McAfee Host Intrusion Prevention 7.0 Product Guide for use with ePolicy Orchestrator 4.0

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

License Attributions

Refer to the product Release Notes.

Contents

Introducing Host Intrusion Prevention 7.0

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 delivers a manageable and scalable intrusion prevention solution for workstations, notebooks, and critical servers, including web and database servers. It proactively blocks zero-day and known attacks with patented technology.

Host Intrusion Prevention protects against unauthorized viewing, copying, modifying, and deleting of information and the compromising of system and network resources and applications that store and deliver information. It accomplishes this through a combination of behavioral rules, host and network signatures, and a system firewall to block attacks and reduce the urgency of patches for new threats.

As soon as Host Intrusion Prevention is installed, you are protected. The default settings allow for a rapid, large-scale deployment. For greater protection, you can apply stricter preset or custom policies.

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

Host Intrusion Prevention functionality is divided into IPS, Firewall, Application Blocking, and General features to provide greater control in delivering protection to users.

Contents

Host Intrusion Prevention protection

As soon as the Host Intrusion Prevention client is installed, intrusion prevention protection is in effect. Communication with the ePO server is required for monitoring and policy and content updates.

ePolicy Orchestrator communicates policy information to Host Intrusion Prevention clients on a regular interval through the ePolicy Orchestrator agent. Host Intrusion Prevention clients enforce the policies, collect event information, and transmit the information back to ePolicy Orchestrator. Client-side management is available through a client console for Windows clients and a troubleshooting utility for non-Windows clients, where you monitor and change protection, including turning features on and off, manually creating client rules, and viewing logs.

Basic protection

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

- IPS protection is enabled; high severity signatures are prevented and all other signatures are ignored.
- Firewall, quarantine, and application blocking protection are not enabled.
- McAfee applications are listed as trusted applications for all rules except IPS self-protection rules.
- Predefined applications and processes are protected.

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. You can do this manually or automatically by enabling learn or adaptive mode.

Types of Host Intrusion Prevention 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 four policy features, each with a set of security options. These are: **IPS**, **Firewall**, **Application Blocking** and **General**. Except for General, each feature contains a "rules" policy with rules that define behavior, and an "options" policy that enables or disables application of 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 (Intrusion Prevention System) feature contains three policies that protect computers with host intrusion prevention technology. It details exceptions, signatures, application protection rules, events, and client-generated exceptions.

- **IPS Options**. Turns on or off IPS protection and application of adaptive mode.
- **IPS Protection**. Defines the reaction to events that signatures generate.
- **IPS Rules**. Defines exceptions, signatures, and application protection rules. This policy, referred to as a multiple-instance policy, allows for a profile of settings through the application of multiple policies under a single policy instance.

Firewall policies

The Firewall feature contains four policies that filter network traffic, allowing legitimate traffic through the firewall and blocking the rest.

- **Firewall Options**. Turns on or off firewall protection and application of adapative or learn mode.
- **Firewall Rules**. Defines firewall rules.
- **Quarantine Options**. Turns on or off quarantine mode.
- **Quarantine Rules**. Defines firewall rules applied during quarantine.

Application Blocking policies

The Application Blocking feature contains two policies that manage application creation and application hooking.

- **Application Blocking Options**. Turns on or off blocking for application creation and hooking and application of adaptive and learn mode.
- **Application Blocking Rules**. Defines application blocking rules that prevent unknown and unwanted applications from running or binding with other applications.

General policies

The General feature contains three policies that apply to all features.

- **Client UI.** Defines access to the Host Intrusion Prevention user interface on Windows client systems, and password-protection on all client systems.
- **Trusted Networks**. Lists IP addresses and networks that are safe for communication
- **Trusted Applications**. Lists applications that are trusted to perform most operations.

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.

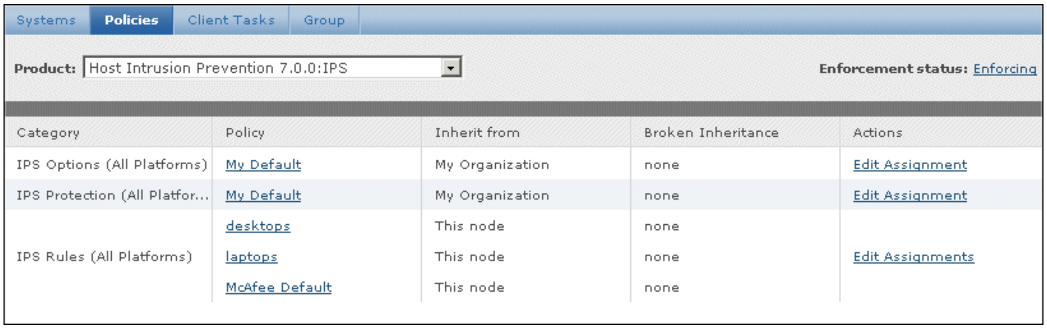
Policies and their categories

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.

The two Host Intrusion Prevention policies without a My Default policy, IPS Rules and Trusted Applications, are called multiple-instance policies because you can assign multiple policy instances under a single policy. The policy instances are automatically combined into one effective policy.



Product: Host Intrusion Prevention 7.0.0:IPS

Enforcement status: Enforcing

Category	Policy	Inherit from	Broken Inheritance	Actions
IPS Options (All Platforms)	My Default	My Organization	none	Edit Assignment
IPS Protection (All Platfor...	My Default	My Organization	none	Edit Assignment
IPS Rules (All Platforms)	desktops	This node	none	Edit Assignments
	laptops	This node	none	
	McAfee Default	This node	none	

Figure 1: IPS Rules policy with three policy instances

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.

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.

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

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 configuration criteria, including system type (server or desktop), use of major applications (web, database, or mail server), and strategic locations (DMZ or intranet). You can place 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 can 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 "out-of-the-box" protection requires no tuning and generates few events. Clients can be initially deployed on a large scale, even before you tune the deployment. For many environments this basic protection may 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.

Adaptive and learn mode

To further 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* or *learn* mode. In adaptive mode, available for IPS, Firewall, and Application Blocking features, client rules are created without interaction from the user. In learn mode, available for Firewall and Application Blocking features, the user responds to alerts, indicating whether or not to create a client rule.

After client rules are created, you can analyze them decide which if any to convert to to server-mandated policies. Adaptive and learn modes can be turned off at any time to tighten the system's protection.

Often in a large organization, avoiding disruption to business takes priority over security concerns. For example, new applications may need to be installed periodically on some computers, and you may 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 will 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.

Tuning

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

Stronger IPS rules, for example, 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 will be applied. The other levels can be raised incrementally as tuning progresses.

You can reduce the number of false positives by creating *exception rules*, *trusted applications*, and *firewall rules*.

- Exception rules are mechanisms for overriding a security policy in specific circumstances.
- Trusted applications are application processes that ignore all IPS, Firewall, or Application Blocking 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 IPS deployment includes monitoring, analyzing, and reacting to activities; changing and updating policies; and performing system tasks.

Contents

Management of information

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

Host IPS activities and dashboards

Dashboards, a collection of monitors, 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, provided 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 a default dashboard with these monitors:

- Firewall Status
- Host IPS Status
- Service Status
- Count of IPS Client Rules
- Content Versions
- Top 10 NIPS Events by Source IP

For more information about creating and using dashboards, refer to the ePolicy Orchestator 4.0 documentation.

Queries for Host IPS activities

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.

Your options include:

- 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, and filter the reports as needed. You can print the reports and export 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.

You can organize and maintain these queries to suit your needs. For example, if you customize settings for a report, you can export these settings as a template. You can also create custom templates and organize templates in logical groupings. For example, you can group queries that you run daily, weekly, and monthly.

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

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

Custom queries

You can create threeHost IPS queries with the Query Builder wizard: Application Blocking Client Rules, Firewall Client Rules, and IPS Client Rules. Query parameters include:

Application Blocking Client Rules	Firewall Client Rules	IPS Client Rules
• Create Reaction	• Creation Date	• Creation Date
• Creation Date	• Direction	• Enabled
• Enabled	• Domain List	• Full Process Name
• Full Process Name	• Effective Reaction	• Include All Processes
• Hash	• Enabled	• Include All signatures
• Hook Reaction	• End Time	• Include All Users
• Local Version	• Full Process Name	• Last Modified Date
• Modified Date	• Hash	• Local Version
• Process Eval Option	• IP Protocol	• Process Name
• Process Name	• Local Service	• Process Path
• Process Path	• Local Service type	• Reaction
	• Local Version	• Signature ID
	• Log Status	• User Name
	• Match Intrusion	
	• Modified Date	

Application Blocking Client Rules	Firewall Client Rules	IPS Client Rules
	• Non-IP Protocol • Process Eval Option • Process Name • Process Path • Props schema ID • Reaction • Remote Address • Remote Address Type • Remote Service • Rule Name • Start Time • Switch When Expired • Time Restriction • Time Task	

In addition, you can create queries using these Host IPS properties:

- Agent type
- Application Blocking Adaptive Mode Status
- Application Blocking Learn Mode Status
- Application Blocking Status
- Blocked Attackers
- Client Version
- Content Version
- Firewall Adaptive Mode Status
- Firewall Inbound Learn Mode Status
- Firewall Outbound Learn Mode Status
- Firewall Rule Count
- Firewall Status
- IPS Status
- Install Directory
- IPS Adaptive Mode Status
- Language
- Local Exception Rule Count
- NIPS Status
- Plug-in Version
- Product Status
- Service Running

Pre-defined queries

Select from these Host IPS queries:

HIP Query	Summary
App Block Create Status	Displays where Application Blocking Creation is enabled on managed systems.
App Block Hook Status	Displays where Application Blocking Hooking is enabled or disabled on managed systems.
Client Versions	Displays top three client versions with a single category for all other versions.
Content Versions	Displays top three content versions with a single category for all other versions.
Firewall Status	Displays where Firewall protection is enabled or disabled on managed systems.
Host IPS Status	Displays where IPS protection is enabled or disabled on managed systems.
Service Status	Displays where Host IPS is installed and an update has occurred in the last week on managed systems.
Count of AB Client rules	Displays the number of Application Blocking client rules created over time.
Count of FW Client Rules	Displays the number of Firewall client rules created over time.

HIP Query	Summary
Count of IPS Client Rules	Displays the number of IPS client rules created over time.
Top 10 Blocked Applications	Displays the top 10 blocked applications for the past three months.
Top 10 Quarantined Systems	Displays the top 10 systems that were quarantined for the past three months.
Top 10 Triggered Signatures	Displays the top 10 triggered IPS signatures.
Top 10 IPS Events by Target	Displays the top 10 systems with the most IPS events.
Top 10 IPS Events By Source IP	Displays the top 10 network intrusion events by source IP addresses for the past three months.

Management of policies

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.

How to set and tune protection

Host Intrusion Prevention works out-of-the box with little or no attention for basic protection. It allows greater protection through custom settings obtained through manual or automatic tuning.

Out-of-the-box protection

Host Intrusion Prevention ships with a set of default policies that provide basic, "out-of-the-box" protection for your environment.

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 over a period of time of events and client rules being created.

- For IPS protection, monitor events for false positives and create rules for 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 exception rules, trusted application rules, and trusted network rules.
- 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, Firewall, and Application Blocking policies, or apply learn mode for Firewall and Application Blocking 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.
- In learn mode, the user receives an alert message and must indicate whether to allow or block an activity. As a result, client rules are created.
- Review the lists of client rules.
- Promote appropriate client rules to administrative policy rules.
- After a few weeks turn off the adaptive or learn 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.

Where to find policies

ePolicy Orchestrator provides two locations to view and manage Host Intrusion Prevention policies:

- **Systems | System Tree | Policies** tab of a selected group in the System Tree
- **Systems | Policy Catalog**

Policies tab

Use the **Policies** tab to view the policies of a particular feature of the product, view details of the policy, view inheritence information, edit policy assignment, and edit custom policies or create a new policy relating to a selected group or system.

Policy Catalog

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, and view assignments where policy enforcement is disabled.

To...	Do this...
Create a policy	Click **New Policy**, name it, and edit the settings.
Edit a policy	Click **Edit** (only available for My Default or custom policies).
View a policy	Click **View** (only available for McAfee Default or preconfigured policies).
Rename a policy	Click **Rename** and change the name of the policy (not available for default or preconfigured policies).
Duplicate a policy	Click **Duplicate**, change the name of the policy, and edit the settings.

To...	Do this...
Delete a policy	Click **Delete** (not available for default or preconfigured policies). NOTE: When you delete a policy, all groups to which it is currently applied inherit the policy of this category from their parent. Before deleting a policy, look at all of the nodes to which it is assigned, and assign a different policy if you don't want the policy to inherit from the parent. If you delete a policy that is applied at the top level, the default policy of this category is applied.
Assign a policy owner	Click the owner of the policy and select another owner from a list (not available for default or preconfigured policies).
Export a policy	Click **Export**, then name and save the policy (an XML file) to the desired location.
Export all policies	Click **Export all policies**, then name and save the policy XML file to the desired location.
Import policies	Click **Import** at the top of the Policy Catalog page, select the policy XML file, then click **OK.**

For details on any of these features, refer to the ePolicy Orchestrator 4.0 documentation.

Configuring polices

After you install the Host Intrusion Prevention software, McAfee recommends that you configure policies to provide the greatest amount of security while not conflicting with day-to-day activities. The default policies in Host Intrusion Prevention fit the broadest set of customer environments and may meet your needs. To 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 day-to-day work of users, adjust the severity level to a lower level.
- Configure dashboards for a quick overview of compliance and issues.
- Configure notifications 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.

Clients and planning your deployment

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

- **Determine your initial client rollout plan**. Although you will 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 on which 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 are installed with a default set of IPS, Firewall, Application Blocking, and General rule policies. New policies with updated rules can later be pushed from the server.
- **Group the clients logically**. Clients can be grouped according to any criteria that fits in the 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 have installed and grouped your clients, you have completed the deployment. 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 quarantine and application blocking, marked as intrusion, HIPS, or NIPS.

To analyze client rules, view the **IPS, Firewall, and Application Blocking 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 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.

Automatic tuning with clients

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

These modes analyze events first for the most malicious attacks, such as buffer overflow. If the activity is considered regular and necessary for business, client exception rules are created. By setting representative clients in adaptive or learn mode, you can 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 or learn modes to tighten the system’s intrusion prevention protection.

- Run clients in adaptive or learn mode for at least a week. This allows the clients time to encounter all the activity they would normally encounter. Try to do this during times of scheduled activity, such as backups or script processing.
- As each activity is encountered, IPS events are generated and exceptions are created. Exceptions are activities that are distinguished as legitimate behavior. For example, a policy

might deem certain script processing as illegal behavior, but certain systems in your engineering groups need to perform such tasks. Allow exceptions to be created for those systems so they can 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 Internet. The firewall scans all incoming and outgoing traffic at the packet level. As it reviews each arriving or departing packet, the firewall checks its list of firewall rules, which is a set of criteria with associated actions. If a packet matches all the criteria in a rule, the firewall performs the action specified by the rule — either allowing the packet through the firewall, or blocking it.

Management of systems

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

Permission sets for Host IPS

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. For users who are global administrators, all permissions to all products and features are automatically assigned. 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.

When you install the Host IPS extension it adds a section to the permission sets without applying any permissions. The global administrators must grant permissions and create new permission sets.

With Host Intrusion Prevention, permission can be granted for each feature of the product and whether the user has read or read/write permission.

For this 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.
Application Blocking	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 permissions to handle other items that work with Host Intrusion Prevention, including queries, dashboards, and notifications. To access information on the Host IPS tab under Reporting, view permissions are needed for Event Log, Systems, and System Tree access. For example, to analyze and manage Firewall Client rules found on the Host IPS tab, a user needs permissions to view events under Event Log, to view the System Tree tab under Systems, to view sections of the System Tree under System Tree access, and to view and change settings under the Host Intrusion Prevention 7.0 Firewall feature. For more information on permission sets, see the ePolicy Orchestrator 4.0 documentation.

Host IPS server tasks

Host Intrusion Prevention provides a single server task that enables review and promotion of client rules to administrative policy.

Property Translator

The Property Translator 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, which runs automatically every 15 minutes and requires no user interaction. You can, however, select it and run it immediately if needed. For more information on server tasks, see the ePolicy Orchestrator 4.0 documentation.

Notifications for Host IPS events

Notifications can alert you to any events that occur on Host Intrusion Prevention client systems. You can configure rules to send email or SNMP traps, or run external commands when specific events are received and processed by the ePolicy Orchestrator server. You can specify the event categories that generate a notification message and the frequency that notifications are sent. For complete details, see the ePolicy Orchestrator 4.0 documentation.

How notifications work

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

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

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

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

Notification rules

You can create rules for many event categories, including:

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

All rules are created in the same basic manner:

1. Describe the rule.
2. Set filters for the rule.
3. Set thresholds for the rule.
4. Create the message to be sent and the type of delivery.

Notification categories

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

- Host Intrusion detected and handled
- Network Intrusion detected and handled
- Application blocked
- Quarantined computer update failed
- Unknown

Notifications can be configured for all or none of the Host (or Network) IPS signatures. Host Intrusion Prevention supports the specification of a single IPS signature ID as the threat or rule name in the notification rule configuration. By internally mapping the signature ID attribute of an event to the threat name, a rule is created to uniquely identify an IPS signature.

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

Parameters	**Host and Network IPS Events Values**	**Blocked Application Event Values**	**Quarantine Event Values**
Actual threat or rule names	SignatureID	none	none
Source systems	Remote IP address	computer name	computer name
Affected objects	Process Name	Application name	IP address of computer
Time notification sent	Incident time	Incident time	Incident time
Event IDs	ePO mapping of event ID	ePO mapping of event ID	ePO mapping of event ID
AdditionalInformation	Localized Signature Name (from client computer)	Application full path	none

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.

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

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

Checking in update packages

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

Task

- Use one of these two methods:

Automatic check-in	**Manual check-in**
1 Go to **Software | Master Repository**, then click **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, and whether to pull all or selected packages, then click **Next**. **4** Schedule the task as needed, then click **Next**. **5** Verify the information, then click **Save**. 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.	**1** Download the file from **McAfeeHttp** or **McAfeeFtp**. **2** Go to **Software | Master Repository**, then click **Check in package**. **3** Select the package type and package location, then click **Next**. The **Package Options** page appears. **4** Select the branch where to install the package, then click **Save.** The package appears on the Master Repository tab.

Updating clients with content

After the update package is checked in to the master repository, you can send the updates to the client by scheduling an update task or by sending an agent wakeup call to update immediately. A client can also request updates on demand if a McAfee Agent icon appears in the client computer's system tray.

Task

- Use one of these two methods:

From the server	**From the client**
1 Go to **Systems | System Tree | Client Tasks**, select the group where you want to send content updates, and click **New Task**. **2** Name and describe the task, and select **Update (McAfee Agent)** as the type of task, then click **Next**. **3** Schedule the task as desired, then click **Next**. **4** Review the details, then click **Save**.	• Right-click the ePO 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 details on exceptions, signatures, and application protection rules.

Contents

Overview of IPS policies

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

Signature rules and how they work

Signature rules are patterns of characters than can be matched against a traffic stream. For example, a signature rule might look for a specific string in an HTTP request. If the string matches one in a known attack, action is taken. These rules provide protection against known attacks.

Signatures are designed for specific applications and 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 and network IPS signature rules

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

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

Host intrusion prevention signatures

Host IPS 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.

Benefits of host IPS

- Protects against an attack and the results of an attack, such as preventing a program from writing a file.
- Protects laptops when they are outside the protected network.
- Protects 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.
- Provides a last line of defense against attacks that have evaded other security tools.
- Prevents internal attack or misuse of devices located on the same network segment.
- Protects against attacks where the encrypted data stream terminates at the system being protected by examining the decrypted data and behavior.
- Independent of network architecture; protects systems on obsolete or unusual network architectures such as Token Ring or FDDI.

Network intrusion prevention 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.

Benefits of network IPS

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

Behavioral rules

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

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

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

Events

IPS events are generated when a client recognizes a violation of a signature or behavioral rule. Events are logged in the Events tab of the IPS Rules 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.

Reactions

A reaction is what a client does when it recognizes a signature of a specific severity.

A client reacts in one of three ways:

- **Ignore** — No reaction; the event is not logged and the 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 may state, for example, that when a client recognizes an Information level signature, it logs the occurrence of that signature and allows the operation to occur; and when it recognizes a High level signature, it prevents the operation.

NOTE: Logging can be enabled directly on each signature.

Exception rules

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

Working with IPS Options policies

The IPS Options policy turns on and off IPS protection and allows you to apply adaptive mode on clients to create new exception rules.

This policy category contains three preconfigured policies and an editable **My Default** policy. You can view and duplicate preconfigured policies; you can, create, edit, rename, duplicate, delete, and export custom policies.

Preconfigured policies include:

On (McAfee Default)

- Enable Host IPS
- Enable Network IPS
- Automatically Block Network Intruders for 10 minutes
- Retain Blocked Hosts
- Retain Client Rules

Off

- Retain Blocked Hosts
- Retain Client Rules

Adaptive

- Enable Host IPS
- Enable Network IPS
- Retain Blocked Hosts
- Enable Adaptive Mode
- Retain Client Rules

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

▸ Configuring the IPS Options policy

Configuring the IPS Options policy

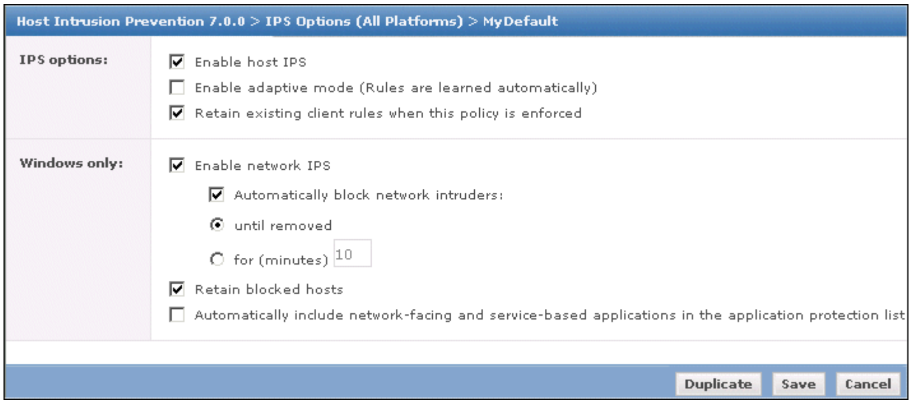
Use this task to turn IPS protection on and off and apply adaptive mode.

Task

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

1 Go to **Systems | 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.



Host Intrusion Prevention 7.0.0 > IPS Options (All Platforms) > MyDefault

IPS options:

- ☑ Enable host IPS
- ☐ Enable adaptive mode (Rules are learned automatically)
- ☑ Retain existing client rules when this policy is enforced

Windows only:

- ☑ Enable network IPS
  - ☑ Automatically block network intruders:
  - ● until removed
  - ○ for (minutes) 10
- ☑ Retain blocked hosts
- ☐ Automatically include network-facing and service-based applications in the application protection list

Figure 2: IPS Options

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

Working with IPS Protection policies

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 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.

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

Preconfigured policies include:

Basic Protection (McAfee Default)

- Prevent high severity level signatures and ignore the rest.

Enhanced Protection

- Prevent high and medium severity level signatures and ignore the rest.

Maximum Protection

- Prevent high, medium, and low severity level signatures and log the rest.

Prepare for Enhanced Protection

- Prevent high and log medium severity level signatures and ignore the rest.

Prepare for Maximum Protection

- Prevent high and medium severity level signatures, log low severity level signatures, and ignore the rest.

Warning

- Log high severity level signatures and ignore the rest.

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

- Configuring the IPS Protection policy

Configuring the IPS Protection policy

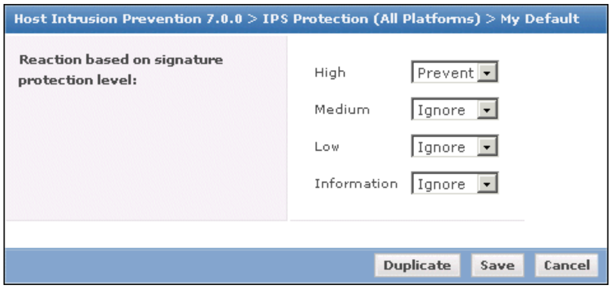
Use this task to set the protective reaction for signature severity levels. These settings instruct clients what to do when an attack or suspicious behavior is detected.

Task

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

1 Go to **Systems | Policy Catalog** and select **Host Intrusion Prevention: IPS** in the **Product** list and **IPS Protection** in the **Category** list. The list of policies appears.

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



Host Intrusion Prevention 7.0.0 > IPS Protection (All Platforms) > My Default

Reaction based on signature protection level:

High: Prevent
Medium: Ignore
Low: Ignore
Information: Ignore

Figure 3: IPS Protection

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

Working with IPS Rules policies

The IPS Rules policy applies intrusion prevention safeguards. This policy is a multiple-instance policy that can have multiple instances assigned. For example, for an IIS Server you might apply a general default policy, a server policy, and an IIS policy, the latter two configured to specifically target systems runnings as IIS servers.

Each policy contains details on:

- Exception Rules
- Signatures
- Application Protection Rules

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

- IPS Events
- IPS Client Rules

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.

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

To assign more than one instance of the IPS Rules policy on the **Policy Assignment** page, click **New Policy Instance,** and select a policy from the **Assigned Polices** list for the additional policy instances.

Tasks

- ▸ Working with IPS signatures
- ▸ Working with IPS Application Protection rules
- ▸ Working with IPS Exceptions
- ▸ Working with IPS events
- ▸ Managing IPS client rules

Working with IPS signatures

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

- **High** — 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 may 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 signatures** — Default host intrusion prevention signatures.
- **Custom host signatures** — Custom host intrusion prevention signatures that you create.
- **Network signatures** — Default network intrusion prevention signatures.

Default host IP 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 host IP 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 IP 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.

Tasks

▸ Configuring IPS Rules signatures

▸ Creating signatures

▸ Creating signatures using the wizard

Configuring IPS Rules signatures

Use this task to edit default signatures; create, edit or delete custom signatures; and move signatures to another policy.

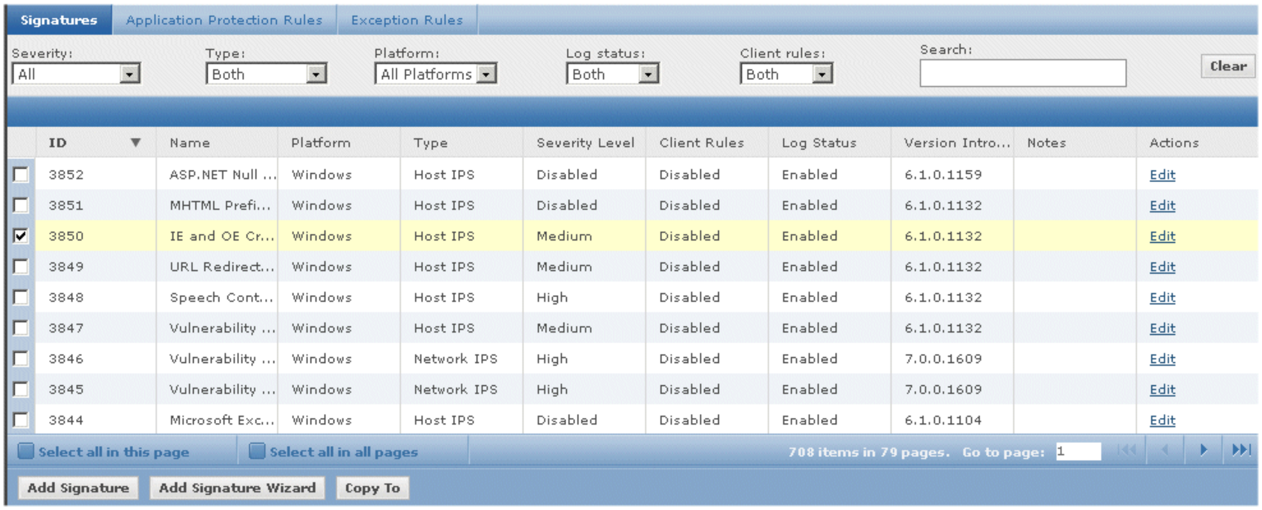
Task

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

1 On the Policy Catalog page, select **Host Intrusion Prevention: IPS** on the **Product** list and select **IPS Rules** on 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 Use the filters at the top of the signatures list to filter the view of all signatures in the policy. You can filter on signature severity, type, platform, log status, whether client rules are allowed, or specific text that includes signatures' name, notes, or content version. Click **Clear** to remove filter settings.



Severity: All
Type: Both
Platform: All Platforms
Log status: Both
Client rules: Both
Search:

	ID	Name	Platform	Type	Severity Level	Client Rules	Log Status	Version Intro...	Notes	Actions
□	3852	ASP.NET Null ...	Windows	Host IPS	Disabled	Disabled	Enabled	6.1.0.1159		Edit
□	3851	MHTML Prefi...	Windows	Host IPS	Disabled	Disabled	Enabled	6.1.0.1132		Edit
☑	3850	IE and OE Cr...	Windows	Host IPS	Medium	Disabled	Enabled	6.1.0.1132		Edit
□	3849	URL Redirect...	Windows	Host IPS	Medium	Disabled	Enabled	6.1.0.1132		Edit
□	3848	Speech Cont...	Windows	Host IPS	High	Disabled	Enabled	6.1.0.1132		Edit
□	3847	Vulnerability ...	Windows	Host IPS	Medium	Disabled	Enabled	6.1.0.1132		Edit
□	3846	Vulnerability ...	Windows	Network IPS	High	Disabled	Enabled	7.0.0.1609		Edit
□	3845	Vulnerability ...	Windows	Network IPS	High	Disabled	Enabled	7.0.0.1609		Edit
□	3844	Microsoft Exc...	Windows	Host IPS	Disabled	Disabled	Enabled	6.1.0.1104		Edit

708 items in 79 pages. Go to page: 1

Figure 4: IPS Signatures tab

4 Under **Actions**, click **Edit** for the signature you want to modify.

- If the signature is a default signature, 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 their default settings by clicking **Revert** under Actions.
- 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.

5 Click **Add Signature** or **Add Signature Wizard** to add a new signature to the list.

6 Under **Actions**, click **Delete** for the custom signature you want to delete**.**

NOTE: Only custom signatures can be deleted.

7 Select a signature and click **Copy To** to move it to another policy**.** Indicate the policy to which to move the signature and click **OK**.

NOTE: You can move several signatures at one time by selecting all the signatures before clicking **Copy To**.

8 Click **Save** to save changes.

Creating signatures

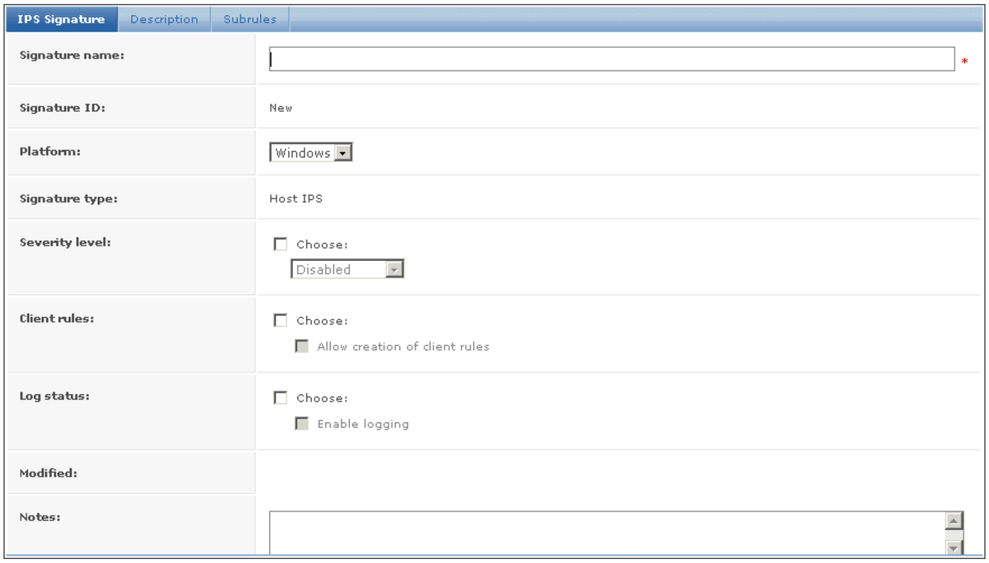
Use this task to create custom host intrusion prevention signatures to protect specific operations.

Task

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

1 On the IPS Rules policy **Signatures** tab, click **Add Signature**. A blank **Signature** page appears.

2 On the signature's **IPS Signature** tab, enter a name and select the platform, severity level. log status, and whether to allow the creation of client rules.

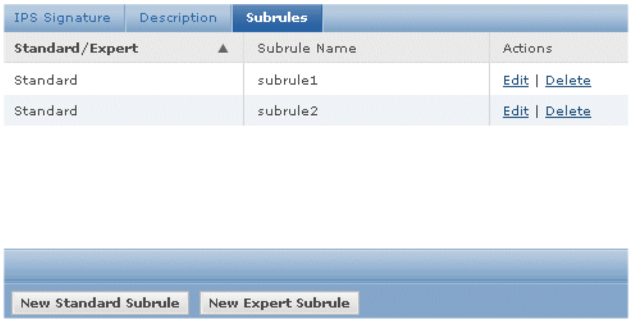


Signature name:	*
Signature ID:	New
Platform:	Windows
Signature type:	Host IPS
Severity level:	□ Choose: Disabled
Client rules:	□ Choose: □ Allow creation of client rules
Log status:	□ Choose: □ Enable logging
Modified:	
Notes:	

Figure 5: New Custom Signature—IPS Signature tab

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 **Sub-Rule** tab, select either **Add Standard Sub-Rule** or Add **Expert Sub-Rule** to create a rule.



Standard/Expert ▲	Subrule Name	Actions
Standard	subrule1	Edit | Delete
Standard	subrule2	Edit | Delete

Figure 6: New Custom Signature—Sub-Rules tab

To use Standard method:	To use Expert method:
The Standard method limits the number of types you can include in the signature rule.	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

To use Standard method:	To use Expert method:
	signature. Before writing a rule, make sure you understand rule syntax.
1 Enter a name for the signature and choose a type. **2** Specify the operations that trigger the signature. **3** Indicate whether to include or exclude a particular parameter, what the parameter is and its value. **4** 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.	**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.

5 Click **OK**.

NOTE: You can include multiple rules in a signature.

Creating signatures using the wizard

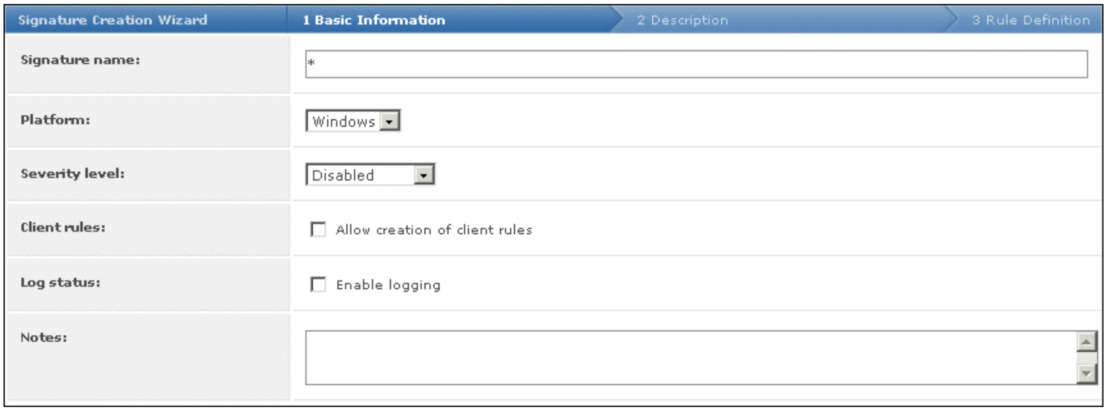
Use this task to creation a signature using a wizard. This is recommended if you are new to creating signatures. Note that signatures created with the wizard do not offer any flexibility for the operations the signature is protecting because you cannot change, add, or delete operations.

Task

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

1 On the IPS Rules **Signatures** tab, click **Add Signature Wizard**.

2 On the **Basic Information** tab, enter a name and select the platform, severity level. log status, and whether to allow the creation of client rules. Click **Next** to continue.

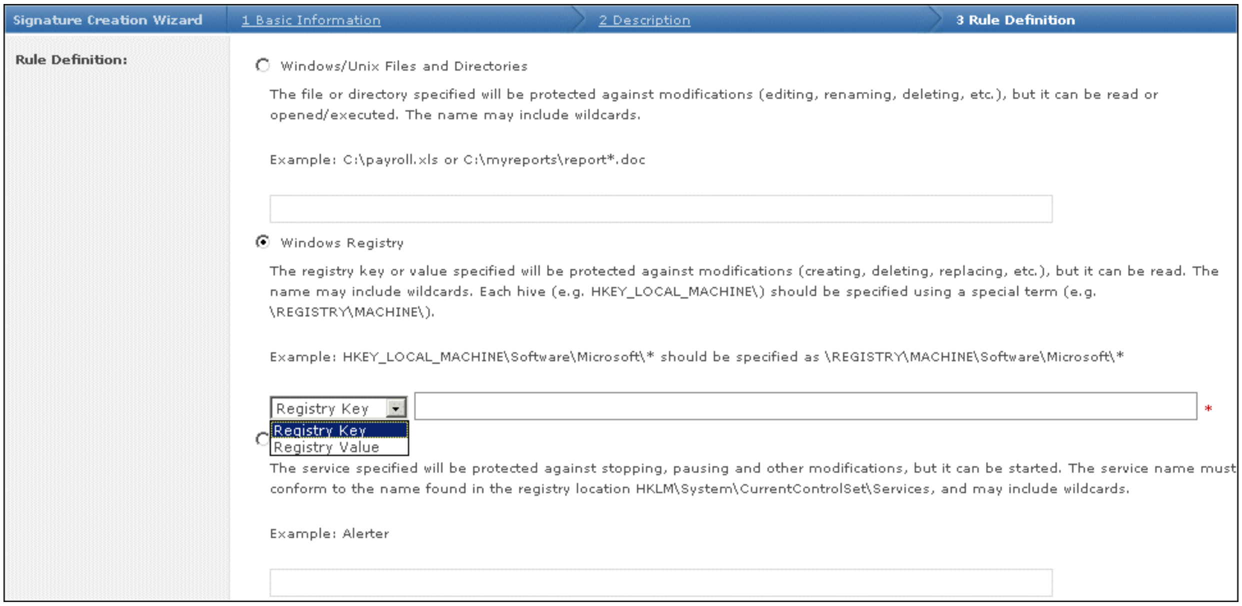


Signature name:	*
Platform:	Windows
Severity level:	Disabled
Client rules:	□ Allow creation of client rules
Log status:	□ Enable logging
Notes:	

Figure 7: Signature Creation Wizard— Basic Information

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.



Rule Definition:

○ Windows/Unix Files and Directories

The file or directory specified will be protected against modifications (editing, renaming, deleting, etc.), but it can be read or opened/executed. The name may include wildcards.

Example: C:\payroll.xls or C:\myreports\report*.doc

● Windows Registry

The registry key or value specified will be protected against modifications (creating, deleting, replacing, etc.), but it can be read. The name may include wildcards. Each hive (e.g. HKEY_LOCAL_MACHINE\) should be specified using a special term (e.g. \REGISTRY\MACHINE\).

Example: HKEY_LOCAL_MACHINE\Software\Microsoft\* should be specified as \REGISTRY\MACHINE\Software\Microsoft\*

The service specified will be protected against stopping, pausing and other modifications, but it can be started. The service name must conform to the name found in the registry location HKLM\System\CurrentControlSet\Services, and may include wildcards.

Example: Alerter

Figure 8: Signature Creation Wizard— Rule Definitions

5 Click **OK**.

Working with IPS Application Protection rules

Application protection rules alleviate compatibility and stability issues resulting from process hooking. 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.

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

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

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

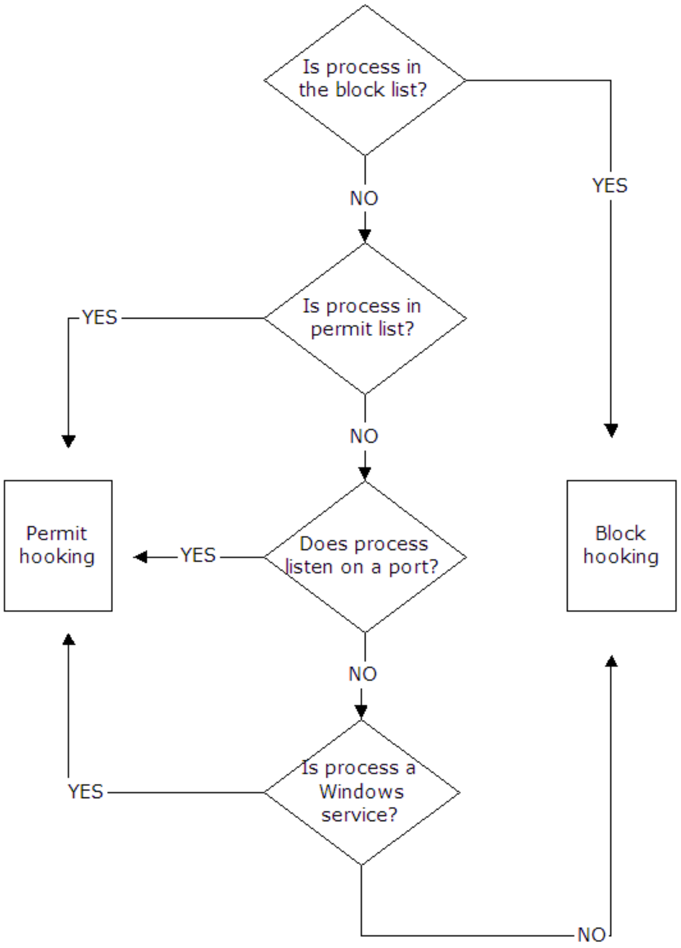

Is process in the block list?
NO
YES
Is process in permit list?
YES
NO
Permit hooking
YES
Does process listen on a port?
Block hooking
NO
Is process a Windows service?
YES
NO

Figure 9: 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 will be 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 will be hooked. If the lists indicate that a process should not be hooked and it is already hooked, that process will be unhooked.

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

Tasks

- Configuring IPS Rules application protection rules
- Creating application protection rules

Configuring IPS Rules application protection rules

Use this task to create, view, edit, or delete application protection rules and move application protection rules to another policy.

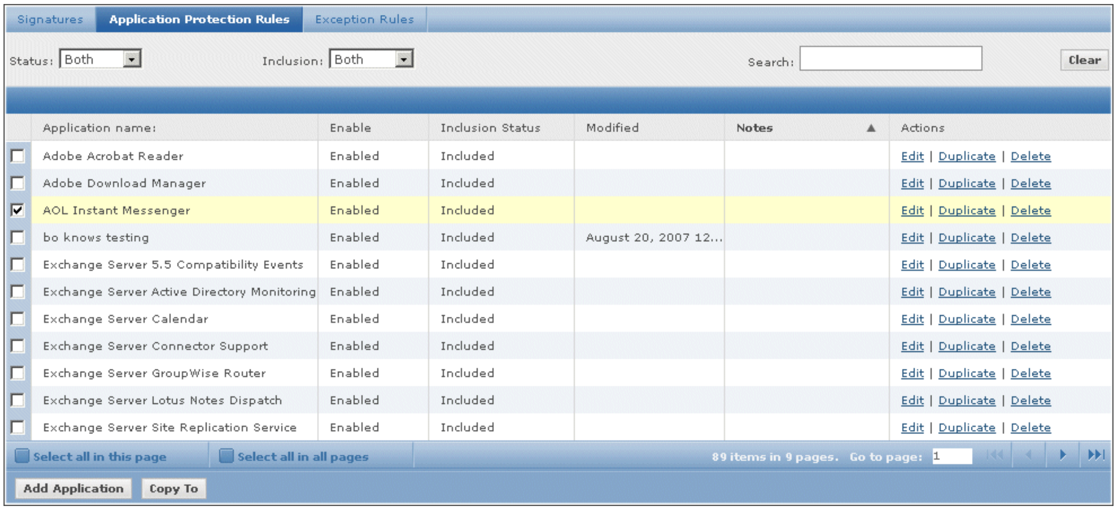
Task

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

1 On the Policy Catalog page, select **Host Intrusion Prevention: IPS** on the **Product** list and select **IPS Rules** on 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 Use the filters at the top of the list to filter the view of all application protection rules in the policy. 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.



Status: Both

Inclusion: Both

Search:

	Application name:	Enable	Inclusion Status	Modified	Notes ▲	Actions
□	Adobe Acrobat Reader	Enabled	Included			Edit | Duplicate | Delete
□	Adobe Download Manager	Enabled	Included			Edit | Duplicate | Delete
☑	AOL Instant Messenger	Enabled	Included			Edit | Duplicate | Delete
□	bo knows testing	Enabled	Included	August 20, 2007 12...		Edit | Duplicate | Delete
□	Exchange Server 5.5 Compatibility Events	Enabled	Included			Edit | Duplicate | Delete
□	Exchange Server Active Directory Monitoring	Enabled	Included			Edit | Duplicate | Delete
□	Exchange Server Calendar	Enabled	Included			Edit | Duplicate | Delete
□	Exchange Server Connector Support	Enabled	Included			Edit | Duplicate | Delete
□	Exchange Server GroupWise Router	Enabled	Included			Edit | Duplicate | Delete
□	Exchange Server Lotus Notes Dispatch	Enabled	Included			Edit | Duplicate | Delete
□	Exchange Server Site Replication Service	Enabled	Included			Edit | Duplicate | Delete

89 items in 9 pages. Go to page: 1

Figure 10: IPS Rules—Application Protection Rules

4 Under **Actions**, click **Edit** for the rule you want to modify. Click **OK to save changes**.

5 Click **Add Application** to add a new rule to the list.

6 Under **Actions**, click **Delete** for the rule you want to delete**.**

7 Select a rule and click **Copy To** to move it to another policy**.** Indicate the policy to which to move the rule and click **OK**.

NOTE: You can move several rules at one time by selecting all the rule before clicking **Copy To**.

8 Click **Save** to save changes.

Creating application protection rules

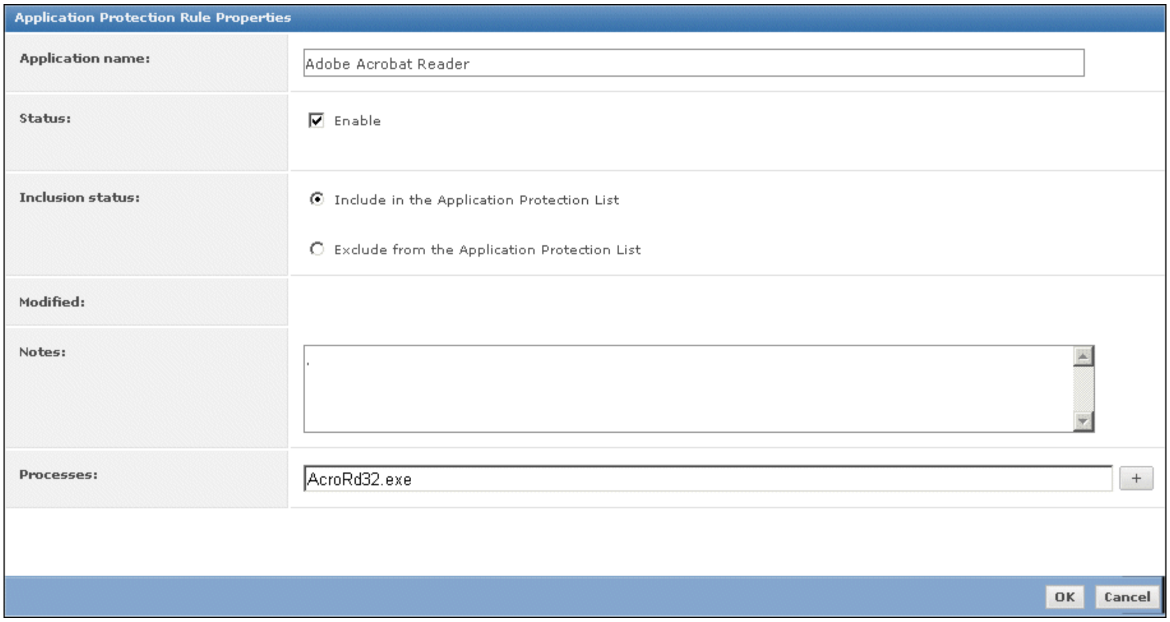
Use this task to create application protection rules.

Task

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

1 On the IPS Rule policy **Application Protection Rules** tab, do one of the following:
   - Click **Add Application Rule**. A blank **Application Protection Rule** page appears.
   - Select a rule and click **Duplicate**. After naming and saving the new rule, click **Edit**.

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



Application Protection Rule Properties

Application name:	Adobe Acrobat Reader
Status:	☑ Enable
Inclusion status:	● Include in the Application Protection List ○ Exclude from the Application Protection List
Modified:	
Notes:	
Processes:	AcroRd32.exe

Figure 11: Application Protection Rule

3 Click **OK**.

Working with IPS Exceptions

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, minimizes needless data flowing to the console, and ensures that the alerts are legitimate security threats.

For example, during the process of testing clients, a client recognizes the **Outlook Envelope - Suspicious Executable Mod.** signature. This signature signals that the Outlook e-mail application is attempting to modify an application outside the envelope of usual resources for Outlook. Thus, an event triggered by this signature is cause for alarm, because Outlook may be modifying an application not normally associated with 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.

Tasks

▸ Configuring IPS Rules exceptions
▸ Creating exception rules

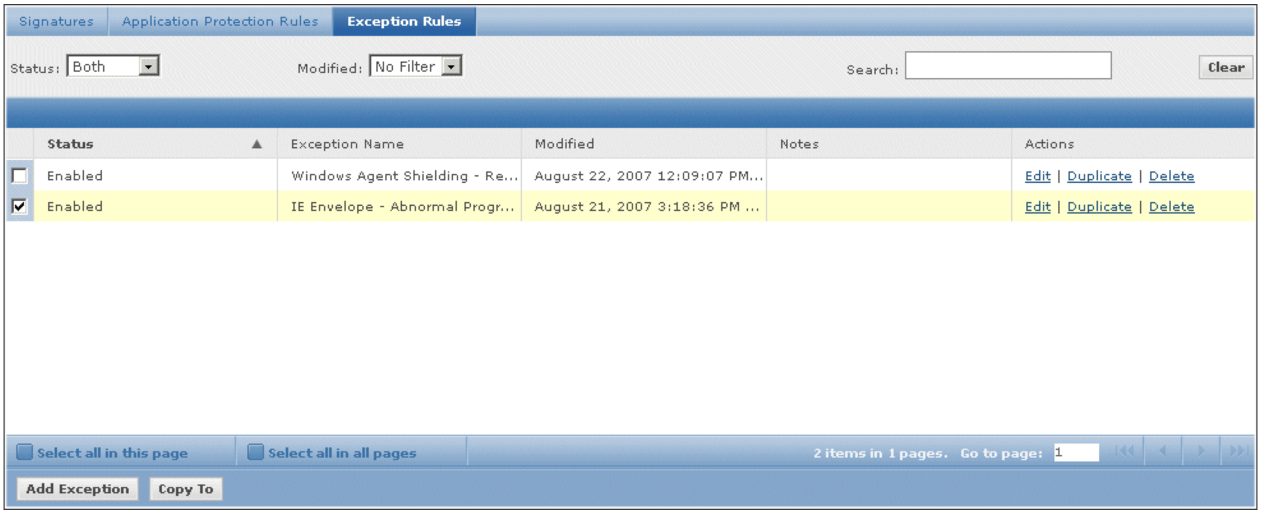
Configuring IPS Rules exceptions

Use this task to create, view, edit, or delete exception rules and move exception rules to another policy

Task

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

1. On the Policy Catalog page, select **Host Intrusion Prevention: IPS** on the **Product** list and select **IPS Rules** on 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. Use the filters at the top of the list to filter the view of all exception rules in the policy. You can filter on rule status, modified date, or specific text that includes rule or notes text. Click **Clear** to remove filter settings.



Status: Both
Modified: No Filter
Search:

	Status	Exception Name	Modified	Notes	Actions
□	Enabled	Windows Agent Shielding - Re...	August 22, 2007 12:09:07 PM...		Edit | Duplicate | Delete
☑	Enabled	IE Envelope - Abnormal Progr...	August 21, 2007 3:18:36 PM ...		Edit | Duplicate | Delete

Figure 12: IPS Rules—Application Protection Rules

4. Under **Actions**, click **Edit** for the rule you want to modify. Click **OK to save changes**.
5. Click **Add Exception** to add a new rule to the list.
6. Under **Actions**, click **Delete** for the rule you want to delete**.**
7. Select a rule and click **Copy To** to move it to another policy**.** Indicate the policy to which to move the rule and click **OK**.

   NOTE: You can move several rules at one time by selecting all the rules before clicking **Copy To**.

8. Click **Save** to save changes.

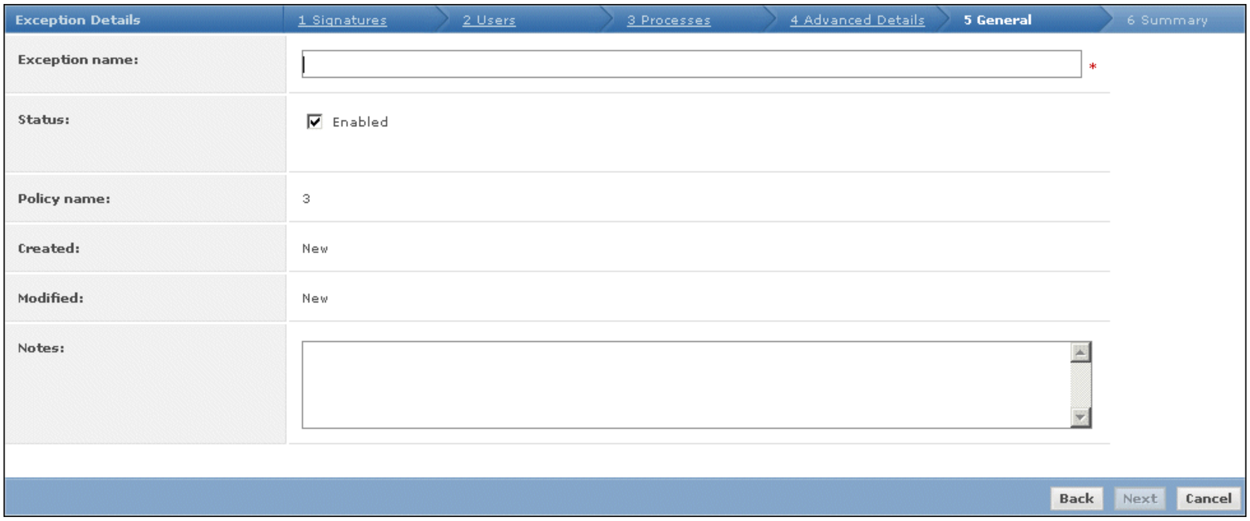
Creating exception rules

Use this task to create exception rules. When creating an exception rule, you need to define the exception and indicate the signature to which the exception applies.

Task

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

1. On the IPS Rule policy **Exception Rules** tab, click **Add Exception**.
2. Enter the required data on each tab of the Exception wizard. These include: **Signatures, Users, Processes, Advanced Details** and **General** tab. The **Summary** tab displays the settings made in the previous tabs.



Exception name:	*
Status:	☑ Enabled
Policy name:	3
Created:	New
Modified:	New
Notes:	

Figure 13: IPS Exception

3. Click **Save**.

Working with IPS events

An IPS event is triggered when a security violation, as defined by a signature, is detected. For example, Host Intrusion Prevention compares the start of any application against a signature for that operation, which may represent an attack. If a match occurs, an event is generated.

When Host Intrusion Prevention recognizes an IPS event, it flags it on the Host IPS **Events** tab 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 may 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 may find clients recognizing the signature E-mail access. Typically, an event triggered by this signature is cause for alarm. Hackers may 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 (Eudora, Netscape, Outlook), create an exception to that event.

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

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

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.

Tasks

- Managing IPS events

Managing IPS events

Use this task to analyze IPS events and, in reaction to them, create exceptions or trusted applications.

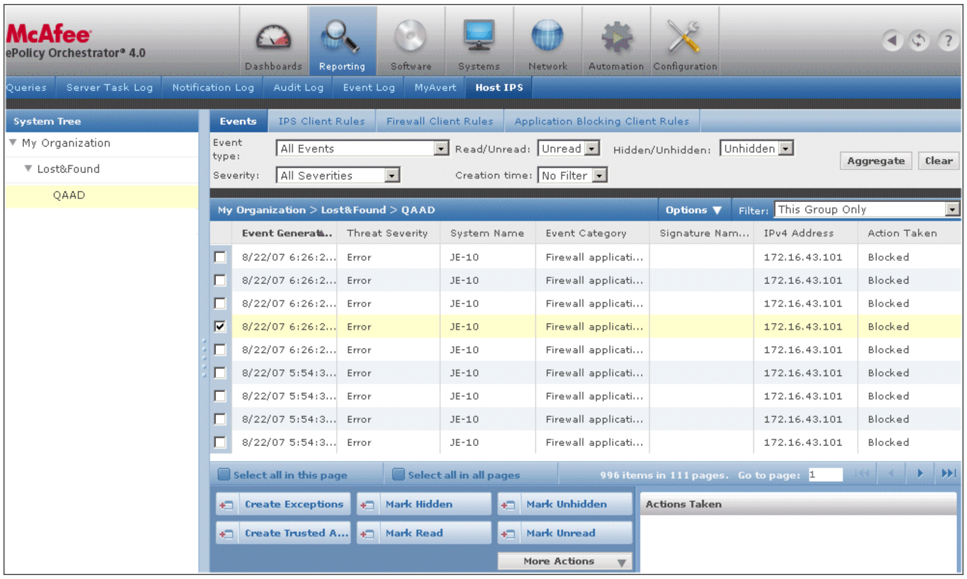
NOTE: IPS events also appear on the Event Log tab under Reporting combined with all other events for all systems. Access to the events tabs under Reporting requires additional permission sets, including view permissions for Event Log, Systems, and System Tree access.

Task

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

1 Go to **Reporting | Host IPS | IPS 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.



Event type: All Events Read/Unread: Unread Hidden/Unhidden: Unhidden
Severity: All Severities Creation time: No Filter
Filter: This Group Only

	Event Generat...	Threat Severity	System Name	Event Category	Signature Nam...	IPv4 Address	Action Taken
□	8/22/07 6:26:2...	Error	JE-10	Firewall applicati...		172.16.43.101	Blocked
□	8/22/07 6:26:2...	Error	JE-10	Firewall applicati...		172.16.43.101	Blocked
□	8/22/07 6:26:2...	Error	JE-10	Firewall applicati...		172.16.43.101	Blocked
☑	8/22/07 6:26:2...	Error	JE-10	Firewall applicati...		172.16.43.101	Blocked
□	8/22/07 6:26:2...	Error	JE-10	Firewall applicati...		172.16.43.101	Blocked
□	8/22/07 5:54:3...	Error	JE-10	Firewall applicati...		172.16.43.101	Blocked
□	8/22/07 5:54:3...	Error	JE-10	Firewall applicati...		172.16.43.101	Blocked
□	8/22/07 5:54:3...	Error	JE-10	Firewall applicati...		172.16.43.101	Blocked
□	8/22/07 5:54:3...	Error	JE-10	Firewall applicati...		172.16.43.101	Blocked

996 items in 111 pages. Go to page: 1

Figure 14: IPS Events tab

3 Determine how you want to view the list of events:

To...	Do this...
Select columns to display	Select **Choose Columns** from the Options menu. In the Select Columns page, add, remove, or reorder the columns for the display.
Sort by a column	Click the column header.
Filter for groups	From the Filter menu select **This Group Only** or **This Group and All Subgroups.**
Filter for events criteria	Select event type, marked status, severity level, or date of creation, then click **Filter**. Click **Clear** to remove filter settings.
Aggregate exceptions	Click **Aggregate**, select the criteria on which to aggregate events, then click **OK**. Click **Clear** to remove aggregation settings

4 Mark events by selecting one or more events, then clicking the appropriate command:

Click...	To...
Mark Read	Mark the event as read
Mark Unread	Mark a read event as unread
Mark Hide	Hide the event
Mark Unhidden	Show hidden events. Note: You must first filter for hidden events to be able to select them.

5 Select an event and click **Create Exception** to create an exception; or click **Create Trusted Application** to create an application rule. Follow the directions for creating an exception under Creating exception rules, for creating a trusted application under Creating and editing Trusted Application rules.

Managing IPS client rules

Use this task to analyze IPS client rules created automatically when clients are in adaptive mode, or manually on the client provided the Client UI policy option to allow manual creation of client rules is enabled.

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.

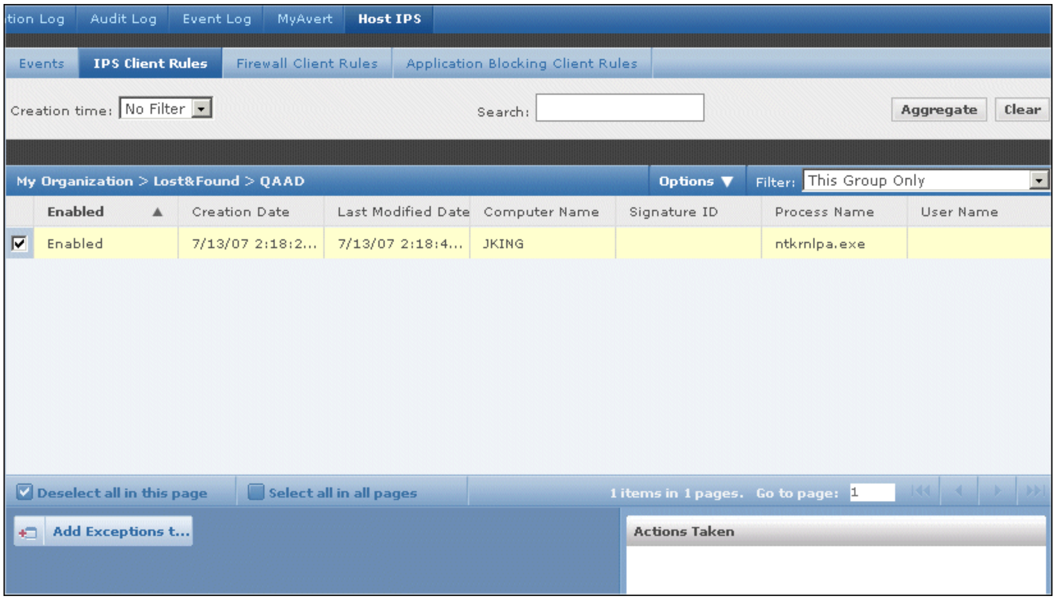
You can sort, filter, and aggregate the list of rules to find specific exceptions and see their details. You can then promote some or all of the client exception rules to a particular IPS Rules policy to reduce false positives for a particular system environment.

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.

Task

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

1 Go to **Reporting | Host IPS | IPS Client Rules**.



Creation time: No Filter

My Organization > Lost&Found > QAAD

Filter: This Group Only

	Enabled ▲	Creation Date	Last Modified Date	Computer Name	Signature ID	Process Name	User Name
☑	Enabled	7/13/07 2:18:2...	7/13/07 2:18:4...	JKING		ntkrnlpa.exe	

1 items in 1 pages. Go to page: 1

Figure 15: 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:

To...	Do this...
Sort by a column	Click the column header.
Filter for groups	From the Filter menu select **This Group Only** or **This Group and All Subgroups.**

To...	Do this...
Filter for exception criteria	Select time criteria; type process path, process name, user name, computer name, or signature ID in the search text box; then click **Filter**. Click **Clear** to remove filter settings.
Aggregate exceptions	Click **Aggregate**, select the criteria on which to aggregate exceptions., then click **OK**. Click **Clear** to remove aggregation settings.

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 Firewall policies of Host Intrusion Prevention protect computers by filtering all network traffic, allowing legitimate traffic through the firewall, and blocking the rest. 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.

Contents

Overview of Firewall policies

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

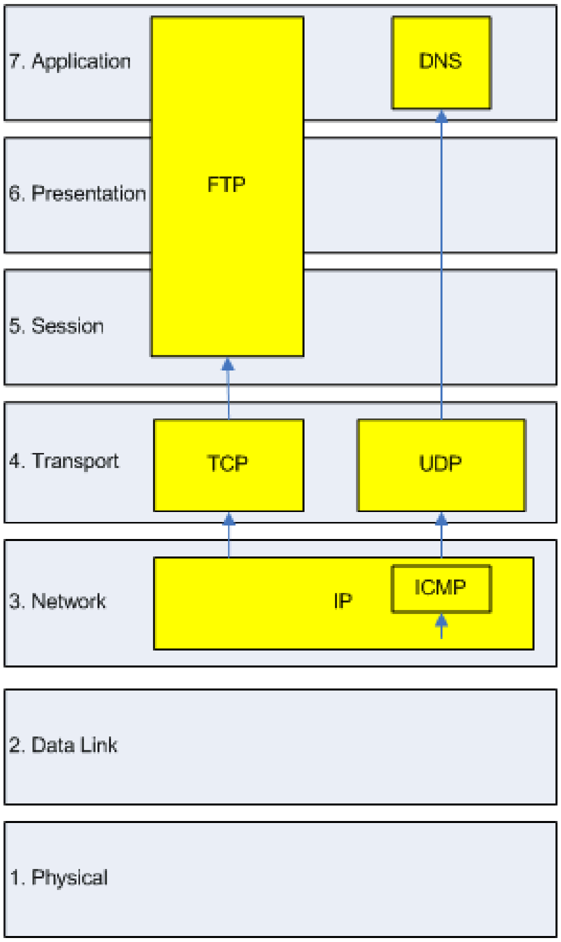


Figure 16: Network layers and protocols

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

NOTE: When using IPv6, stateful functionality is only supported on Vista.

Stateful packet filtering

Stateful packet filtering is the stateful tracking of TCP/UDP/ICMP protocol information at Transport Layer 4 and lower of the OSI network stack. Each packet is examined and if the inspected packet matches an existing firewall 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

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.

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 Preventions supports both standards.
- **Local and remote computer port numbers** — A computer sends and receives services using numbered ports. For example, HTTP service typically is available on port 80, and FTP services on port 21. Port numbers range from 0 to 65535.
- **Process ID (PID)** — A unique identifier for the process associated with a connection's traffic.
- **Timestamp** — The time of the last incoming or outgoing packet associated with the connection.
- **Timeout**: — The time limit (in seconds), set with the Firewall Options policy, after which the entry is removed from the table if no packet matching the connection is received. The timeout for TCP connections is enforced only when the connection is not established.
- **Direction** — The direction (incoming or outgoing) of the traffic that triggered the entry. After a connection is established, bidirectional traffic is allowed even with unidirectional rules, provided the entry matches the connection's parameters in the state table.

State table functionality

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 firewall rules work

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

Host Intrusion Prevention uses precedence to apply rules: the rule at the top of the firewall rules list is applied first.

If the traffic meets this rule's conditions, Host Intrusion Prevention allows or blocks the traffic. It does not try to apply any other rules in 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.

Ordering the firewall rules list

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

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

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

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

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

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 these steps:

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

   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.

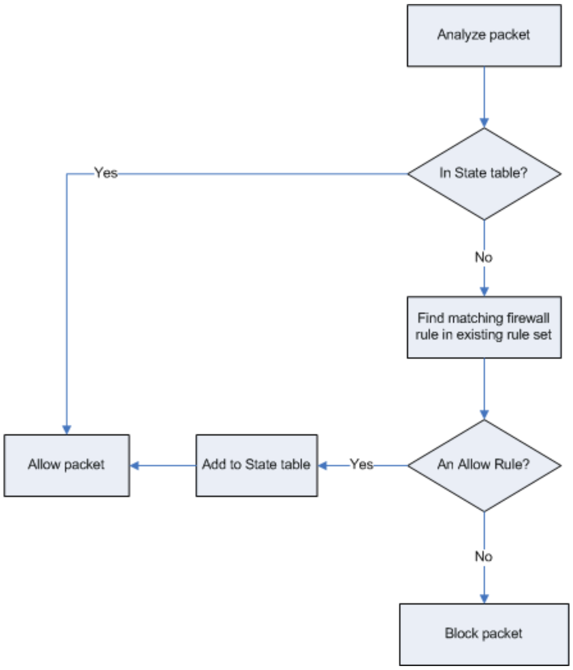


Figure 17: Stateful filtering process

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

Protocol	Description of handling
UDP	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.
ICMP	Only ICMP Echo Request and Echo Reply message types are tracked. NOTE: In contrast to the reliable, connection-oriented TCP protocol, UDP and ICMP are less reliable, connectionless protocols. To secure these protocols, the firewall considers generic UDP and ICMP connections to be virtual connections, held only as long as the connection is not idle longer than the timeout period specified for the connection. The timeout for virtual connections is set in the Firewall Options policy.
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.
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): • 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.

Rule groups and connection-aware groups

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

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

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

- IP address
- DNS suffix
- Gateway IP
- DHCP IP
- DNS server queried to resolve URLs
- WINS server used

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

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

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

- If Connection type is **LAN**.

or

If Connection type is **Wireless.**

or

If Connection type is **Any** and the DNS suffix list or the IP Address List is populated.

- If **IP Address List** 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.

Connection isolation in connection-aware groups

The connection isolation option in Connection-Aware Groups (CAG) prevents undesirable traffic from accessing a designated network 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 for a CAG, and an active Network Interface Card (NIC) matches the CAG criteria, the only types of traffic processed are traffic matching allow rules above the CAG in the firewall rules list, and traffic matching the CAG criteria. All other traffic is blocked.

The process of connection isolation with Connection-Aware Groups begins when the firewall processes traffic against its list of rules until a Connection-Aware Group (CAG) is encountered. At the CAG:

- If the traffic through a NIC matches the CAG's criteria, the firewall evaluates the CAG's rules for a match.
- If the traffic through a NIC does not match the CAG's criteria, and the connection isolation option is not enabled, the firewall skips the CAG and continues analyzing against the rules that follow the CAG.

- If the traffic through a NIC does not match the CAG criteria, and the connection isolation option is enabled, the traffic is blocked.

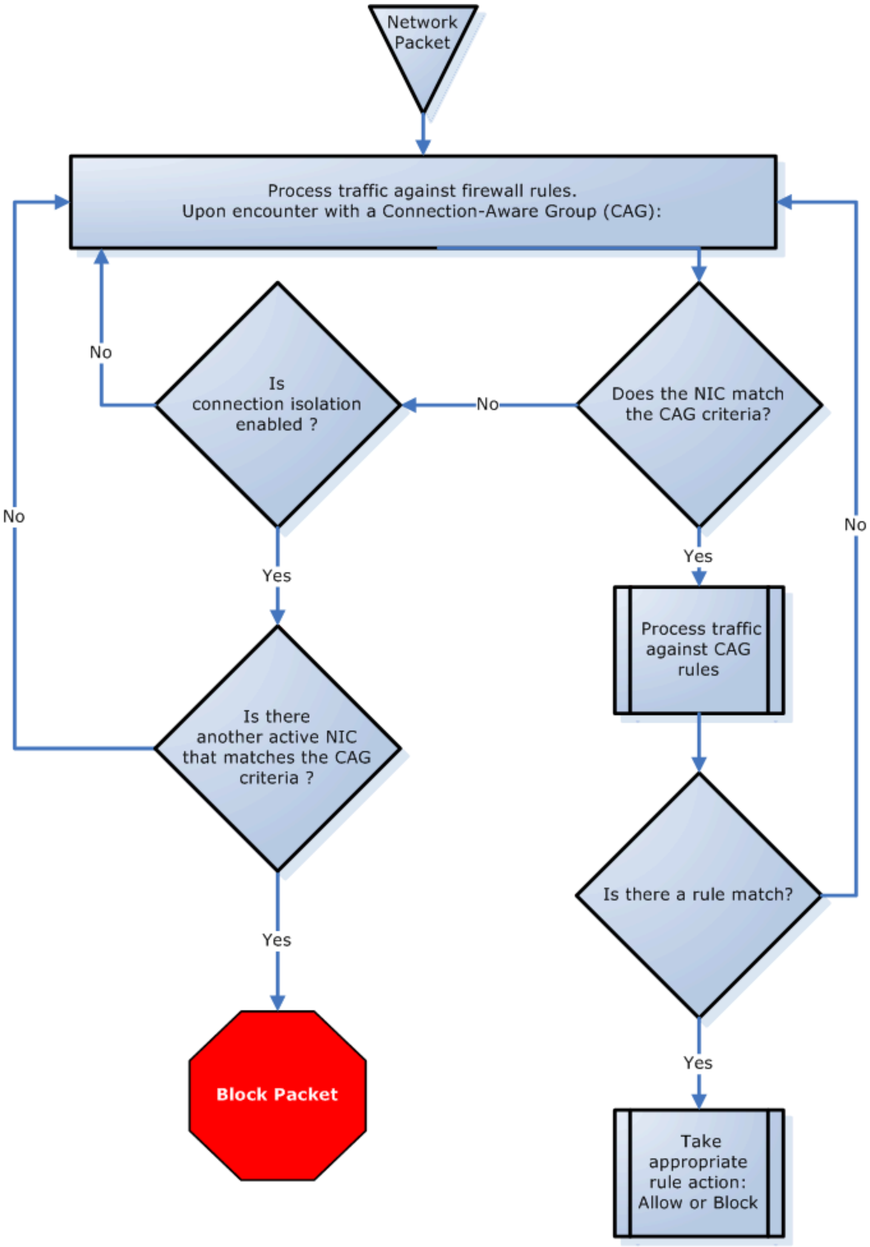

Network Packet
Process traffic against firewall rules.
Upon encounter with a Connection-Aware Group (CAG):
Does the NIC match the CAG criteria?
No
Is connection isolation enabled ?
No
Yes
Is there another active NIC that matches the CAG criteria ?
No
Yes
Block Packet
Yes
Process traffic against CAG rules
Is there a rule match?
No
Yes
Take appropriate rule action: Allow or Block

Figure 18: 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. CAG with corporate LAN connection rules
4. CAG with VPN connection rules.

Connection isolation on the corporate network

Connection rules are processed until the Connection-Aware Group with corporate LAN connection rules is encounterd. This CAG contains these settings:

- Connection type=LAN
- DNS suffix=mycompany.com
- Isolate this Connection =yes

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

Connection isolation at a hotel

Connection rules are processed until the Connection-Aware Group with VPN connection rules is encounterd. This CAG contains these settings:

- Connection type=Any
- 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 CAG. The only traffic the firewall allows is inside the VPN tunnel and the basic traffic on the actual adapter. Attempts by other hotel guests to access the computer over the network, either wired or wireless, are blocked.

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 bock rule, and automatically creates dynamic allow rules for non-matching traffic.

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 will be 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 with adaptive and learn mode

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

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 s 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 can create Firewall client rules to allow blocked activity. In addition, rules can 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.

Quarantine policies and rules

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

NOTE: Host Intrusion Prevention enforces quarantine rules for *all* ePolicy Orchestrator-managed applications. If you use ePolicy Orchestrator to manage clients with VirusScan Enterprise, Host Intrusion Prevention will quarantine any returning client where VirusScan Enterprise tasks fail to run; for example, if an update task fails to deliver the latest DAT files.

Out-of-date policies and files can create security holes and leave systems vulnerable to attack. By quarantining users until ePolicy Orchestrator updates them, unnecessary security risks are avoided. For example, a quarantine policy is useful for laptops whose policies and files may become out of date when they are away from the corporate network for a few days.

When you enable the Quarantine Options policy, both ePolicy Orchestrator and Host Intrusion Prevention participate. ePolicy Orchestrator detects whether a user has all the latest information they need. Host Intrusion Prevention enforces the quarantine until the client has all the necessary policies and files.

NOTE: If a user connects to the network using VPN software, set quarantine rules to allow any traffic required to both connect and authenticate over the VPN.

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

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

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

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

In addition, the Quarantine Options policy allows you select startup protection, so that when a client starts it will be quarantined and network access will be blocked until a Firewall Rules policy can be applied.

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

Working with Firewall Options policies

The Firewall Options policy turns on and off the firewall and allows you to apply adaptive or learn mode to create new firewall rules.

This policy category contains four preconfigured policies and an editable **My Default** policy. You can view and duplicate preconfigured policies; you can, create, edit, rename, duplicate, delete, and export custom policies.

Preconfigured policies include:

Off (McAfee Default)

All settings are disabled

On

- Enable Firewall
- Enable regular protection
- Retain client rules

Adaptive

- Enable Firewall
- Enable Adaptive mode
- Retain client rules

Learn

- Enable Firewall
- Enable Learn mode, Incoming and Outgoing
- Retain client rules

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy’s assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

- Configuring the Firewall Options policy

Configuring the Firewall Options policy

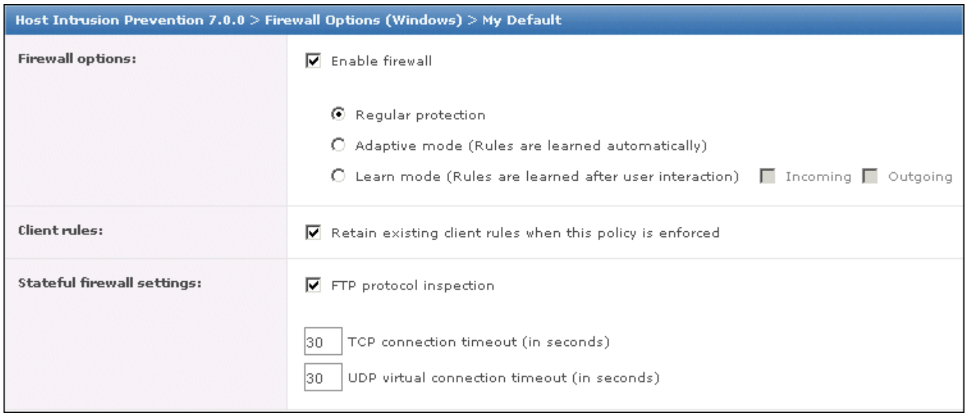
Use this task to turn the firewall on and off and to apply adaptive or learn mode.

Task

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

1 Go to **Systems | 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.



Host Intrusion Prevention 7.0.0 > Firewall Options (Windows) > My Default

Firewall options:	☑ Enable firewall ● Regular protection ○ Adaptive mode (Rules are learned automatically) ○ Learn mode (Rules are learned after user interaction) □ Incoming □ Outgoing
Client rules:	☑ Retain existing client rules when this policy is enforced
Stateful firewall settings:	☑ FTP protocol inspection 30 TCP connection timeout (in seconds) 30 UDP virtual connection timeout (in seconds)

Figure 19: Firewall Options

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

Working with Firewall Rules policies

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

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

Preconfigured policies include:

Minimal (Default)

- Blocks any incoming ICMP traffic that an attacker could use to gather information about your computer. Host Intrusion Prevention allows all other ICMP traffic.

- Allows Windows file sharing requests from computers in the same subnet, and blocks file sharing requests from anyone else. (The Trusted Networks policy must have **Include Local Subnet Automatically** selected.)
- Allows you to browse Windows domains, workgroups, and computers.
- Allows all high incoming and outgoing UDP traffic.
- Allows traffic that uses BOOTP, DNS, and Net Time UDP ports.

Learning Starter

- Blocks incoming ICMP traffic that an attacker could use to gather information about your computer. Host Intrusion Prevention allows all other ICMP traffic.
- Allows Windows file sharing requests from computers in the same subnet, and blocks file sharing requests from anyone else. (The Trusted Networks policy must have **Include Local Subnet Automatically** selected.)
- Allows you to browse Windows domains, workgroups, and computers.
- Allows traffic that uses BOOTP, DNS, and Net Time UDP ports.

Client High

Use this protection level if you are under attack or at high risk of an attack. This protection level allows only minimal traffic in and out of your system.

- Allows only ICMP traffic necessary for proper networking. This protection blocks both incoming and outgoing pings.
- Allows only UDP traffic necessary for accessing IP information (such as your own IP address or the network time).
- Blocks Windows file sharing.

Minimal (Default)

- Blocks any incoming ICMP traffic that an attacker could use to gather information about your computer. Host Intrusion Prevention allows all other ICMP traffic.
- Allows Windows file sharing requests from computers in the same subnet, and blocks file sharing requests from anyone else. (The Trusted Networks policy must have **Include Local Subnet Automatically** selected.)
- Allows you to browse Windows domains, workgroups, and computers.
- Allows all high incoming and outgoing UDP traffic.
- Allows traffic that uses BOOTP, DNS, and Net Time UDP ports.

Learning Starter

- Blocks incoming ICMP traffic that an attacker could use to gather information about your computer. Host Intrusion Prevention allows all other ICMP traffic.
- Allows Windows file sharing requests from computers in the same subnet, and blocks file sharing requests from anyone else. (The Trusted Networks policy must have **Include Local Subnet Automatically** selected.)
- Allows you to browse Windows domains, workgroups, and computers.
- Allows traffic that uses BOOTP, DNS, and Net Time UDP ports.

Client High

Use this protection level if you are under attack or at high risk of an attack. This protection level allows only minimal traffic in and out of your system.

- Allows only ICMP traffic necessary for proper networking. This protection blocks both incoming and outgoing pings.

- Allows only UDP traffic necessary for accessing IP information (such as your own IP address or the network time).
- Blocks Windows file sharing.

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

- ▶ Configuring the Firewall Rules policy
- ▶ Creating and editing firewall rules
- ▶ Creating firewall rule groups
- ▶ Creating firewall connection-aware groups
- ▶ Adding predefined firewall rules
- ▶ Managing Firewall client rules

Configuring the Firewall Rules policy

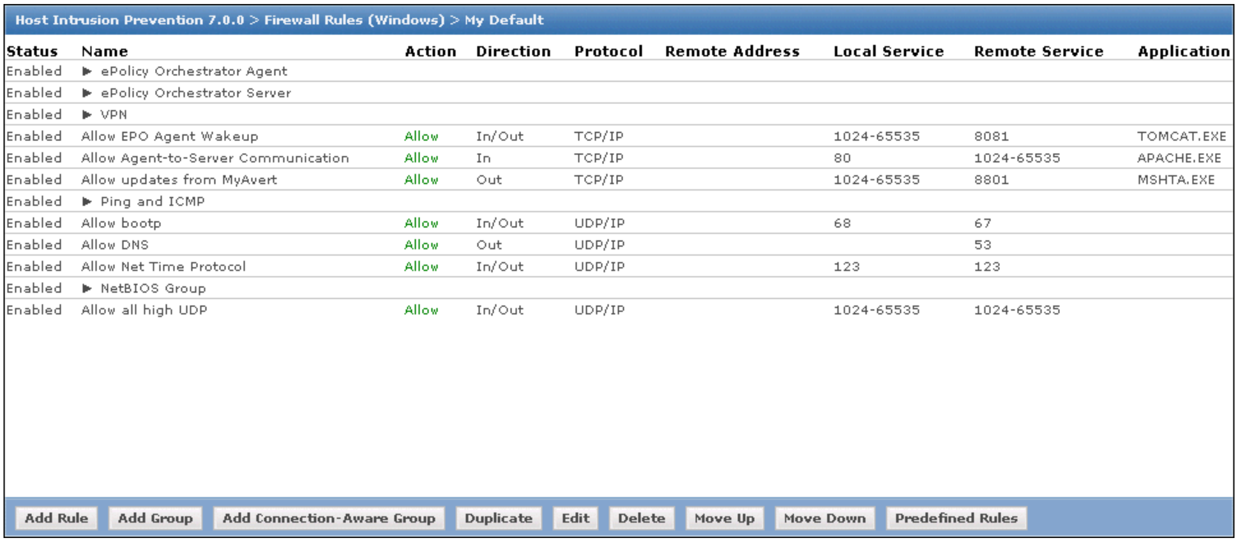
Use this task to add, edit, or remove firewall rules and rule groups, and reorder the list of rules.

Task

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

1 On the Policy Catalog page, select **Host Intrusion Prevention: Firewall** on the **Product** list and select **Firewall Rules** on the Category list. The list of policies appears.

2 Click **Edit** to make changes on the **Firewall Rules** page.



Host Intrusion Prevention 7.0.0 > Firewall Rules (Windows) > My Default

Status	Name	Action	Direction	Protocol	Remote Address	Local Service	Remote Service	Application
Enabled	▶ ePolicy Orchestrator Agent							
Enabled	▶ ePolicy Orchestrator Server							
Enabled	▶ VPN							
Enabled	Allow EPO Agent Wakeup	Allow	In/Out	TCP/IP		1024-65535	8081	TOMCAT.EXE
Enabled	Allow Agent-to-Server Communication	Allow	In	TCP/IP		80	1024-65535	APACHE.EXE
Enabled	Allow updates from MyAvert	Allow	Out	TCP/IP		1024-65535	8801	MSHTA.EXE
Enabled	▶ Ping and ICMP							
Enabled	Allow bootp	Allow	In/Out	UDP/IP		68	67	
Enabled	Allow DNS	Allow	Out	UDP/IP			53	
Enabled	Allow Net Time Protocol	Allow	In/Out	UDP/IP		123	123	
Enabled	▶ NetBIOS Group							
Enabled	Allow all high UDP	Allow	In/Out	UDP/IP		1024-65535	1024-65535	

Figure 20: Firewall Rules list

3 Do any of the following:

To...	Do this
Add a rule	Click **Add Rule or Add Predefined Rules**. See *Working with firewall rules* or *Working with predefined firewall rules* for details.
Add a group	Click **Add Group**. See Working with rule groups for details.
Add a connection-aware group	Click **Add Connection-Aware Group**. See *Working with connection-aware groups* for details.
Perform an action on a single rule	Select the rule and click: **Edit** to edit an exisintg rule. See *Working with firewall rules* for details. **Duplicate** to make a copy of the rule withing the same policy and named 'copy of' the original rule. **Delete** to delete rule. **Copy To** to copy the rule to another policy. You are prompted to indicate the policy. **Move Up** to move the rule up in the list. **Move Down** to move the rule down in the list.

4 Click **Save** to save changes.

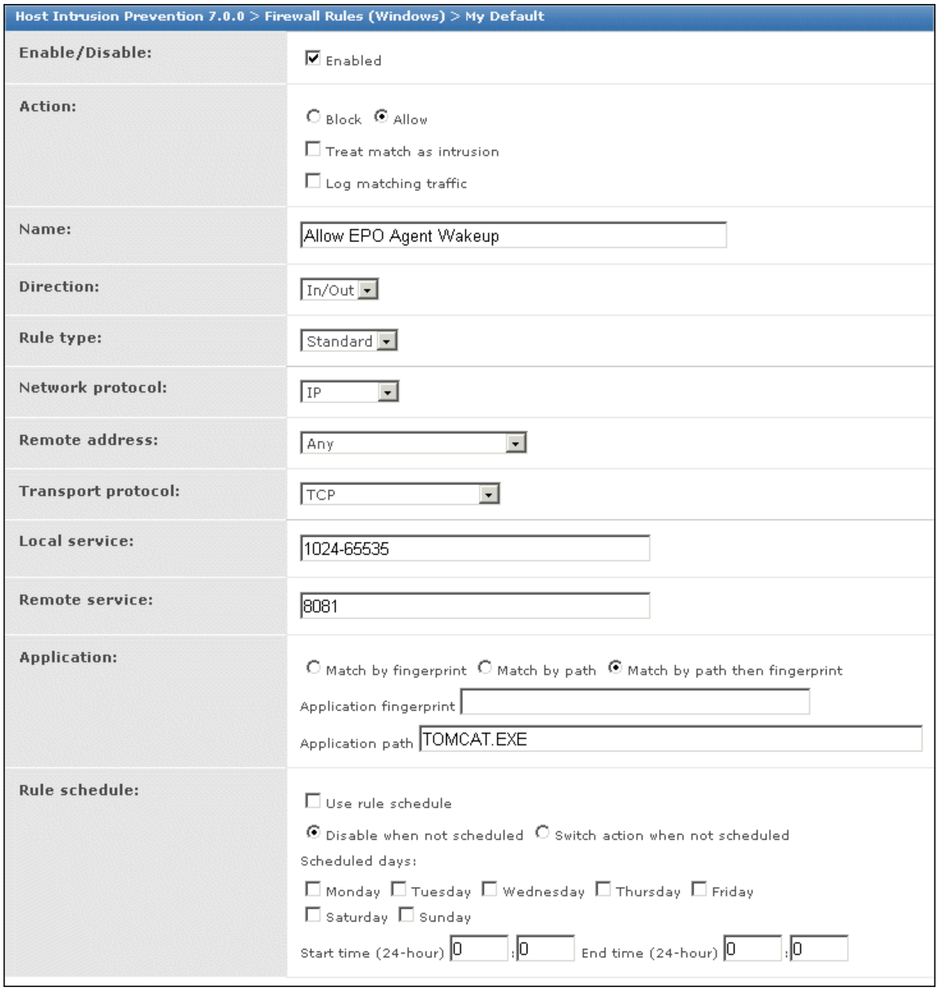
Creating and editing firewall rules

Use this task to create a new firewall rule or edit an existing one.

Task

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

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



Host Intrusion Prevention 7.0.0 > Firewall Rules (Windows) > My Default

Enable/Disable:	☑ Enabled
Action:	○ Block ● Allow ☐ Treat match as intrusion ☐ Log matching traffic
Name:	Allow EPO Agent Wakeup
Direction:	In/Out
Rule type:	Standard
Network protocol:	IP
Remote address:	Any
Transport protocol:	TCP
Local service:	1024-65535
Remote service:	8081
Application:	○ Match by fingerprint ○ Match by path ● Match by path then fingerprint Application fingerprint Application path TOMCAT.EXE
Rule schedule:	☐ Use rule schedule ● Disable when not scheduled ○ Switch action when not scheduled Scheduled days: ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday Start time (24-hour) 0 : 0 End time (24-hour) 0 : 0

Figure 21: Firewall Rule

2 Select or type the needed options.

3 Click **OK**.

Creating firewall rule groups

Use this task to create a group to contain a set of rules with a single purpose, such as rules that allow for VPN connection. Groups appear in the rule list in black preceded by an arrow. Click the arrow to show or hide the rules within the group.

Task

1 On the **Firewall Rules** policy page, click **Add Group**.

2 In the **Name** field of the **Firewall Rule Group** page, type a name for the group.

3 Click **OK**.

4 Create new rules within this group, or move existing rules into it from the firewall rule list by selecting the rule and clicking **Move Up** or **Move Down**.

Creating firewall connection-aware groups

Use this task to create a connection-aware group. These groups let you manage a set of rules that apply only when connecting to a network using a wired, wireless, or non-specific connection with particular parameters. Groups appear in the rule list in blue preceded by an arrow. Click the arrow to show or hide the rules within the group

Task

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

1. On the **Firewall Rules** policy page, click **Add Connection Aware Group**.
2. Type a name for the group in the **Name** field.
3. Under **Connection type**, select the type of connection (**LAN, Wireless, Any**) to which to apply the rules in this group.
4. Select **Isolate this connection** to block traffic coming from sources other than from a single specified connection.
5. Under New Criterion, select a category of criterion to apply to the rule. Click **Add Criterion** to display an additional field in which to type the new matching criterion.

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

6. Click the Add button to append more criteria in the same category. Click the Remove button or **Remove All** to eliminate one or all of the previously added criteria in the selected category.
7. Click **OK**.

Adding predefined firewall rules

Use this task to add predefined firewall rules that match your needs immediately or after you have edited them.

Task

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

1. On the **Firewall Rules** policy page, click **Predefined Rules**.
2. Select one or more predefined groups, or one or more predefined rules within a group.
3. Click **Add to Policy** to add the selected groups and rules; click **View** to view details of a selected group or rule.
4. Click **Cancel** to return to the **Firewall Rules**policy page.

Managing Firewall client rules

Use this task to analyze Firewall client rules created either automatically in adaptive or learn mode or manually for a group of clients, then determine which if any client rules to move to a Firewall Rules policy.

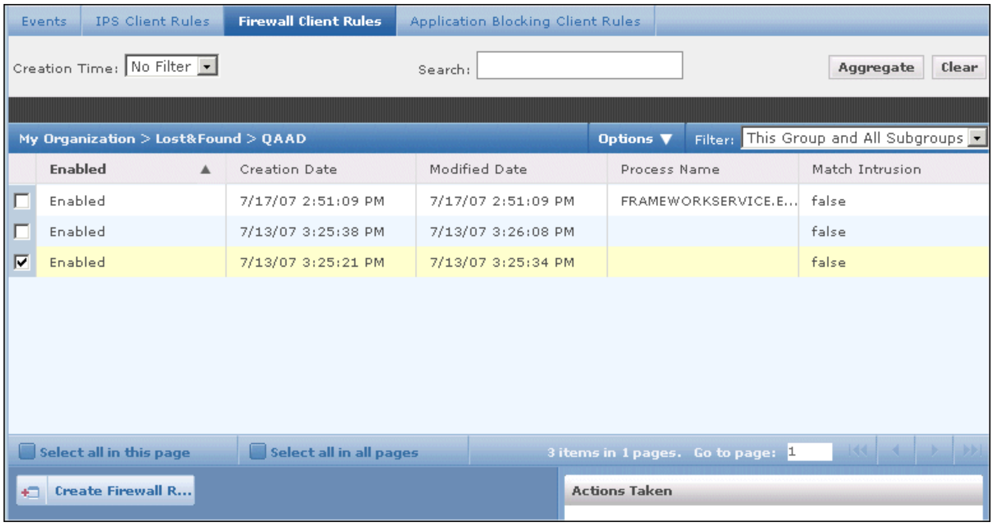
NOTE:

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 Go to **Reporting | Host IPS | Firewall Client Rules**.



Creation Time: No Filter

Search:

My Organization > Lost&Found > QAAD

Filter: This Group and All Subgroups

	Enabled ▲	Creation Date	Modified Date	Process Name	Match Intrusion
□	Enabled	7/17/07 2:51:09 PM	7/17/07 2:51:09 PM	FRAMEWORKSERVICE.E...	false
□	Enabled	7/13/07 3:25:38 PM	7/13/07 3:26:08 PM		false
☑	Enabled	7/13/07 3:25:21 PM	7/13/07 3:25:34 PM		false

□ Select all in this page   □ Select all in all pages   3 items in 1 pages. Go to page: 1

Figure 22: Firewall 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 rules:

To...	Do this...
Select columns to display	Select **Choose Columns** from the Options menu. In the Select Columns page, add, remove, or reorder the columns for the display.
Sort by a column	Click the column header.
Filter for groups	From the Filter menu select **This Group Only** or **This Group and All Subgroups.**
Filter for creation time	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.
Filter for searched text	Type the process path, process name, user name, computer name, or signature ID to filter on. Click **Clear** to remove filter settings.
Aggregate rules	Click **Aggregate**, select the criteria on which to aggregate rules., then click **OK**. Click **Clear** to remove aggregation settings.

4 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.

Working with Quarantine Options policies

The Quarantine Options policy turns on and off quarantine mode and quarantine notifications, defines quarantined networks, and configures fail options.

This policy category contains a preconfigured policy, which has all settings disabled, and an editable **My Default** policy. You can view and duplicate preconfigured policies; you can, create, edit, rename, duplicate, delete, and export custom policies.

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

- Configuring the Quarantine Options policy

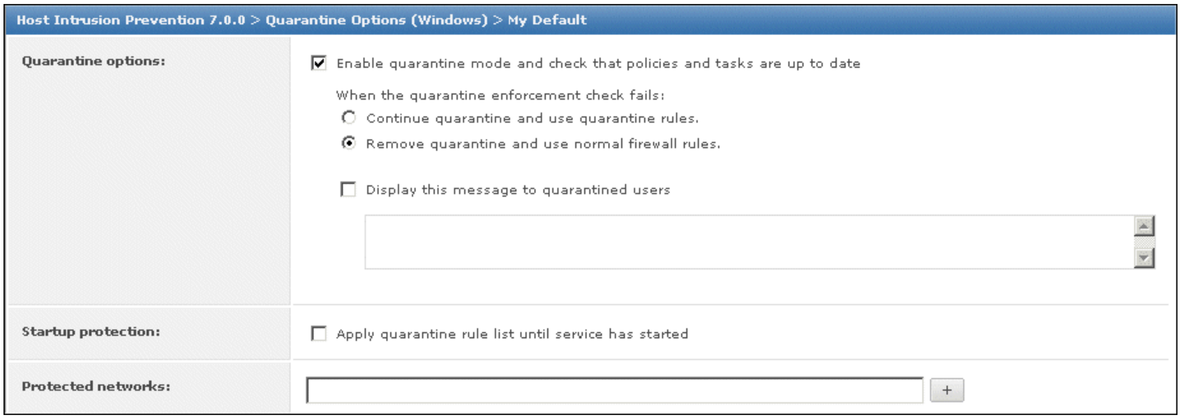
Configuing the Quarantine Options policy

Use this task to enable or disable quarantine mode and set other quarantine options.

Task

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

1. Go to **Systems | Policy Catalog** and select **Host Intrusion Prevention: Firewall** in the **Product** list and **Quarantine Options** in the **Category** list. The list of policies appears.
2. In the **Quarantine Options** policy list, click **Edit** under **Actions** to change the settings for a custom policy.



Host Intrusion Prevention 7.0.0 > Quarantine Options (Windows) > My Default

Quarantine options:
☑ Enable quarantine mode and check that policies and tasks are up to date
When the quarantine enforcement check fails:
○ Continue quarantine and use quarantine rules.
● Remove quarantine and use normal firewall rules.
□ Display this message to quarantined users

Startup protection:
□ Apply quarantine rule list until service has started

Protected networks:

Figure 23: Quarantine Options

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

Working with Quarantine Rules policies

The Quarantine Rules policy is a special set of firewall rules that is enforced when quarantine mode is enabled. You create and manage quarantine rules by applying a Quarantine Rules policy with the appropriate settings.

NOTE: If users connect to the network using VPN software, make certain that quarantine rules allow any traffic required to connect and authenticate over the VPN. You can use the regular Firewall feature to determine which VPN-related rules you need for **quarantine mode**. Enable the firewall's learn mode or adaptive mode, and then connect using VPN software. Host Intrusion Prevention automatically generates relevant VPN rules, which you can then reproduce in your quarantine rules.

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

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

- Configuring the Quarantine Rules policy
- Creating and editing quarantine rules
- Creating quarantine rule groups
- Adding predefined quarantine rules

Configuring the Quarantine Rules policy

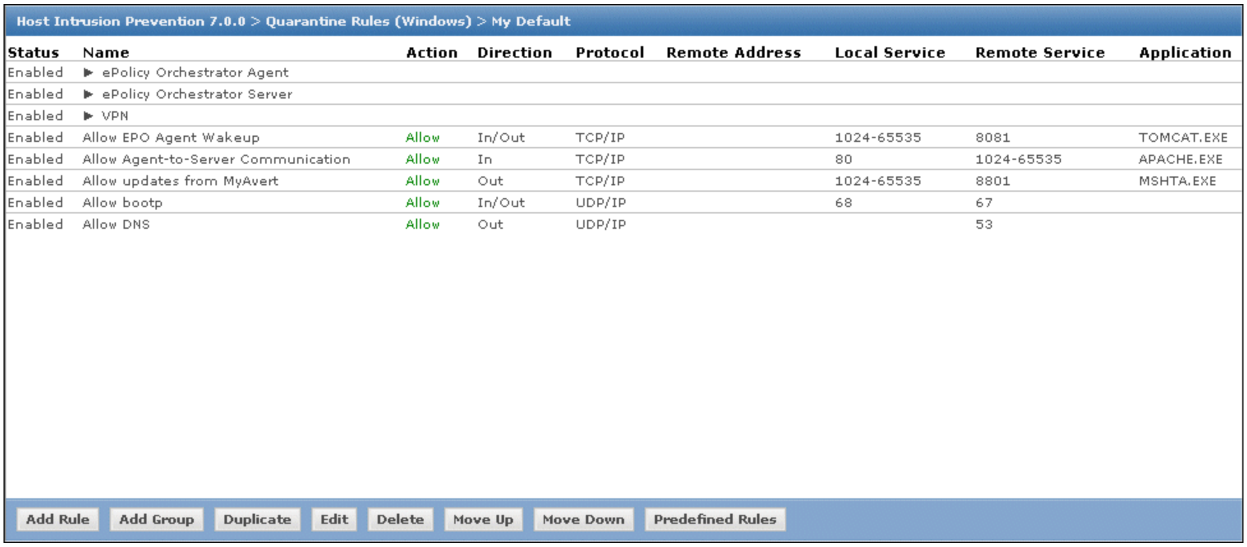
Create new policies or edit existing policies by adding or removing rules, or moving rules between policies. View and edit rules from the Quarantine Rules page.

Task

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

1. On the Policy Catalog page, select **Host Intrusion Prevention: Firewall** on the Product list and select **Quarantine Rules** on the Category list. The list of policies appears.

2. Click **Edit** to make changes on the **Quarantine Rules** page.



Host Intrusion Prevention 7.0.0 > Quarantine Rules (Windows) > My Default

Status	Name	Action	Direction	Protocol	Remote Address	Local Service	Remote Service	Application
Enabled	▶ ePolicy Orchestrator Agent							
Enabled	▶ ePolicy Orchestrator Server							
Enabled	▶ VPN							
Enabled	Allow EPO Agent Wakeup	Allow	In/Out	TCP/IP		1024-65535	8081	TOMCAT.EXE
Enabled	Allow Agent-to-Server Communication	Allow	In	TCP/IP		80	1024-65535	APACHE.EXE
Enabled	Allow updates from MyAvert	Allow	Out	TCP/IP		1024-65535	8801	MSHTA.EXE
Enabled	Allow bootp	Allow	In/Out	UDP/IP		68	67	
Enabled	Allow DNS	Allow	Out	UDP/IP			53	

Figure 24: Quarantine Rules list

To...	Do this...
Add a rule	Click **Add Rule or Predefined Rules**. See *Working with quarantine rules* or *Working with predefined quarantine rules* for details.
Add a group	Click **Add Group**. See *Working with rule groups* for details.
Perform an action on a single rule	Select the rule and click: **Edit** to edit an exisintg rule. See *Working with quarantine rules* for details. **Duplicate** to make a copy of the rule withing the same policy and named 'copy of' the original rule. **Delete** to delete rule. **Copy To** to copy the rule to another policy. You are prompted to indicate the policy. **Move Up** to move the rule up in the list. **Move Down** to move the rule down in the list.

3. Click **Save** to save changes.

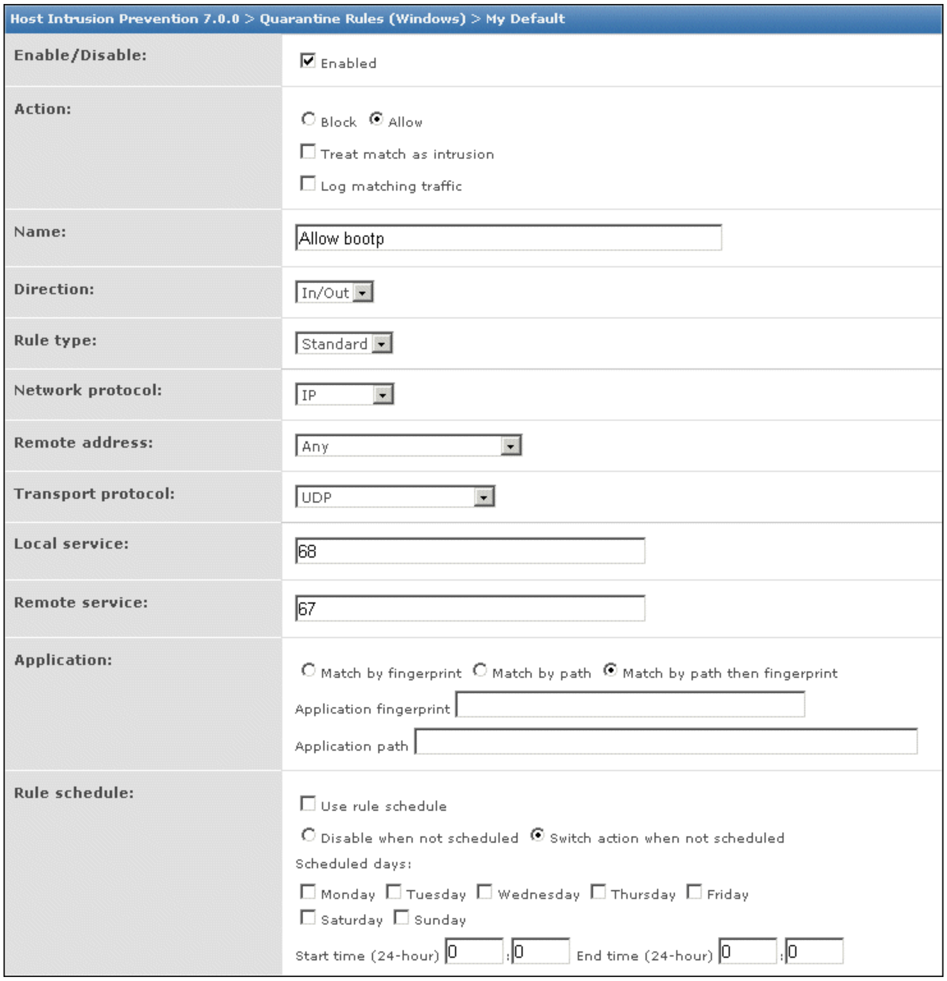
Creating and editing quarantine rules

Use this task to create a new quarantine rule or edit an existing one.

Task

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

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



Host Intrusion Prevention 7.0.0 > Quarantine Rules (Windows) > My Default

Enable/Disable:	☑ Enabled
Action:	○ Block ● Allow □ Treat match as intrusion □ Log matching traffic
Name:	Allow bootp
Direction:	In/Out
Rule type:	Standard
Network protocol:	IP
Remote address:	Any
Transport protocol:	UDP
Local service:	68
Remote service:	67
Application:	○ Match by fingerprint ○ Match by path ● Match by path then fingerprint Application fingerprint Application path
Rule schedule:	□ Use rule schedule ○ Disable when not scheduled ● Switch action when not scheduled Scheduled days: □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday Start time (24-hour) 0 : 0 End time (24-hour) 0 : 0

Figure 25: Quarantine Rule page

2 Select or type the needed options.

3 Click **OK**.

Creating quarantine rule groups

Use this task to create a group to contain a set of quarantine rules with a single purpose. Groups appear in the rule list in black preceded by an arrow. Click the arrow to show or hide the rules within the group.

Task

1 On the **Quarantine Rules** policy page, click **Add Group**.

2 In the **Name** field of the **Quarantine Firewall Rule Group** page, type a name for the group.

3 Click **OK**.

4 Create new rules within this group, or move existing rules into it from the quarantine rule list by selecting the rule and clicking **Move Up** or **Move Down**.

Adding predefined quarantine rules

Use this task to add predefined quarantine rules that match your needs immediately or after you have edited them.

Task

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

1. On the **Quarantine Rules** policy page, click **Predefined Rules**.
2. Select one or more predefined groups, or one or more predefined rules within a group.
3. Click **Add to Policy** to add the selected groups and rules; click **View** to view details of a selected group or rule.
4. Click **Cancel** to return to the **Quarantine Rules** policy page.

Configuring Application Blocking Policies

The Application Blocking feature of Host Intrusion Prevention manages a set of applications that you allow to run (known as application creation) or bind (known as application hooking) with other applications.

Contents

Overview of Application Blocking policies

The Application Blocking feature monitors applications being used and allows or blocks them.

Host Intrusion Prevention offers two types of application blocking:

- Application creation
- Application hooking

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

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

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

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

Application Blocking client rules

Clients in adaptive or learn mode can create client rules to allow blocked application creation or hooking. You can view these rules in a filtered or aggregated view to analyze them to create 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.

Working with Application Blocking policies

The Application Blocking Options policy turns on and off application blocking rules and allows you to apply adaptive or learn mode to create new rules.

This policy category contains four preconfigured policies and an editable **My Default** policy. You can view and duplicate preconfigured policies; you can, create, edit, rename, duplicate, delete, and export editable custom policies.

Preconfigured policies include:

Off (McAfee Default)

All settings are disabled

On

- Application Creation Blocking, Regular Protection. (Only follows rules in rules list.)
- Application Hooking Blocking, Regular Protection. (Only follows rules in rules list.)

Adaptive

- Application Creation Blocking, Adaptive mode, (Rules are learned automatically.)
- Application Hooking Blocking, Adaptive mode, (Rules are learned automatically.

Learn

- Application Creation Blocking, Learn mode. (Rules are learned after user interaction.)
- Application Hooking Blocking, Learn mode. (Rules are learned after user interaction.)

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

▸ Configuring an Application Blocking Options policy

Configuring an Application Blocking Options policy

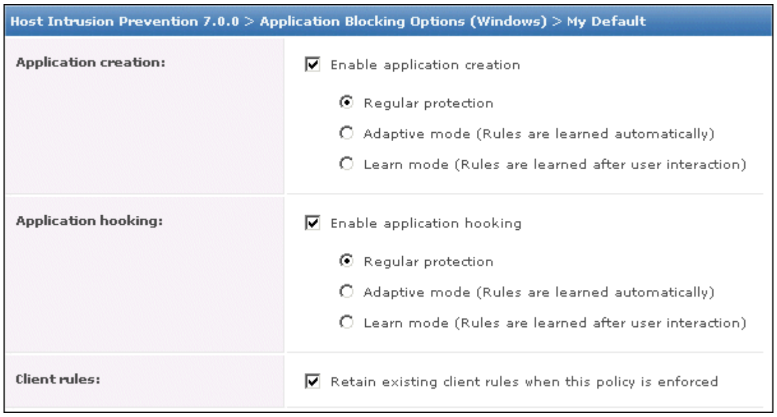
Use this task to enable or disable application blocking rules and apply adaptive or learn mode.

Task

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

1 Go to **Systems | Policy Catalog** and select **Host Intrusion Prevention: Application Blocking** in the Product list and **Application Blocking Options** in the **Category** list. The list of policies appears.

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



Host Intrusion Prevention 7.0.0 > Application Blocking Options (Windows) > My Default

Application creation:
☑ Enable application creation
● Regular protection
○ Adaptive mode (Rules are learned automatically)
○ Learn mode (Rules are learned after user interaction)

Application hooking:
☑ Enable application hooking
● Regular protection
○ Adaptive mode (Rules are learned automatically)
○ Learn mode (Rules are learned after user interaction)

Client rules:
☑ Retain existing client rules when this policy is enforced

Figure 26: Application Blocking Options

3 In the **Application Blocking Options** page that appears, make any needed changes, then click **Save**.

Working with Application Blocking Rules policies

Application blocking rules determine whether specific applications are blocked from running, hooking, or both. Apply application blocking rules only after having run in adaptive or learn mode to determine which applications are present and perhaps vulnerable in your environment. You should examine all learned rules before moving them to a policy. Use application blocking rules only after a set period of over all policy fine-tuning. If applications change regularly, application blocking is not recommended; however, if your environment has a fairly fixed set of applications, this feature can add another layer of security without additional administrative work.

This policy category contains a single default policy, which provides application blocking for McAfee and general Windows applications, and an editable **My Default** policy. You can view and duplicate the preconfigured policy as wall as copy selected rules in it to another policy; you can edit, rename, duplicate, delete, and export custom policies.

Within the policy you can add, edit, duplicate, or delete rules. You can also move rules up or down in the list or to another policy.

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

- Configuring an Application Blocking Rules policy

- Creating and editing Application Blocking rules
- Managing Application Blocking client rules

Configuring an Application Blocking Rules policy

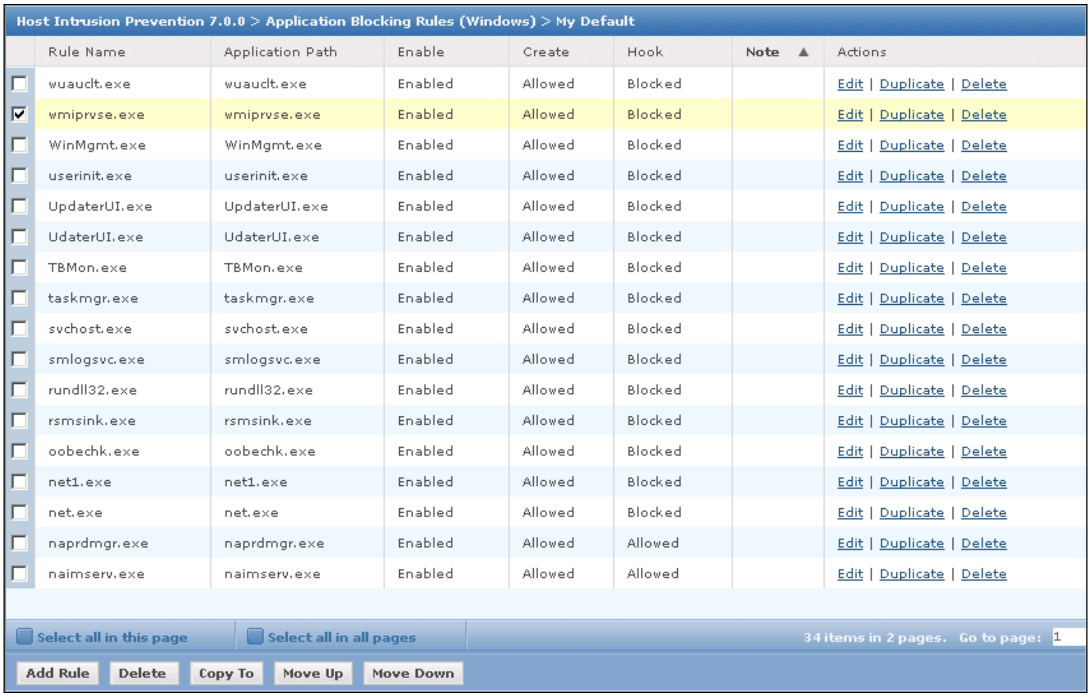
Use this task to add or remove rules in a policy and move rules between policies.

Task

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

1 Go to **Systems | Policy Catalog** and select **Host Intrusion Prevention: Application Blocking** in the Product list and **Application Blocking Rules** in the **Category** list. The list of policies appears.

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



Host Intrusion Prevention 7.0.0 > Application Blocking Rules (Windows) > My Default

	Rule Name	Application Path	Enable	Create	Hook	Note ▲	Actions
☐	wuauclt.exe	wuauclt.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☑	wmiprvse.exe	wmiprvse.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	WinMgmt.exe	WinMgmt.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	userinit.exe	userinit.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	UpdaterUI.exe	UpdaterUI.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	UdaterUI.exe	UdaterUI.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	TBMon.exe	TBMon.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	taskmgr.exe	taskmgr.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	svchost.exe	svchost.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	smlogsvc.exe	smlogsvc.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	rundll32.exe	rundll32.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	rsmsink.exe	rsmsink.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	oobechk.exe	oobechk.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	net1.exe	net1.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	net.exe	net.exe	Enabled	Allowed	Blocked		Edit | Duplicate | Delete
☐	naprdmgr.exe	naprdmgr.exe	Enabled	Allowed	Allowed		Edit | Duplicate | Delete
☐	naimserv.exe	naimserv.exe	Enabled	Allowed	Allowed		Edit | Duplicate | Delete

☐ Select all in this page ☐ Select all in all pages 34 items in 2 pages. Go to page: 1

Figure 27: Application Blocking Rules policy

3 In the In the **Application Blocking Rules** page that appears, do any of the following:

To...	Do this...
Add a rule	Click **Add Rule**. See Creating and editing Application Blocking rules for details.
Perform an action on one or more rules at the same time	Select them and click: **Delete**to delete rules. **Copy To** to copy rules to another policy. You are prompted to indicate the policy. **Move Up** to move rules up in the list. **Move Down** to move rules down in the list.

To...	Do this...
To perform an action on a single rule	Click: **Edit** to edit an existing rule. See Creating and editing Application Blocking rules for details. **Duplicate** to make a copy of the rule within the same policy and named 'copy of' the original rule. **Delete** to remove the rule from the list.

4 Click **Save**.

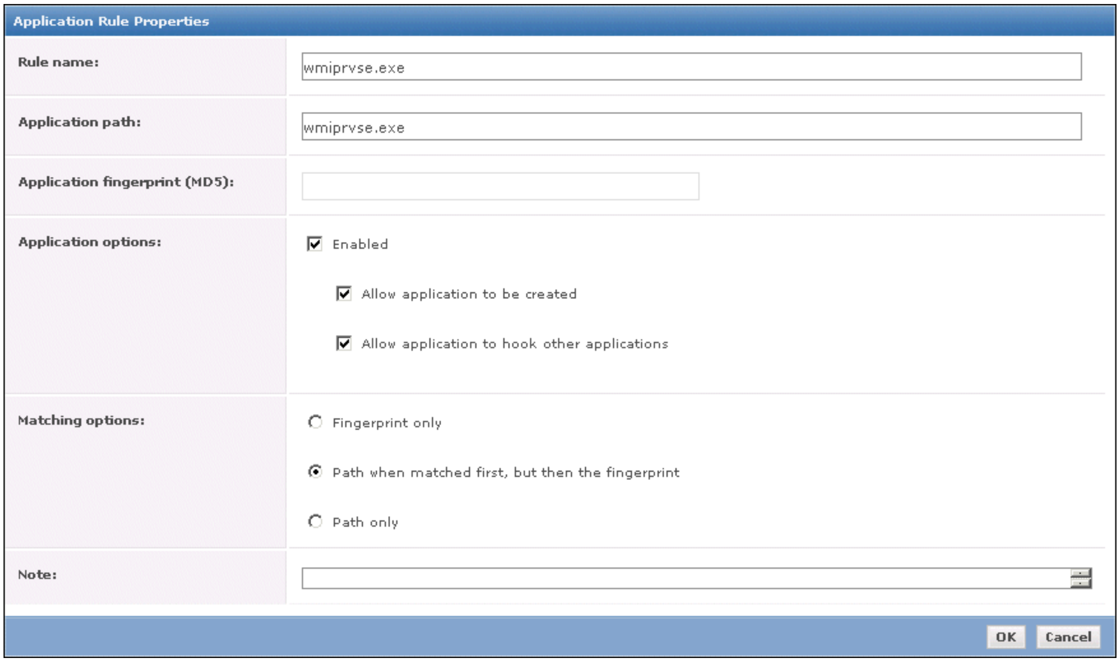
Creating and editing Application Blocking rules

Use this task to create a new or edit an existing application blocking rule.

Task

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

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



Application Rule Properties

Rule name: wmiprvse.exe

Application path: wmiprvse.exe

Application fingerprint (MD5):

Application options:
☑ Enabled
☑ Allow application to be created
☑ Allow application to hook other applications

Matching options:
○ Fingerprint only
● Path when matched first, but then the fingerprint
○ Path only

Note:

Figure 28: Application Rule dialog box

2 In the **Application Rule** page, type or edit the name for the rule and its path name. Wildcards are accepted.

3 Enter a MD5 fingerprint hash for the rule to match against a fingerprint. For client rules this is filled in automatically.

4 Select **Application Options**:

Select this option...	To do this...
Enable	Enable this rule.
Allow application to be created	Allow the application to run.

Select this option...	To do this...
Allow application to hook other applications	Allow the application to bind to other applications.

5 Select **Matching Options**:

Select this option...	To do this...
Fingerprint only	Match against the fingerprint. only if the client's application is the same version of the application referenced on the server.
Path when matched first, then the fingerprint	When the application is launched for the first time, it will be matched based on the path specified by the user. If it matches, the fingerprint will be calculated at the client. From that point on, the rule will match based only on the fingerprint of the application.
Path only	When the application is launched, it will be matched based only on the path specified by the user.

6 Enter a note, if desired.

7 Click **OK** to save changes.

Managing Application Blocking client rules

Use this task to analyze Application Blocking client rules created automatically in adaptive mode or manually for a group of clients, then determine which if any client rules to move to an Application Blocking policy.

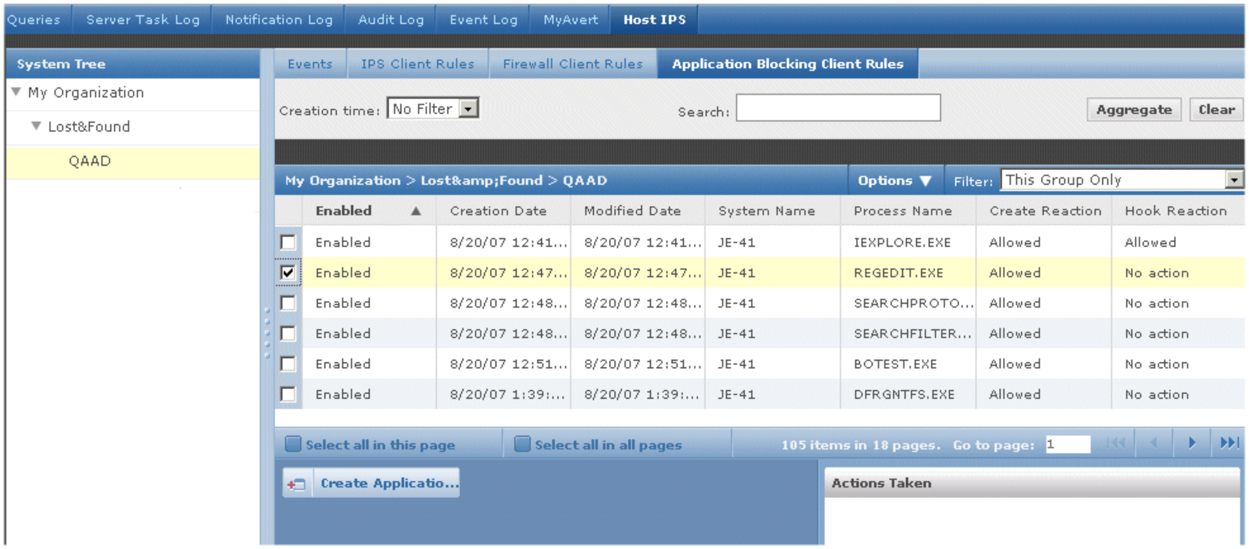
NOTE:

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

Task

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

1 Go to **Reporting | Host IPS | Application Blocking Client Rules**.



Creation time: No Filter

Search:

My Organization > Lost&amp;Found > QAAD

Filter: This Group Only

	Enabled	Creation Date	Modified Date	System Name	Process Name	Create Reaction	Hook Reaction
□	Enabled	8/20/07 12:41:...	8/20/07 12:41:...	JE-41	IEXPLORE.EXE	Allowed	Allowed
☑	Enabled	8/20/07 12:47:...	8/20/07 12:47:...	JE-41	REGEDIT.EXE	Allowed	No action
□	Enabled	8/20/07 12:48:...	8/20/07 12:48:...	JE-41	SEARCHPROTO...	Allowed	No action
□	Enabled	8/20/07 12:48:...	8/20/07 12:48:...	JE-41	SEARCHFILTER...	Allowed	No action
□	Enabled	8/20/07 12:51:...	8/20/07 12:51:...	JE-41	BOTEST.EXE	Allowed	No action
□	Enabled	8/20/07 1:39:...	8/20/07 1:39:...	JE-41	DFRGNTFS.EXE	Allowed	No action

105 items in 18 pages. Go to page: 1

Figure 29: Application Blocking 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 rules:

To...	**Do this...**
Sort by a column	Click the column header.
Filter for groups	From the Filter menu, select **This Group Only** or **This Group and All Subgroups.**
Filter for rules criteria	Select **Time creation** criteria; or in the **Search** text box type a process path, process name, or computer name. Click **Clear** to remove filter settings.
Aggregate rules	Click **Aggregate**, select the criteria on which to aggregate rules, then click **OK**. Click **Clear** to remove aggregation settings.

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

Configuring General Policies

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

Contents

Overview of General policies

The **Client UI** policy 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. Only the password functionality is used for clients on both Windows and non-Windows platforms.

The **Trusted Networks** policy lists IP addresses and networks 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.

The **Trusted Applications Rules** policy 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 and application blocking 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.

Working with Client UI policies

The Client UI policy determines which options are available to a Windows client computer protected with Host Intrusion Prevention. These include icon display settings, intrusion event reactions, and access for administrators and client users. For non-Windows clients, only the password feature is available.

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

User type	Functionality
Regular	The average user who has the Host Intrusion Prevention client installed on a desktop or laptop. The Client UI policy enables this user to: • View the Host Intrusion Prevention client icon in the system tray and launch the client user interface. • Get pop-up intrusion alerts or prevent them. • Create additional IPS, firewall, and application blocking rules.
Disconnected	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.
Administrator	An IT administrator for all computers who needs to perform special operations on a client computer, overriding any administrator-mandated policies. The Client UI policy enables this user to obtain a non-expiring administrator password to perform administrative tasks. Administrative tasks for both disconnected and administrator users include: • Enabling or disabling IPS, Firewall, and Application Blocking Options policies. • Creating additional IPS, Firewall, and Application Blocking rules if certain legitimate activity is blocked. 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.

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

- Configuring a Client UI policy
- Configuring Client UI passwords
- Configuring Client UI tray icon control
- Configuring Client UI troubleshooting

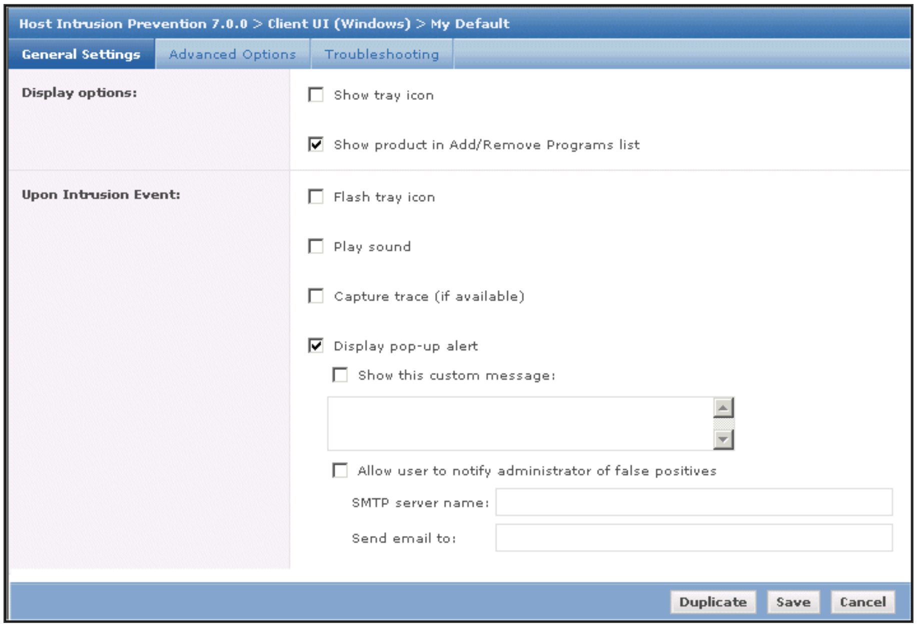
Configuring a Client UI policy

Use this task to determine what options are available to a Windows client computer. These include icon display settings, intrusion event reactions, and administrator and client user access. For non-Windows clients, only the password feature is available.

Task

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

1. Go to **Systems | 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.


Host Intrusion Prevention 7.0.0 > Client UI (Windows) > My Default
General Settings
Advanced Options
Troubleshooting
Duplicate
Save
Cancel

Display options:

□ Show tray icon

☑ Show product in Add/Remove Programs list

Upon Intrusion Event:

□ Flash tray icon

□ Play sound

□ Capture trace (if available)

☑ Display pop-up alert

□ Show this custom message:

□ Allow user to notify administrator of false positives

SMTP server name:

Send email to:

Figure 30: Client UI—General Settings tab

3. In the **Client UI** page, select a tab (General Options, Advanced Options, Troubleshooting Options) and make any needed changes.
4. Click **Save to save changes**.

Configuring Client UI passwords

The Client UI policy is where you create the password required to unlock the client UI if it appears on a Windows client or to 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 UI remains unlocked until it is closed. To reopen the client UI, reenter the administrator password.
- A time-based password, which has an expiration date and time. This password is automatically generated. In addition, you have the option of disabling this password by deselecting the checkbox and applying the policy. The client UI remains unlocked, even if closed, as long as the time-based password is valid.

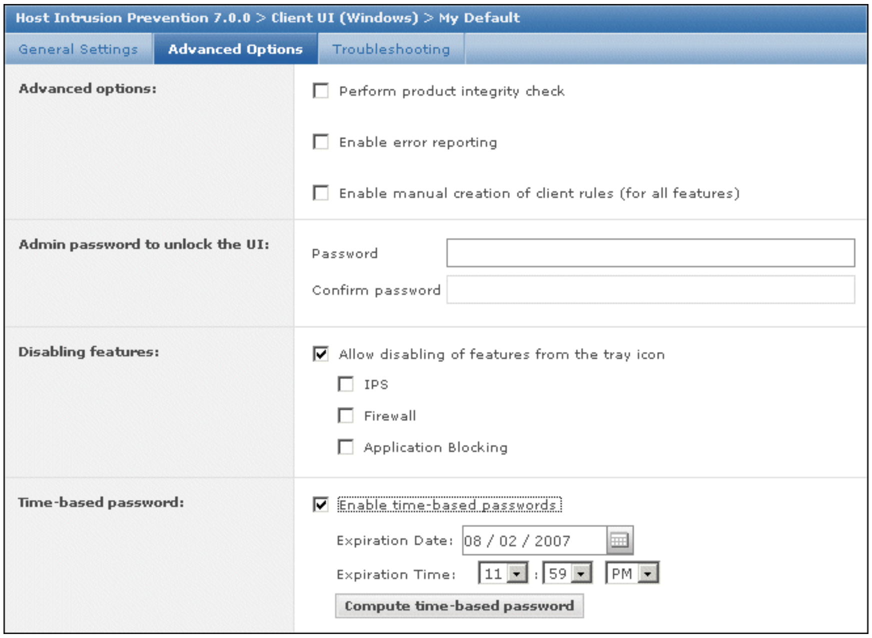
NOTE: Policies are NOT enforced on the client when the client UI is unlocked.

For details on using a password to unlock the Client UI, see *Unlocking the Windows client interface*.

Use this task to create the two types of passwords.

Task

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


Host Intrusion Prevention 7.0.0 > Client UI (Windows) > My Default
General Settings
Advanced Options
Troubleshooting
Compute time-based password

Advanced options:
- □ Perform product integrity check
- □ Enable error reporting
- □ Enable manual creation of client rules (for all features)

Admin password to unlock the UI:
- Password
- Confirm password

Disabling features:
- ☑ Allow disabling of features from the tray icon
  - □ IPS
  - □ Firewall
  - □ Application Blocking

Time-based password:
- ☑ Enable time-based passwords
- Expiration Date: 08 / 02 / 2007
- Expiration Time: 11 : 59 PM

Figure 31: Client UI—Advanced Options tab

2 Determine the type of password you want to create:

For this type of password...	Do this...
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, and then click **Compute time-based password**. The password with its expiration date and time appear in a dialog box.

3 Click **Save** to make the password valid.

Configuring Client UI tray icon control

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

After the policy is applied to the client, the Host Intrusion Prevention icon appears in the system tray, and its menu expands to include options that disable and restore features. The disabled feature remains disabled until restored by the menu command or a new policy is applied to the client. Note the following:

- Disabling IPS disables both host IPS and network IPS protection.
- Disabling App Blocking disables both Application creation blocking and Application hooking blocking protection.

- If the Client UI is unlocked, the menu commands have no effect.

For details on using the tray icon menu, see the section on working with the Host IPS client.

Use this task to configure the tray icon control.

Task

1 Click the **General Settings** tab of the Client UI policy and select **Show tray icon**.

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

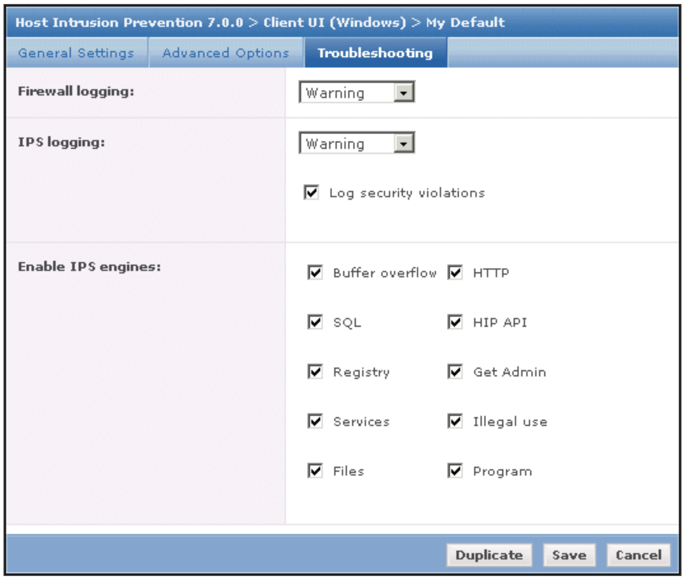
Configuring Client UI troubleshooting

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.

Use this task to apply troubleshooting controls without going directly to a client.

Task

1 Click the **Troubleshooting** tab in the Client UI policy.


Host Intrusion Prevention 7.0.0 > Client UI (Windows) > My Default
General Settings
Advanced Options
Troubleshooting
Duplicate
Save
Cancel

Firewall logging: Warning

IPS logging: Warning

☑ Log security violations

Enable IPS engines:

☑ Buffer overflow ☑ HTTP
☑ SQL ☑ HIP API
☑ Registry ☑ Get Admin
☑ Services ☑ Illegal use
☑ Files ☑ Program

Figure 32: Client UI—Troubleshooting tab

2 Select the policy settings you want to apply:

To	Do this...
Turn on firewall logging	Select from the list the message type to trigger logging of Firewall events. **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. The path of the log file on Windows clients is: C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention\FireSvc.log; on Windows Vista: C:\Program Data\McAfee\Host Intrusion Prevention\FireSvc.log.

To	Do this...
Turn on IPS logging	Select from the list the message type to trigger logging of IPS events. **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. The path of the log file on Windows clients is: C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention\HipShield.log; on Windows Vista: C:\Program Data\McAfee\Host Intrusion Prevention\HipShield.log
Include security violations in the IPS log	Select **Log security violations**.
Turn engines on and off	Deselect the checkbox to disable, select a checkbox to enable an engine

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

Working with Trusted Network policies

The Trusted Networks policy enables you to maintain a list of network addresses and subnets, which you can tag as trusted for clients on Windows.

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.

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

▸ Configuring a Trusted Networks policy

Configuring a Trusted Networks policy

Trusted Networks enable you to maintain a list of network addresses and subnets that you can tag as trusted for clients on Windows. You can:

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

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

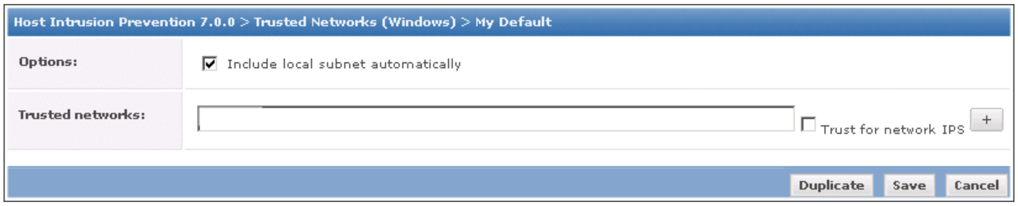
Use this task to set trusted network options and list trusted networks.

Task

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

1 Go to **Systems | 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.



Host Intrusion Prevention 7.0.0 > Trusted Networks (Windows) > My Default

Options: ☑ Include local subnet automatically

Trusted networks: □ Trust for network IPS

Figure 33: Trusted Networks

3 Do any of the following:

Select...	To do this...
Include Local Subnet Automatically	Automatically treat all users on the same subnet as trusted, even those not in the list.
Trusted Network	Add a trusted network address to the list.
Trust for network IPS	Mark the network as trusted for network IPS signatures.
Add/Remove button	Remove or add a trusted network address.

4 Click **Save** to save changes.

Working with Trusted Applications policies

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

You can assign more than one policy instance of this policy, 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; you can edit, rename, duplicate, delete, and export custom policies you create.

On the **Policy Catalog** policy list page, click **New Policy** to create a new custom policy; click **Duplicate** under **Actions** to create a new custom policy based on an existing policy.

Change the policy's assignment on the **Policy Assignment** page. For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

Tasks

- Configuring a Trusted Applications policy
- Creating and editing Trusted Application rules

Configuring a Trusted Applications policy

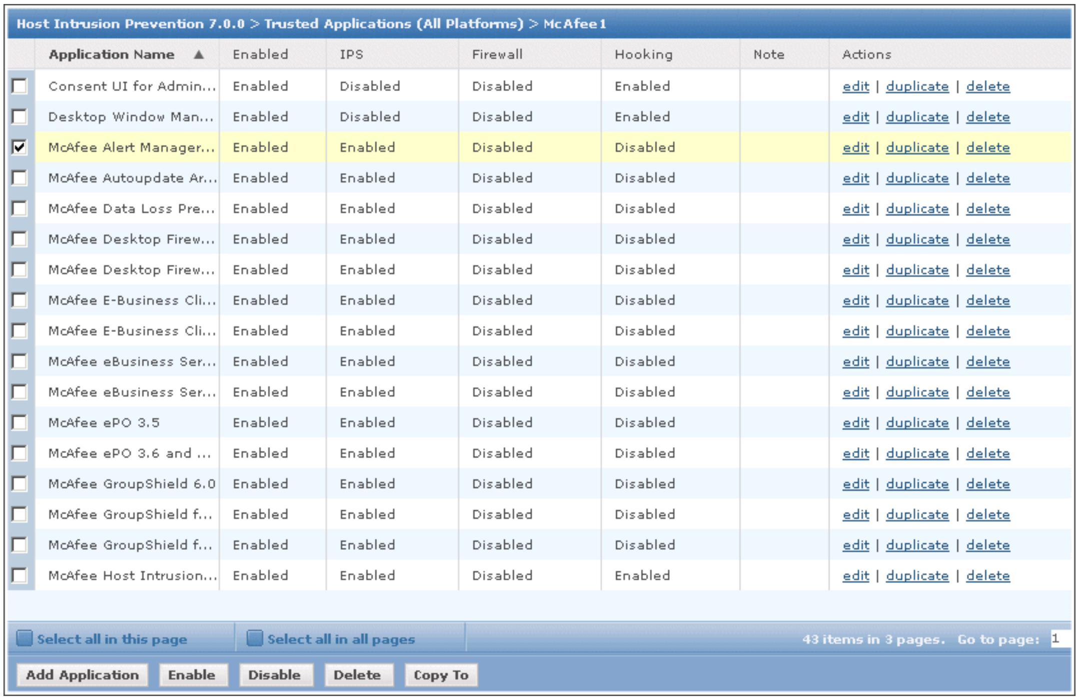
Use this task to list applications deemed safe in a particular environment for a Trusted Applications policy.

Task

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

1 Go to **Systems | 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.



Host Intrusion Prevention 7.0.0 > Trusted Applications (All Platforms) > McAfee1

	Application Name ▲	Enabled	IPS	Firewall	Hooking	Note	Actions
□	Consent UI for Admin...	Enabled	Disabled	Disabled	Enabled		edit | duplicate | delete
□	Desktop Window Man...	Enabled	Disabled	Disabled	Enabled		edit | duplicate | delete
☑	McAfee Alert Manager...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee Autoupdate Ar...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee Data Loss Pre...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee Desktop Firew...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee Desktop Firew...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee E-Business Cli...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee E-Business Cli...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee eBusiness Ser...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee eBusiness Ser...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee ePO 3.5	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee ePO 3.6 and ...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee GroupShield 6.0	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee GroupShield f...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee GroupShield f...	Enabled	Enabled	Disabled	Disabled		edit | duplicate | delete
□	McAfee Host Intrusion...	Enabled	Enabled	Disabled	Enabled		edit | duplicate | delete

43 items in 3 pages. Go to page: 1

Figure 34: Trusted Applications list

3 Do any of the following:

To...	Do this...
Add an application	Click **Add Application**. See Creating and editing Trusted Application rules for details.

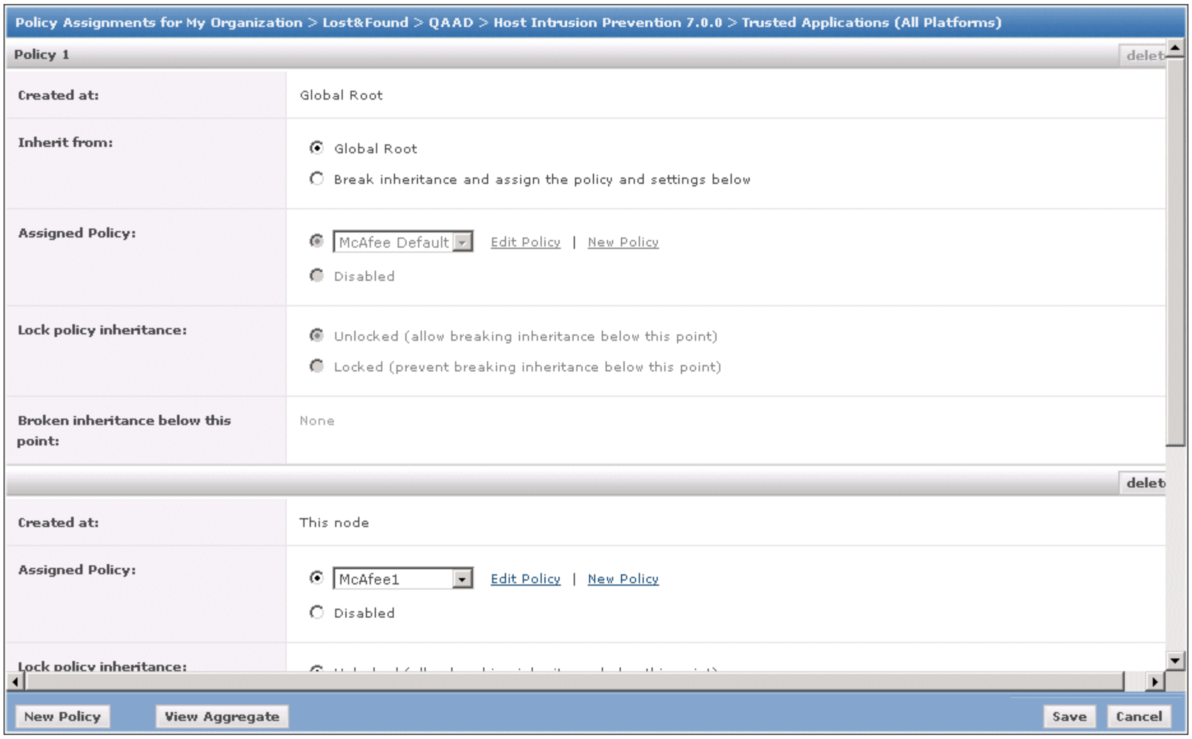
To...	Do this...
Perform an action on one or more applications at the same time	Select them and click: **Enable** to enable a disabled application. **Disable** to disable an enabled application. **Delete**to delete applications. **Copy to** to copy applications to another policy. You are prompted to 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.

5 To assign more than one instance of the Trusted Applications policy do either of the following:

- For a group, go to **Systems | System Tree**, select a group, and then on the **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 **More Actions | Modify Policies on a Single System.**

6 On the **Policy Assignment** page, click **New Policy Instance** to assign the additional policy instance, Select **Disabled** to disable the additional policy instance.



Policy Assignments for My Organization > Lost&Found > QAAD > Host Intrusion Prevention 7.0.0 > Trusted Applications (All Platforms)

Policy 1

Created at: Global Root

Inherit from:
● Global Root
○ Break inheritance and assign the policy and settings below

Assigned Policy:
● McAfee Default
○ Disabled

Lock policy inheritance:
● Unlocked (allow breaking inheritance below this point)
○ Locked (prevent breaking inheritance below this point)

Broken inheritance below this point: None

Created at: This node

Assigned Policy:
● McAfee1
○ Disabled

Lock policy inheritance:

Figure 35: Assigning multiple instances of the policy

7 Click **Save** to apply all changes.

Creating and editing Trusted Application rules

Use this task to create a new trusted application or edit an existing one from the **Trusted Applications** policy page.

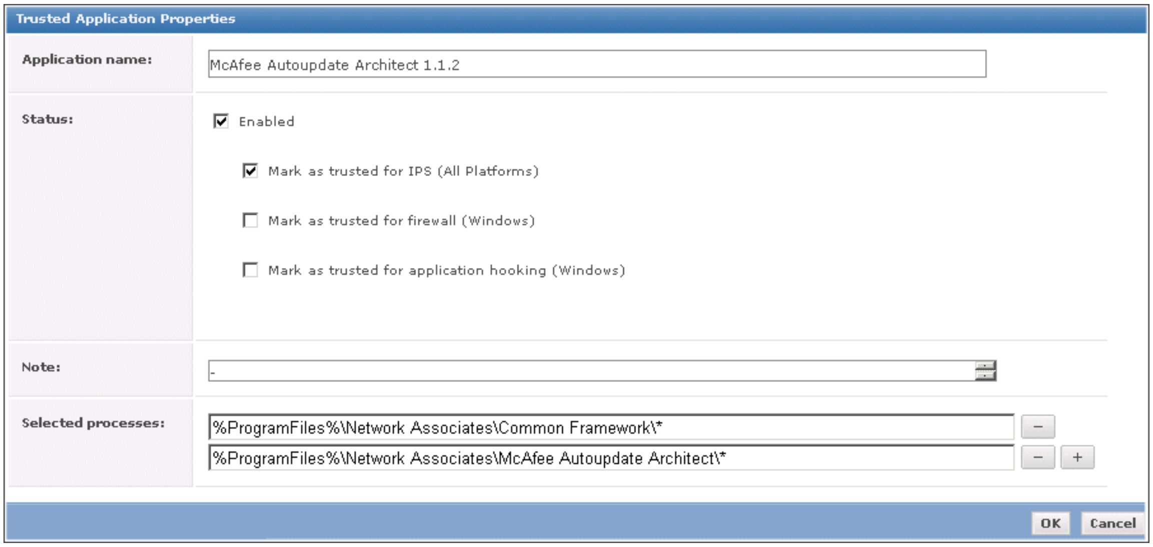
Task

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

1 On the **Trusted Applications** policy page, click **Add Rule** 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 event-based exceptions and trusted applications*.

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



Trusted Application Properties

Application name: McAfee Autoupdate Architect 1.1.2

Status:
☑ Enabled
☑ Mark as trusted for IPS (All Platforms)
□ Mark as trusted for firewall (Windows)
□ Mark as trusted for application hooking (Windows)

Note: -

Selected processes:
%ProgramFiles%\Network Associates\Common Framework*
%ProgramFiles%\Network Associates\McAfee Autoupdate Architect*

Figure 36: Trusted Application

3 Type or edit the processes for the trusted application.

4 Click **OK** to save 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. This section describes the basic features of each client version.

- 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 interface. To display the client console, double-click the client icon in the system tray, or, on the **Start** menu, select **Programs | McAfee | Host Intrusion Prevention**.

When the client console first appears, most options are locked; you can only view current settings and manually create client rules (if the Client UI policy has manual creation of client rules enabled). For complete control of all settings in the console, unlock the interface with a password. For details on these Client UI policy settings, see *Configuring the Client UI policy*.

System tray icon

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

Icon	Host Intrusion Prevention status
🛡	Working properly
❗	A potential attack was detected
🛡🚫	Turned off, or not working properly

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

Click...	To do this...
Configure	Open the Host Intrusion Prevention client console.

Click...	To do this...
About...	Open the **About Host Intrusion Prevention** dialog box, which displays the version number and other product information.

If the **Allow disabling of features from the tray icon** option is applied to the client, some or all of these additional commands are available:

Click...	To do this...
Restore Settings	Enable all disabled features. Available only if one or more features have been disabled.
Disable All	Disable IPS, Firewall, Application Blocking features. Available only if all the features are enabled.
Disable IPS	Disable the IPS feature. This includes both Host IPS and Network IPS functionality. Available only if the feature is enabled.
Disable Firewall	Disable the Firewall feature. Available only if the feature is enabled.
Disable App Blocking	Disable the Application Blocking feature. This includes both Application Creation Blocking and Application Hooking Blocking. Available only if the feature is enabled.

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:

- Double-click the icon in the system tray.
- Right-click the icon and select **Configure.**
- On the **Start** menu select **Programs | McAfee | Host Intrusion Prevention.**

The console lets you configure and view information about Host Intrusion Prevention features. It contains several tabs, which correspond to a specific Host Intrusion Prevention feature.

Unlocking the Windows client interface

An administrator remotely managing Host Intrusion Prevention using ePolicy Orchestrator can password protect the interface to prevent accidental changes. With a time-based password, an administrator or user can temporarily unlock the interface and make changes.

Task

1 Obtain a password from the Host Intrusion Prevention administrator.

NOTE: For details on creating a password, see *Configuring Client UI passwords*.

2 On the **Task** menu, select **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.

Task

1. On the client console **Edit** menu, click **Options**.
2. In the **Host Intrusion Prevention Options** dialog box, select and deselect options as needed.

Select...	For this...
Display pop-up alert	An alert appears when an attack occurs.
Play sound	A sound plays when an attack occurs.
Flash tray icon	The icon toggles between regular status and attack status when an attack occurs.
Create Sniffer Capture if available	A Sniffer Capture column is added to the Activity Log, indicating that intrusion packet data has been captured. Save this data to a McAfee Sniffer.cap file for further analysis.
Show tray icon	The Host Intrusion Prevention icon appears in the system tray.
Error Reporting	The software error reporting utility is enabled to submit errors to McAfee.

Client error reporting

Host Intrusion Prevention includes an error reporting utility that tracks and logs software failures. When enabled, it prompts the user to forward detected problem data to McAfee technical support, where it can be used to open a support case, if appropriate.

NOTE: To use the error reporting utility, a computer must have Internet access and a web browser that is Java Script enabled.

If McAfee Alert Manager is installed on the network where a computer failed, it informs the network administrator that a problem was detected. The network administrator can guide the user on how to handle the problem.

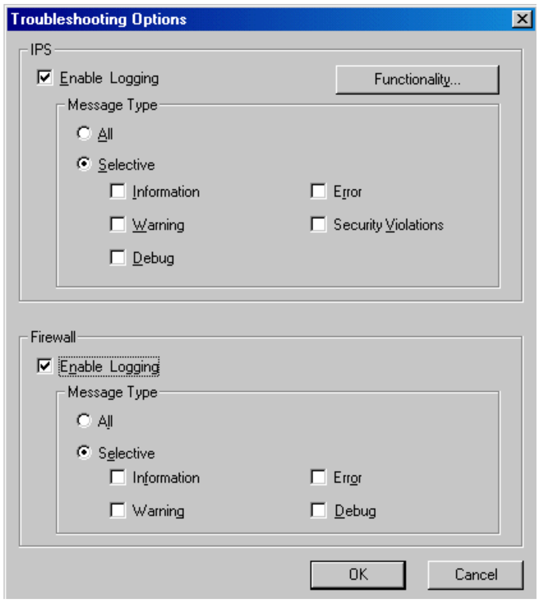
When the utility detects a failure, the user selects an option:

- **Submit Data —** Thisconnects to the McAfee Technical Support website and submits the data.
- **Ignore Error —** No connection is made.

When submitting data to the McAfee Technical Support website, the user may be asked for additional information. If the problem has a known cause, the user may be directed to a web page that provides information about the problem and how to deal with it.

Troubleshooting the Windows client

Host Intrusion Prevention includes a **Troubleshooting** option on the Help menu, which is available when the interface is unlocked. Options include enabling IPS and firewall logging and disabling system engines.



Troubleshooting Options

IPS

☑ Enable Logging

Message Type
○ All
● Selective
□ Information
□ Error
□ Warning
□ Security Violations
□ Debug

Firewall

☑ Enable Logging

Message Type
○ All
● Selective
□ Information
□ Error
□ Warning
□ Debug

Figure 37: Troubleshooting Options

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 available from the McAfee.com product download site. Refer to the documentation that accompanies the utility for directions on usage, including details on parameters and security

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. Select the IPS **Enable Logging** checkbox.
2. Select the message type (**All** or a combination of **Information**, **Warning**, **Debug**, **Error**, **Security Violations).** At a minimum, you must select **Error** and **Security Violations**.
3. Click **OK**. The information is written to C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention\HipShield.log; on Windows Vista: C:\Program Data\McAfee\Host Intrusion Prevention\HipShield.log. After the file reaches 100 MB, a new file is created.

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 to enable Firewall logging.

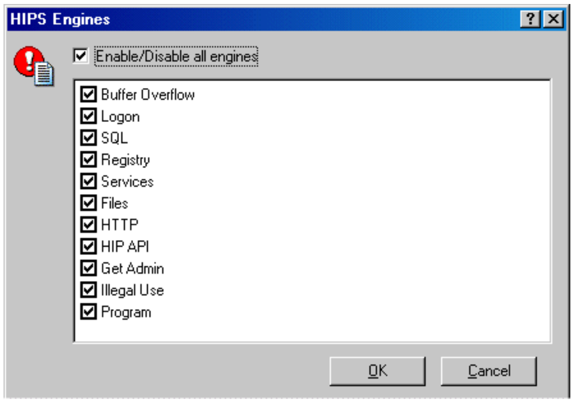
Task

1. Select the Firewall **Enable Logging** checkbox.
2. Select the message type (All or a combination of **Information**, **Warning**, **Error**, **Debug**).
3. Click **OK**. The information is written to C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention\FireSvc.log; on Windows Vista: C:\Program Data\McAfee\Host Intrusion Prevention\FireSvc.log folder. After the file reaches 100 MB, a new file is created.

Disabling Host IPS engines

As part of troubleshooting, you can also disable engines that protect a client. McAfee recommends that only administrators communicating with McAfee support use this troubleshooting procedure.

For access, click **Functionality** in the **Troubleshooting Options** dialog box. In the **HIPS Engines** dialog box that appears, disable one or more client system engines by deselecting the checkbox next to the engine. After the problem has been resolved, and to return to a normal operating environment, be sure all engines are selected.



☑ Enable/Disable all engines

☑ Buffer Overflow
☑ Logon
☑ SQL
☑ Registry
☑ Services
☑ Files
☑ HTTP
☑ HIP API
☑ Get Admin
☑ Illegal Use
☑ Program

Figure 38: HIPS Engines

NOTE:

SQL and HTTP appear in the list only if the client is running a server operating system.

Windows client alerts

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

Responding to Intrusion alerts

If you enable IPS protection and the **Display pop-up alert** option, this alert automatically appears when Host Intrusion Prevention detects a potential attack. If the client is in adaptive mode, this alert appears only if the **Allow Client Rules** option is disabled for the signature that caused the event to occur.

The **Intrusion Information** tab displays details about the attack that generated the alert, including a description of the attack, the user/client computer where the attack occurred, the process involved in the attack, and the time and date when Host Intrusion Prevention intercepted it. In addition, a generic administrator-specified message can appear.

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

Task

1 On the **Application Information** tab of the alert dialog box, do one of the following:
   - Click **Deny** to block this and all similar traffic.
   - Click **Allow** to permit this and all similar traffic through the firewall
2 Optional: On the **Connection Information** tab, select options for the new firewall rule:

Select...	To do this...
Create a firewall application rule for all ports and services	Create a rule to allow or block an application’s traffic over any port or service. If you do not select this option, the new firewall rule allows or blocks only specific ports: • If the intercepted traffic uses a port lower than 1024, the new rule allows or blocks only that specific port. • If the traffic uses port 1024 or higher, the new rule allows or blocks the range of ports from 1024 to 65535.
Remove this rule when the application terminates	Create a temporary allow or block rule that is deleted when the application is closed. If you do not select this options, the new firewall rule is created as a permanent client rule.

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

Responding to Application Blocking alerts

When application creation or application hooking is enabled in the **Application Blocking Options** policy, Host Intrusion Prevention monitors application activities and allows or blocks them based on the rules in the **Application Blocking Rules** policy.

If you enabled **learn** mode for either creation blocking or hooking blocking, Host Intrusion Prevention displays an **Application Creation Alert** or **Application Hook Alert** whenever it detects an unknown application trying to run or bind to another program.

The **Application Information** tab displays information about the application attempting to run (creation) or to hook (hook) to another process, including application name, path, and version.

Use this dialog box to select an action:

- Click **Allow** to let the application complete its action:
- For an **Application Creation Alert**, clicking **Allow** lets the application run.
- For an **Application Hook Alert**, clicking **Allow** lets the application bind itself to another program.
- Click **Deny** to block the application:
- For an **Application Creation Alert**, clicking **Deny** prevents the application from running.
- For an **Application Hook Alert**, clicking **Deny** blocks the application from binding itself to another program.

When you click **Allow** or **Deny**, Host Intrusion Prevention creates a new application rule based on your choice. After collecting client properties, this rule is added to the **Application Client Rule** tab of the **Application Rules** policy. The application is then allowed or blocked automatically.

Responding to Quarantine alerts

If you enable Quarantine mode and include the IP address of the client for quarantine enforcement in the **Quarantine Options** policy, a quarantine alert appears in the following situations:

- Changing the client computer’s IP address
- Disconnecting and then reconnecting the client Ethernet connection
- Restarting the client

Responding to Spoof Detected alerts

If you enable the IPS feature, this alert automatically appears if Host Intrusion Prevention detects an application on your computer sending out spoofed network traffic. This means that the application is trying to make it seem like traffic from your computer actually comes from a different computer. It does this by changing the IP address in the outgoing packets. Spoofing is always suspicious activity. If you see this dialog box, immediately investigate the application that sent the spoofed traffic.

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 on two tabs — the **Application Information** tab, and the **Connection Information** tab.

The **Application Information** tab displays:

- The IP address that the traffic pretends to come from.
- Information about the program that generated the spoofed traffic.
- The time and date when Host Intrusion Prevention intercepted the traffic.

The **Connection Information** tab provides further networking information. In particular, **Local Address** shows the IP address that the application is pretending to have, while **Remote Address** shows your actual IP address.

When Host Intrusion Prevention detects spoofed network traffic, it tries to block both the traffic and the application that generated it. It does this by adding a new rule to the end of the firewall rule list. This **Block spoofing attacker** rule specifically blocks all traffic created by the suspicious application, unless another rule in the rule list overrides it.

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 the section on Configuring IPS policies.

IPS Policy tab displays exception rules relevant to the client and provides summary and detailed information for each rule.

This column...	Displays
Exception	The name of the exception.
Signature	The name of the signature against which the exception is created.
Application	The application that this rule applies to, including the program name and executable file name.

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. Use this task to customize IPS options.

Task

1 In the Host IPS client console, click the **IPS Policy** tab.

2 Select or deselect an option as needed.

Select...	To do this...
Enable Host IPS	Enable host intrusion prevention protection.

Select...	To do this...
Enable Network IPS	Enable network intrusion prevention protection.
Enable Adaptive Mode	Enable adaptive mode to automatically create exceptions to intrusion prevention signatures.
Automatically block attackers	Block network intrusion attacks automatically for a set period of time. Select **Until removed** to block an attack until it is removed, or select **for X min**. to block an attack for set a number of minutes, with the default at 30.

Editing IPS Policy exception rules

Use this task to view and edit IPS exception rules.

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:

To...	Do this...
View the details of a rule or edit a rule	Double-click a rule, or select a rule and click **Properties**. The **Exception Rule** dialog box appears displaying rule information that can be edited.
Make a rule active/inactive	Select or clear the Exception rule is Active checkbox in the **Exception Rule** dialog box. You can also select or clear the checkbox next to the rule icon in the list.
Delete a rule	Select a rule and click **Remove**.

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 more details on firewall policies, see the section on 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.

This column...	Displays...
Description	The purpose of this rule or rule group.
Protocol	Which protocol(s) the rule applies to (TCP, UDP, ICMP).Whether the rule permits traffic, or blocks it:⊕ Permits traffic.⊖ Blocks traffic.Whether the rule applies to incoming traffic, outgoing traffic, or both:⇦ Incoming traffic. ⇨ Outgoing traffic.⇔ Both directions.

This column...	Displays...
❗	Whether Host Intrusion Prevention treats traffic that matches this rule as an intrusion (an attack) on your system.
🕒	Whether this rule only applies at specific times.
Service (L)	Services on your computer where this rule applies. When possible, this column shows associated port numbers. You can define an individual service, a range of services, a list of specific services, or specify all (**Any**) or no services (**N/A**).
Service (R)	Services where this rule applies on the computer you are sending traffic to, or receiving traffic from. When possible, this column shows associated port numbers. You can define an individual service, a range of services, a list of specific services, or specify all (**Any**) or no services (**N/A**).
Address	The IP address, subnet, domain, or other specific identifier that this rule applies to.
Application	The application that this rule applies to, including the program name and executable file name.

Customizing Firewall Policy options

Use this task to customize Firewall options.

Task

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

Select...	To do this...
Enable Firewall	Enable firewall policy protection.
Learn Mode Incoming	Enable learn mode for incoming traffic.
Learn Mode Outgoing	Enable learn mode for outgoing traffic
Adaptive Mode	Enable adaptive mode.
Trusted...	View trusted networks.

Creating and editing Firewall rules

The Firewall rules list displays client rules that you can view and edit. For details on working with firewall rules, see the section *Configuring Firewall Policies*.

NOTE: You cannot add firewall connection-aware groups from the client. This functionality is available only in the Firewall Rules policy managed at the ePolicy Orchestrator server.

About the Application Policy tab

Use the **Application Policy** tab to configure the Application Blocking feature. You can specify whether an application can run (known as application creation), or whether it can bind itself to other programs (known as application hooking), whether to enable learn mode for application creation and hooking, and configure client application rules. For more details on application blocking, see Chapter 5, Working with Application Blocking Policies.

The application rules list displays rules relevant to the client and provides summary and detailed information for each rule.

This column...	Displays...
Description	The purpose of this rule.
Create	⊕ Permits application to run.⊖ Blocks application from running.
Hook	⊕ Permits application to hook other programs.⊖ Blocks application from hooking other programs.
Application	The file name and path of the application that this rule applies to.

Customizing Application Policy options

Use this task to customize Application Blocking options.

Task

1. Click the **Application Policy** tab.
2. Select or deselect an option as needed.

Select...	To do this...
Enable Application Creation Blocking	Enable application creation blocking. The Enable Learn Mode Application Creation options is enabled.
Enable Application Hooking Blocking	Enable application hooking blocking.The Enable Learn Mode Application Hooking options is enabled
Enable Learn Mode Application Creation	Enable learn mode for application creation, where the user is prompted to allow or block application creation.
Enable Learn Mode Application Hooking	Enable learn mode for application hooking, where the user is prompted to allow or block application hooking.

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.

Column	What it shows
Source	• The IP address that Host Intrusion Prevention is blocking.
Blocked Reason	• An explanation of why Host Intrusion Prevention is blocking this address. 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 **Treat rule match as intrusion** option, this column lists the name of the relevant firewall rule.If you added this address manually, this column lists only the IP address that you blocked.

Column	What it shows
Time	• The time and date when you added this address to the blocked addresses list.
Time Remaining	• How long Host Intrusion Prevention will continue to block this address. 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 the list.If you specified that you wanted this address blocked until you manually removed it from the list, this column displays **Until removed**.

Editing the Blocked Hosts list

Use this task to edit the list of blocked addresses. Edits include adding, removing, editing blocked hosts, and viewing blocked host details.

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**.
3. Determine how long to block the IP address:
   - Select **Until Removed** to keep the host blocked until deleted.
   - Select **For** and type the number of minutes, up to 60, to keep the host blocked for a fixed period of time.
4. Click **OK**.

   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:

To...	Do this...
View the details of or edit a blocked host	Double-click a host entry, or select a host and click **Properties**. The **Blocked Host** dialog box displays information that can be edited.
Delete a blocked host	Select a host and click **Remove**.

About the Application Protection tab

The **Application Protection** tab displays a list of applications protected on the client. This is a view-only list populated by administrative policy and a client-specific application list created heuristically.

This list shows all monitored processes on the client.

Column	What it shows
Process	The application process.
PID	The process ID, which is the key for the cache lookup of a process.
Process Full Path	The full path name of the application process.

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.

Column	What it shows
Time	The date and time of the Host Intrusion Prevention action.
Event	The feature that performed the action. • **Traffic** indicates a firewall action. • **Application** indicates an application blocking action. • **Intrusion** indicates an IPS action. • **System** indicates an event relating to the software"s internal components. • **Service** indicates an event relating to the software"s service or drivers.
Source	The remote address that this communication was either sent to, or sent from.
Intrusion Data NOTE: This column only appears if you select **Create Sniffer Capture...** in the **McAfee Host Intrusion Prevention Options** dialog box.	An icon indicating that Host Intrusion Prevention saved the packet data associated with this attack. (This icon only appears for IPS log entries.) You can export the packet data associated with this log entry. Right-click the log entry to save the data to a Sniffer file.
Application	The program that caused the action.
Message	A description of the action, with as much detail as possible.

You can clear the list either by deleting the log contents or saving it to a .txt file.

To...	Do this...
Permanently delete the contents of the log	Click **Clear**.
Save the contents of the log and delete the list from the tab	Click **Save**. In the **Save Log File To** dialog box that appears, name and save the .txt file.

Customizing Activity Log options

Use this task to customise activity log opions.

Task

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

Select...	To do this...
Traffic Logging - Log All Blocked	Log all blocked firewall traffic.
Traffic Logging - Log All Allowed	Log all allowed firewall traffic.
Filter Options - Traffic	Filter the data to display blocked and allowed firewall traffic.

Select...	To do this...
Filter Options - Applications	Filter the data to display events caused by applications.
Filter Options - Intrusions	Filter the data to display intrusions.

NOTE: You can enable and disable logging for the firewall traffic, but not for the IPS or application blocking features. However, you can choose to hide these events in the log by filtering them out.

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.

With this policy...	These options are available...
HIP 7.0 GENERAL:	
Client UI	None except **admin** 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**.**
HIP 7.0 IPS:	
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.
IPS Events	All
IPS Client Rules	All
Search IPS Exception Rules	All
HIP7.0 FIREWALL	None
HIP 7.0 APPLICATION BLOCKING	None

Solaris client issues

After the Solaris client is installed and started, it protects its host. However, you may need to troubleshoot installation or operation issues.

Client installation issues

If a problem was caused while installing or uninstalling the client, there are several things to investigate. These can include ensuring that all required files were installed in the correct directory, uninstalling and then reinstalling the client, and checking process logs.

Client operations issues

The Solaris client has no user interface to troubleshoot operation issues. It does offer a command-line troubleshooting tool, *hipts,* located in the /opt/McAfee/hip directory. To use this tool, you must provide a Host Intrusion Prevention client password. Use the default password that ships with the client (abcde12345), or send a Client UI policy to the client with either an administrator's password or a time-based password set with the policy, and use this password.

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:

File/Directory Name	Description
HipClient; HipClient-bin	Solaris client
HipClientPolicy.xml	Policy rules
hipts; hipts-bin	Troubleshooting tool
*.so	Host Intrusion Prevention and ePO agent shared object modules
log directory	Contains debug and error log files

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.

Troubleshooting the Solaris 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:

Run this command...	**To do this...**
hipts status	Obtain the current status of the client indicating which type of logging is enabled, and which engines are running.
hipts logging on	Turn on logging of specific messages types.
hipts logging off	Turn off logging of all message types. Logging is off by default.
hipts message <message name>:on	Display the message type indicated when logging is set to "on." Messages include: • error • warning • debug • info • violations
hipts message <message name>:off	Hide the message type indicated when logging is set to "on." Message error is off by default.
hipts message all:on	Display all message types when logging is set to "on."
hipts message all:off	Hide all message types when logging is set to "on."
hipts engines <engine name>:on	Turn on the engine indicated. Engine is on by default. Engines include: • MISC • FILES • GUID • MMAP • BO • ENV • HTTP
hipts engines <engine name>:off	Turn off the engine indicated.
hipts engines all:on	Turn on all engines.
hipts engines all:off	Turn off all engines.

TIP: In addition to using the troubleshooting tool, consult the HIPShield.log and HIPClient.log files in the /opt/McAfee/hip/log directory to verify operations or track issues.

Stopping the Solaris client

You may 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.
- Run the command: hipts engines MISC:off.

2. Run the command: /etc/rc2.d/S99hip stop.

Restarting the Solaris client

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

Task

1. To restart a client, run the command: /etc/rc2.d/S99hip restart.
2. Enable IPS protection. Use one of these procedures, depending on which you used to stop the client:
   - Set **IPS Options** to **On** in the ePO console and apply the policy to the client.
   - Run the command: hipts engines MISC:on.

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 leverages the native SELinux protection mechanism, translating IPS policies into SELinux rules and SELinux events back to IPS events, and provides easy management from the ePO console.

Policy enforcement with the Linux client

Not all policies that protect a Windows client are available for the Linux client. In brief, Host Intrusion Prevention protects the host server from harmful attacks but does not offer network intrusion protection, including buffer overflow. The policies that are valid are listed here.

With this policy...	**These options are available...**
HIP 7.0 GENERAL:	
Client UI	None except **admin** 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**.**
HIP 7.0 IPS:	
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.
IPS Events	All

With this policy...	These options are available...
IPS Client Rules	All
Search IPS Exception Rules	All
HIP 7.0 FIREWALL	None
HIP 7.0 APPLICATION BLOCKING	None

Notes about the Linux client

- If you have an existing SELinux policy in place or are using default protection settings, installing a Linux client replaces the policy with a default McAfee Host Intrusion Prevention policy. Uninstalling the Linux client restores the previous SELinux policy.
- The Linux client requires that SELinux be installed and enabled (set to enforce or permissive). If it is installed but disabled, enable it, set it to targeted policy, and restart the computer before installing the Linux client.
- Linux controls file attribute changes with a single SELinux permission (file:setattr). It does not have individual control of chdir or symlink, control of changing directory, or control of creating a symbolic link.
- SELinux uses a mandatory access control mechanism implemented in the Linux kernel with the Linux Security Modules (LSM) framework. This framework checks for allowed operations after standard Linux discretionary access controls are checked. Because the Linux client uses LSM, any other application that uses LSM will not work unless stacking is implemented.

Linux client issues

After the Linux client is installed and started, it protects its host. However, you may need to troubleshoot installation or operation issues.

Linux client installation issues

If a problem was caused while installing or uninstalling the client, there are several things to investigate. These can include ensuring that all required files were installed in the correct directory, uninstalling and then reinstalling the client, and checking process logs.

Linux client operation issues

The client might be installed correctly, but you might encounter problems with the operation of the client. You can check whether the client is running, and stop and restart the client.

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:

File Name	Description
HipClient; HipClient-bin	Linux client
HipClientPolicy.xml	Policy rules
hipts; hipts-bin	Troubleshooting tool

File Name	Description
*.so	Host Intrusion Prevention and ePO agent shared object modules
log directory	Contains debug and error log files

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
```

Troubleshooting the Linux 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 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:

Run this command...	To do this...
hipts status	Obtain the current status of the client indicating which type of logging is enabled, and which engines are running
hipts logging on	Turn on logging of specific messages types.
hipts logging off	Turn off logging of all message types. Logging is off by default.
hipts message <message name>:on	Display the message type indicated when logging is set to “on.” Messages include: • error • warning • debug • info • violations
hipts message <message name>:off	Hide the message type indicated when logging is set to “on.” Message error is off by default.
hipts message all:on	Display all message types when logging is set to “on.”
hipts message all:off	Hide all message types when logging is set to “on.”
hipts engines <engine name>:on	Turn on the engine indicated. Engine is on by default. Engines include: • MISC • FILES

Run this command...	To do this...
hipts engines <engine name>:off	Turn off the engine indicated.
hipts engines all:on	Turn on all engines.
hipts engines all:off	Turn off all engines.

TIP: In addition to using the troubleshooting tool, consult the HIPShield.log and HIPClient.log files in the McAfee/hip/log directory to verify operations or track issues.

Stopping the Linux client

You may 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 may 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`.

Index