under Reporting in the ePO console or on the client system.

Enable IPS protection

The IPS Options policy determines how IPS protection is applied. It offers options for Windows and non-Windows platforms.

For all platforms

These options are available for clients on all platforms:

- **Host IPS enabled** — Select to turn on IPS protection through the enforcement of host IPS rules.

  NOTE: This control is also available directly on the client.
• **Adaptive mode enabled (rules are learned automatically)** — Select to enable adaptive mode, where clients create exception rules automatically to allow blocked behavior. Use only temporarily while tuning a deployment.

   **NOTE:** This control is also available directly on the client.

• **Retain existing client rules when this policy is enforced** — Select to allow clients to keep exception rules created on the client, either automatically with adaptive mode or manually on a Windows client, when this policy is enforced.

**For Windows platforms only**

These options are available for clients on Windows platforms only:

• **Network IPS enabled** — Select to enforce network IPS rules. This option is available independently from the application of host IPS rules.

• **Automatically block network intruders** — Select this option to block incoming and outgoing traffic on a host until it is manually removed from a blocked list on the client for the number of minutes indicated. Available only if Network IPS is enabled.

   **NOTE:** These controls are also available directly on the client.

• **Retain blocked hosts** — Select to allow a client to block a host IP address until the parameters set under "Automatically block network intruders." If not selected, the host is blocked only until the next policy enforcement.

• **Automatically include network-facing and service-based applications in the application protection list** — Select to allow a client to add high-risk applications automatically to the list of protected applications in the IPS Rules policy.

• **Startup IPS protection enabled** — Select to apply a hard-coded set of file and registry protection rules until the Host IPS service has started on the client.

**Policy selections**

This policy category contains a preconfigured policy, and an editable My Default policy, based on the McAfee Default policy. You can view and duplicate preconfigured policies; you can, create, edit, rename, duplicate, delete, and export custom policies.

The preconfigured policy has these settings:

**McAfee Default**

Host IPS and Network IPS protection is disabled, and these options are are selected to be applied when IPS protection is enabled:

• Automatically block network intruders for 10 minutes (Windows only)

• Retain blocked hosts (Windows only)

• Retain client rules

**TIP:** To activate IPS protection on client systems, the Host Intrusion Prevention administrator must first enable the Host IPS and Network IPS options in this policy, and then apply the policy to client systems. IPS protection on client systems is not automatic as in earlier versions of the product.

**Configuring the IPS Options policy**

Configure settings in this policy to turn IPS protection on and off or apply adaptive mode.
Task
For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog and select Host Intrusion Prevention:IPS in the Product list and IPS Options in the Category list. The list of policies appears.

2. In the IPS Options policy list, click Edit under Actions to change the settings for a custom policy.

   NOTE: For editable policies, other options include: Rename, Duplicate, Delete, and Export. For non-editable policies, options include View and Duplicate.

3. In the IPS Options page that appears, make any needed changes, including status, startup, and network IPS settings, then click Save.

Set the reaction for IPS signatures

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** — Signatures 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** — Signatures 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** — 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** — Signatures 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 severity 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.

Policy selections

This policy category contains six preconfigured policies and an editable My Default policy, based on the McAfee Default policy. You can view and duplicate preconfigured policies; you can, create, edit, rename, duplicate, delete, and export custom policies.

Preconfigured policies include:

<table>
<thead>
<tr>
<th>Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Protection (McAfee Default)</td>
<td>Prevent high-severity signatures and ignore the rest.</td>
</tr>
<tr>
<td>Enhanced Protection</td>
<td>Prevent high- and medium-severity signatures and ignore the rest.</td>
</tr>
</tbody>
</table>
**Function Name** | **Function**
--- | ---
Maximum Protection | Prevent high-, medium-, and low-severity signatures and log the rest.
Prepare for Enhanced Protection | Prevent high-severity signatures, log medium-severity signatures, and ignore the rest.
Prepare for Maximum Protection | Prevent high- and medium-severity signatures, log low-severity signatures, and ignore the rest.
Warning | Log high-severity signatures and ignore the rest.

### Configuring the IPS Protection policy

Configure settings in this policy to set the protective reactions for signatures of a particular severity level. These settings instruct clients what to do when an attack or suspicious behavior is detected.

**Task**
For option definitions, click ? in the interface.

1. Click **Menu | Policy | Policy Catalog** and select **Host Intrusion Prevention: IPS** in the **Product** list and **IPS Protection** in the **Category** list.
2. In the **IPS Protection** policy list that appears, click **Edit** under **Actions** to change the settings for a custom policy.
   
   **NOTE:** For editable policies, other options include Rename, Duplicate, Delete, and Export. For non-editable policies, options include View and Duplicate.

3. In the **IPS Protection** page that appears, make any needed changes, then click **Save**.

### Define IPS protection

The IPS Rules policy applies intrusion prevention safeguards. This policy is a multiple-instance policy that can have multiple instances assigned.

Each IPS Rules policy contains configurable details on:

- Signatures
- Application Protection Rules
- Exception Rules

You also need to go to the Host IPS page under Reporting to work with:

- IPS Events
- IPS Client Rules

### Policy selections

This policy category contains a preconfigured default policy, which provides basic IPS protection. You can view and duplicate the preconfigured policy; you can edit, rename, duplicate, delete, and export custom policies you create. You can also assign more than one instance of the policy for a union of various policy rules.
Configuring the IPS Rules policy

Configure settings in this policy to define signatures, applications protection rules, and exceptions.

**Task**

For option definitions, click `?` in the interface.

1. Click **Menu | Policy | Policy Catalog** and select **Host Intrusion Prevention: IPS** in the **Product** list and **IPSRules** in the **Category** list. The list of policies appears.

2. In the **IPSRules** policy list, click **Edit** under **Actions** to change the settings for a custom policy.

   **NOTE:** For editable policies, other options include: Rename, Duplicate, Delete, and Export. For non-editable policies, options include View and Duplicate.

3. In the **IPSRules** page that appears, make any needed changes, then click **Save**. See *Configuring IPS signatures*, *Configuring IPS application protection rules*, and *Configuring IPS exceptions* for details.

Assigning multiple instances of the policy

Assigning one or more instances of the policy to a group or system in the ePolicy Orchestrator System Tree provides for single policy multi-purpose protection.

The IPS Rules policy and the Trusted Applications policy are multiple-instance policies that can have more than one instance assigned. A multiple-instance policy can be useful for an IIS Server, for example, where 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. When assigning multiple instances, you are assigning a union of all the elements in each instance of the policy.

**NOTE:** The McAfee Default policy for both IPS Rules and Trusted Applications are updated when content is update. McAfee recommends that these two policies always be applied to make sure protection as up to date as possible.

For the policies that have multiple instances, an Effective Policy link appears to provide a view of the details of the combined policy instances.

**Task**

For option definitions, click `?` in the interface.

1. Click **Menu | Systems | System Tree** and select a group in the System Tree.

   **NOTE:** For a single system, select a group in the System Tree that contains the system, then on the **Systems** tab, select the system and select **Actions | Agent | Modify Policies on a Single System**.

2. Under Assigned Policies, select **Host Intrusion Prevention 8.0 : IPS/General** in the **Product** list, and for **IPSRules/TrustedApplications** click **Edit Assignments**.

3. On the **Policy Assignment** page, click **New Policy Instance**, and select a policy from the **Assigned Polices** list for the additional policy instance. To view the effective or combined effect of multiple instance rule sets, click **View Effective Policy**.

4. Click **Save** to save all changes.
FAQ — Multiple-instance policies

Host Intrusion Prevention offers two multiple-instance policies: IPS Rules and Trusted Applications. These policies allow the application of more than one policy concurrently on a single client. All other policies are single-instance policies.

The McAfee Default versions of these policies are automatically updated each time Host Intrusion Prevention security content is updated. For this reason, these policies always need to be assigned to clients to ensure that security content updates are applied. When more than one instance is applied, what results is a union of all the instances, called the effective policy.

How can I use multi-slot policy assignment to streamline my deployment?

First, define groups of users for the deployment that have an essential property in common that dictates what resources need to be protected and what resources need exceptions to work properly. This property could be based on:

- Department — Each department should require protection of a unique set of resources and exceptions for a unique set of business activities.
- Location — Each location may have its own unique security standards or unique set of resources that need to be protected, and exceptions required for business activity.
- Computer type — Each type of computer (laptops, workstations, servers) might have a unique set of applications that need to be protected but also allowed to perform essential business functions.

Next, protect resources and create exceptions and trusted applications for each group. You can use adaptive mode to determine which resources to protect or trust for a given group. After this, create instances of IPS Rules and Trusted Applications policies for each group of users (one IPS Rules policy for a particular department, one for a particular location, and one for a particular computer type), then apply the appropriate instance. Without a multiple-instance IPS Rules policy, a combination of three departments, three locations, and three computer types would require 27 policies; with the multiple-instance approach, only nine are needed.

But rules in different assigned policies contradict each other! How is the effective policy calculated?

It is possible that a rule in one instance has settings that contradict those for the same rule in another policy instance. Host IPS has rules for handling these conflicts in establishing the total effective policy.

For IPS Rules:

- The effective severity for a signature is the highest customized severity. The precedence is: High, Medium, Low, Information, Disabled. If the severity is not customized, the default value is applied.
- The effective log status for a signature is the customized log status. If customized in two or more applied IPS Rules policies, enabled customized log status takes precedence over disabled. If the log status is not customized, the default value is applied.
- The effective client rules setting for a signature is the customized setting. If customized in two or more assigned IPS Rules policies, enabled customized client rules takes precedence over disabled. If the client rules setting is not customized, the default value is applied.
- The effective set of exceptions is the union of all applied exceptions.

For Trusted Applications:

- The effective set of Trusted Applications is the union of all Trusted Applications.
• Marking an application as Trusted for IPS or Firewall takes precedence even if the same application is not marked as Trusted for that feature in another assigned Trusted Applications policy.

How IPS signatures work

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** — 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** — 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 might want to prevent those signatures after fine-tuning.

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

• **Information** — 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 types of signatures:

• **Host IPS signatures** — Default host intrusion prevention signatures.

• **Custom IPS signatures** — Custom host intrusion prevention signatures that you create.

• **Network IPS signatures** — Default network intrusion prevention signatures.

Host IPS signatures

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

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

When triggered, host-based signatures generate an IPS event that appears in the Events tab of the Host IPS tab under Reporting.

Custom IPS signatures

Custom signatures are host-based signatures that you can create for protection beyond the default protection. For example, when you create a new folder with important files, you can create a custom signature to protect it.

**NOTE:** You cannot create network-based custom signatures.
Network IPS signatures

Network-based intrusion prevention signatures detect and prevent known network-based attacks that arrive on the host system. They appear in the same list of signatures as the host-based signatures.

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

You can create exceptions for network-based signatures; however, you cannot specify any additional parameter attributes such as operating system user or process name. Advanced details contain 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 Events tab and exhibit the same behavior as host-based events.

To work with signatures, click the Signatures tab in the IPS Rules policy.

Configuring IPS signatures

Edit default signatures, add custom signatures, and move signatures to another policy from the Signatures tab of the IPS Rules policy.

Task

For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog and select Host Intrusion Prevention: IPS in the Product list and IPS Rules in the Category list. The list of policies appears.

2. Under Actions, click Edit to make changes on the IPS Rules page, then click the Signatures tab.

3. Do any of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find a signature in the list</td>
<td>Use the filters at the top of the signatures list. You can filter on signature severity, type, platform, log status, whether client rules are allowed, or specific text that includes signature name, notes, or content version. Click Clear to remove filter settings.</td>
</tr>
</tbody>
</table>

Edit a signature

Under Actions, click Edit.

- If the signature is a default signature, you can modify the Severity Level, Client Rules, or Log Status settings, and enter notes in the Note box to document the change. Click OK to save any modifications. Edited default signatures can be reverted to their default settings by clicking Revert under Actions.

  NOTE: When you edit a signature and save the change, the signature is resorted in the list. As a result, you might need to search the list to find the edited signature.

- If the signature is a custom signature, modify the Severity Level, Client Rules, Log Status or Description settings, and enter notes in the Note box to document the change. Click OK to save any modifications.

  NOTE: You can make changes to several signatures at once, by selecting the signatures and clicking Edit.
To... | Do this...
---|---
Multiple. In the page that appears, select the settings for the three editable items, then click **OK**.
Add a signature | Click **New** or **New (Wizard)**.
Delete a custom signature | Under **Actions**, click **Delete**.
**NOTE:** Only custom signatures can be deleted.
Copy a signature to another policy | Select a signature and click **Copy To** to copy it to another policy. Indicate the policy to which to copy the signature and click **OK**.
**NOTE:** You can copy several signatures at one time by selecting all the signatures before clicking **Copy To**.

4 Click **Save** to save any changes.

### Creating custom signatures

Create custom host intrusion prevention signatures from the Signatures tab of the IPS Rules policy to protect specific operations not covered by default signatures.

**Task**

For option definitions, click ? in the interface.

1. On the IPS Rules policy **Signatures** tab, click **New**. A blank **Signature** page appears.
2. On the signature’s **IPS Signature** tab, type a name (required) and select the platform, severity level, log status, and whether to allow the creation of client rules. For severity level, client rules, and log status, select the checkbox to change the default values.
3. On the **Description** tab, type a description of what the signature is protecting. This description appears in the **IPS Event** when the signature is triggered.
4. On the **Subrules** tab, select **New Standard Sub-Rule** or **New Expert Subrule** to create a rule.

<table>
<thead>
<tr>
<th>Standard method</th>
<th>Expert method</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Standard method limits the number of types you can include in the signature rule.</td>
<td>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. Before writing a rule, make sure you understand rule syntax.</td>
</tr>
</tbody>
</table>

1. Type a name for the signature (required) and choose a rule class type. Options include: Files, Hook, HTTP, Program, Registry, Services, and SQL.
2. Specify the class operations that are **blocked** and will trigger the signature.
3. Indicate whether to include or exclude a particular parameter, what the parameter is and its value.
4. Include an executable as a parameter with information on at least one of these four values:

1. Type the rule syntax for the signatures, which can include a name for the rule. Use ANSI format and TCL syntax.
2. Click **OK** and the rule is added to the list at the top of the Subrule tab. The rule is compiled and the syntax is verified. If the rule fails verification, a dialog box describing the error appears. Fix the error and verify the rule again.
Creating custom signatures with a wizard

Use the custom signature wizard to simplify creating new signatures.

NOTE: Signatures created with the wizard do not offer any flexibility for the operations that the signature is protecting because you cannot change, add, or delete operations.

Task
For option definitions, click ? in the interface.

1 On the IPS Rules Signatures tab, click New (Wizard).
2 On the Basic Information tab, type a name and select the platform, severity level, log status, and whether to allow the creation of client rules. Click Next to continue.
3 On the Description tab, type a description of what the signature is protecting. This description appears in the IPS Event when the signature is triggered.
4 On the Rule Definition tab, select the item to protect against modifications and enter details.
5 Click OK.

FAQ — Use of wildcards in IPS Rules

Host IPS Rules permits the use of wildcards when entering values in certain fields.

Which wildcards can I use for path and address values?

For paths of files, registry keys, executables, and URLs, use these wildcards:

<table>
<thead>
<tr>
<th>Character</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (question mark)</td>
<td>A single character.</td>
</tr>
<tr>
<td>* (one asterisk)</td>
<td>Multiple characters, excluding / and . Use to match the root-level contents of a folder with no subfolders.</td>
</tr>
<tr>
<td>** (two asterisks)</td>
<td>Multiple characters, including / and .</td>
</tr>
<tr>
<td></td>
<td>Wildcard escape.</td>
</tr>
<tr>
<td></td>
<td>NOTE: For ** the escape is</td>
</tr>
</tbody>
</table>
Which wildcards can I use for all other values?

For values that normally do not contain path information with slashes, use these wildcards:

<table>
<thead>
<tr>
<th>Character</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (question mark)</td>
<td>A single character.</td>
</tr>
<tr>
<td>* (one asterisk)</td>
<td>Multiple characters, including / and .</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Which wildcards can I use for signature expert subrule values?

For all values when creating a subrule using the expert method:

<table>
<thead>
<tr>
<th>Character</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (question mark)</td>
<td>A single character.</td>
</tr>
<tr>
<td>* (one asterisk)</td>
<td>Multiple characters, including / and . Example: files { Include &quot;C:*.txt&quot; }</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. Example: files { Include &quot;C:\test\&amp;.txt&quot; }</td>
</tr>
<tr>
<td>! (exclamation point)</td>
<td>Wildcard escape. Example: files { Include &quot;C:\test\yahoo!*.txt&quot; }</td>
</tr>
</tbody>
</table>

How IPS application protection rules work

Application protection rules control which processes receive generic buffer overflow protection from Host Intrusion Prevention. These rules permit or block user-level API hooking for defined and generated lists of processes. Kernel-level file and registry hooking are not affected. Only processes in the list with the inclusion status of included receive the buffer overflow protection.

Host Intrusion Prevention provides a static list of processes that are permitted or blocked. This list is updated with content update releases that apply in the McAfee Default IPS Rules policy. In addition, processes that are permitted to hook are added dynamically to the list when process analysis is enabled. This analysis is performed under these circumstances:

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

**NOTE:** For the dynamic update of the list, the IPS Options policy option to "automatically include network-facing and service-based applications in the application protection list" must be selected. This option implicitly includes all Windows services and applications that listen on network ports.

This analysis involves checking first if the process is excluded from the Application Protection list. If not, it checks whether the process is included in the Application Protection list. If not, the process is analyzed to see if it listens on a network port or runs as a service. If not, hooking
is blocked and the process is not protected; if it listens on a port or runs as a service, hooking is permitted and the process is protected.

Figure 1: 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 user interface to retrieve the list of currently hooked processes, which is updated whenever a process is hooked or unhooked. A hooked process becomes unhooked if the server 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’s not already hooked, that process is hooked. If the lists indicate that a process should not be hooked and it is already hooked, that process is 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 static list of all hooked application processes.

NOTE: To prevent injection of a DLL into an executable when using hook:set_windows_hook, include the executable in the Application Protection List.

**Configuring IPS application protection rules**

Edit, add, and delete rules and move rules to another policy from the Application Protection Rules tab of the IPS Rules policy.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog and select Host Intrusion Prevention: IPS in the Product list and IPS Rules in the Category list. The list of policies appears.
2. Under Actions, click Edit to make changes on the IPS Rules page, then click the Application Protection Rules tab.
3. Perform any of the following operations:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find an application rule in the list</td>
<td>Use the filters at the top of the application list. You can filter on rule status, inclusion, or specific text that includes process name, process path, or computer name. Click Clear to remove filter settings.</td>
</tr>
<tr>
<td>Edit an application rule</td>
<td>Under Actions, click Edit.</td>
</tr>
<tr>
<td>Add an application rule</td>
<td>Click New.</td>
</tr>
<tr>
<td>Delete an application rule</td>
<td>Under Actions, click Delete.</td>
</tr>
<tr>
<td>Copy an application rule to another policy</td>
<td>Select a rule and click Copy To to copy it to another policy. Indicate the policy to which to copy the rule and click OK. NOTE: You can copy several rules at one time by selecting all the rules before clicking Copy To.</td>
</tr>
</tbody>
</table>

4. Click Save to save any changes.

**Creating application protection rules**

If the IPS Rules policy does not have an application protection rule that you need in your environment, you can create one.

**Task**

For option definitions, click ? in the interface.

1. On the IPS Rules policy Application Protection Rules tab, do one of the following:
• Click New. A blank Application page appears.

• Select a rule and click Duplicate. After naming and saving the new rule, click Edit.

2 Enter the name (required), status, whether the application rule is included in the protection list, and the executables to which you want to apply the rule.

NOTE: You can add an existing executable from the Host IPS Catalog by clicking Add From Catalog. For details on the catalog, see How the Host IPS catalog works under Configuring Firewall Policies.

3 Click Save.

How IPS exceptions work

Sometimes behavior that would be interpreted as an attack can 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.

Exceptions enable you to reduce false positive alerts, minimize needless data flowing to the console, and ensure 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 might be modifying an application not normally associated with email, 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 email, for example, saving a file with Outlook.exe, you need to create an exception that allows this action.

TIP: If you create a custom signature that prevents modification of files (editing, renaming, deleting) in a particular folder, but you want to allow a single application to make modifications, create an exception that would allow the application to make changes to the files. Alternatively, you could add in the custom signature's subrule the parameter with the application set to Exclude.

Configuring IPS exceptions

Edit, add, and delete exceptions and move exceptions to another policy from the Exceptions tab of the IPS Rules policy.

Task

For option definitions, click ? in the interface.

1 Click Menu | Policy | Policy Catalog and select Host Intrusion Prevention: IPS in the Product list and IPS Rules in the Category list. The list of policies appears.

2 Under Actions, click Edit to make changes on the IPS Rules page, then click the Exception Rules tab.

3 Perform any of the following operations:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find an exception rule in the list</td>
<td>Use the filters at the top of the exception list. You can filter on rule status, modified date, or specific text that includes rule or notes text. Click Clear to remove filter settings.</td>
</tr>
</tbody>
</table>
To... | Do this...
---|---
Edit an exception rule | Under Actions, click Edit.
Add an exception rule | Click New.
Delete an exception rule | Under Actions, click Delete.
Copy an exception rule to another policy | Select a rule and click Copy To to copy it to another policy. Indicate the policy to which to copy the rule and click OK. 
**NOTE:** You can copy several rules at one time by selecting all the rules before clicking Copy To.

4 Click **Save** to save changes.

Creating exception rules
To allow behavior prevented by a signature, create an exception for that signature. This can entail defining exception parameters and values. See *Writing Custom Signatures and Exceptions* for details on this aspect.

**Task**
For option definitions, click ? in the interface.

1 On the IPS Rule policy **Exception Rules** tab, click New.
2 Name the exception, be sure it is enabled, then include the signatures to which the exception applies.
3 Set executables, parameters, or Domain groups that play a role as a behavioral exception to the signature.
4 Click **Save**.

Monitor IPS events
An IPS event is triggered when a security violation, as defined by a signature, is detected and reported to the ePO server.

The IPS event appears on the Events tab of the Host IPS tab (or the Event Log tab along with all the other events for all the other products that ePolicy Orchestrator is managing) under Reporting with one of four severity level criteria: High, Medium, Low, and Information.

**NOTE:** When two events are triggered by the same operation, the highest signature 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** — Rules that override a signature rule.
- **Trusted Applications** — Applications that are labeled trusted whose operations might otherwise be blocked by a signature.

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

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 a trusted application rule for that behavior.

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

For example, when testing clients, you might find clients recognizing the signature email access. Typically, an event triggered by this signature is cause for alarm. Hackers can install Trojan applications that use TCP/IP Port 25 typically reserved for email applications, and this action would be detected by the TCP/IP Port 25 Activity (SMTP) signature. On the other hand, normal email 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 email, like Notepad.exe, you might reasonably suspect that a Trojan was planted. If the process initiating the event is normally responsible for sending email (for example, Outlook), create an exception to that event.

You might also find, for example, that a number of clients are triggering the signature startup programs, which indicates 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 starts up, recognition of this signature might indicate that someone is attempting to tamper with the system. Or it might indicate something as benign as one of your employees installing WinZip on their computer. The installation of WinZip adds a value to the Run registry key.

To eliminate the triggering of events every time someone installs authorized software, you create exceptions for these events.

Filtering and aggregating events

Applying filters generates a list of events that satisfies all of the variables defined in the filter criteria. The result is a list of events that includes all of the criteria. Aggregating events generates a list of events grouped by the value associated with each of the variables selected in the "Select columns to aggregate" dialog box. The result is a list of events displayed in groups and sorted by the value associated with the selected variables.

Managing IPS events

Viewing IPS events coming from clients and creating exceptions or trusted applications from them helps tune and tighten security.

NOTE: IPS events also appear on the Event Log tab under Reporting combined with all other events for all systems. Access to the events tabs under Reporting requires additional permission sets, including view permissions for Event Log, Systems, and System Tree access.

Task

For option definitions, click ? in the interface.

1. Click Menu | Reporting | Host IPS 8.0, then click Events.
   
2. Select the group in the System Tree for which you want to display IPS events. All events associated with the group appear. By default, not all events are displayed. Only events over the last 30 days appear.
3  Determine how you want to view the list of events:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select columns to display</td>
<td>Select Options</td>
</tr>
<tr>
<td>Sort by a column</td>
<td>Click the column header.</td>
</tr>
<tr>
<td>Filter for groups</td>
<td>From the Filter menu, select This Group Only or This Group and All Subgroups.</td>
</tr>
<tr>
<td>Filter for events criteria</td>
<td>Select event type, marked status (read, unread, hidden, hidden), severity level, or date of creation. Click Clear to remove filter settings.</td>
</tr>
<tr>
<td>Aggregate exceptions</td>
<td>Click Aggregate, select the criteria on which to aggregate events, then click OK. Click Clear to remove aggregation settings.</td>
</tr>
<tr>
<td>View details of the event</td>
<td>Click the event. The Event Log details page appears.</td>
</tr>
</tbody>
</table>

4  Mark events to facilitate their filtering and tracking: select the checkbox of one or more events, then select the appropriate command.

<table>
<thead>
<tr>
<th>Select...</th>
<th>To...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Mark Read</td>
</tr>
<tr>
<td>Actions</td>
<td>Mark Unread</td>
</tr>
<tr>
<td>Actions</td>
<td>Mark Hidden</td>
</tr>
<tr>
<td>Actions</td>
<td>Mark Unhidden</td>
</tr>
</tbody>
</table>

5  Create an exception or trusted application rule. Select an event and select Actions | New Exception to create an exception; or select Actions | New Trusted Application to create an application rule. See Creating an exception from an event or Creating a trusted application from an event for details.

### Creating an exception from an event

For an event that appears under Reporting in the Host IPS 8.0 Events tab or on the Event Log page, you have the option of creating an exception.

**Task**

For option definitions, click ? in the interface.

1  Select the checkbox of the event for which you want to create an exception.

2  Select Actions | New Exception.

3  In the dialog box that appears, select a destination IPS Rules policy and click OK. The exception is created and added automatically to the bottom of the list of exceptions of the destination IPS Rules policy.
Creating a trusted application from an event

For an event that appears under Reporting in the Host IPS 8.0 Events tab or on the Event Log page, you have the option of creating a trusted application.

**Task**

For option definitions, click ? in the interface.

1. Select the checkbox of the event for which you want to create a trusted application.
2. Select **Actions | New Trusted Application**.
3. In the dialog box that appears, select a destination Trusted Application policy and click **OK**.

The exception is created and added automatically to the bottom of the list of exceptions of the destination Trusted Application policy. From there, you can view or edit details of the new application.

Monitor IPS client rules

You need to periodically analyze IPS client rules created automatically when clients are in adaptive mode, or manually on the client whenever the Client UI policy option allows manual creation of client rules.

IPS client rules are exceptions created on a client to allow a functionality blocked by a signature. Pay particular attention to exceptions to high severity signatures, as these might indicate a serious issue or simply a false positive. If a false positive, move the exception to an IPS Rules policy or adjust the severity of the signature.

**NOTE:** Access to IPS Client Rules on the Host IPS tab under Reporting requires additional permissions other than that for Host Intrusion Prevention IPS, including view permissions for Event Log, Systems, and System Tree access.

You can sort, filter, and aggregate the exceptions and view their details. You can then promote some or all of the client exceptions to a particular IPS Rules policy to reduce false positives for a particular system environment.

Use the aggregation feature 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 allows for easily finding IPS protection trouble spots on clients.

Managing IPS client rules

Viewing IPS client rules created automatically in adaptive mode or manually on a client and moving them to an IPS Rules or Trusted Application policy allows for easy tuning of IPS protection.

**NOTE:** Access to IPS Client Rules on the Host IPS tab under Reporting requires additional permissions other than that for Host Intrusion Prevention IPS, including view permissions for Event Log, Systems, and System Tree access.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Reporting | Host IPS 8.0**, then click **IPS Client Rules**.
2. Select the group in the System Tree for which you want to display client rules.
3  Determine how you want to view the list of client exceptions:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort by a column</td>
<td>Click the column header.</td>
</tr>
<tr>
<td>Filter for groups</td>
<td>From the Filter menu select This Group Only or This Group and All Subgroups.</td>
</tr>
<tr>
<td>Filter for exception criteria</td>
<td>Select time criteria; type process path, process name, user name, computer name, or signature ID in the search text box and press Return. Click Clear to remove filter settings.</td>
</tr>
<tr>
<td>Aggregate exceptions</td>
<td>Click Aggregate, select the criteria on which to aggregate exceptions, then click OK. Click Clear to remove aggregation settings.</td>
</tr>
</tbody>
</table>

4  To move exceptions to a policy, select one or more exceptions in the list, click Create Exception, then indicate the policy to which to move the exceptions.
Configuring Firewall Policies

The Host Intrusion Prevention firewall policies turn protection on and off and provide rules to stop network intrusions that could compromise data, applications, or the operating system.

Contents
- Overview of Firewall policies
- Enable firewall protection
- Define firewall protection

Overview of Firewall policies

The Host Intrusion Prevention firewall feature provides security by filtering traffic into and out of networked systems running Windows. Stateful filtering and packet inspection identify packets for different types of connections, and hold in memory the attributes of network connections from start-to-finish of transmission.

A Host IPS catalog simplifies rule creation by allowing you to add existing rules, groups, network options, applications, executables, and locations from the catalog to new and existing firewall rules and groups. It also allows the addition of these elements to the catalog either on an item-by-item basis or by batch process.

Available policies

There are three Firewall policies:

Firewall Options — Enables firewall protection. It turns firewall protection on and off, defines stateful firewall settings, and enables special firewall-specific protection such as allowing outgoing traffic only until the firewall service has started, and blocking IP spoofing and malicious traffic.

Firewall Rules — Defines firewall protection. It consists of a set of rules that defines what traffic is allowed and what is blocked. You can define rules broadly (for example, all IP traffic) or narrowly (for example, identifying a specific application or service), with various network, transport, application, and schedule options. You can group rules according to a work function, service, or application for easier management. Like rules, rule groups can be defined by network, transport, application, schedule, and location options.

Firewall DNS Blocking — Defines a set of domain name patterns, which can include wildcards, that are to be blocked. When applied, this policy dynamically adds a rule near the top of the firewall rules list that prevents resolving the IP address of the specified domain.
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 an action to 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 the list. If, however, the traffic does not meet the first rule’s conditions, Host Intrusion Prevention looks at the next rule in the list. It works its way down through the firewall rules 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, the user is prompted for an action to be taken. If adaptive mode is activated, an allow rule is created for the traffic. Sometimes the intercepted traffic matches more than one rule in the list. In this case, precedence means that Host Intrusion Prevention applies only the first matching rule in the list.

Best practices

When you create or customize a firewall rules policy, place the more specific rules at the top of the list, and the more general rules at the bottom. This ensures that Host Intrusion Prevention filters traffic appropriately.

For example, to allow all HTTP requests except from a specific address (for example, IP address 10.10.10.1), you need to create two rules:

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

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

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

Firewall protocols

Firewall protection works at several layers of the network architecture, where different criteria are used to restrict network traffic. This network architecture is built on the Transmission Control Protocol/Internet Protocol (TCP/IP) suite.

- **Link Layer**
  The link layer protocol describes the media access control (MAC) method, and some minor error-detection facilities.
  Ethernet LAN (802.3), wireless Wi-Fi (802.11x), and virtual LAN (VPN) are in this layer. Both firewall rules and groups distinguish between wired, wireless, and virtual links.

- **Network Layer**
  The network layer protocols define whole-network addressing schemes, routing, and network control schemes.
It likewise supports arbitrary non-IP protocols, but cannot detect any network or transport layer parameters for them. At best, this allows the administrator to block or allow these network layer protocols. The numbers associated with the non-IP protocols are based on the Ethernet numbers defined by the Internet Assigned Numbers Authority (IANA), and published at http://www.iana.org/assignments/ethernet-numbers.


**Transport Layers**

IP can be used as the network protocol for a number of different transport protocols. In practice, four are commonly used: TCP, the User Datagram Protocol (UDP), the Internet Control Message Protocol version 4 and version 6 (ICMPv4 and ICMPv6).

**TCP**

TCP is a connection-oriented reliable transport protocol. It guarantees that the data contained in network packets are delivered reliably, and in order. It also controls the rate at which data is received and transmitted. This entails a certain amount of overhead, and makes the timing of TCP operations unpredictable when network conditions are sub-optimal.

TCP is the transport layer for the vast majority of application protocols. HTTP, FTP, SMTP, RDP, SSH, POP, and IMAP all use TCP.

TCP multiplexes between application-layer protocols using the concept of “ports.” Each TCP packet contains a source and destination port number, from 0 to 65535. Usually, the server end of a TCP connection listens for connections on a fixed port.

Ports 0 to 1023 are reserved as “well-known ports.” Numbers in this range are usually assigned to protocols by the IANA (www.iana.org/assignments/protocol-numbers), and most operating systems require a process to have special permissions to listen on one of these ports.

Firewall rules are generally constructed to block certain ports and allow others, thereby limiting the activities that can occur on the network.

**UDP**

UDP is a connectionless best-effort transport protocol. It makes no guarantees about reliability or packet order, and lacks flow control features. In practice, it has some very desirable properties for certain classes of traffic.

UDP is often used as a transport protocol for performance-critical applications (which might implement some of the reliability and packet-ordering features of TCP in the application protocol), and in real-time multi-media applications, where a dropped packet causes only a momentary glitch in the data stream, and is thus more acceptable than a stream that has to stop and wait for re-transmission. IP telephony and videoconferencing software often uses UDP, as do some multi-player video games.

The UDP multiplexing scheme is identical to that of TCP: each datagram has a source and destination port, ranging from 0 to 65535.

**ICMP**

ICMP is used as an out-of-band communication channel between IP hosts. It is useful in troubleshooting, and necessary to the proper function of an IP network, as it is the error reporting mechanism.

IPv4 and IPv6 have separate, unrelated ICMP protocol variants. ICMPv4 is often referred to as simply ICMP.
ICMPv6 is additionally important in an IPv6 network, as it is used for several critical tasks, such as neighbor discovery (which ARP handles in an IPv4 network). Users are strongly discouraged from blocking ICMPv6 traffic if IPv6 is supported on their network.

Instead of port numbers, both versions of ICMP define a handful of "message types." "Echo Request" and "Echo Reply" are used for ping. "Destination Unreachable" messages indicate routing failures. ICMP also implements a Traceroute facility, though UDP and TCP can be used for this purpose as well.

Other transport protocols
IP supports well over a hundred other transport protocols, but most are rarely used. Nevertheless, the complete list of IANA-recognized protocols is at least minimally supported. Rules can be created to block or allow traffic over all IP transport protocols, though the firewall does not support any multiplexing mechanism these protocols might use.

Several are used to overlay other types of networks on top of an IP network (network tunneling). Some of these (notably GRE, AH, and ESP) are used for IP encryption and VPNs. IP protocol numbers are listed at www.iana.org/assignments/protocol-numbers.

Common Unsupported Protocols
There are several network protocols that the Host IPS firewall does not support. Traffic belonging to these protocols, usually with an unparsable EtherType, is either always blocked, or always allowed, depending on whether the option "Allow traffic for unsupported protocols" in the Firewall Options policy is selected.

How firewall rule groups work
Group firewall rules for easier management. Rule groups do not affect the way Host Intrusion Prevention handles the rules within them; they are still processed from top to bottom.

Groups are associated with many of the items associated with rules, including network options, transport options, applications, and schedules. In addition to these, groups have location settings, which allow you to make groups location-aware and create connection isolation. The settings for the group are processed before the settings for the rules it contains. If there is any conflict between these, the settings of the group take precedence.

NOTE: If connection isolation on the Location tab is enabled, a group cannot have associated transport options and applications.

Making groups location-aware
Host Intrusion Prevention allows you to make a group and the rules it contains location-aware. The Location tab and the Network Options tab of the group allows you to make the groups network adapter-aware, so that computers with multiple network interfaces can have rules apply that are adapter-specific. After enabling location status and naming the location, parameters for allowed connections can include any or all of the following for each network adapter:

On the Location tab:
- Connection-specific DNS suffix
- Gateway IP
- DHCP IP
- DNS server queried to resolve URLs
- WINS server used
• Registry key
On the Network Options tab:
• Local IP address
• Media type

If two location-aware groups apply to a connection, Host Intrusion Prevention uses normal precedence and processes the first applicable group in its rule list. If no rule in the first group matches, rule processing continues and might match a rule in the next group.

When Host Intrusion Prevention matches a location-aware group’s parameters to an active connection, it applies the rules within the 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.

Note the following:
• If Location status is selected, a location name is required.
• If Local Network 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 must match at least one of the list entries.
• If DHCP Server is selected, the adapter DHCP server IP must match at least one of the list entries.
• If DNS Server List 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.

**Firewall rule group connection isolation**

A connection isolation option is available for groups to prevent undesirable traffic from accessing a designated network. This can be done through other active network interfaces on a computer, such as a wireless adapter connecting to a wi-fi hotspot while a wired adapter is connected to a LAN.

When the Isolate this connection option is selected under a group’s Location settings, and an active Network Interface Card (NIC) matches the group criteria, the only types of traffic
processed are traffic matching allow rules above the group in the firewall rules list, and traffic matching the group criteria. All other traffic is blocked.

**NOTE:** Any group with connection isolation enabled cannot have associated transport options or applications.

Figure 2: Network 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. Group with corporate LAN connection rules
4. Group with VPN connection rules

**Connection isolation on the corporate network**

Connection rules are processed until the group with corporate LAN connection rules is encountered. This group contains these settings:

- Media type = Wired
• Connection-specific DNS suffix = mycompany.com
• Default gateway address
• 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 group. 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 group with VPN connection rules is encountered. This group contains these settings:
• Connection type = virtual
• DNS suffix = 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 group. 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.

How the Host IPS catalog works

The Host IPS catalog simplifies firewall rule and group creation by allowing you to reference existing rules, groups, network addresses, applications, executables, and group location data. In addition, you can reference executables for applications involved in IPS protection.

When referencing a catalog item, you create a dependent link between it and a firewall rule or group. This means a change of the item in the catalog changes it wherever it is used. You can also break the link between the catalog item and a rule or group, to remove the dependency.

The Host IPS Catalog, found in ePolicy Orchestrator under Policy, contains six pages listing previously placed firewall rule and firewall group items. Items can be created individually in the catalog, added by linking to them to ones created in new firewall and rule groups, or imported from xml-format exports of Firewall Rules policies.

The catalog pages include:
• Group — List of firewall groups and properties
• Rule — List of firewall rules and properties
• Application — List of applications that can be referenced in a firewall group or rule
• Executable — List of executables attached to applications that can be referenced in a firewall group or rule or in IPS-related applications
• Network — List of IP addresses that can be referenced in a firewall group or rule
• Location — List of location-specific information for firewall groups

Table 7: Host IPS Catalog as source for items

<table>
<thead>
<tr>
<th>Feature</th>
<th>Policy Item</th>
<th>Policy</th>
<th>Catalog Item</th>
<th>Dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Firewall Rules</td>
<td>Firewall Rule</td>
<td>Rule</td>
<td>Yes</td>
</tr>
<tr>
<td>Firewall</td>
<td>Firewall Rules</td>
<td>Firewall Group</td>
<td>Group</td>
<td>Yes</td>
</tr>
<tr>
<td>Firewall</td>
<td>Firewall Rules</td>
<td>Firewall Group Location</td>
<td>Location</td>
<td>Yes</td>
</tr>
<tr>
<td>Firewall</td>
<td>Firewall Rules</td>
<td>Firewall Rule/Group</td>
<td>Network</td>
<td>Yes</td>
</tr>
<tr>
<td>Firewall</td>
<td>Firewall Rules</td>
<td>Firewall Rule/Group Application</td>
<td>Application</td>
<td>Yes</td>
</tr>
<tr>
<td>Firewall</td>
<td>Firewall Rules</td>
<td>Firewall Rule/Group Application</td>
<td>Executable</td>
<td>Yes</td>
</tr>
<tr>
<td>IPS</td>
<td>IPS Rules</td>
<td>Application Protection Rule</td>
<td>Executable</td>
<td>No</td>
</tr>
<tr>
<td>General</td>
<td>Trusted Applications</td>
<td>Trusted Application</td>
<td>Executable</td>
<td>No</td>
</tr>
</tbody>
</table>

Catalog filters

Each catalog page contains a filter to search for items in the list on the page. Click Hide/Show Filter Options to hide or show the filter, click Set Filter to filter with the criteria entered, click Clear to reset the filter.

Copying from the catalog

When using the Firewall Rule Builder or Firewall Group Builder, click the Add from Catalog button to add the appropriate item from the catalog. This creates a dependent link between the items, which can be broken when required.

Adding to the catalog

You add to the catalog in one of three ways:

• Click New in the catalog page, enter the information, and save the item.

• Click Add to Catalog next to the item when creating or editing rules or groups using the Firewall Rule Builder or Firewall Group Builder.

• Click Import to add previously exported Host IPS catalog data in .xml format.

  **NOTE:** Policy Catalog exports in .xml format are not compatible with the Host IPS Catalog .xml format. This means you cannot export a Firewall Rules policy from the Policy Catalog and import it in to the Host IPS Catalog to populate it with firewall rules data from the policy. To get firewall policy data into the Host IPS Catalog, use the Add to Catalog links.

Firewall stateful packet filtering and inspection

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

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 allow rule, the packet 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, its entry is removed from the state table.
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 the FTP protocol.

**Firewall state table**

A stateful firewall includes 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, the current standard for IP addresses permits addresses 32 bits long, whereas IPv6, a newer standard, permits addresses 128 bits long. IPv6 is already 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.

Note the following about the state table:

- 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.
- When the process ends all entries in the state table associated with a process are deleted.

**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 that any packet matched to a rule in the state table is automatically permitted.
The filtering process includes the following:

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.

   **NOTE:** 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, which secures 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. If the option for FTP inspection has been set with the Firewall Options policy, 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.
With the control channel open, the client communicates with the FTP server. The firewall parses the PORT command in the packet and creates a second entry in the state table to allow the data connection.

When the FTP server is in active mode, it opens the data connection; in passive mode, the client initiates the connection. When the FTP server receives the first data transfer command (LIST), it opens the data connection toward 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 types of protocol connections monitored by the stateful firewall and how they are handled are summarized here.

<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>
</tbody>
</table>
| ICMPv4/v6| Only ICMP Echo Request and Echo Reply message types are tracked.  
  **NOTE:** In contrast to the reliable, connection-oriented TCP protocol, UDP and ICMPv4/v6 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 in the Firewall Options policy.  
  When using IPv6, stateful firewall functionality is supported only on Windows Vista and later platforms. |
| TCP      | TCP protocol works on the S3-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 in 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. |
| DNS      | Query/response matching ensures 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. |
| DHCP     | Query/response matching ensures that return packets are allowed only for legitimate queries, Thus incoming DHCP responses are allowed if:  
  - The connection in the state table has not expired.  
  - The response transaction ID matches the one from the request. |
### Description of handling Protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description of handling</th>
</tr>
</thead>
</table>
| FTP      | • 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.  
• FTP inspection is performed only on the packets that carry new information. Retransmitted packets are ignored.  
• Dynamic rules are created depending on direction (client/server) and mode (active/passive):  
  • 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.  
  • Server FTP Active Mode: the firewall creates a dynamic outgoing rule after parsing the incoming port command.  
  • 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.  
  • Server FTP Passive Mode: the firewall creates a dynamic incoming rule. |

### How learn and adaptive modes affect the firewall

When you enable the firewall, 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 is operating in learn mode or adaptive mode.

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. You can enable learn mode for incoming communication only, for outgoing communication only, or both.

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 more information on using the adaptive mode with the firewall, see [FAQ — Adaptive mode](#) under [Managing Your Protection](#).

For security reasons, when the learn mode or adaptive mode is applied, 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

When adaptive or learn mode is applied with the stateful firewall, the filtering process creates a new rule to handle the incoming packet. This is the filtering process:

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 dropped.
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.

**Firewall client rules**

A client in adaptive or learn mode creates firewall client rules to allow blocked activity. Rules can also be created manually on the client computer. You can track the client rules and view them in a filtered or aggregated view. Use these client rules to create new policies or add them to existing policies.

**Filtering and aggregating rules**

Applying filters generates a list of rules that satisfies all of the variables defined in the filter criteria. The result is a list of rules that includes all of the criteria. Aggregating rules generates a list of rules grouped by the value associated with each of the variables selected in the Select columns to aggregate dialog box. The result is a list of rules displayed in groups and sorted by the value associated with the selected variables.

**Enable firewall protection**

The Firewall Options policy enables firewall protection and provides TrustedSource™ and stateful firewall settings.

**General settings**

These general options are available:

- **Enabled**: Select to make the firewall active, and then select the type of protection:
  - **Regular (default)** — Use this setting when not tuning a deployment.
  - **Adaptive mode** — Select to have rules created automatically to allow traffic. Use only temporarily while tuning a deployment.
  - **Learn mode** — Select to have rules created after input from the user to allow traffic. Select also to allow incoming or outgoing traffic or both. Use only temporarily while tuning a deployment.
  - **Allow traffic for unsupported protocols** — Select to allow all traffic that uses unsupported protocols. With this option disabled, all traffic using unsupported protocols is blocked.
  - **Allow bridged traffic** — Select to allow traffic with a local MAC address that is not the local system’s MAC address but is one of the MAC addresses in the list of VMs that the firewall supports. Use this option to allow traffic through a bridged environment with virtual machines.
  - **Retain existing client rules when this policy is enforced** — Select to allow clients to keep rules created on the client, automatically with adaptive mode, through user interaction with learn mode, or manually on a client, when this policy is enforced.

**Protection settings**

These settings enable special firewall-specific protection:
• **Allow only outgoing traffic until the Host IPS service has started** — Select to allow outgoing traffic but no incoming traffic until the Host IPS firewall service has started on the client.

• **Enable IP spoof protection** — Select to block network traffic from non-local host IP addresses or from local processes that attempt to spoof their IP address.

• **Send events to ePO for TrustedSource violations** — Select to send events to the ePO server if the TrustedSource block threshold setting for incoming or outgoing traffic is matched.

• **Incoming TrustedSource block threshold** — Select from the list the TrustedSource rating at which to block incoming traffic from a network connection. Options include: High Risk, Medium Risk, Unverified, and Do not block.

• **Outgoing TrustedSource block threshold** — Select from the list the TrustedSource rating at which to block outgoing traffic to a network connection. Options include: High Risk, Medium Risk, Unverified, and Do not block.

**Stateful firewall settings**

The stateful firewall settings are available:

• **FTP protocol inspection** — A stateful firewall setting that allows FTP connections to be tracked so that they require only one firewall rule for outgoing FTP client traffic, and one for incoming FTP server traffic. If this option is not selected, FTP connections require an additional rule for incoming FTP client traffic and outgoing FTP server traffic. This should always be selected.

• **TCP connection timeout** — The time in seconds a TCP connection that is not established remains active if no more packets matching the connection are sent or received.

• **UDP and ICMP echo virtual connection timeout** — The time in seconds a UDP or ICMP echo virtual connection remains active if no more packets matching the connection are sent or received. It is reset to its configured value every time a packet that matches the virtual connection is sent or received.

**Policy selections**

This policy category contains one preconfigured policy and an editable My Default policy, based on the McAfee Default policy. You can view and duplicate preconfigured policies, and create, edit, rename, duplicate, delete, and export custom policies.

The preconfigured policy has these settings:

**McAfee Default**

Firewall protection is disabled, and these options are selected to be applied when the firewall is enabled:

• Allow bridged traffic

• Retain client rules

• Enable IP spoof protection

• Use FTP protocol inspection

**Configuring the Firewall Options policy**

Configure settings in this policy to turn firewall protection on and off or apply adaptive or learn mode.
Task
For option definitions, click ? on the page displaying the options.

1. Click Menu | Policy | Policy Catalog and select Host Intrusion Prevention: Firewall in the Product list and Firewall Options in the Category list. The list of policies appears.

2. In the Firewall Options policy list, click Edit under Actions to change the settings for a custom policy.

   NOTE: For editable policies, other options include Rename, Duplicate, Delete, and Export. For non-editable policies, options include View and Duplicate.

3. In the Firewall Options page that appears, change the default settings as needed, then click Save.

FAQ — McAfee TrustedSource and the firewall

Two options in the Firewall Options policy allow you to block incoming and outgoing traffic from a network connection that McAfee TrustedSource™ has rated high risk. This FAQ explains what TrustedSource does and how it affects the firewall.

What is TrustedSource?

TrustedSource is a global Internet reputation intelligence system that determines what is good and bad behavior on the Internet by using real-time analysis of worldwide behavioral and sending patterns for email, web activity, malware, and system-to-system behavior. Using data obtained from the analysis, TrustedSource dynamically calculates reputation scores that represent the level of risk posed to your network when you visit a web page. The result is a database of reputation scores for IP addresses, domains, specific messages, URLs, and images.

How does it work?

When the TrustedSource options are selected, two firewall rules are created: TrustedSource -- Allow Host IPS Service and TrustedSource -- Get Rating. The first rule allows a connection to TrustedSource and the second rule blocks or allows traffic based on the connection’s reputation and the block threshold set.

What do you mean by "reputation"?

For each IP address on the Internet, TrustedSource calculates a reputation value based on sending or hosting behavior and various environmental data that TrustedSource automatically collects, aggregates and correlates from customers and partners about the state of Internet threat landscape. The reputation is expressed in four classes:

- **Minimal Risk (Do Not Block)** — Our analysis indicates this is a legitimate source or destination of content/traffic.

- **Unverified** — Our analysis indicates that this appears to be a legitimate source or destination of content/traffic, but also displays certain properties suggesting that further inspection is necessary.

- **Medium Risk** — Our analysis indicates that this source/destination shows behavior we believe is suspicious and content/traffic to or from it requires special scrutiny.

- **High Risk** — Our analysis indicates that this source/destination does or will send/host potentially malicious content/traffic and we believe it presents a serious risk.
Does it introduce latency? How much?

When TrustedSource is contacted to do a reputation lookup, some latency is inevitable. McAfee has done everything it can to minimize this.

First, a check of reputations is made only when the options are selected. Second, there is an intelligent caching architecture. In normal network usage patterns, most desired connections are resolved by the cache without a live reputation query.

What if the firewall can't reach the TrustedSource servers? Does traffic stop?

If the firewall cannot reach any of the TrustedSource servers, it automatically assigns all applicable connections a default reputation that is allowed and an analysis of the rules that follow continues.

Define firewall protection

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 and a Firewall DNS Blocking policy with the appropriate settings.

Firewall Rules policy selections

The Firewall Rules policy category contains two preconfigured policies and an editable My Default policy, based on the McAfee Default policy. You can view and duplicate the preconfigured policy, and edit, rename, duplicate, delete, and export editable custom policies.

Table 8: Preconfigured Firewall Rules policies

<table>
<thead>
<tr>
<th>Policy</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal (Default)</td>
<td>Use this policy for default minimal protection. It does the following:</td>
</tr>
<tr>
<td></td>
<td>• Blocks any incoming ICMP traffic that an attacker could use to gather information about your computer. Host IPS 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 (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>Typical Corporate Environment</td>
<td>Use this policy as a starting point and combine with the results from applying the adaptive mode to learn and verify any additional rules.</td>
</tr>
<tr>
<td></td>
<td>This policy should generate fewer learned client rules in adaptive mode as compared to existing default firewall policies.</td>
</tr>
<tr>
<td></td>
<td>The policy is full-featured and meets the needs for most organizational firewalls.</td>
</tr>
</tbody>
</table>
Firewall DNS Blocking policy selections

The Firewall DNS Blocking policy contains one preconfigured policy and an editable My Default policy, based on the McAfee Default policy. You can view and duplicate the preconfigured policy, and edit, rename, duplicate, delete, and export editable custom policies.

Configuring the Firewall Rules policy

Configure settings in this policy to define rules for firewall protection.

**TIP:** Do not try to create a policy from scratch. Simply duplicate an existing policy then edit the rules and groups in the policy to meet your needs.

**Task**

For option definitions, click ? on the page displaying the options.

1. Click Menu | Policy | Policy Catalog and select Host Intrusion Prevention: Firewall in the Product list and Firewall Rules in the Category list. The list of policies appears.

2. In the Firewall Rules policy list, click Edit under Actions to change the settings for a custom policy.

   **NOTE:** For editable custom policies, other options include Rename, Duplicate, Delete, and Export. For non-editable policies, options include View and Duplicate.

3. Do any of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a firewall rule</td>
<td>Click New Rule or Add Rule from Catalog. See Creating and editing firewall rules or Using the Host IPS catalog for details.</td>
</tr>
<tr>
<td>Add a firewall group</td>
<td>Click New Group or Add Group from Catalog. See Creating and editing firewall rule groups or Using the Host IPS catalog for details.</td>
</tr>
</tbody>
</table>
   | Perform an action on a single rule or group | • Select the rule or group to display a summary of the item's settings in the right-hand pane.  
   |                                   | • Select the rule or group and click:                                       |
   |                                   |   • Edit under Actions to edit an item.                                    |
   |                                   |   • Add to Catalog under Actions to add the item to the firewall catalog.   |
   |                                   |   • Move Up to move the item up in the list.                              |
   |                                   |   • Move Down to move the item down in the list.                          |
   |                                   |   • Duplicate to make a copy of the item.                                 |
   |                                   |   • Delete to delete the item.                                           |

4. Click Export to export the all the rule and group information in the policy to an xml file. This file can then be imported into the firewall catalog or to another policy.

5. Click Save to save changes.
Creating and editing firewall rules

Edit or add a new firewall rule to the list of rules in a Firewall Rules policy if specific operations are not covered by the default list.

**Task**

For option definitions, click ? on the page displaying the options.

1. On the **Firewall Rules** policy page, click **New Rule** to create a new rule; click **Edit** under **Actions** to edit an existing rule.

2. Enter the appropriate information on each tab, which you access by clicking **Next** or the tab link.

<table>
<thead>
<tr>
<th>On this tab...</th>
<th>Set these options...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Name (required), action, direction, status.</td>
</tr>
<tr>
<td>Network</td>
<td>Network protocol, media type, local and remote networks</td>
</tr>
<tr>
<td>Transport</td>
<td>Transport protocol</td>
</tr>
<tr>
<td>Application</td>
<td>Applications and executables</td>
</tr>
<tr>
<td>Schedule</td>
<td>Status and time settings</td>
</tr>
</tbody>
</table>

3. On the **Summary** tab, review the details of the rule and click **Save**.

Creating and editing firewall rule groups

Create or edit a firewall rule group for a Firewall Rules policy to create a set of rules with a single purpose.

Use a single purpose group with rules to allow, for example, VPN connection. Groups appear in the rule list preceded by an arrow, which can be clicked to show or hide the rules within the group.

**Task**

1. On the **Firewall Rules** policy page, click **New Group** to create a new group; click **Edit** under **Actions** to edit an existing group.

2. Enter the appropriate information on each tab, which you access by clicking **Next** or the tab link.

<table>
<thead>
<tr>
<th>On this tab...</th>
<th>Set these options...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Name (required), direction, status</td>
</tr>
<tr>
<td>Location</td>
<td>Location-aware settings, including connection isolation</td>
</tr>
<tr>
<td>Network</td>
<td>Network protocol, media type (wired, wireless, virtual), local and remote networks</td>
</tr>
<tr>
<td>Transport</td>
<td>Transport protocol</td>
</tr>
<tr>
<td>Application</td>
<td>Applications and executables</td>
</tr>
<tr>
<td>Schedule</td>
<td>Status and time settings, including enabling timed groups</td>
</tr>
</tbody>
</table>

3. On the **Summary** tab, review the details of the group and click **Save**.
4 Create new rules within this group, or move existing rules into it from the firewall rule list or the Host IPS catalog.

Creating connection isolation groups

Create a connection isolation firewall rules group to establish a set of rules that apply only when connecting to a network with particular parameters.

Task

For option definitions, click ? on the page displaying the options.
1 On the Firewall Rules policy page, click New Group or Add Group from Catalog.
2 On the Description tab, type a descriptive name in the Name field.
3 On the Location tab, select Enabled for both Location status and Connection isolation, type a Name for the location, then select a DNS suffix, default gateway, or other criteria for matching.
4 On the Network tab, under Media types, select the type of connection (Wired, Wireless, Virtual) to which to apply the rules in this group.
   NOTE: Transport Options and Applications are not available for connection isolation groups.
5 On the Summary tab, click Save.
6 Create new rules within this group, or move existing rules into it from the firewall rule list or the Host IPS catalog.

Blocking DNS traffic

To refine firewall protection you can create a list of domain name servers that Host IPS blocks by not allowing the resolving of their IP address.

NOTE: Do not use this feature to block fully qualified domains; instead, block the FQDN remote address in a firewall rule.

Task

For option definitions, click ? on the page displaying the options.
1 On the Firewall DNS Blocking policy page, click New Rule to create a new rule; click Edit under Actions to edit an existing rule.
2 Click Add Blocked Domain.
3 In the text box type the name of the domain name server you want to block. Use the wildcards * and ?; for example, *domain.com. One name per entry.
4 Click the add button to add other addresses, click the remove button to delete addresses.
5 Click Save to save any changes.

Using the Host IPS catalog

The Host IPS catalog allows you to add new items or reference existing items for use with the firewall. This task helps you find and edit existing catalog items, create and add new catalog items, or import and export catalog items.
### Task

For option definitions, click ? in the interface.

1. Click **Menu | Policy | Host IPS Catalog**.
2. Under **Item Type** select a catalog item. Choices include: **Group, Rule, Application, Process, Network,** and **Location**.
3. Do any of the following on the catalog page:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter for an item</td>
<td>Enter filter criteria, then click <strong>Set Filter</strong>. Click <strong>Clear</strong> to return to the default view.</td>
</tr>
<tr>
<td>Change the view of items</td>
<td>Select **Options</td>
</tr>
<tr>
<td>Edit an item</td>
<td>Click the link associated with the item. Click <strong>Edit</strong> to edit the item, click <strong>Duplicate</strong> to create a copy of the item, click <strong>Delete</strong> to remove the item. <strong>NOTE:</strong> If you delete an item that has a dependent link, a new and independent copy of the deleted item is placed with the linking rule or group.</td>
</tr>
<tr>
<td>Create and add an item</td>
<td>Click <strong>New</strong>. In the page or pages that appear, enter the appropriate data, then click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Export a single item</td>
<td>Click the <strong>Export</strong> link associated with the item.</td>
</tr>
<tr>
<td>Export all items of the catalog type</td>
<td>Click <strong>Export</strong> in the upper-right corner of the page, then name and save the xml-format file.</td>
</tr>
<tr>
<td>Import items of the catalog type</td>
<td>Click <strong>Import</strong> in the upper-right corner of the page, then locate and open the xml-format file with catalog data.</td>
</tr>
</tbody>
</table>

**NOTE:** To add an item from the catalog while creating a firewall rule or group, click **Add From Catalog** at the bottom of the appropriate builder page. To add an item that you created while working in the firewall rule or group builder, click the **Add to Catalog** link next to the item. When you add an item from or to the catalog you create a dependent link between the item and the catalog with a **Break Catalog Reference** link. Clicking this link breaks the dependency between the item and the catalog and creates a new and independent item in its place with the linking rule or group.

### Managing firewall client rules

Viewing firewall client rules created automatically in adaptive or learn mode or manually on a client and moving them to a Firewall Rules policy can tune and tighten security.

**NOTE:** Access to Firewall Client Rules on the Host IPS tab under Reporting requires additional permissions other than that for Host Intrusion Prevention Firewall, including view permissions for Event Log, Systems, and System Tree access.

#### Task

For option definitions, click ? on the page displaying the options.

1. Click **Menu | Reporting | Host IPS**, then click **Firewall Client Rules**.
2. Select the group in the System Tree for which you want to display client rules.
Determine how you want to view the list of client rules:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select columns to display</td>
<td>Select Choose Columns from the Options menu. In the Select Columns page, add, remove, or reorder the columns for the display.</td>
</tr>
<tr>
<td>Sort by a column</td>
<td>Click the column header.</td>
</tr>
<tr>
<td>Filter for groups</td>
<td>From the Filter menu select This Group Only or This Group and All Subgroups.</td>
</tr>
<tr>
<td>Filter for creation time</td>
<td>Select the time the rule was created: None, Since, or Between. When selecting Since, enter a beginning date; when selecting Between, enter both a beginning and ending date. Click Clear to remove filter settings.</td>
</tr>
<tr>
<td>Filter for searched text</td>
<td>Type the process path, process name, user name, computer name, or signature ID to filter on. Click Clear to remove filter settings.</td>
</tr>
<tr>
<td>Aggregate rules</td>
<td>Click Aggregate, select the criteria on which to aggregate rules, then click OK. Click Clear to remove aggregation settings.</td>
</tr>
</tbody>
</table>

To move rules to a policy, select one or more in the list, click Create Firewall Rule, then indicate the policy to which to move the rules.

FAQ — Use of wildcards in Firewall Rules

When entering values in certain fields in firewall rules, Host IPS permits the use of wildcards.

Which wildcards can I use for path and address values?

For paths of files, registry keys, executables, and URLs, use these wildcards:

<table>
<thead>
<tr>
<th>Character</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (question mark)</td>
<td>A single character.</td>
</tr>
<tr>
<td>* (one asterisk)</td>
<td>Multiple characters, excluding / and . Use to match the root-level contents of a folder with no subfolders.</td>
</tr>
<tr>
<td>** (two asterisks)</td>
<td>Multiple characters, including / and .</td>
</tr>
<tr>
<td></td>
<td>(pipe)</td>
</tr>
<tr>
<td></td>
<td>Note: For ** the escape is</td>
</tr>
</tbody>
</table>

**NOTE:** Registry key paths for firewall group locations do not recognize wildcard values.

Which wildcards can I use for all other values?

For values that normally do not contain path information with slashes, use these wildcards:

<table>
<thead>
<tr>
<th>Character</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (question mark)</td>
<td>A single character.</td>
</tr>
<tr>
<td>* (one asterisk)</td>
<td>Multiple characters, including / and .</td>
</tr>
<tr>
<td></td>
<td>(pipe)</td>
</tr>
</tbody>
</table>
Configuring General Policies

The General feature of Host Intrusion Prevention provides access to policies that are general in nature and not specific to either IPS or the firewall.

Contents
- Overview of General policies
- Define client functionality
- Define trusted networks
- Define trusted applications

Overview of General policies

General policies work with both the IPS and firewall features and control client access and both trusted networks and applications.

All policies and options apply to Windows operating systems. On non-Windows systems, only select policies and options apply. For details refer to Policy enforcement with the Solaris/Linux client under Working with Host IPS Clients.

Available policies

There are three General policies:

Client UI — Determines which options are available for a Windows client computer, including whether the Host IPS client icon appears in the system tray, types of intrusion alerts, passwords for access to the client interface, and troubleshooting options. The password functionality is used for clients on both Windows and non-Windows platforms.

Trusted Networks — Lists IP addresses and networks, including TrustedSource exceptions, that are safe for communication. Trusted networks can include individual IP addresses or ranges of IP addresses. Marking networks as trusted eliminates or reduces the need for network IPS exceptions and additional firewall rules. For Windows clients only.

Trusted Applications — Lists applications that are safe and have no known vulnerabilities. Marking applications as trusted eliminates or reduces the need for IPS exceptions and additional firewall rules. Like the IPS Rules policy, this policy category can contain multiple policy instances. For clients on both Windows and non-Windows platforms.

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

The Client UI policy determines how Host IPS clients appear and function. For Windows clients this includes icon display settings, intrusion event reactions, and access for administrators and client users. For non-Windows clients, only the password feature for administrative access is valid.

The options in this policy make it possible to meet the demands of three typical user roles:

<table>
<thead>
<tr>
<th>User type</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular</td>
<td>The average user who has the Host Intrusion Prevention client installed on a desktop or laptop. The Client UI policy enables this user to:</td>
</tr>
<tr>
<td></td>
<td>• View the Host Intrusion Prevention client icon in the system tray and launch the client console.</td>
</tr>
<tr>
<td></td>
<td>• Get pop-up intrusion alerts or prevent them.</td>
</tr>
<tr>
<td></td>
<td>• Temporarily turn off IPS and firewall protection.</td>
</tr>
<tr>
<td>Disconnected</td>
<td>The 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 time-based password to perform administrative tasks, or to turn protection features on or off.</td>
</tr>
<tr>
<td>Administrator</td>
<td>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:</td>
</tr>
</tbody>
</table>
|                | • Enabling or disabling IPS and Firewall policies. |行政指令的管理。
|                | • Creating additional IPS and Firewall rules if certain legitimate activity is blocked. |

**NOTE:** Administrative policy changes made from the ePolicy Orchestrator console will be enforced only after the password expires. Client rules created during this time are retained if allowed by administrative rules.

The Client UI policy contains a preconfigured policy and an editable My Default policy. You can view and duplicate the preconfigured policy; you can, create, edit, rename, duplicate, delete, and export editable custom policies.

Configuring a Client UI policy

Configure the settings in the policy to indicate icon display, intrusion event reactions, and administrator and client user access on Windows clients and administrator access on non-Windows clients.

**Task**

For option definitions, click ? on the page displaying the options.

1. Click Menu | Policy | Policy Catalog and select Host Intrusion Prevention: General in the Product list and Client UI in the Category list. The list of policies appears.
2. In the Client UI policy list, click Edit under Actions to change the settings for a custom policy.
3. In the Client UI page, select a tab (General Options, Advanced Options, Troubleshooting Options) and make any needed changes. See Setting Client UI general options, Setting Client UI advanced options, or Setting Client UI troubleshooting options for details.
4 Click **Save** to save any changes.

**Setting Client UI general options**

Configure settings on the General Settings tab of the Client UI policy to determine icon display and intrusion event reactions for Windows clients only.

On this tab you set the Client UI display options and indicate how the client responds upon an intrusion event.

**Task**

For option definitions, click ? in the interface.

1 Click the **General Settings** tab of the Client UI policy and under **Display options** select the option to display the tray icon for menu access to the client console or display the application in the Add/Remove Programs list.

   **NOTE:** Users who need to temporarily turn off a Host Intrusion Prevention feature to access a legitimate but blocked application or network site, they can use the Host Intrusion Prevention tray icon menu to disable a feature without opening the client console. The disabled feature remains disabled until restored by the menu command or the next policy enforcement. Note the following:

   - Disabling IPS disables both host IPS and network IPS protection.
   - If the Client UI is unlocked, the menu commands have no effect.

   For this feature, select to display the icon, then on the **Advanced Options** tab, select **Allow disabling of features from the tray icon** and select any or all of the features to be disabled.

2 Under **Upon intrusion event**, select the options that control how the client reacts when it encounters an intrusion.

**Setting Client UI advanced options and passwords**

Configure settings on the Advance Options tab of the Client UI policy for password access on Windows and non-Windows clients.

Passwords unlock the Windows client console and access troubleshooting control on Windows and non-Windows clients. 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 console remains unlocked until it is closed. To reopen the client console controls, retype the administrator password.

- A time-based password, which has an expiration date and time. This password is automatically generated. You can indicate the single system on which to create the password or create the password in the Client UI policy for all systems to which the policy is applied. The client console remains unlocked until it is closed.

   **NOTE:** Policies are *not* enforced on the client when the client console is unlocked.

   For details, see *Unlocking the Windows client interface*. 

---

McAfee Host Intrusion Prevention 8.0 Product Guide for ePolicy Orchestrator 4.5
Task

1. Click the **Advanced Options** tab in the Client UI policy that is applied to a system or a group.
2. Determine the type of password you want to create.

<table>
<thead>
<tr>
<th>For this type of password...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Administrator               | • Type a password in the **Password** text box. It must have at least ten characters.  
                              | • Retype the password in the **Confirm Password** text box.  
                              | • Click **Save**. |
| Time-based                  | • Select **Enable time-based password**.  
                              | • Enter the date and time when the password expires, then click **Compute time-based password**. The password and its expiration date and time appear in a dialog box.  
                              | • Click **Save**. |

Creating passwords on a per system basis

You can create and assign time-based passwords on a per system basis.

Task

1. Verify on the Advanced tab in the Client UI policy that the time-based passwords option is enabled.
2. Click **Save** if you made any changes to the policy.
3. Go to **Systems | System Tree**.
4. Apply the Client UI policy to the group that contains the single system to which to apply the password.
5. Select the group, then on the **Systems** tab select a single system.
6. Select **Actions | Create Time-Based Password**.
7. Set the password expiration date and time, then click **Compute time-based password**.  
The password appears in the dialog box.

Setting Client UI troubleshooting options

Configure settings on the Troubleshooting tab of the Client UI policy for logging options and turning on and off engines.

Instead of using the troubleshooting feature on the individual client, you can apply policy-level troubleshooting options that trigger logging of IPS and firewall events and that disable particular IPS engines. When disabling engines, remember to reenable them after completing the troubleshooting.

Task

1. Click the **Troubleshooting** tab in the Client UI policy.
2. Select the policy settings you want to apply:
## Define trusted networks

The Trusted Networks policy maintains a list of network addresses and subnets, which you can tag as trusted for clients on Windows and apply to firewall rules whose remote address is set to trusted and network IPS exceptions.

This policy category contains a preconfigured policy, which includes local subnets automatically but lists no network addresses, and an editable My Default policy. You can view and duplicate the preconfigured policy; you can create, edit, rename, duplicate, delete, and export editable custom policies.

### Configuring General Policies

#### Define trusted networks

<table>
<thead>
<tr>
<th>To</th>
<th>Do this...</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn on firewall logging</td>
<td>Select from the list the message type to trigger logging of Firewall events.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Debug</strong> logs all messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Information</strong> logs Information, Warning, and Error messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Warning</strong> logs Warning and Error messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Error</strong> logs error messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> logs no messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The path of the log file on Windows clients is:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention\FireSvc.log; on Windows Vista, Windows 2008, and Windows 7: C:\Program Data\McAfee\Host Intrusion Prevention\FireSvc.log.</td>
<td></td>
</tr>
<tr>
<td>Turn on IPS logging</td>
<td>Select from the list the message type to trigger logging of IPS events.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Debug</strong> logs all messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Information</strong> logs Information, Warning, and Error messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Warning</strong> logs Warning and Error messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Error</strong> logs error messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> logs no messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The path of the log file on Windows clients is:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention\HipShield.log; on Windows Vista, Windows 2008, and Windows 7: C:\Program Data\McAfee\Host Intrusion Prevention\HipShield.log</td>
<td></td>
</tr>
<tr>
<td>Include security violations in the IPS log</td>
<td>Select <strong>Log security violations</strong> to have security violations events appear in the IPS log.</td>
<td></td>
</tr>
<tr>
<td>Set the size in MB of the events log on the client</td>
<td>Change the size of the log from the default 1 MB to a larger number.</td>
<td></td>
</tr>
<tr>
<td>Turn engines on and off</td>
<td>Deselect the checkbox to disable an engine, then reselect it to reenable the engine.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** For details on working with the HIP client directly, see *Working with Host Intrusion Prevention Clients*. 
Configuring a Trusted Networks policy

Configure settings in this policy to set trusted network options and maintain a list of network addresses and subnets mark as trusted for Windows clients only.

You can:

- Set up trusted network options, including TrustedSource exceptions.
- Add or delete addresses or subnets in the trusted list.

**NOTE:** For firewall rules, you must set the remote address to Trusted to take advantage of this feature.

**Task**

For option definitions, click ? on the page displaying the options.

1. Click Menu | Policy | Policy Catalog and select Host Intrusion Prevention: General in the Product list and Trusted Networks in the Category list. The list of policies appears.

2. In the Trusted Networks policy list, click Edit under Actions to change the settings for a custom policy.

3. Do any of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically treat all users on the same subnet as trusted, even those not in the list,</td>
<td>Select Enabled under Include Local Subnet Automatically.</td>
</tr>
<tr>
<td>Add a trusted network address to the list,</td>
<td>Type a trusted IP address, address range, or subnet in the Trusted Networks text box.</td>
</tr>
<tr>
<td>Mark the network as trusted for network IPS signatures or HTTP type host and custom IPS signatures,</td>
<td>Select Trust for IPS.</td>
</tr>
<tr>
<td>Remove or add a trusted network address entry,</td>
<td>Click the Remove ( – ) or Add ( + ) button.</td>
</tr>
</tbody>
</table>

4. Click Save to save any changes.

Define trusted applications

The Trusted Applications policy is the mechanism you use to create a list of applications that are trusted and should cause no event to be generated. Maintaining a list of safe applications for a system reduces or eliminates most false positives.

The Trusted Applications policy is a multiple instance policy, so you can assign more than one policy instance, which allows for a more detailed profile of trusted application usage.

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.

**NOTE:** 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.
This policy category contains a preconfigured policy, which provides a list of specific McAfee applications and Windows processes. You can view and duplicate the preconfigured policy, or edit, rename, duplicate, delete, and export custom policies.

**Configuring a Trusted Applications policy**

Configure settings in the policy to list applications deemed safe in a particular environment.

**Task**

For option definitions, click ? on the page displaying the options.

1. Click **Menu | Policy | Policy Catalog** and select **Host Intrusion Prevention: General** in the **Product** list and **Trusted Applications** in the **Category** list. The list of policies appears.

2. In the **Trusted Applications** policy list, click **Edit** under **Actions** to change the settings for a custom policy.

3. Do any of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add an application</td>
<td>Click <strong>Add Application</strong>. See Creating and editing Trusted Application rules for details.</td>
</tr>
</tbody>
</table>
| Perform an action on one or more applications at the same time | Select them and click:  
  • **Enable** to enable a disabled application.  
  • **Disable** to disable an enabled application.  
  • **Delete** to delete applications.  
  • **Copy to** to copy applications to another policy. You are prompted to indicate the policy. |
| To perform an action on a single application | Click:  
  • **Edit** to edit an existing application. See Creating and editing Trusted Application rules for details.  
  • **Duplicate** to make a copy of the application within the same policy and named ‘copy of’ the original application.  
  • **Delete** to remove the application from the list. |

4. Click **Save** to save changes.

**Creating and editing Trusted Application rules**

Edit existing or create new trusted applications to have a list of all applications deemed safe for your environment.

**Task**

For option definitions, click ? on the page displaying the options.
1. On the Trusted Applications policy page, click **New Trusted Application** to create a new rule; click **Edit** under **Actions** to edit an existing rule.

   **NOTE:** You can also create trusted applications based on an event. For details, see *Creating a trusted application from an event* under Configuring IPS Policies.

2. Type or edit the name and indicate the status of the application, including whether the application is trusted for IPS, firewall, or both.

3. Click **New** to add an executable for the application.

   **NOTE:** You can add an existing executable from the Host IPS Catalog by clicking **Add From Catalog**. For details on the catalog, see *How the Host IPS catalog works* under Configuring Firewall Policies.

4. Click **OK** to save changes.

### Assigning multiple instances of the policy

Assigning one or more instances of the policy to a group or system in the ePolicy Orchestrator System Tree provides for single policy multi-purpose protection.

The IPS Rules policy and the Trusted Applications policy are multiple-instance policies that can have more than one instance assigned. A multiple-instance policy can be useful for an IIS Server, for example, where 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. When assigning multiple instances, you are assigning a union of all the elements in each instance of the policy.

**NOTE:** The McAfee Default policy for both IPS Rules and Trusted Applications are updated when content is update. McAfee recommends that these two policies always be applied to make sure protection as up to date as possible.

For the policies that have multiple instances, an Effective Policy link appears to provide a view of the details of the combined policy instances.

#### Task

For option definitions, click **?** in the interface.

1. Click **Menu | Systems | System Tree** and select a group in the System Tree.

   **NOTE:** For a single system, select a group in the System Tree that contains the system, then on the **Systems** tab, select the system and select **Actions | Agent | Modify Policies on a Single System**.

2. Under Assigned Policies, select **Host Intrusion Prevention 8.0 : IPS/General** in the **Product** list, and for **IPS Rules/Trusted Applications** click **Edit Assignments**.

3. On the **Policy Assignment** page, click **New Policy Instance**, and select a policy from the **Assigned Policies** list for the additional policy instance. To view the effective or combined effect of multiple instance rule sets, click **View Effective Policy**.

4. Click **Save** to save all changes.
Working with Host Intrusion Prevention Clients

The Host Intrusion Prevention client can be installed on Windows, Solaris, and Linux platforms. Only the Windows client has an interface, but all versions have troubleshooting functionality. The basic features of each client version are described here.

Contents
- Overview of the Windows client
- Overview of the Solaris client
- Overview of the Linux client

Overview of the Windows client

Direct client-side management of the Host Intrusion Prevention Windows client is available through a client console. To display it, use the McAfee tray icon menu, or run \texttt{McAfeeFire.exe} in C:\Program Files\McAfee\Host Intrusion Prevention.

When the client console first appears, options are locked and you can only view current settings. For complete control of all settings in the console, unlock the interface with a password. For details on creating and using passwords, see \textit{Setting Client UI advanced options and passwords} under Configuring General Policies.

System tray icon menu

When the McAfee icon appears in the system tray, it provides access to the Host IPS client console. Functionality differs depending on the version of the McAfee Agent that is installed on the client.

With McAfee Agent 4.0

Right-click the McAfee Agent icon, then select \textbf{Host Intrusion Prevention} to display a shortcut menu, from which you can open the console.

Table 9: McAfee Agent 4.0 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 \textit{About Host Intrusion Prevention} dialog box, which displays the version number and other product information.</td>
</tr>
</tbody>
</table>
If **Allow disabling of features from the tray icon** is selected in an applied Client UI policy, these additional commands are available:

**Table 10: McAfee Agent 4.0 menu with Allow disabling**

<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 either feature has been disabled.</td>
</tr>
<tr>
<td>Disable All</td>
<td>Disable IPS and Firewall features. Available only if both 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>
</tbody>
</table>

If **Enable timed group from McAfee tray icon menu** on the Schedule tab is selected for a firewall group in an applied Firewall Rules policy, these additional commands are available:

**Table 11: McAfee Agent 4.0 menu with Enable timed group**

<table>
<thead>
<tr>
<th>Click...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Host IPS Timed Firewall Groups</td>
<td>Enable timed firewall groups for a set amount of time to allow non-network access to the Internet before rules restricting access are applied. Each time you select this command, you reset the time for the groups.</td>
</tr>
<tr>
<td>View Host IPS Timed Firewall Groups Status</td>
<td>View the names of the timed groups and the amount of time remaining for each group to be active.</td>
</tr>
</tbody>
</table>

**With McAfee Agent 4.5**

Right-click the McAfee Agent icon in the system tray, then select **Manage Features | Host Intrusion Prevention** to open the console.

**NOTE:** Both the McAfee Agent and the Host IPS client must be set to display an icon for this access. If the McAfee Agent does not appear in the system tray, there is no access to Host IPS with a system tray icon, even though the client may be set to display a tray icon.

Under **Quick Settings**, these Host Intrusion Prevention options are available if the **Allow disabling of features from the tray icon** option is selected in an applied Client UI policy:

**Table 12: McAfee Agent 4.5 menu Quick Settings**

<table>
<thead>
<tr>
<th>Click...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IPS</td>
<td>Toggle Host IPS protection on and off.</td>
</tr>
<tr>
<td>Network IPS</td>
<td>Toggle Network IPS protection on and off</td>
</tr>
<tr>
<td>Firewall</td>
<td>Toggle Firewall protection on and off.</td>
</tr>
</tbody>
</table>

Also under **Quick Settings**, if the **Enable timed group from McAfee tray icon menu** option on the Schedule tab is selected for a firewall group in an applied **Firewall Rules** policy, these additional commands are available:

**Table 13: McAfee Agent 4.5 menu with Enable timed group**

<table>
<thead>
<tr>
<th>Click...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Host IPS Timed Firewall Groups</td>
<td>Enable timed firewall groups for a set amount of time to allow non-network access to the Internet before rules</td>
</tr>
</tbody>
</table>
### Client console for Windows clients

The Host Intrusion Prevention client console gives you access to several configuration options. To open the console, do one of the following:

- With McAfee Agent 4.0, right-click the McAfee icon, select **Host Intrusion Prevention**, then **Configure**.
- With McAfee Agent 4.5, right-click the McAfee icon, select **Manage Features, Host Intrusion Prevention**, then **Configure**.
- In the C:\Program Files\McAfee\Host Intrusion Prevention folder, run **McAfeeFire.exe**.

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.

### Unlocking the Windows client interface

An administrator remotely managing Host Intrusion Prevention using ePolicy Orchestrator can password protect the interface to prevent accidental changes. Fixed passwords that do not expire and temporary time-based passwords, allow an administrator or user to temporarily unlock the interface and make changes.

**Before you begin**

Be sure that the Host IPS General: Client UI policy, which contains the password settings, has been applied to the client. This occurs at the scheduled policy update or by forcing an immediate policy update. The client does not recognize the password until the policy update takes place.

**Task**

1. Obtain a password from the Host Intrusion Prevention administrator.
   
   **NOTE:** For details on creating a password, see **Setting Client UI advanced options and passwords** under **Configuring General Policies**.

2. Open the client console, and select **Task | Unlock User Interface**.
3. In the **Login** dialog box, type the password and click **OK**.

### Setting client UI options

The Host Intrusion Prevention client console provides access to some settings delivered by the Client UI policy, and enables you to customize these settings for the individual client.

**Before you begin**

To perform the following task, you must first unlock the client console with a password.
Task

1. In the client console select **Task | Set User Interface Language**.

2. Select the language for the client console interface and click **OK**. Options include: Chinese, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish. Selecting "Automatic" displays the interface in the language of the operating system on which the client is installed.

3. Select **Edit | Options**.

4. In the **Host Intrusion Prevention Options** dialog box, select and deselect options as needed, then click **OK**.

   **Table 14: Client console options**

<table>
<thead>
<tr>
<th>Select...</th>
<th>To have this happen...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display pop-up alert</td>
<td>An alert appears when an attack occurs (IPS only).</td>
</tr>
<tr>
<td>Play sound</td>
<td>A sound plays when an attack occurs (IPS only).</td>
</tr>
<tr>
<td>Display notification on system tray</td>
<td>The system tray icon indicates an attack status when an attack occurs (IPS only).</td>
</tr>
<tr>
<td>Create Sniffer capture if available</td>
<td>A capture column is added to the Activity Log, indicating that sniffer intrusion data has been captured. It is saved to a FirePacketX.cap file at C:\Program Data\McAfee\Host Intrusion Prevention\McAfee Fire Saved Events or C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention\McAfee Fire Saved Events (IPS only).</td>
</tr>
<tr>
<td>Show tray icon</td>
<td>Host Intrusion Prevention appears under the McAfee Agent system tray icon menu.</td>
</tr>
</tbody>
</table>

**Troubleshooting the Windows client**

Host Intrusion Prevention includes a troubleshooting function, which is available from the Help menu when the interface is unlocked. These options are available:

**Table 15: Troubleshooting options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging: Firewall</td>
<td>Determines which Firewall message type to log.</td>
</tr>
<tr>
<td>Logging: IPS *</td>
<td>Determines which IPS message type to log.</td>
</tr>
<tr>
<td>Log security violations *</td>
<td>Enable the logging of IPS security violations in the IPS log.</td>
</tr>
<tr>
<td>Show product in Add/Remove Program list</td>
<td>Allow Host IPS to appear in the Add/Remove Program list and be removed from the client.</td>
</tr>
<tr>
<td>Functionality *</td>
<td>Disable/re-enable Host IPS class engines as part of troubleshooting.</td>
</tr>
</tbody>
</table>

* This option is available only with IPS protection.

**NOTE:** McAfee provides a utility (ClientControl.exe) to help automate upgrades and other maintenance tasks when third-party software is used for deploying Host Intrusion Prevention on client computers. This command-line utility, which can be included in installation and maintenance scripts to temporarily disable IPS protection and activate logging functions, is delivered as part of the installation and is located on the client at C:\ Program Files\McAfee\Host Intrusion Prevention. See **Clientcontrol.exe utility** under **Appendix B -- Troubleshooting** for details.
Setting options for IPS logging

As part of troubleshooting you can create IPS activity logs that can be analyzed on the system or sent to McAfee support to help resolve problems. Use this task to enable IPS logging.

**Task**

1. In the Host IPS console, select Help | Troubleshooting.
2. Select the IPS message type:
   - Debug
   - Disabled
   - Error
   - Information
   - Warning
   If the message type is set to Disabled, no message is logged.
3. Click OK. The information is written to HipShield.log at C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention; on Windows Vista and later at C:\Program Data\McAfee\Host Intrusion Prevention.

Settings options for Firewall logging

As part of troubleshooting you can create firewall activity logs that can be analyzed on the system or sent to McAfee support to help resolve problems. Use this task to enable Firewall logging.

**Task**

1. In the Host IPS console, select Help | Troubleshooting.
2. Select the Firewall message type:
   - Debug
   - Disabled
   - Error
   - Information
   - Warning
   If the message type is set to Disabled, no message is logged.
3. Click OK. The information is written to FireSvc.log at C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention; on Windows Vista and later at C:\Program Data\McAfee\Host Intrusion Prevention. After the file reaches 100 MB, a new file is created.

Disabling Host IPS engines

As part of troubleshooting, you can also disable class engines that protect a client. McAfee recommends that only administrators communicating with McAfee support use this troubleshooting procedure. For a better understanding of what each class protects, see the section on Writing Custom Signatures.
**Task**

For option definitions, click ? in the interface.

1. In the Host IPS console, select **Help | Troubleshooting**, and click **Functionality**.
2. In the HIPS Engines dialog box, deselect one or more engines. To disable all engines, deselect **Enable/Disable all engines**.
   
   **NOTE:** SQL and HTTP appear in the list only if the client is running a server operating system.

3. Click **OK**.
4. After the problem has been resolved, reselect all deselected engines in the HIPS Engines dialog box.

**Windows client alerts**

A user can encounter several types of alert messages and needs to react to them. These include intrusion detection, firewall, and spoof detection alerts. Firewall alerts appear only when the client is in learn mode for these features.

**Responding to Intrusion alerts**

If you enable IPS protection and the Display pop-up alert option, an alert appears automatically 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.

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 Host IP 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 is always included in the exception.

If the alert is the result of a Network IPS 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.

**NOTE:** 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.
Responding to Firewall alerts

If you enable firewall protection and the learn mode for either incoming or outgoing traffic, a firewall alert appears, and the user needs to respond to it.

The Application Information section displays information about the application attempting network access, including application name, path, and version. The Connection Information section displays information about the traffic protocol, address, and ports.

NOTE: Previous and Next buttons are available in the Connection Information section if additional protocol or port information for an application is available. Previous and Next buttons are available at the bottom of the dialog box if more than one alert has been sent.

Task
1. In 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: Select options for the new firewall rule:

<table>
<thead>
<tr>
<th>Select...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a firewall application rule for all ports and services</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• If the intercepted traffic uses a port lower than 1024, the new rule allows or blocks only that specific port.</td>
</tr>
<tr>
<td></td>
<td>• If the traffic uses port 1024 or higher, the new rule allows or blocks the range of ports from 1024 to 65535.</td>
</tr>
<tr>
<td>Remove this rule when the application terminates</td>
<td>Create a temporary allow or block rule that is deleted when the application is closed. If you do not select this options, the new firewall rule is created as a permanent client rule.</td>
</tr>
</tbody>
</table>

Host Intrusion Prevention creates a new firewall rule based on the options selected, adds it to the Firewall Rules policy list, and automatically allows or blocks similar traffic.

Responding to Spoof Detected alerts

If you enable firewall protection, a spoof alert automatically appears if Host Intrusion Prevention detects an application on your computer sending out spoofed network traffic, and a user needs to respond to it.

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.

NOTE: 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 in two areas — the Application Information section, and the Connection Information section.
The Application Information section 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 section 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.

When Host Intrusion Prevention detects spoofed network traffic, it blocks both the traffic and the application that generated it.

### About the 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 [Configuring IPS policies](#).

IPS Policy tab 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 and executable file name.</td>
</tr>
</tbody>
</table>

### Customizing 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.

#### Task

1. In the Host IPS client console, 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. Indicate the number of minutes in the min. field.</td>
</tr>
</tbody>
</table>
Creating and editing IPS Policy exception rules

View, create, and edit IPS exception rules on the IPS Policy tab on the client.

**Task**

1. In the **IPS Policy** tab, click **Add** to add a rule.
2. In the **Exception Rule** dialog box, 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**.
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 of a rule or edit a rule</td>
<td>Double-click a rule, or select a rule and click <strong>Properties</strong>. The <strong>Exception Rule</strong> dialog box appears displaying rule information that can be edited.</td>
</tr>
<tr>
<td>Make a rule active/inactive</td>
<td>Select or clear the Exception rule is Active checkbox in the <strong>Exception Rule</strong> dialog box. You can also select or clear the checkbox next to the rule icon in the list.</td>
</tr>
<tr>
<td>Delete a rule</td>
<td>Select a rule and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Apply changes immediately</td>
<td>Click <strong>Apply</strong>. If you do not click this button after making changes, a dialog box appears asking you to save the changes.</td>
</tr>
</tbody>
</table>

About the 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 details on firewall policies, see Configuring Firewall Policies.

The firewall rules list displays rules and rule groups relevant to the client and provides summary and detailed information for each rule. Rules in italics cannot be edited.

**Table 17: Firewall Policy tab**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkbox</td>
<td>Indicates whether the rule is enabled (checked) or disabled (unchecked). For rules not in italics, you can enable and disable the rule with the checkbox.</td>
</tr>
<tr>
<td>Firewall group</td>
<td>Displays the list of rules it contains. Click the plus box to display the rules; click the minus box to hide the rules.</td>
</tr>
<tr>
<td>Timed group</td>
<td>Indicates the group is a timed group.</td>
</tr>
<tr>
<td>Location-aware group</td>
<td>Indicates the group is a location-aware group.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Firewall rule</td>
<td>Displays the basic properties of the rule. Click the plus box to display the properties; click the minus box to hide the properties.</td>
</tr>
<tr>
<td>Rule action</td>
<td>Indicates whether the rule allows traffic, or blocks it.</td>
</tr>
<tr>
<td>Rule direction</td>
<td>Indicates whether the rule applies to incoming traffic, outgoing traffic, or both.</td>
</tr>
</tbody>
</table>

### Customizing Firewall Policy options
Options at the top of the tab control settings delivered by the server-side Firewall policies after the client interface is unlocked.

**Task**
1. In the Host IPS client console, click the **Firewall Policy** tab.
2. Select or deselect an option as needed.

<table>
<thead>
<tr>
<th>To...</th>
<th>Select...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable firewall policy protection</td>
<td>Enable Firewall</td>
</tr>
<tr>
<td>Enable learn mode for incoming traffic</td>
<td>Learn Mode Incoming</td>
</tr>
<tr>
<td>Enable learn mode for outgoing traffic</td>
<td>Learn Mode Outgoing</td>
</tr>
<tr>
<td>Enable adaptive mode</td>
<td>Adaptive Mode</td>
</tr>
<tr>
<td>View trusted networks</td>
<td>Trusted Networks</td>
</tr>
</tbody>
</table>

### Creating and editing Firewall rules
View, create, and edit Firewall rules on the Firewall Policy tab on the client.

**Task**
1. In the **Firewall Policy** tab, click **Add** to add a rule.
   
   **NOTE:** You can create only rules and not groups in the client console.

2. On the **General** page, type the name of the rule and select information on rule action and direction.

3. Click **Next** to proceed to the other pages to change the default settings.

   **NOTE:** Each page of the rule builder corresponds to a tab of the firewall rule builder in the Firewall Rules policy.

<table>
<thead>
<tr>
<th>For this page...</th>
<th>Enter this information...</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>The name, status, action, and direction of the rule.</td>
</tr>
<tr>
<td>Networks</td>
<td>The IP address, subnet, domain, or other specific identifiers for this rule.</td>
</tr>
</tbody>
</table>
For this page... | Enter this information...
---|---
Transport | The protocol and the local or remote addresses where this rule applies. You can define an individual address, a range of addresses, a list of specific addresses, or specify all addresses.
Applications | The applications that this rule applies to, including the executable file name.
Schedule | The schedule, if any, for the rule.

4. Click **Finish** to save the new rule.
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 a rule or edit a rule</td>
<td>Select a rule and click <strong>Properties</strong>. The firewall rule builder dialog box appears displaying rule information. If the rule is not in italic, you can edit it.</td>
</tr>
<tr>
<td>Make a rule active/inactive</td>
<td>Select or clear the checkbox next to Enabled on the <strong>General</strong> page of the firewall rule. You can also select or clear the checkbox next to the rule in the list.</td>
</tr>
<tr>
<td>Make a copy of an existing rule</td>
<td>Select the rule, usually a default rule that cannot be edited, and click <strong>Duplicate</strong>.</td>
</tr>
<tr>
<td>Delete a rule</td>
<td>Select a rule and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Apply changes immediately</td>
<td>Click <strong>Apply</strong>. If you do not click this button after making changes, a dialog box appears asking you to save the changes.</td>
</tr>
</tbody>
</table>

### About the 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. 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.

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 18: Blocked Hosts tab**

<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. &lt;br&gt; 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. If Host Intrusion Prevention added this address because one of its firewall rules used the <strong>Treat rule match as intrusion</strong> option, this column lists the name of the relevant firewall rule. &lt;br&gt; If you added this address manually, this column lists only the IP address that you blocked.</td>
</tr>
<tr>
<td>Time</td>
<td>The time and date when you added this address to the blocked addresses list.</td>
</tr>
</tbody>
</table>
| Time Remaining | How long Host Intrusion Prevention continues to block this address. <br> If you specified an expiration time when you blocked the address, this column shows the number of minutes left until Host Intrusion Prevention removes the address from
Editing the Blocked Hosts list

Edit the list of blocked addresses to add, remove, change, or view blocked hosts.

**Task**

1. Click **Add** to add a host.
2. In the Blocked Host dialog box, enter the IP address you want to block. To search for an IPS address by domain name, click **DNS Lookup**. If you find the host name there, click **Use**.
3. Type the number of minutes, up to 60, to block the IP address.
4. Click **OK**.

**NOTE:** 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 <strong>Properties</strong>. 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 <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Apply changes immediately</td>
<td>Click <strong>Apply</strong>. If you do not click this button after making changes, a dialog box appears asking you to save the changes.</td>
</tr>
</tbody>
</table>

About the Application Protection List tab

The Application Protection List 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.

This list shows all monitored processes on the client.

**Table 19: Application Protection tab**

<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>Application Full Path</td>
<td>The full path name of the application executable.</td>
</tr>
</tbody>
</table>
About the Activity Log tab

Use the Activity Log tab to configure the logging feature and track Host Intrusion Prevention actions.

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>IP Address/User</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 (appears only for IPS log entries). You can</td>
</tr>
<tr>
<td></td>
<td>export the packet data associated with this log entry. Right-click the log</td>
</tr>
<tr>
<td></td>
<td>entry to save the data to a Sniffer file.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This column appears only if you select Create Sniffer Capture...</td>
</tr>
<tr>
<td></td>
<td>in the McAfee 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>
<tr>
<td>Matched rule</td>
<td>The name of the rule that was matched.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This column is located on the far right of the screen, so you must</td>
</tr>
<tr>
<td></td>
<td>scroll or resize the columns to view the column and its contents.</td>
</tr>
</tbody>
</table>

Customizing Activity Log options

Options at the top of the tab control logging settings delivered by the server-side Client UI policies after the client interface is unlocked.

**Task**

1. In the Host IPS client console, click the Activity Log 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>Traffic Logging - Log All Blocked</td>
<td>Log all blocked firewall traffic.</td>
</tr>
<tr>
<td>Traffic Logging - Log All Allowed</td>
<td>Log all allowed firewall traffic.</td>
</tr>
<tr>
<td>Filter Options - Traffic</td>
<td>Filter the data to display blocked and allowed firewall traffic.</td>
</tr>
</tbody>
</table>
NOTE: You can enable and disable logging for the firewall traffic, but not for the IPS feature. However, you can choose to hide these events in the log by filtering them out.

3  Do any of the following to change the display:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh the display</td>
<td>Click <strong>Refresh</strong>.</td>
</tr>
<tr>
<td>Permanently delete the contents of the log</td>
<td>Click <strong>Clear</strong>.</td>
</tr>
<tr>
<td>Save the contents of the log and delete the list from the tab</td>
<td>Click <strong>Export</strong>. In the dialog box that appears, name and save the .txt file.</td>
</tr>
<tr>
<td>Apply changes immediately</td>
<td>Click <strong>Apply</strong>. If you do not click this button after making changes, a dialog box appears asking you to save the changes.</td>
</tr>
</tbody>
</table>

**Overview of the Solaris client**

The Host Intrusion Prevention 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 20: Solaris client policies**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Available options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Intrusion Prevention 8.0 IPS</strong></td>
<td></td>
</tr>
</tbody>
</table>
| IPS Options | • Enable HIPS  
• Enable Adaptive Mode  
• Retain existing Client Rules |
| IPS Protection | All |
| IPS Rules | • Exception Rules  
• Signatures (default and custom HIPS rules only)  
**NOTE:** NIPS signatures and Application Protection Rules are not available. |
| **Host Intrusion Prevention 8.0 General** | |
| Client UI | None except administrative or time-based password to allow use of the troubleshooting tool. |
| Trusted Networks | None |
### Troubleshooting the Solaris client

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. In addition, you might encounter problems with the operation of the client. You can check whether the client is running, and stop and restart the client.

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>To...</th>
<th>Run...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the current status of the client indicating which type of logging is enabled, and which engines are running.</td>
<td><code>hipts status</code></td>
</tr>
<tr>
<td>Turn on logging of specific messages types.</td>
<td><code>hipts logging on</code></td>
</tr>
<tr>
<td>Turn off logging of all message types. Logging is off by default.</td>
<td><code>hipts logging off</code></td>
</tr>
<tr>
<td>Display the message type indicated when logging is set to “on.” Messages include:</td>
<td><code>hipts message &lt;message name&gt;:on</code></td>
</tr>
<tr>
<td>• error</td>
<td></td>
</tr>
<tr>
<td>• warning</td>
<td></td>
</tr>
<tr>
<td>• debug</td>
<td></td>
</tr>
<tr>
<td>• info</td>
<td></td>
</tr>
<tr>
<td>• violations</td>
<td></td>
</tr>
<tr>
<td>Hide the message type indicated when logging is set to “on.” Message error is off by default.</td>
<td><code>hipts message &lt;message name&gt;:off</code></td>
</tr>
<tr>
<td>Display all message types when logging is set to “on.”</td>
<td><code>hipts message all:on</code></td>
</tr>
<tr>
<td>Hide all message types when logging is set to “on.”</td>
<td><code>hipts message all:off</code></td>
</tr>
<tr>
<td>Turn on the engine indicated. Engine is on by default. Engines include:</td>
<td><code>hipts engines &lt;engine name&gt;:on</code></td>
</tr>
<tr>
<td>• MISC</td>
<td></td>
</tr>
<tr>
<td>• FILES</td>
<td></td>
</tr>
<tr>
<td>• GUID</td>
<td></td>
</tr>
<tr>
<td>• MMAP</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Solaris 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; HipClient-bin</td>
<td>Solaris client</td>
</tr>
<tr>
<td>HipClientPolicy.xml</td>
<td>Policy rules</td>
</tr>
<tr>
<td>hipts; hipts-bin</td>
<td>Troubleshooting tool</td>
</tr>
<tr>
<td>*.so</td>
<td>Host Intrusion Prevention and McAfee Agent shared object modules</td>
</tr>
<tr>
<td>log directory</td>
<td>Contains debug and error log files</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 Solaris 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

Stopping the Solaris client

You might need to stop a running client and restart it as part of troubleshooting.

**Task**

1. To stop a running client, first disable IPS protection. Use one of these procedures:
   - Set **IPS Options** to **Off** in the ePO console and apply the policy to the client.
   - Logged in at root, run the command: hipts engines MISC:off
2. Run the command: /sbin/rc2.d/S99hip stop

Restarting the Solaris client

You might need to stop a running client and restart it as part of troubleshooting.
Task
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.
   • Logged in at root, run the command: hipts engines MISC:on

Overview of the Linux client

The Host Intrusion Prevention Linux client identifies and prevents potentially harmful attempts to compromise a Linux server’s files and applications. It protects the server’s operating system along with Apache web servers, with an emphasis on preventing buffer overflow attacks.

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 21: Linux client policies

<table>
<thead>
<tr>
<th>Policy</th>
<th>Available options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Intrusion Prevention 8.0 IPS</strong></td>
<td></td>
</tr>
</tbody>
</table>
| IPS Options | • Enable HIPS  
• Enable Adaptive Mode  
• Retain existing Client Rules |
| IPS Protection | All |
| IPS Rules | • Exception Rules  
• Signatures (default and custom HIPS rules only)  
**NOTE:** NIPS signatures and Application Protection Rules are not available. |
| **Host Intrusion Prevention 8.0 General** | |
| Client UI | None except administrative or time-based password to allow use of the troubleshooting tool. |
| Trusted Networks | None |
| Trusted Applications | Only Mark as trusted for IPS and New Process Name to add trusted applications. |
| **Host Intrusion Prevention 8.0 Firewall** | None |

Notes about the Linux client

- The Host IPS 8.0 Linux client is incompatible with SELinux in enforce mode. To disable the enforce mode, run the command: system-config-securitylevel, change the setting to disabled, and restart the client system.
When the Host IPS 8.0 Linux kernel modules are loaded, the SUSE kernel is reported to be tainted. The kernel log indicates this flag: `schook: module not supported by Novell, setting U taint flag; hipsec: module not supported by Novell, setting U taint flag`. Novell requirements for third-party modules are causing the Host IPS kernel to be marked tainted. Because the Host IPS 8.0 Linux kernel modules are GPL-licensed, this message should be ignored. McAfee is working with Novell to resolve this issue.

Troubleshooting the Linux client

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 reinstalling the client, and checking process logs. In addition, you might encounter problems with the operation of the client. You can check whether the client is running, and stop and restart the client.

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 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>To...</th>
<th>Run...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the current status of the client indicating which type of logging is enabled, and which engines are running.</td>
<td><code>hipts status</code></td>
</tr>
<tr>
<td>Turn on logging of specific messages types.</td>
<td><code>hipts logging on</code></td>
</tr>
<tr>
<td>Turn off logging of all message types. Logging is off by default.</td>
<td><code>hipts logging off</code></td>
</tr>
<tr>
<td>Display the message type indicated when logging is set to “on.” Messages include:</td>
<td><code>hipts message &lt;message name&gt;:on</code></td>
</tr>
<tr>
<td>• error</td>
<td></td>
</tr>
<tr>
<td>• warning</td>
<td></td>
</tr>
<tr>
<td>• debug</td>
<td></td>
</tr>
<tr>
<td>• info</td>
<td></td>
</tr>
<tr>
<td>• violations</td>
<td></td>
</tr>
<tr>
<td>Hide the message type indicated when logging is set to “on.” Message error is off by default.</td>
<td><code>hipts message &lt;message name&gt;:off</code></td>
</tr>
<tr>
<td>Display all message types when logging is set to “on.”</td>
<td><code>hipts all:on</code></td>
</tr>
<tr>
<td>Hide all message types when logging is set to “on.”</td>
<td><code>hipts all:off</code></td>
</tr>
<tr>
<td>Turn on the engine indicated. Engine is on by default.</td>
<td><code>hipts engines &lt;engine name&gt;:on</code></td>
</tr>
</tbody>
</table>

Engines include:
- MISC
- FILES
- HTTP
Verifying Linux 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; HipClient-bin</td>
<td>Linux client</td>
</tr>
<tr>
<td>HipClientPolicy.xml</td>
<td>Policy rules</td>
</tr>
<tr>
<td>hipts; hipts-bin</td>
<td>Troubleshooting tool</td>
</tr>
<tr>
<td>*.so</td>
<td>Host Intrusion Prevention and McAfee Agent shared object modules</td>
</tr>
<tr>
<td>log directory</td>
<td>Contains debug and error log files</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 Linux 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
```

Stopping the Linux client

You might need to stop a running client and restart it as part of troubleshooting.

**Task**

1. To stop a client, 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`

Restarting the Linux client

You might need to stop a running client and restart it as part of troubleshooting.

**Task**

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`
Appendix A — Writing Custom Signatures and Exceptions

This section describes the structure of IPS signatures, including a list of classes, parameters, and directives, and provides information on how to create custom signatures for the various client platforms. This information can also be used when working with the advanced details page for exceptions.

Contents

- Rule structure
- Windows custom signatures
- Non-Windows 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:

```
Rule {
  SectionA value
  SectionB value
  SectionC value
  ...
}
```

**NOTE:** Be sure to review the syntax 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 * }

Executable { Include * }

user_name { Include * }

directives isapi:request

}
Each executable is specified inside the brackets using `-path`, `-hash`, `-sdn`, `-desc`. There can be multiple brackets for each section and inside the brackets you can have one or more options. The `-path` (file path name), `-sdn` (file signer), and `-desc` (file description) values are strings and need to be TCL escaped if they contain spaces or other TCL reserved characters. The `-hash` (MD5 hash) value is a 32-character hexbin string.

Example: Executable `{Include -path "C:\\Program Files\\McAfee\\VirusScan Enterprise\\Mcshield.exe" -sdn "CN="mcafee,inc.\\", OU=iss, OU=digital id class 3 - microsoft software validation v2, O="mcafee, inc.\\", L=santa clara, ST=california, C=us" -desc "On-Access Scanner service"}

If a rule applies to all executables, use `*`. On UNIX this section is case-sensitive.

The operation types are class dependent, and are listed for each class in the later sections.

<table>
<thead>
<tr>
<th>Section</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| Executable  | `{Include/Exclude file name path, fingerprint, signer or description}` | Each executable is specified inside the brackets using `-path`, `-hash`, `-sdn`, `-desc`. There can be multiple brackets for each section and inside the brackets you can have one or more options. The `-path` (file path name), `-sdn` (file signer), and `-desc` (file description) values are strings and need to be TCL escaped if they contain spaces or other TCL reserved characters. The `-hash` (MD5 hash) value is a 32-character hexbin string. Example: Executable `{Include -path "C:\\Program Files\\McAfee\\VirusScan Enterprise\\Mcshield.exe" -sdn "CN="mcafee,inc.\\", OU=iss, OU=digital id class 3 - microsoft software validation v2, O="mcafee, inc.\\", L=santa clara, ST=california, C=us" -desc "On-Access Scanner service"}

If a rule applies to all executables, use `*`. On UNIX this section is case-sensitive. |

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.

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 `{ ... }`.

NOTE: With the standard subrule, use a single backslash in file paths; with the export subrule, use double backslashes in file paths. The standard subrule translates the single slashes to required double slashes, while the expert subrule performs no translation.

For example, to monitor all the text files in C:\\test\\:

files { Include C:\\\\*.*.txt }

and to monitor all the files except the text files in C:\\test\\:

files { Exclude C:\\\\*.*.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:\\\\*.*.txt }
files { Exclude C:\\\\abc.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:\\\\*.*.txt }
files { Include C:\\\\abc* }

NOTE: In precedence order, exclude wins over include. Here are three examples:
• If a single subrule includes a particular user *marketing\johns* and excludes the same user *marketing\johns*, then the signature does not trigger even when the user *marketing\johns* performs an action triggers the signature.

• If a subrule includes *all* users but excludes the particular user *marketing\johns*, then the signature triggers if the user is NOT *marketing\johns*.

• If a subrule includes user *marketing\* but excludes *marketing\johns*, then the signature triggers only when the user is *marketing\anyone*, unless the user is *marketing\johns*, in which case it does not trigger.

Optional common sections

A rule’s 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 and Non-Windows 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>(Include/Exclude “id of a rule”)</td>
<td>Defines dependencies between rules and prevents the triggering of dependent rules.</td>
</tr>
<tr>
<td>attributes</td>
<td>—no_log</td>
<td>Events from the signature are not sent to the ePO server.</td>
</tr>
<tr>
<td></td>
<td>—not_auditable</td>
<td>No exceptions are generated for the signature when adaptive mode is applied.</td>
</tr>
<tr>
<td></td>
<td>—no_trusted_apps</td>
<td>The trusted application list does not apply to this signature.</td>
</tr>
<tr>
<td></td>
<td>—inactive</td>
<td>The signature is disabled.</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 “the general rule”

Wildcards and variables

Wildcards, meta-symbols, and predefined variables can be used as the value in the available sections.
Wildcards

You can use wildcards for the section values. Note the slightly different use of asterisks with paths and addresses, which normally contain forward or backward slashes. For expert subrules of signatures, the TCL wildcard scheme is used.

Table 22: Wildcards

<table>
<thead>
<tr>
<th>Character</th>
<th>What it represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (question mark)</td>
<td>A single character.</td>
</tr>
<tr>
<td>* (one asterisk)</td>
<td>Multiple characters, including / and . <strong>NOTE</strong>: For paths and addresses, use ** (two asterisks) to include / and ; use * (one asterisk) to exclude / and .</td>
</tr>
<tr>
<td>I (pipe)</td>
<td>Wildcard escape.</td>
</tr>
</tbody>
</table>

Table 23: TCL wildcards

<table>
<thead>
<tr>
<th>Character</th>
<th>What it represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (question mark)</td>
<td>A single character.</td>
</tr>
<tr>
<td>* (one asterisk)</td>
<td>Multiple characters, including / and . Example: files { Include &quot;C:*.txt&quot; }</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. Example: files { Include &quot;C:\test&amp;.txt&quot; }</td>
</tr>
<tr>
<td>! (exclamation point)</td>
<td>Wildcard escape. Example: files { Include &quot;C:\test!yahoo!.txt&quot; }</td>
</tr>
</tbody>
</table>

Use of environment variables

Use environment variables, the iEnv command with one parameter (the variable name) in square brackets [ ... ], as a shorthand to specify Windows file and directory path names.

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>What it represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>iEnv SystemRoot</td>
<td>C:\winnt, where C is the drive that contains the Windows System folder. Example: files {Include [iEnv SystemRoot]\system32\abc.txt }</td>
</tr>
<tr>
<td>iEnv SystemDrive</td>
<td>C:\ where C is the drive that contains the Windows System folder. Example: files {Include [iEnv SystemDrive]\system32\abc.txt}</td>
</tr>
</tbody>
</table>

Use of predefined variables

Host Intrusion Prevention provides predefined variables for rule writing. These variables, are preceded by "$," and are listed below.

Table 24: Windows IIS Web Server

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</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>
</tbody>
</table>
### Table 25: MS SQL Database Server

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</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>

### Table 26: Unix Apache and iPlanet

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</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>
</tbody>
</table>
This section describes how to write custom signatures for the Windows platform.

**NOTE:** Rules in the Windows class Files use double backslashes for paths while rules in the non-Windows class UNIX_file use a single forward slash.

The class used by a signature depends on the nature of the security issue and the protection the signature can offer. Some of the classes and parameters appear in the custom signature user interface, while others do not. For those classes and parameters without a user interface, the expert method for rule creation is the only way to access them. For Windows, these classes are available:

<table>
<thead>
<tr>
<th>Class</th>
<th>When to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Overflow</td>
<td>For protection against buffer overflow</td>
</tr>
<tr>
<td>Files</td>
<td>For protection of file or directory operations</td>
</tr>
<tr>
<td>Hook</td>
<td>For protection of API process hooking</td>
</tr>
<tr>
<td>Illegal API Use</td>
<td>For protection against illegal use of the Host IPS API</td>
</tr>
<tr>
<td>Illegal Use</td>
<td>For protection against illegal use of the API</td>
</tr>
<tr>
<td>Isapi</td>
<td>For monitoring http requests to IIS</td>
</tr>
<tr>
<td>Program</td>
<td>For protection of program operations</td>
</tr>
<tr>
<td>Registry</td>
<td>For protection of registry key and registry value operations</td>
</tr>
<tr>
<td>Services</td>
<td>For protection of services operations</td>
</tr>
<tr>
<td>SQL</td>
<td>For protection of SQL operations</td>
</tr>
</tbody>
</table>

### Windows class Buffer Overflow

The following table lists the possible sections and values for the Windows class Buffer Overflow:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Buffer_Overflow</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>See Common sections.</td>
<td></td>
</tr>
</tbody>
</table>

## Windows custom signatures

Windows custom signatures

This section describes how to write custom signatures for the Windows platform.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Section</td>
<td>Values</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>level</td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
</tr>
<tr>
<td>dependencies</td>
<td>428</td>
</tr>
<tr>
<td>caller module</td>
<td>Path to a module (i.e. a DLL) loaded by an executable that makes a call that causes a buffer overflow</td>
</tr>
<tr>
<td>directives</td>
<td>bo:stack</td>
</tr>
<tr>
<td></td>
<td>bo:heap</td>
</tr>
<tr>
<td></td>
<td>bo:writeable_memory</td>
</tr>
<tr>
<td></td>
<td>bo:invalid_call</td>
</tr>
<tr>
<td></td>
<td>bo:target_bytes</td>
</tr>
<tr>
<td></td>
<td>bo:call_not_found</td>
</tr>
<tr>
<td></td>
<td>bo:call_return_unreadable</td>
</tr>
<tr>
<td></td>
<td>bo:call_different_target_address</td>
</tr>
<tr>
<td></td>
<td>bo:call_return_to_api</td>
</tr>
</tbody>
</table>

**Note 1**

Signature 428, Generic Buffer Overflow, is a generic buffer overflow rule. To avoid triggering this rule, include section “dependencies 428” in the custom signature.

**Windows class Files**

The following table lists the possible sections and values for the Windows 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></td>
<td>See Common sections.</td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Values</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td>(Use this parameter to distinguish between remote and local file access. See Note 3.)</td>
<td></td>
</tr>
<tr>
<td>files</td>
<td>File or folder involved in the operation</td>
<td>One of the required parameters. See Note 1 and Note 2.</td>
</tr>
<tr>
<td>dest_file</td>
<td>Destination files if the operation involves source and destination files</td>
<td>One of the required parameters. Used only with files:rename and files:hardlink. See Note 1 and Note 2.</td>
</tr>
<tr>
<td>drive_type</td>
<td>• Network — Network file access</td>
<td>Allows creation of files class rules specific to drive types.</td>
</tr>
<tr>
<td></td>
<td>• Floppy — Floppy drive access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CD — CD or DVD access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OtherRemovable — USB or other removable drive access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OtherFixed — Local hard disk or other fixed hard disk access</td>
<td></td>
</tr>
<tr>
<td>directives</td>
<td>files:create</td>
<td>Creates a file in a directory, or moves file into another directory.</td>
</tr>
<tr>
<td></td>
<td>files:read</td>
<td>Opens the file with read only access.</td>
</tr>
<tr>
<td></td>
<td>files:write</td>
<td>Opens the file with read-write access.</td>
</tr>
<tr>
<td></td>
<td>files:execute</td>
<td>Executes the file (executing a directory means that this directory will become the current directory).</td>
</tr>
<tr>
<td></td>
<td>files:delete</td>
<td>Deletes the file from a directory, or moves it to another directory.</td>
</tr>
<tr>
<td></td>
<td>files:rename</td>
<td>Renames a file in the same directory. See Note 2.</td>
</tr>
<tr>
<td></td>
<td>files:attribute</td>
<td>Changes the file attributes. Monitored attributes include:</td>
</tr>
<tr>
<td></td>
<td>files:hardlink</td>
<td>Creates a hard link.</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:

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:

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:

Rule {
  tag "Sample1"
  Class Files
  Id 4001
  level 4
  files { Include "C:\test\abc.txt" }
  Executable { Include "**"}
  user_name { Include "**" }
  directives 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:

Rule {
  tag "Sample2"
  Class Files
  Id 4001
  level 4
  dest_file { Include "**\test\abc.txt" }
  Executable { Include "**"}
  user_name { Include "**" }
  directives 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.

**Note 3**

To distinguish between remote file access and local file access for any directive, set the executable file path name to "SystemRemoteClient": Executable { Include -path "SystemRemoteClient" }

This would prevent any directive to execute if the executable is not local.
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. The 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 {
  tag "Sample3"
  Class Files
  Id 4001
  level 4
  files { Include "C:\test\abc.txt" }
  Executable { Include "*" }
  user_name { Include "*" }
  directives 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 severity 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" }.
- **Executable { Include "*" }**: Indicates that this rule is valid for all processes. If you want to limit your rule to specific processes, spell them out here, complete with 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 want to limit your rule to specific user contexts, spell them out here in the form Local/user or Domain/user. See Common Sections for details.
- **directives files:create**: Indicates that this rule covers the creation of a file.

Windows class Hook

The following table lists the possible sections and values for the Windows class Hook:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Hook</td>
<td></td>
</tr>
</tbody>
</table>
### Section Values Notes

<table>
<thead>
<tr>
<th>Id</th>
<th></th>
<th>See Common sections.</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>handler module</td>
<td>Path name of the executable that is being hooked by another executable.</td>
<td>A required parameter.</td>
</tr>
<tr>
<td>directives</td>
<td>hook:set_windows_hook</td>
<td>To prevent injection of a DLL into an executable when using hook:set_windows_hook, include the executable in the Application Protection List.</td>
</tr>
</tbody>
</table>

### Windows class Illegal Host IPS API Use

The following table lists the possible sections and values for the Windows class Illegal API Use:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Illegal_API_Use</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>See Common sections.</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vulnerability_name</td>
<td>Name of the vulnerability</td>
<td></td>
</tr>
<tr>
<td>detailed_event_info</td>
<td>One or more CLSIDs.</td>
<td>This is a 128-bit number that represents a unique ID for a software component. Typically displayed as: &quot;({FAC7A6FB-0127-4F06-9892-8D2FC56E3F76})&quot;</td>
</tr>
<tr>
<td>directives</td>
<td>illegal_api_use:bad_parameter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>illegal_api_use:invalid_call</td>
<td></td>
</tr>
</tbody>
</table>

Use this class to create a custom killbit signature. The killbit is a security feature in web browsers and other applications that use ActiveX. A killbit specifies the object class identifier (CLSID) for ActiveX software controls that are identified as security vulnerability threats. Applications that use ActiveX do not load specified ActiveX software with a corresponding killbit in place.

The primary purpose of a killbit is to close security holes. Killbit updates are typically deployed to Microsoft Windows operating systems via Windows security updates.

Here is an example of a signature:

```
Rule {
  tag "Sample4"
  Class Illegal_API_Use
  Id 4001
  level 4
```


Executable { Include "*" }
user_name { Include "*" }
vulnerability_name {Include "Vulnerable ActiveX Control Loading ?"}
detailed_event_info { Include "0002E533-0000-0000-C000-000000000046" "0002E511-0000-0000-C000-000000000046" }
directives files:illegal_api_use:bad_parameter illegal_api_use:invalid_call
attributes -not_auditable

Windows class Illegal Use

The following table lists the possible sections and values for the Windows class Illegal Use:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Illegal_Use</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td></td>
<td>See Common sections.</td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>One of three values: LsarLookupNames, LsarLookupSids, or ADMCOMConnect</td>
<td></td>
</tr>
<tr>
<td>directives</td>
<td>illegal:api</td>
<td></td>
</tr>
</tbody>
</table>

Windows class Isapi (HTTP)

The following table lists the possible sections and values for the Windows class Isapi with IIS:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Isapi</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td></td>
<td>See Common sections.</td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>url</td>
<td>One of the required parameters. Matched against the URL part of an incoming request. See Notes 1-4.</td>
<td></td>
</tr>
<tr>
<td>query</td>
<td>One of the required parameters. Matched against the query part of an incoming request. See Notes 1-4.</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" is matched against {url} and the section "query" is matched against {query}. For example the following rule is triggered if the http request http://www.myserver.com/search/abc.exe?subject=wildlife&environment=ocean is received by IIS:

Rule {
  tag "Sample6"
  Class Isapi
  Id 4001
  level 1
  url { Include "*abc*" }
  Executable { Include "*" }
  user_name { Include "*" }
  directives 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 match only if the {url} or {query} have more characters than "number-of-chars". For example, "abc*;500" matches strings containing 'abc' that are 500 characters or more; "*abc;xyz*;" matches any string containing 'abc;xyz' regardless of length.

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 (for example, Get, Put, Post, and Query).</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>&quot;Raw&quot; (undecoded and not normalized) Request Line of the incoming HTTP request. Request Line is &quot;&lt;method&gt; &lt;location&gt; &lt;http version&gt; CRLF&quot;.</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. The address contains three parts: host name: address: port number.</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 {
  tag "Sample7"
  Class Isapi
  Id 4001
  level 1
  query { Include "*subject*" }
  method { Include "GET" }
  Executable { Include "*" }
  user_name { Include "*" }
  directives 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 severity 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.
- **Executable { Include "*" }**: Indicates that this rule is valid for all processes. If you want to limit your rule to specific processes, spell them out here, complete with 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 want to limit your rule to specific user contexts, spell them out here in the form Local/username or Domain/username. See **Common Sections** for details.
- **directives isapi:request**: Indicates that this rule covers an HTTP request.

### Windows class Program

The following table lists the possible sections and values for the Windows class Program:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Program</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>See Common sections.</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filename</td>
<td>Name of the process in the operation.</td>
<td>One of the required parameters.</td>
</tr>
<tr>
<td>path</td>
<td>Path name of the process.</td>
<td>One of the required parameters.</td>
</tr>
<tr>
<td>directives</td>
<td>program:run</td>
<td>Select to prevent a target executable from running. (Run target executable, in the user interface.)</td>
</tr>
</tbody>
</table>
|               | program:open_with_any              | The "program:open_with_x" directives handle process access rights created with OpenProcess(). Select to prevent these process-specific access rights:  
- PROCESS_TERMINATE — Required to terminate a process.  
- PROCESS_CREATE_THREAD — Required to create a thread.  
- PROCESS_VM_WRITE — Required to write to memory.  
- PROCESS_DUP_HANDLE — Required to duplicate a handle. |
Windows class Registry

The following table lists the possible sections and values for the Windows class Registry:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>process:open_with_create_thread</td>
<td>Select to prevent this process-specific access right:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PROCESS_CREATE_THREAD — Required to create a thread.</td>
<td>(Open with access to create a thread, in the user interface.)</td>
</tr>
<tr>
<td>program:open_with_modify</td>
<td>Select to prevent these process-specific access rights:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PROCESS_TERMINATE — Required to terminate a process.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PROCESS_CREATE_THREAD — Required to create a thread.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PROCESS_VM_WRITE — Required to write to memory.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PROCESS_DUP_HANDLE — Required to duplicate a handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PROCESS_SET_INFORMATION — Required to set certain information about</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a process, such as its priority class.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PROCESS_SUSPEND_RESUME — Required to suspend or resume a process.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Open with access to modify, in the user interface.)</td>
<td></td>
</tr>
<tr>
<td>program:open_with_terminate</td>
<td>Select to prevent these process-specific access rights:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PROCESS_SUSPEND_RESUME — Required to suspend or resume a process.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PROCESS_TERMINATE — Required to terminate a process.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Open with access to terminate, in the user interface.)</td>
<td></td>
</tr>
<tr>
<td>program:open_with_wait</td>
<td>Select to prevent this process-specific access right:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SYNCHRONIZE — Required to wait for the process to terminate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Open with access to wait, in the user interface.)</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Not available on Microsoft Vista and later platforms.
<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>See Common sections.</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>keys</td>
<td>Registry key operation</td>
<td>One of the required parameters. Use with key operations (create, delete, rename, enumerate, monitor, restore, read, replace, load). See Note 1.</td>
</tr>
<tr>
<td>dest_keys</td>
<td>Registry key operation</td>
<td>Optional. Only for registry:rename when a key is renamed. The target is the name of the key.</td>
</tr>
<tr>
<td>values</td>
<td>Registry key value operation</td>
<td>One of the required parameters. Use with registry value operations (delete, read, modify, create).</td>
</tr>
<tr>
<td>new_data</td>
<td>Registry key value operation. New data of the value.</td>
<td>Optional. Only for registry:modify or registry:create. See Note 2.</td>
</tr>
<tr>
<td>directives</td>
<td>registry:delete</td>
<td>Deletes a registry key or value.</td>
</tr>
<tr>
<td></td>
<td>registry:modify</td>
<td>Modifies the content of a registry value or the info of a registry key.</td>
</tr>
<tr>
<td></td>
<td>registry:create</td>
<td>Allows a registry key to be created.</td>
</tr>
<tr>
<td></td>
<td>registry:permissions</td>
<td>Modifies the permissions of a registry key.</td>
</tr>
<tr>
<td></td>
<td>registry:read</td>
<td>Obtains registry key information (number of subkeys, etc), or gets the content of a registry value.</td>
</tr>
<tr>
<td></td>
<td>registry:enumerate</td>
<td>Enumerates a registry key, that is, gets the list of all the key's subkeys and values.</td>
</tr>
<tr>
<td></td>
<td>registry:monitor</td>
<td>Requests to monitor a registry key.</td>
</tr>
<tr>
<td></td>
<td>registry:restore</td>
<td>Restores a hive from file, like the regedit32 restore function.</td>
</tr>
<tr>
<td></td>
<td>registry:replace</td>
<td>Restores a registry setting but only after a restart.</td>
</tr>
<tr>
<td></td>
<td>registry:load</td>
<td>Loads registry keys or values from a file.</td>
</tr>
<tr>
<td></td>
<td>registry:open_existing_key</td>
<td>Opens an existing registry key.</td>
</tr>
<tr>
<td></td>
<td>registry:rename</td>
<td>Renames a registry key.</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 section 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”}.

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. Note the following:</td>
</tr>
<tr>
<td></td>
<td><strong>For this key</strong></td>
</tr>
<tr>
<td></td>
<td>HKEY_LOCAL_MACHINE\</td>
</tr>
<tr>
<td></td>
<td>HKEY_CURRENT_USER\</td>
</tr>
<tr>
<td></td>
<td>HKEY_CLASSES_ROOT\</td>
</tr>
<tr>
<td></td>
<td>HKEY_CURRENT_CONFIG\</td>
</tr>
<tr>
<td></td>
<td>HKEY_USERS\</td>
</tr>
</tbody>
</table>

| Registry Values | Name of the registry value concatenated with the full name of its key. Note the following: |
|-----------------|**For values in this key** | **Use this syntax** |
|                 | HKEY_LOCAL_MACHINE\Test\ | \REGISTRY\MACHINE\Test\* |
|                 | HKEY_CURRENT_USER\Test\ | \REGISTRY\CURRENT_USER\Test\* |
|                 | HKEY_CLASSES_ROOT\Test\ | \REGISTRY\MACHINE\SOFTWARE\CLASSES\Test\* |
|                 | HKEY_CURRENT_CONFIG\Test\ | REGISTRY\MACHINE\SYSTEM\ControlSet\HARDWARE PROFILES\0001\Test\* |
|                 | HKEY_USERS\Test\ | \REGISTRY\USER\Test\* |

<table>
<thead>
<tr>
<th></th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>old data</td>
<td>Only applicable for registry value changes: data that a registry value contained before it was changed or attempted to be changed.</td>
</tr>
<tr>
<td>new data</td>
<td>Only applicable for registry value changes: data that a registry value contains after it was changed or that it would contain if the change went through.</td>
</tr>
<tr>
<td>old data type</td>
<td>Only applicable for registry value changes: type of data type that a registry value contains before it was changed or attempted to be changed.</td>
</tr>
<tr>
<td>new data type</td>
<td>Only applicable for registry value changes: type of data that a registry value would contain after it was changed or that it would contain if the change went through.</td>
</tr>
</tbody>
</table>

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 {
  tag "Sample8"
  Class Registry
  Id 4001
level 4
values { Include "\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet\\Control\\Lsa\\abc" }
application { Include "*" }
user_name { Include "*" }
directives registry:delete
}

The various sections of this rule have the following meaning:

- **Class Registry**: indicates that this rule relates to requests send 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 severity 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 { Include "\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet\\Control\\Lsa\\abc" }**: Indicates that the rule monitors registry value abc under registry key "\\HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Lsa . If the rule covers multiple values, add them in this section in different lines.
- **application { Include "*" }**: Indicates that this rule is valid for all processes. If you want to limit your rule to specific processes, spell them out here, complete with 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 want to limit your rule to specific user contexts, spell them out here in the form Local/user or Domain/user. See Common Sections for details.
- **directives registry:delete**: Indicates that this rule covers deletion of a registry key or value.

## Windows class Services

The following table lists the possible sections and values for the Windows class Services:

<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>See Common sections.</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></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>One of the required parameters. 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>One of the required parameters. This name appears in the Services manager. See Note 1.</td>
</tr>
<tr>
<td>directives</td>
<td>services:delete</td>
<td>Deletes a service.</td>
</tr>
<tr>
<td></td>
<td>services:create</td>
<td>Creates a service.</td>
</tr>
<tr>
<td></td>
<td>services:start</td>
<td>Starts a service.</td>
</tr>
<tr>
<td>Section</td>
<td>Values</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>services:stop</td>
<td></td>
<td>Stops a service.</td>
</tr>
<tr>
<td>services:pause</td>
<td></td>
<td>Pauses a service.</td>
</tr>
<tr>
<td>services:continue</td>
<td></td>
<td>Continues a service after a pause.</td>
</tr>
<tr>
<td>services:startup</td>
<td></td>
<td>Modifies the startup mode of a service.</td>
</tr>
<tr>
<td>services:profile_enable</td>
<td></td>
<td>Enables a hardware profile.</td>
</tr>
<tr>
<td>services:profile_disable</td>
<td></td>
<td>Disables a hardware profile.</td>
</tr>
<tr>
<td>services:logon</td>
<td></td>
<td>Modifies the logon information of a service.</td>
</tr>
</tbody>
</table>

**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 manager, which is found in registry value HKLM_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<name-of-service>\.

**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 displayed in the Services manager.</td>
<td></td>
</tr>
<tr>
<td>services</td>
<td>System name of the Windows service in HKLM\CurrentControlSet\Services. This may be different from the name displayed in the Services manager.</td>
<td>Boot, System, Automatic, Manual, Disabled</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></td>
</tr>
<tr>
<td>new startup</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>logon</td>
<td>Only applicable for changes in the logon mode of a service: logon information (system or user account) used by the service.</td>
<td></td>
</tr>
</tbody>
</table>
The following rule would prevent deactivation of the Alerter service.

Rule {
    tag "Sample9"
    Class Services
    Id 4001
    level 4
    Service { Include "Alerter" }
    application { Include "*" }
    user_name { Include "*" }
    directives 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 severity 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 covers multiple services, add them in this section in different lines.
- **application { Include "*" }**: Indicates that this rule is valid for all processes. If you want to limit your rule to specific processes, spell them out here, complete with 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 want to limit your rule to specific user contexts, spell them out here in the form Local/user or Domain/user. See **Common Sections** for details.
- **directives service:stop**: Indicates that this rule covers deactivation of a service.

## Windows class SQL

The following table lists the possible sections and values for the Windows class SQL:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>MSSQL</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>See Common sections.</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication_mode</td>
<td>Boolean value that specifies whether Windows authentication (set to 1) or SQL authentication (set to 0) was used.</td>
<td>Example: OSQL-32, Internet Information Services</td>
</tr>
<tr>
<td>client_agent</td>
<td>Name of the utility sending the request on the client system.</td>
<td>Example: OSQL-32, Internet Information Services</td>
</tr>
</tbody>
</table>
### Section | Values | Notes
--- | --- | ---
**db_user_name** | Name of the user if SQL authentication was used, and "Trusted User" if Windows authentication is used. | Example: sa
**sp_name** | Stored procedure name. | This should match a stored procedure name. A stored procedure is identified by a supplied list of procedure names that is included for every SQL agent release (currently SPLlist.txt in the Agent directory).
**sp_param_char_len_one** | Contains the length of the parameter in number of characters. | 
**sp_param_one** | Contains the value of the parameter. | 
**sp_param_orign_len_one** | Contains the length of the parameter in number of bytes. | 
**sql_line_comment** | This value is set to 1 if the query includes a single line comment "-" containing a single quote. | 
**sql_original_query** | This contains the full SQL query exactly as it was received (including strings and whitespaces). | 
**sql_query** | This is the SQL query string with string values, whitespaces, and everything behind the comments stripped out. | 
**sql_user_password** | This is set to 1 if the password is NULL and 0 otherwise. | This is always set to 0 for non-SQL users. 
**transport** | On MSSQL 2005/2008, this is hard coded to: Shared memory (LPC). | 
**directives** | sql:request. | For incoming SQL requests

### Classes and directives per Windows platform

A list of the effective classes and directives per Windows platform:

- Windows XP, SP2, SP3, 32- and 64-bit (XP)
- Windows 2003, R2, R2 SP2, 32- and 64-bit (2K3)
- Windows Vista, 32- and 64-bit (V)
- Windows 2008 R2, (32- and 64-bit (2K8)
- Windows 7, 32- and 64-bit (7)
### Class Buffer Overflow

<table>
<thead>
<tr>
<th>Directives</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td>bo:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>XP</td>
<td>2K3</td>
<td>V</td>
</tr>
<tr>
<td>stack</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>heap</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>writeable_memory</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>invalid_call</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>target_bytes</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>call_not_found</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>call_return_unreadable</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>call_different_target</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>call_return_to_api</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### Class Files

<table>
<thead>
<tr>
<th>Directives</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td>files:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>XP</td>
<td>2K3</td>
<td>V</td>
</tr>
<tr>
<td>create</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>read</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>write</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>execute</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>delete</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>rename</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>attribute</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>writeop</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>hardlink</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### Class Hook

<table>
<thead>
<tr>
<th>Directives</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td>hook:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>XP</td>
<td>2K3</td>
<td>V</td>
</tr>
<tr>
<td>set_windows_hook</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
### Class Illegal API Use

<table>
<thead>
<tr>
<th>Directives</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td>illegal_api_use:</td>
<td>XP 2K3 V 2K8 7</td>
<td>XP 2K3 V 2K8 7</td>
<td>XP 2K3 V 2K8 7</td>
</tr>
<tr>
<td>bad_parameter</td>
<td>x x x x x</td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>invalid_call</td>
<td>x x x x x</td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
</tbody>
</table>

### Class Illegal Use

<table>
<thead>
<tr>
<th>Directives</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td>illegal:</td>
<td>XP 2K3 V 2K8 7</td>
<td>XP 2K3 V 2K8 7</td>
<td>XP 2K3 V 2K8 7</td>
</tr>
<tr>
<td>api</td>
<td>x x x x x</td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
</tbody>
</table>

### Class ISAPI

<table>
<thead>
<tr>
<th>Directives</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td>isapi:</td>
<td>XP 2K3 V 2K8 7</td>
<td>XP 2K3 V 2K8 7</td>
<td>XP 2K3 V 2K8 7</td>
</tr>
<tr>
<td>request</td>
<td>x x</td>
<td>x x</td>
<td>x x</td>
</tr>
<tr>
<td>requrl</td>
<td>x x</td>
<td>x x</td>
<td>x x</td>
</tr>
<tr>
<td>reqquery</td>
<td>x x</td>
<td>x x</td>
<td>x x</td>
</tr>
<tr>
<td>rawdata</td>
<td>x x</td>
<td>x x</td>
<td>x x</td>
</tr>
<tr>
<td>response</td>
<td>x x</td>
<td>x x</td>
<td>x x</td>
</tr>
</tbody>
</table>

### Class Program

<table>
<thead>
<tr>
<th>Directives</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td>program:</td>
<td>XP 2K3 V 2K8 7</td>
<td>XP 2K3 V 2K8 7</td>
<td>XP 2K3 V 2K8 7</td>
</tr>
<tr>
<td>run</td>
<td>x x x x x</td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>open_with_any</td>
<td>x x x x x</td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>open_with_create_thread</td>
<td>x x x x x</td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>open_with_modify</td>
<td>x x x x x</td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>open_with_terminate</td>
<td>x x x x x</td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
<tr>
<td>open_with_wait</td>
<td>x x</td>
<td>x x</td>
<td>x x</td>
</tr>
</tbody>
</table>

### Class Registry

<table>
<thead>
<tr>
<th>Directives</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td>registry:</td>
<td>XP 2K3 V 2K8 7</td>
<td>XP 2K3 V 2K8 7</td>
<td>XP 2K3 V 2K8 7</td>
</tr>
<tr>
<td>create</td>
<td>x x x x x</td>
<td>x x x x x</td>
<td>x x x x x</td>
</tr>
</tbody>
</table>
### Directives

<table>
<thead>
<tr>
<th>registry:</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>XP</td>
<td>2K3</td>
<td>V</td>
</tr>
<tr>
<td>read</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>delete</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>modify</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>permissions</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>enumerate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>monitor</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>restore</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>replace</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>load</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>open_existing_key</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>rename</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### Class Services

<table>
<thead>
<tr>
<th>services:</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>XP</td>
<td>2K3</td>
<td>V</td>
</tr>
<tr>
<td>start</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>stop</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>pause</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>continue</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>startup</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>profile_enable</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>profile_disable</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>logon</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>create</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>delete</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### Class SQL

<table>
<thead>
<tr>
<th>sql:</th>
<th>32-bit processes on 32-bit Windows OS (x32)</th>
<th>32-bit processes on 64-bit Windows OS (x64)</th>
<th>64-bit processes on 64-bit Windows OS (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>XP</td>
<td>2K3</td>
<td>V</td>
</tr>
<tr>
<td>request</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Non-Windows custom signatures

This section describes how to write custom signatures for the Solaris and Linux platforms.

**NOTE:** Rules in the Windows class Files use double slashes, while rules in the non-Windows class UNIX_file use a single slash.

The class of the signature depends on the nature of the security issue and the protection the signature can offer. For Solaris and Linux, these classes are available:

<table>
<thead>
<tr>
<th>Class</th>
<th>When to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIX_file</td>
<td>For file or directory operations on Solaris and Linux.</td>
</tr>
<tr>
<td>UNIX_apache</td>
<td>For http requests on Solaris and Linux.</td>
</tr>
<tr>
<td>UNIX_Misc</td>
<td>For safeguarding access protection on Solaris and Linux.</td>
</tr>
<tr>
<td>UNIX_bo</td>
<td>For buffer overflow. Solaris only.</td>
</tr>
<tr>
<td>UNIX_map</td>
<td>For mapping files or devices into memory. Solaris only.</td>
</tr>
<tr>
<td>UNIX_GUID</td>
<td>For allowing users to run an executable with the permissions of the executable's owner or group. Solaris only.</td>
</tr>
</tbody>
</table>

Solaris/Linux class UNIX_file

The following table lists the possible sections and values for the Unix-based class UNIX_file:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>UNIX_file</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td></td>
<td>See Common sections.</td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>files</td>
<td>File or folder involved in the operation</td>
<td>One of the required parameters. Files to look for. See Note 1.</td>
</tr>
<tr>
<td>source</td>
<td>Target file names</td>
<td>One of the required parameters. See Note 1.</td>
</tr>
<tr>
<td>file</td>
<td>List of permissions of source file names</td>
<td>Solaris Only. Optional. See Note 2.</td>
</tr>
<tr>
<td>new</td>
<td>Permission mode of newly created file or modified permission</td>
<td>Solaris Only. Optional. See Note 2.</td>
</tr>
<tr>
<td>zone</td>
<td>Name of the zone to which the signature applies</td>
<td>Solaris 10 or later. See Note 5.</td>
</tr>
<tr>
<td>directives</td>
<td>unixfile:chdir</td>
<td>Changes the working directory.</td>
</tr>
<tr>
<td></td>
<td>unixfile:chmod</td>
<td>Changes the permissions on a directory or file.</td>
</tr>
<tr>
<td></td>
<td>unixfile:chown</td>
<td>Changes the ownership of a directory or file.</td>
</tr>
<tr>
<td></td>
<td>unixfile:create</td>
<td>Creates a file.</td>
</tr>
</tbody>
</table>
### Section Values Notes

<table>
<thead>
<tr>
<th>unixfile:link</th>
<th>Creates a hard link. See Note 3.</th>
</tr>
</thead>
<tbody>
<tr>
<td>unixfile:mkdir</td>
<td>Creates a directory.</td>
</tr>
<tr>
<td>unixfile:read</td>
<td>Opens a file in read only mode.</td>
</tr>
<tr>
<td>unixfile:rename</td>
<td>Renames a file. See Note 4.</td>
</tr>
<tr>
<td>unixfile:rmmdir</td>
<td>Removes a directory.</td>
</tr>
<tr>
<td>unixfile:symlink</td>
<td>Creates a symbolic link.</td>
</tr>
<tr>
<td>unixfile:unlink</td>
<td>Deletes a file from a directory or deletes a directory.</td>
</tr>
<tr>
<td>unixfile:write</td>
<td>Opens a file in read/write mode.</td>
</tr>
<tr>
<td>unixfile:setattr</td>
<td><strong>Linux only.</strong> Changes the permissions and ownership of the directory or file.</td>
</tr>
<tr>
<td>unixfile:mknod</td>
<td>Creates a node.</td>
</tr>
<tr>
<td>unixfile:access</td>
<td>Changes the file attributes. Monitored attributes are “Read-only”, “Hidden”, “Archive” and “System”.</td>
</tr>
<tr>
<td>unixfile:foolaccess</td>
<td><strong>Solaris Only.</strong> File name has 512 consecutive ‘/’.</td>
</tr>
<tr>
<td>unixfile:prioctrl</td>
<td><strong>Solaris Only.</strong> Displays or sets scheduling parameters.</td>
</tr>
</tbody>
</table>

### Note 1

**Relevant 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>chdir</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</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>link</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mknod</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rename</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>rmdir</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>setattr</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>symlink</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unlink</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>
</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.

Note 5
By default, all zones are protected by the signature. To restrict protection to a particular zone, add a zone section in the signature and include the name of the zone.
For example, if you have a zone named "app_zone" whose root is /zones/app, then the rule:
```
Rule {
...
file { Include "/tmp/test.log" }
zone { Include "app_zone" }
... }
```
would apply only to the file in the zone "app_zone" and not in the global zone.
Note that in this release, web server protection cannot be restricted to a particular zone.

Advanced details
Some or all of the following parameters appear in the Advanced Details tab of security events for the class UNIX_file. 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). Solaris only.</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. Solaris only.</td>
</tr>
</tbody>
</table>
Solaris/Linux class UNIX_apache (HTTP)

The following table lists the possible sections and values for the UNIX-based class apache:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>UNIX_apache</td>
<td></td>
</tr>
<tr>
<td>Id</td>
<td>See Common sections.</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>url</td>
<td>Optional. Matched against the url part of an incoming request. See Notes 1-4.</td>
<td></td>
</tr>
<tr>
<td>query</td>
<td>Optional. Matched against the query part of an incoming request. See Notes 1-4.</td>
<td></td>
</tr>
<tr>
<td>method</td>
<td>“GET”, “POST”, “INDEX” and all other allowed http methods</td>
<td>Optional. See Note 4.</td>
</tr>
<tr>
<td>zone</td>
<td>Name of the zone to which the signature applies</td>
<td>Solaris 10 or later. See Note 5.</td>
</tr>
<tr>
<td>directives</td>
<td>apache:requrl</td>
<td>For URL requests.</td>
</tr>
<tr>
<td></td>
<td>apache:reqquery</td>
<td>For query requests.</td>
</tr>
<tr>
<td></td>
<td>apache:rawdata</td>
<td>For raw data requests.</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" is matched against {url} and the section "query" is matched against {query}.

For example the following rule is triggered if the http request http://www.myserver.com/search/abc.exe?subject=wildlife&environment=ocean is received by IIS:

Rule {
  Class UNIX_apache
  Id 4001
  level 1
  url { Include "*abc*" }
  time { Include "*" }
  application { Include "*" }
  user_name { Include "*" }
  directives 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 matches 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 apache:request}

Note 4
A rule needs to contain at least one of the optional sections url, query, method.

Note 5
By default, all zones are protected by the signature. To restrict protection to a particular zone, add a zone section in the signature and include the name of the zone.
For example, if you have a zone named "app_zone" whose root is /zones/app, then the rule:

Rule {
... 
file { Include "/tmp/test.log" } 
zone { Include "app_zone" } 
... }

would apply only to the file in the zone "app_zone" and not in the global zone.

Note that in this release, web server protection cannot be restricted to a particular zone.

Solaris/Linux class UNIX_Misc

The following table lists the possible sections and values for the Solaris or Linux class UNIX_misc:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>UNIX_misc</td>
<td>A miscellaneous class that safeguards access protection.</td>
</tr>
<tr>
<td>Id</td>
<td>See Common sections.</td>
<td></td>
</tr>
</tbody>
</table>


Solaris class UNIX_bo

The following table lists the possible sections and values for the Solaris class_bo (Buffer Overflow):

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>zone</td>
<td>Name of the zone to which the signature applies</td>
<td>Solaris 10 or later.</td>
</tr>
<tr>
<td>directives</td>
<td>unixmisc:killagent</td>
<td>Prevents SIGKILL signal to be sent to the client.</td>
</tr>
</tbody>
</table>

**Note 1**

By default, all zones are protected by the signature. To restrict protection to a particular zone, add a zone section in the signature and include the name of the zone.

For example, if you have a zone named "app_zone" whose root is /zones/app, then the rule:

Rule {
  ...
  file { Include "/tmp/test.log" }
  zone { Include "app_zone" }
}
would apply only to the file in the zone "app_zone" and not in the global zone.
Note that in this release, web server protection cannot be restricted to a particular zone.

**Solaris class UNIX_map**

The following table lists the possible sections and values for the Solaris class Unix_map:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>UNIX_map</td>
<td>Use this class to map UNIX files or devices into memory.</td>
</tr>
<tr>
<td>Id</td>
<td>See Common sections.</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>zone</td>
<td>Name of the zone to which the signature applies</td>
<td>Solaris 10 or later.</td>
</tr>
<tr>
<td>directives</td>
<td>mmap:mprotect</td>
<td>Sets the access protection of memory pages.</td>
</tr>
<tr>
<td></td>
<td>mmap:mmap</td>
<td>Maps files or devices into memory.</td>
</tr>
</tbody>
</table>

**Solaris class UNIX_GUID**

The following table lists the possible sections and values for the Solaris class UNIX_GUID:

<table>
<thead>
<tr>
<th>Section</th>
<th>Values</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>UNIX_GUID</td>
<td>Use this class to set Unix access rights flags that allow users to run an executable with the permissions of the executable's owner or group.</td>
</tr>
<tr>
<td>Id</td>
<td>See Common sections.</td>
<td></td>
</tr>
<tr>
<td>level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>zone</td>
<td>Name of the zone to which the signature applies</td>
<td>Solaris 10 or later.</td>
</tr>
<tr>
<td>directives</td>
<td>guid:setuid</td>
<td>Sets user ID to allow a user to run an executable with the permissions of the executable's owner.</td>
</tr>
<tr>
<td></td>
<td>guid:seteuid</td>
<td>Sets effective user ID.</td>
</tr>
<tr>
<td></td>
<td>guid:setreuid</td>
<td>Sets the real and effective user ID.</td>
</tr>
<tr>
<td></td>
<td>guid:setgid</td>
<td>Sets group ID to allow a group to run an executable with the permissions of the executable's group.</td>
</tr>
<tr>
<td></td>
<td>guid:setegid</td>
<td>Sets effective group ID.</td>
</tr>
</tbody>
</table>
### Classes and directives per UNIX platform

A list of the effective classes and directives per non-Windows platform:

**Class UNIX_bo**

<table>
<thead>
<tr>
<th>Directives</th>
<th>RedHat Linux</th>
<th>SuSE Linux</th>
<th>Solaris 9</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>unixbo:binargs</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>unixbo:illegal_address</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>unixbo:exec</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>unixbo:environment</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>unixbo:binenv</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>unixbo:libc</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

**Class UNIX_file**

<table>
<thead>
<tr>
<th>Directives</th>
<th>RedHat Linux</th>
<th>SuSE Linux</th>
<th>Solaris 9</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>unixfile:chdir</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:chmod</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:chown</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:create</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:link</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:mkdir</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:rename</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:rmkdir</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:setattr</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:symlink</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:unlink</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:write</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:mknod</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:access</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:foolaccess</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>unixfile:procntl</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
### Class UNIX_Misc

<table>
<thead>
<tr>
<th>Directives</th>
<th>RedHat Linux</th>
<th>SuSE Linux</th>
<th>Solaris 9</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>unixmisc:killagent</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

### Class UNIX_apache

<table>
<thead>
<tr>
<th>Directives</th>
<th>RedHat Linux</th>
<th>SuSE Linux</th>
<th>Solaris 9</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>apache:requrl</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>apache:reqquery</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>apache:rawdata</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

### Class UNIX_map

<table>
<thead>
<tr>
<th>Directives</th>
<th>RedHat Linux</th>
<th>SuSE Linux</th>
<th>Solaris 9</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>mmap:mprotect</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mmap:mmap</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

### Class UNIX_GUID

<table>
<thead>
<tr>
<th>Directives</th>
<th>RedHat Linux</th>
<th>SuSE Linux</th>
<th>Solaris 9</th>
<th>Solaris 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>guid:setuid</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>guid:seteuid</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>guid:setreuid</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>guid:setgid</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>guid:setegid</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>guid:setregid</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Appendix B — Troubleshooting

KnowledgeBase articles on the McAfee Support site http://mcafee.com offer you the most up-to-date support information on issues and troubleshooting. Refer to KB69184 for the latest information.

Contents
- General issues
- Host IPS logs
- Clientcontrol.exe utility

General issues

Which Host Intrusion Prevention services should be installed and running on the client system for proper functioning of the software?

These services should always be active to provide intrusion prevention protection with either or both IPS and firewall:
- McAfee Host Intrusion Prevention Service (FireSvc.exe)
- McAfee Firewall Core Service (mfefire.exe)
- McAfee Validation Trust Protection Service (mfevtps.exe)

These services should be active when called:
- McAfee Host Intrusion Prevention system tray icon service (FireTray.exe).
- McAfee Host Intrusion Prevention client console (McAfeeFire.exe)

How do I prevent the firewall from blocking non-IP traffic?

Unless specifically indicated in a firewall rule, some types of non-IP traffic are not recognized by the firewall and as a result are blocked. Additionally, the adaptive and learn modes do not dynamically detect and create firewall rules for non-IP protocols. To prevent non-IP protocols from being dropped, select Allow traffic for unsupported protocols in the Firewall Options policy. You can then check the Activity Log for Allowed Incoming/Outgoing Non-IP Protocol: 0xXXX, where 0xXXX indicates the IANA Ethernet number of the protocol (see http://www.iana.org/assignments/ethernet-numbers). Use this information to determine the non-IP traffic that is needed and create a firewall rule that allows it.
What should I do if an application fails or functionality is impaired after Host Intrusion Prevention is installed or content is updated?

If you have an application whose behavior changed after installing or updating the Host Intrusion Prevention client or a content update, you need to determine if it is a signature or some other element that is causing the problem.

If the issue occurs because of an IPS signature:

1. Enable IPS logging (written to HipShield.log) and firewall logging (written to FireSvc.log) on the client or in the Client UI policy on the ePolicy Orchestrator server and reproduce the issue.
3. If a new signature is blocking activity because of an event, go to the Event tab of Host IPS under Reporting on the ePolicy Orchestrator server, find the event, and create an exception. Be sure to make the exception as granular as possible by using the advanced parameters for the event.
4. If there are limited advanced parameters for the event, view the signature related to the event. If a Common Vulnerabilities and Exposures (CVE) item is referenced in the IPS signature description, this indicates a security update patch is available. Apply the patch and disable the signature.

If the issue is not related to an IPS signature:

1. Disable all Host Intrusion Prevention modules (IPS, Network IPS, and Firewall), and retest to verify the issue occurs.
2. Disable IPS and stop the Host Intrusion Prevention client service (FireSvc.exe), then retest to verify the issue occurs.
3. If issue did not occur, select Allow traffic for unsupported protocols in the Firewall Options policy from the ePolicy Orchestrator server and apply the policy to the client. Retest with this option set. Note: Even if the firewall is disabled, traffic can still be dropped when Host Intrusion Prevention is active.
4. If these steps do not resolve the issue, disable the McAfee NDIS Intermediate Filter Miniport adapter, and retest to verify if the issue occurs.
5. If these steps do not resolve the issue, uninstall the McAfee NDIS Intermediate Filter Miniport adapter, and retest to verify if the issue occurs. For details, refer to KnowledgeBase article 51676 at http://knowledge.mcafee.com.
6. If the issue does not occur with NDIS uninstalled, refer to KnowledgeBase article 68557 at http://knowledge.mcafee.com and test with NDIS uninstalled and the Microsoft Pass Thru driver installed.

If the issue occurs only with the IPS module enabled and no <Event> violations occurred in HipShield.log:

1. Identify the executables associated with the application.
2. Exclude the executables for protection from the Host IPS Application Protection List.
3. Repeat test for application functionality. Note the results.
4. Include the executables you excluded in step 2.
5. Isolate the IPS engine that might be causing the issue. For details, refer to KnowledgeBase article 54960 at http://knowledge.mcafee.com.
6. Identify the IPS engine that causes the issue.
How do I isolate a component in Host IPS to find out which one is causing a problem?

NOTE: This process includes steps that might require repeated restarts, logons, or recreating issues. The following steps should be performed on the local client system with the Host IPS console. If you find the cause of the issue but cannot resolve it, forward the logs you obtain to McAfee Support.

Disable all components and test for failure:

1. Disable IPS: Click the **IPSPolicy** tab, and deselect **Enable Host IPS** and **Enable Network IPS**.
2. Disable Firewall: Click the **Firewall Policy** tab, and deselect **Enable Firewall**.
3. Clear the Blocked Hosts list: Click the Blocked Hosts tab and clear the list by selecting each entry and clicking **Remove**.
4. Enable Activity logging: Click the **ActivityLog** tab and verify that all traffic logging and filter option checkboxes are selected.
5. Test the system to see if the problem recurs:
   - If the problem persists, continue to Step 6,
   - If the problem stops, skip to Step 1 of the Iterative testing phase.
6. Check the following:
   - Stop the McAfee Host IPS service and retest. If the problem goes away, report the issue as associated directly with the service.
   - Uninstall the Host IPS client from the local system and retest. If the problem goes away, report the issue as associated with installed files and not a specific component.

Iterative Testing phase of each component:

**Test Host IPS**

1. Click the **Activity Log** tab and clear the log.
2. Click the **IPSPolicy** tab and select **Enable Host IPS**.
3. Test the system to determine if the problem recurs:
   - If the problem does not recur, skip to Step 5, Test Network IPS.
   - If the problem recurs:
     1. Deselect **Enable Host IPS**.
     2. Retest to verify the problem goes away. If the problem is resolved, Host IPS can potentially be associated with the issue.
     3. Save a copy of the Activity log and name it **Host IPS Activity Log wProb**, for reporting to support.
     4. Select **Enable Host IPS** and verify that the problem returns.

**Test all IPS engines**

1. Click **Help** and select **Troubleshooting**.
2. Select **Error** reporting under IPS logging.
3. Select **Log security violations**.
4. Click **Functionality**.
5. On the HIPS Engines dialog box, deselect **Enable / Disable all engines** and click **OK**.
6. Test the system to determine if the problem recurs.
7 Do one of the following:
   • If the problem recurs, note whether the problem is associated with the IPS component but not the specific engines. Review hipshield.log to see if the IPS component is the problem.
   • If the problem does not recur, the issue might be associated with a specific engine. Continue to the next step, Test Each IPS Engine.

**Test each IPS engine**
1 Click Help and select Troubleshooting.
2 Select Error reporting under IPS logging.
3 Select Log security violations.
4 Click Functionality.
5 Select the engines, one at a time, and retest.
6 Save a copy of the hipshield log for each test and label with the name of the engine tested, for reporting to support.
7 When testing is complete, enable all the engines to continue to the next step.

**Test IPS Adaptive Mode**
1 Click the Activity Log tab and clear the log.
2 Click the IPS Policy tab and select Enable Adaptive Mode.
3 Test the system to determine if the problem recurs.
4 Do one of the following:
   • If the problem recurs, deselect Enable Adaptive Mode and retest to see if the problem is resolved. If it is, Host IPS in Adaptive Mode can potentially be associated with the issue. Save a copy of the Activity log and name it Host IPS Adaptive Activity Log wProb, for reporting to support.
   • If the problem does not recur, deselect Enable Host IPS and continue to the next step.

**Test Network IPS**
1 Click the Activity Log tab and clear the log.
2 Click the IPS Policy tab and select Enable Network IPS.
3 Test the system to determine if the problem recurs.
4 Do one of the following:
   • If the problem recurs, deselect Enable Network IPS and retest to see if the problem is resolved. If it is, Network IPS can potentially be associated with the issue. Save a copy of the Activity log and name it Network IPS Activity Log wProb, for reporting to support.
   • If the problem does not recur, select Enable Network IPS and continue to the next step.

**Test Automatic Blocking of Network IPS**
1 Click the Activity Log tab and clear the log.
2 Click the IPS Policy tab and select Enable Network IPS.
3 Click the Automatically Block Attackers checkbox.
4 Test the system to determine if the problem recurs. If it does:
a Deselect **Automatically Block Attackers** and retest to see if the problem is resolved. If it is, Network IPS in Block Attackers Mode can potentially be associated with the issue.

b Click the **Blocked Hosts** tab, note any blocked attacker entries, and review for false positives.

c Save a copy of the **Activity log** and name it to **Network IPS Adaptive Activity Log wProb**, for reporting to support.

5 If the problem does not recur, deselect **Enable Network IPS** and continue to the next step.

**Test Firewall Policy**

1 Click the **Activity Log** tab and clear the log.

2 Click the **Firewall Policy** tab and select **Enable Firewall**.

3 Test the system to determine if the problem recurs. If it does:
   a Deselect **Enable Firewall**.
   b Retest to verify the problem is resolved. If it is, Host IPS Firewall can potentially be associated with the issue.
   c Save a copy of the **Activity log** and name it **Firewall Activity Log wProb**.

4 If the problem does not recur, select **Enable Firewall** and continue to the next step.

**Test Firewall Learn Mode**

1 Click the **Activity Log** tab and clear the log.

2 Click the **Firewall Policy** tab and select **Learn Mode** and **Incoming**. Deselect **Outgoing**.

3 Test the system to determine if the problem recurs. If it does:
   a Deselect **Incoming**.
   b Retest to verify the problem is resolved. If it is, Firewall Incoming Learn Mode can potentially be associated with the issue.
   c Save a copy of the **Activity log** and name it **Firewall Activity Log LearnIN wProb**, for reporting to support.
   d Click the **Activity Log** tab and clear the log.

4 Click the **Activity Log** tab and clear the log.

5 Click the **Firewall Policy** tab and select **Learn Mode** and **Outgoing**. Deselect **Incoming**.

6 Test the system to determine if the problem recurs. If it does:
   a Deselect **Outgoing**.
   b Retest to verify the problem is resolved. If it is, Firewall Outgoing Learn Mode can potentially be associated with the issue.
   c Save a copy of the **Activity log** and name it **Firewall Activity Log LearnOUT wProb**, for reporting to support.
   d Click the **Activity Log** tab and clear the log.

7 Navigate to the **Firewall Policy** tab.

8 Click the **Firewall Policy** tab and select **Learn Mode** and both **Incoming** and **Outgoing**.

9 Test the system to determine if the problem recurs. If it does:
   a Deselect **Incoming** and **Outgoing**.
b Retest to verify the problem is resolved. If it is, Firewall Incoming and Outgoing Learn Mode can potentially be associated with the issue.

c Save a copy of the Activity log and name it **Firewall Activity Log LearnINOUT wProb**, for reporting to support.

**Test with a Firewall Any Any rule**

**NOTE:** This step might need to be configured from the ePO management console as it is imperative that the first rule in the firewall rule list be the Any Any test rule. If other policies have been configured from the console, they take precedence over the locally created rules.

1 Create a new rule and name it **Any Any**.

2 Set the Action to **Permit**.

3 Set the Protocol to **IP TCP**.

4 Set the Direction to **Either**.

5 Save the rule. If the rule is created in a policy on the ePO console, move the **Any Any** rule to be the first rule in the policy list. If the rule is created locally, ensure no other rules precedes it.

6 Test the system to determine if the problem recurs. If it does:

   a Disable the **Any Any** rule.

   b Retest to verify the problem is resolved. If it is, there is probably a configuration error with the rules.

   c Take a screenshot of the list of firewall on the **Firewall Policy** tab.

   d Save a copy of the **Activity log** and name it to **Firewall Activity Log AnyAny Test**.

   e Export the **Host IPS policy** settings:

      a Log on to the ePO console.

      b Navigate to the **Policy Catalog** object in the ePO System Tree.

      c Locate **Host IPS** and expand it.

      d Click **Export all policies**.

7 Click the **Firewall Policy** tab, deselect the **Enable Firewall** checkbox, and continue to the next step.

**Test Blocked Hosts Policy**

1 Click the **Activity Log** tab and clear the log.

2 Click the **Blocked Hosts** tab and remove all blocked hosts from the list.

3 Test the system to determine if the problem recurs. If it does, it is probably not associated with Blocked Hosts.

If you still have not found the cause of the issue, contact McAfee Support, explain the issue, and attach data obtained by going through this process.

---

**Host IPS logs**

**Where are log files located?**

All log files are in one of these directories on the client system, depending on the operating system:
How do I enable logging?

You can set Host IPS logging with the Host IPS client console or with the Host IPS Client UI Policy from the ePolicy Orchestrator console.

To enable logging from the client:

1. From the tray icon, open the Host IPS console. Unlock the user interface with an administrator or time-based password.
2. Select Help | Troubleshooting.
3. Select the required logging settings:
   - **Debug** — logs all messages.
   - **Information** — logs Information, Warning, and Error messages.
   - **Warning** — logs Warning and Error messages.
   - **Error** — logs Error messages.
   - **Disabled** — logs no messages.

   Firewall and IPS logging are controlled independently. These logging settings remain in effect until the client console is locked and a subsequent policy enforcement occurs.

   **NOTE:** Logging can also be set locally by adding the DWORD 'debug_enabled' value in the HKLM\Software\McAfee\HIP registry key. A value of decimal 1 turns on verbose debug logging. The use of the local registry key to enable debug logging overrides any policy set using ePolicy Orchestrator.

To enable logging from ePolicy Orchestrator:

1. Under Host IPS: General, edit the Client UI policy that is to be applied to a client.
2. Click the **Troubleshooting** tab.
3. Select the required logging settings:
   - **Debug** — logs all messages.
   - **Information** — logs Information, Warning, and Error messages.
   - **Warning** — logs Warning and Error messages.
   - **Error** — logs Error messages.
   - **Disabled** — logs no messages.

   Firewall and IPS logging are controlled independently. These logging settings are applied at the next policy enforcement.

Which log files are associated with the Host IPS component?

The primary log file for the Host IPS component is **HipShield.log**. This log file grows to 128 MB and rotates with 1 back up.

Log file rotation is controlled by the DWORD entries `log_rotate_size_kb` and `log_rotate_count` in the HKLM\SOFTWARE\McAfee\HIP registry key. The `log_rotate_count` key determines the number of backup log files to preserve, and the DWORD `entrylog_rotate_size_kb` is the approximate size in KB of a backup log file, where 0 means log rotation is disabled.
When the log_rotate_size_kb specified size has been exceeded, the file is closed and renamed with the suffix \1. If a file with that name already exists, the suffix is incremented by one. When the specified number of backup files is reached, the oldest is deleted.

**NOTE:** When collecting data for incidents escalated to McAfee Support, we strongly recommend that the `debug_enabled` registry value be created and set to 1. This registry value logs all Host and Network IPS events to HIPShield.log, regardless of the Log Status setting under signature properties. Be sure to stop the service, delete old log files, restart the service, and perform the reproduction. This minimizes the size of the log files.

**What are things to look for in HipShield.log?**

A run of the Host IPS component begins with a banner statement that identifies the build run and the date/time stamp of the session. Each entry of the HipShield log shows a date/time stamp, followed by an indication as to whether this data is informational, debugging, or error. The data contained in the HipShield is ad-hoc, and differs between portions of the Host IPS component.

Key areas of interest:

- Lines beginning with `In install modules new` describe the copying of files as part of the start of the Host IPS component. Failure to copy these files prevents the Host IPS component from starting.
- A line beginning with `Scrutinizer initialized successfully` indicates that loading of the Host IPS component has been successful up through the initialization of the Scrutinizer, which depends on the above-mentioned files having been copied properly.
- A line beginning with `New Process: Pid=` indicates the Host IPS component is able to monitor process creation.
- A line beginning with `IIS-Start` indicates that IIS monitoring is beginning.
- A line beginning with `Scrutinizer started successfully ACTIVATED status` indicates that the Scrutinizer has successfully started.
- A line beginning with `Hooking xxx` indicates that process hooking is proceeding. The number `xxx` indicates the PID (process ID) of the process being hooked.
- A series of lines beginning with `Processing Buffer xxx.scn` is reporting the results of the Scanner processing of scanfile `xxx.scn`, where `xxx` is a name like `EnterceptMgmtServer`, as shown above. Errors in the Scanners processing of scan files are reported here.
- Lines in the format `signature=111 level=2, log=True` report that an individual signature has been loaded. The signature ID and level are included along with an indication of whether logging is enabled for this signature.

**NOTE:** `Shield.db` and `except.db` are created in the same directory as the logs only when debugging is enabled. These files contain a dump of the rules and exceptions that are sent to the kernel after the AgentNT.dll has processed the content.

**Which log files are associated with the firewall component?**

The primary log files for the Firewall component and what they contain:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Contains this data</th>
</tr>
</thead>
<tbody>
<tr>
<td>FireSvc.log</td>
<td>Main service log</td>
<td>• Debug level logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Location matching output</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TrustedSource connection rating output</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Errors/warnings</td>
</tr>
</tbody>
</table>
### ClientControl.exe Utility

This command line utility helps automate upgrades and other maintenance tasks when third-party software is used to deploy Host Intrusion Prevention on client computers. It can be included in installation and maintenance scripts to temporarily disable IPS protection and activate logging functions.

#### Function and Setup

This utility allows administrators to perform the following on the McAfee Host IPS client:

- Start the Host IPS service.
- Stop the Host IPS service (requires administrator or time-based password).
- Change log settings (requires administrator or time-based password).
- Start/stop the Host IPS engines (requires administrator or time-based password).
- Export the activity log to a formatted text file.
- Display the NaiLite license data residing in the registry on the client computer.
- Export configuration settings to a formatted text file.
- Replace configuration settings with default policy settings.
- Export IPS startup protection rules from the registry.
The utility records its activities to ClientControl.log at: C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention; or C:\ProgramData\McAfee\Host Intrusion Prevention on Windows Vista, Windows 2008, and Windows 7.

To enable logging, modify HKLM\Software\McAfee\HIP in the registry by adding the DWORD type FwLogLevel entry with a value of 0x7.

**Stopping Host IPS services**

The /stop parameter stops Host IPS services if the user has administrative authority to stop services. If the user has authority to stop services on the computer, the following occurs:

- Host IPS services are turned off. The **Host IPS checkbox on the IPS Policy tab is automatically deselected**.
- Host IPS services are not stopped. An entry is made in ClientControl.log.
- The McAfee Agent enforces policies at next policy enforcement interval.
- If the McAfee Agent enforces policies while you are engaged in an activity that requires that protection be disabled (e.g. patching Windows), your activity might be blocked by the enforced policies.

Even if stopping Host IPS services is successful, policy settings might allow the McAfee Agent to restart them at the next Agent-Server Communication Interval (ASCI). To prevent this:

1. In ePolicy Orchestrator, open the Host Intrusion Prevention: General policy.
2. Select the **Advanced** tab.
3. Deselect **Perform product integrity check**.
4. Run an agent wake-up call.

**Command-line syntax**

**Conventions:**
- [ ] means **required**.
- [xxx, ...] means **one or more**.
- < > means **user-entered data**.

**Major arguments:**

Only one of the following *major* arguments is allowed per invocation:

- /help
- /start
- /stop
- /log
- /engine
- /export

However, you can specify more than one log option when changing log settings.

Running the utility with the /help command provides the most up-to-date help information and notes.

**Usage:**

clientcontrol [arg]

**Argument definitions:**

- /help
Displays command-line syntax and notes.

- **/start**
  Starts the service.

- **/stop <password>**
  Stops the service.

- **/log <password> [log type] [log options]**
  Generates logs. Log options are processed in order.
  Log type definitions:
  - 0 = HIPS (create a HipShield.log)
  - 1 = Firewall (create a FireSvc.log)

  Log option definitions:
  - 0 = off
  - 1 = error
  - 2 = warning
  - 3 = info
  - 4 = debug
  - 5 = security violation (IPS only)

- **/engine <password> [engine type] [engine option]**
  Turns engines off and on.
  Engine type definitions:
  - 0 = all
  - 1 = Buffer Overflow
  - 2 = SQL (server only)
  - 3 = Registry
  - 4 = Services
  - 5 = Files
  - 6 = HTTP (server only)
  - 7 = Host IPS API
  - 8 = Illegal Use
  - 9 = Program
  - 10 = Hook

  Engine option definitions:
  - 0 = off
  - 1 = on

- **/export /s <path of export source file> <path of event log export file>**
  Exports the event log to a formatted text file. The source file path is optional. Do not include "/s" if there is no source file.

- **/readNaiLic**
  Displays the NaiLite license data.

- **/exportConfig <path of export file> <config type>**
Exports configuration settings to a formatted text file.

Configuration type definitions:

- 0 = all
- 1 = application protection
- 2 = blocked hosts
- 3 = firewall
- 4 = host IPS custom signatures
- 5 = IPS exceptions
- 6 = settings
- 7 = trusted applications
- 8 = trusted networks
- 9 = network IPS signatures
- 10 = host IPS signatures
- 11 = host IPS engines
- 12 = logon sessions
- 13 = DNS blocking rules

- `/defConfig <password>`
  Replaces the configuration settings with client default policies for application protection, firewall, and trusted applications settings.

- `/bootTimeRules <password> <path_of_export_file>`
 Exports IPS startup rules to a formatted text file.

**NOTE:**

- There must be at least one space between the argument, the password, and any other required parameters.

**Sample workflows**

**Applying a patch to a computer protected by McAfee Host IPS**

1. Open a command shell.
2. Run `clientcontrol.exe /stop <password>`
3. Perform your maintenance activity.
4. Run `clientcontrol.exe /start` (to restart Host IPS services).

**Exporting the Host IPS Activity Log to a text file**

1. Open a command shell.
2. Run `clientcontrol.exe /export <path_of_export_file>`
3. Copy the exported log file to another computer for collection and analysis.

**Turn on logging as part of a troubleshooting exercise**

1. Open a command shell.
2. Run `clientcontrol.exe /log <password> [log type] [log option, ...]`
3. Perform activity to generate log entries.
4. Review HipShield.log or FireSvc.log for relevant information.
Turning off specific Host IPS engines as part of a troubleshooting exercise

1. Open a command shell.
2. Run `clientcontrol.exe /<password> [engine type] [engine option]`
3. Perform activity to generate reactions and log entries.
4. Review `HipShield.log` or `FireSvc.log` for relevant information.
Index

A
activity logs, Host IPS
customizing options 93
deleting entries 93
firewall logging options 85
IPS logging options 85
viewing 93
working with Activity Log tab 93
adaptive mode
applying 21
FAQ 21
rules not created automatically 21
with IPS vs firewall 21
about 10
automatic tuning 18
exception and 32
Firewall Options policies 64
Firewall Rules policies 67
IPS Options policy 34
placing Host IPS clients in 20, 33
advanced properties, Host IPS
automatic responses 26
alerts, Host IPS
firewall 87
intrusion alerts 86
learn mode and unknown network traffic 63
responding to 86, 87
setting options for clients 83
spoof detected 87
Windows clients 86
allow and block actions
network communications, Firewall Policy 89
stateful firewall filtering 60
application protection rules
about 33
configuring 45
creating 45
IPS Rules policy 33, 36, 45
overview 43
processes, allowed or blocked 43
working with 43
automatic responses, Host IPS
about 26
configuring 17
rules and events 26
buffer overflow
configuring Trusted Applications policy 78
IPS behavioral rules and 32
preventing on Solaris client 94
C
client rules
Firewall 64, 71
creating, with adaptive and learn modes 10
creating exceptions 32
Firewall 64, 71
Host IPS queries 13
IPS 36
IPS Rules policy, overview 50
Client UI policy
about 8
configuring 74
define 74
General tab, configuring 75
options 83
overview 73
passwords 75
tray icon control, configuring 75
troubleshooting 76
ClientControl utility
command-line syntax 144
function and setup 144
stopping services 144
using to troubleshoot 144
clients
analyzing data on Host IPS clients 19
Linux (See Linux client) 97
naming conventions for Host IPS 19
queries for groups of 13
Solaris (See Solaris client) 94
tuning Host IPS 19
updating with task or agent wake-up call 28
Windows (See Windows client) 81
working with, in Host IPS 19
command-line options
ClientControl.exe, upgrade automation 84
Solaris client, restarting 96
stopping and restarting Linux client 99
stopping the Solaris client 96
verifying Linux client is running 99
verifying Solaris client is running 96
compliance
configuring Host IPS dashboards to view 17
custom signatures
common sections 102
directives valid on Windows 123
directives valid on Linux 134
directives valid on Solaris 134
Linux 127
Linux, UNIX_apache (HTTP) 130
Index

custom signatures (continued)
  Linux, UNIX_file (Files) 127
  Linux, UNIX_misc 131
  optional sections 104
  overview for Linux and Solaris 127
  overview for Windows 107
  rule structure 101
  section value variables 104
  Solaris 127
  Solaris, UNIX_apache (HTTP) 130
  Solaris, UNIX_bo 132
  Solaris, UNIX_file (Files) 127
  Solaris, UNIX_GUID 133
  Solaris, UNIX_map 133
  Solaris, UNIX_misc 131
  wildcards 104
  Windows, Buffer Overflow 107
  Windows, directives per platform 123
  Windows, Files 108
  Windows, Hook 111
  Windows, Illegal 113
  Windows, Illegal API Use 112
  Windows, Isapi 113
  Windows, Program 116
  Windows, Registry 117
  Windows, Services 120
  Windows, SQL 122

D
dashboards
  default Host IPS monitors 12
  managing information in Host IPS 12
  queries and Host Intrusion Prevention 10
  viewing compliance and Host IPS issues 17

deployment
  Host IPS policies and 10
  initial Host IPS client rollout 19
  server tasks for Host IPS 23
  usage profiles in Host IPS 10

dNS blocking rules
  creating and editing 70

E
effective policy
  with multiple-instance policies 38

enveloping and shielding 30

events, Host IPS
  automatic responses 26
  analyzing and tuning 10
  automatic responses 26
  behavioral rules 32
  exceptions 32
  firewall, activity logs 93
  intrusion alerts, responding to 86
  IPS Rules policy 36
  logging and IPS Events tab 33
  managing 48
  signature violations 33
  working with 47

exception rules (continued)
  creating 47
  creating, based on an event 47
  defined 10
  editing IPS policies 89
  events and 47
  IPS Rules policy 36, 46
  list, Windows client and 88
  working with 46

F
false positives
  exceptions and IPS Rules policy 46
  Trusted Applications policy, reducing 78
  tuning Host IPS policies 10

FAQ
  adaptive mode 21
  multiple-instance policies 38

filters
  Host IPS events and queries 10
  how firewall stateful filtering works 60
  querying Host IPS activities 13

Firewall DNS Blocking policy
  about 8
  define 67
  overview 52

Firewall Options policy
  TrustedSource 66
  about 8
  configuring 65
  overview 52
  working with 64

Firewall policies, Host IPS
  feature overview 52

firewall protection
  disable 64
  enable 64

firewall rules
  creating and editing 69

Firewall Rules policy
  wildcards 72
  about 8
  client rules, managing 71
  configuring 68
  define 67
  groups, creating 69
  overview 52

firewall, Host IPS
  stateful packet inspection 59, 61
  about 8
  actions, allow and block 60
  alerts 87
  client rules 13, 64
  customizing options 90
  DNS blocking rules 70
  Firewall Options, configuring 65
  firewall rule groups, creating 69
  firewall rules 10, 67, 69
  firewall rules list, ordering 53
  Firewall Rules, configuring 68
  how firewall rules work 53
  learn and adaptive modes 63
  list of rules 68, 89, 90
  location-aware groups 70
  logging options 85
firewall, Host IPS (continued)
  overview 52
  permissions for 23
  queries 13
  rule groups 55
  rule groups, location-aware 55
  rules, allow and block 53
  state table 60
  stateful filtering, how it works 60
  stateful packet filtering 59
  stateful packet inspection 59, 61
  stateful protocol tracking 62

G
General policies, Host IPS
  feature overview 73
  permissions for 23
  Trusted Applications policy page 79
global administrators
  assigning permission sets 23
groups, Host IPS
  and inheritance 9
  assigning policies to 9
  configuration criteria 10
  deleting policies and inheritance for 16
  firewall location-aware, creating 70
  how policies are applied 9

H
host intrusion prevention signatures 31
Host IPS
  activities and dashboards 12
  basic and advanced protection 7
  features and categories 9
  how it works 7
  how to set and tune protection 18
  Intrusion Information tab 86
  permission sets 23
  policies and their categories 9
  responding to alerts 86
  types of policies 8
Host IPS Catalog
  adding to 70
  contents 58
  dependencies 58
  editing 70
  explanation 58
  exporting from 70
  exporting to 70
  filtering 70
  using 70
Host IPS Property Translator task 25

I
information management
  analyzing Host IPS client data 19
  dashboards and queries for Host IPS 12
  predefined and custom queries for Host IPS 13
intrusion prevention (IPS) (continued)
  delivery methods 30
  editing exception rules 89
  engines and drivers 30
  enveloping and shielding 30
  exceptions 32
  Firewall logging options 85
  HIPS, about 31
  IPS Protection policy 35
  logging options 85
  NIPS, about 31
  overview 29
  reactions 32
  signatures, defined 31
  system call interception 30
IP address
  configuring trusted networks 78
  firewall rules and 89
  location-aware groups 55
  monitoring blocked hosts 91
  rule groups 55
  stateful firewall, IPv4 vs. IPv6 60
IPS events
  about 33
  exceptions, creating 47
  managing 48
  overview 47
  trusted applications, creating 47
  working with 47
IPS Options policy
  about 8
  adaptive mode 33
  configuring 34
  overview 29
  preset policies 34
  working with 33
IPS protection
  disable 33
  enable 33
IPS Protection policy
  about 8
  configuring 36
  overview 29
  reactions, setting 36
  severity levels, setting 35
  working with 35
IPS Rules policy
  wildcards 42
  about 8
  application protection rules 33, 43, 45
  application protection rules, configuring 37
  configuring 37, 45
  define 36
  events, working with 47
  exception rules 46
  exceptions, configuring 37
  logging events 33
  managing exceptions 46
  overview 29
  signatures, configuring 37
  signatures, working with 39
IPS, Host IPS
  permissions for 23
L
language, Host IPS
setting options for clients 83
learn mode
about 10
Firewall Options policies 64
firewall rules 63
Firewall Rules policies 67
placing Host IPS clients in 20
Linux client 97, 98, 99
considerations 97
overview 97
policy enforcement 97
stopping and restarting 99
troubleshooting 98, 99
verifying installation files 99
location-aware groups
connection isolation 56
creating 70
log files, Host IPS
Client UI troubleshooting 76
firewall activity 85
IP policy activity 85
Linux client, installation history 99
Solaris client, installation history 96
troubleshooting 95, 98
logs
enabling 141
FireSvc.log 141
for firewall functionality 141
for IPS functionality 141
HipShield.log 141
using for troubleshooting 141

M
McAfee Default policy
Client UI 74
DNS Blocking 67
Firewall Options 64
Firewall Rules 67
Host IPS 9
IPS Options 33
IPS Protection 35
IPS Rules 36
Trusted Applications 78
Trusted Networks 77
McAfee recommendations
contact McAfee support to disable HIPS engine 85
group Host IPS clients logically 19
group systems by Host IPS criteria 10
phased Host IPS deployment 19
tune Host IPS default policies 17
use IPS Protection to stagger impact of events 10
migration
policies 22
policy version 7 to 8 22
monitored processes, viewing 92
multiple-instance policies
effective policy 38
FAQ 38
use in deployment 38
assigning 37, 80
My Default policy
Client UI 74
DNS Blocking 67

My Default policy (continued)
Firewall Options 64
Firewall Rules 67
Host IPS 9
IPS Options 33
IPS Protection 35
IPS Rules 36
Trusted Applications 78
Trusted Networks 77

N
network adapters
conditions to allow connection 55
network intrusion prevention signatures 31
NIPS (network intrusion prevention signatures) 91

P
packages
Host IPS content updates 27
passwords
for Client UI policy 75
unlocking the Windows client console 83
using hips troubleshooting tool 95
permission sets
assigning 24
Host IPS permissions 23
managing Host IPS deployment 23
who configures the system 17
policies, Host IPS
migration 22
and their categories 9
assigned owner 9
assigning 18
client rules, creating exceptions 10
configuring IPS Options 34
creating new 18
defaults, basic protection 7
defined 9
feature overview 29
firewall (See firewall, Host IPS) 8
Firewall DNS Blocking 67
Firewall Options 64, 65
Firewall Rules 67, 68
how policies are applied 9
inheritance 10
managing 16
multiple instances 37, 80
overriding, with client exceptions 10
overview of features 8
Policy Catalog 16
preset protection 10
responding to alerts 87
tuning defaults 17
usage profiles and tuning 10
viewing policies 16
where to find 16
policy assignment
changing 18
enable firewall protection 64
Host IPS 9
Policy Catalog
Client UI 74
custom firewall policies, creating 64, 67
managing Host IPS policies 16
ownership for Host IPS policies 8

152 McAfee Host Intrusion Prevention 8.0 Product Guide for ePolicy Orchestrator 4.5
Policy Catalog (continued)
  Trusted Applications 78
  Trusted Networks 77
policy enforcement
  Host IPS 9
  Host IPS clients and ePO 7
  Linux client and 97
  Solaris client and 94
policy management
  accessing Host IPS policies 16
  analyzing Host IPS events and client rules 16
  Linux client and 97
  Policies tab, Host IPS 16
  tracking Host IPS policies 10
  tuning Host IPS 10, 18
ports
  blocked traffic and firewall rules 63
  connections and firewall alerts 87
  firewall and state table entries 60
  FTP connections and stateful packet inspection 61
precedence
  firewall rules list 53
  General policies, Host IPS and 73
  Network IPS and IP addresses 78
  Trusted Networks policy 78
preconfigured policies
  Client UI 74
  Firewall Rules 67
  IPS Options 33
  IPS Protection 35
  Trusted Applications 78
  Trusted Networks 77
protocols
  tracking, and stateful firewall 62
Q
queries, Host IPS
  custom, parameters for 13
  managing information 12
  predefined and custom 13
  reports 10
  tracking activities 13
R
reactions
  about 32
  firewall alerts, responding to 87
  intrusion alerts, responding to 86
  IPS Protection, configuring 35
  mapping to IPS severity 10
  setting, for signature severity levels 36
  spoof detected alerts, responding to 87
  types of 32
rule groups, Host IPS
  firewall rule groups, creating 69
rule structure
  custom signatures 101
rules lists
  exceptions for Host IPS 88
  firewall rules for Host IPS 90
S
server tasks, Host IPS
  checking in updates 27
  server tasks, Host IPS (continued)
    Export Policies 25
    Export Queries 25
    managing deployment 23, 25
    Property Translator 25
    Purge Event Log 25
    Purge Threat Event Log 25
    Repository Pull 25
    Run Query 25
severity levels, IPS
  events and 47
  IPS Protection policy 35
  mapping to a reaction 10
  setting and tuning protection 18
  setting reactions for 36
  tuning 10, 17
  working with signatures 39
shielding and enveloping
  IPS behavioral rules and 32
signature security levels
  types of 39
signatures
  alerts and NIPS signatures 86
  configuring IPS Rules policy 40
  creating custom host IPS 41
  creating with expert method 41
  creating with standard method 41
  custom 39
  default host IPS 39
  defined 31
  exception rules list 88
  exceptions 32
  HIPS, about 31
  host 39
  host IP, and exceptions 86
  IPS Rules policy 36
  network 39
  NIPS, about 31
  severity levels 39
  severity levels for 35
  tuning Host IPS policies 10
  types of 39
  using the wizard to create 42
  working with 39
Solaris client
  installation files 96
  overview 94
  preventing buffer overflow 94
  stopping and restarting 96
  troubleshooting 95
  verifying client is running 96
Spoof Detected alerts 87
state table, firewall
  functionality 60
  overview 60
stateful firewall
  how stateful filtering works 60
  packet inspection, how it works 61
  protocol tracking 62
system call interception 30
system management
  automatic responses for Host IPS events 26
  server tasks for Host IPS 23, 25
  updating Host IPS protection 27