McAfee® Host Intrusion Prevention delivers a manageable and scalable intrusion prevention solution for workstations, notebooks, and critical servers, including web and database servers. It ensures availability, integrity and confidentiality of business processes by proactively blocking zero-day and known attacks with patented, award-winning technology.

Manageability and scalability

ePolicy Orchestrator manages Host Intrusion Prevention, delivering and enforcing its policies along with other critical security solutions such as AV protection. This approach provides a single management solution that allows for mass deployment — up to 100,000 agents — in multiple languages across an entire enterprise for true global coverage.

Security

McAfee Host Intrusion Prevention combines behavioral rules, 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.

Policy feature

Host Intrusion Prevention contains four policy features:
- General
- IPS
- Firewall
- Blocked Applications

(See the next two pages for details.)

Quick access links

A quick access bar provides links to a feature’s frequently used policy tabs and rules.

Policy name

The name of a preset or custom policy. Click the link to view policy details.

Policy editing

Click Edit to select another policy or create a new policy.

Multiple-instance policy

This type of policy allows you to apply related policy instances to create a profile of settings. Only IPS Rules (IPS feature) and Trusted Applications (General feature) policies have this function. They appear on a brown background to distinguish them from the single-instance policies. To add an additional policy instance, click Assign additional policy.

mcafee.com
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: General, IPS, Firewall, and Application Blocking.

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 or the global administrator. Deleting a policy can be done only in the Policy Catalog.

General policies
The General feature contains four policies that apply to IPS and firewall settings. These policies override settings in individual IPS and firewall policies.

1. **Enforce Policies.** Turns administrative policy enforcement on or off. Preset policies:
   - Yes (McAfee Default)
   - No
2. **Client UI.** Defines access to the Host Intrusion Prevention user interface on client systems. Preset policies:
   - (McAfee Default)
3. **Trusted Networks.** Lists IP addresses and subnets that are safe for communication. Preset policies:
   - (McAfee Default)
4. **Trusted Applications.** Lists applications that are safe, have no known vulnerabilities, and are allowed to perform any operation. This multiple-instance policy is a profile of settings with one or more policies. Preset policies:
   - (McAfee Default)

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.

1. **IPS Options.** Turns on or off host and network IPS protection. Preset policies:
   - On (McAfee Default)
   - Off
   - Adaptive
2. **IPS Protection.** Defines the reaction to events. Preset policies:
   - Basic (McAfee Default)
   - Prepare for Enhanced
   - Enhanced
   - Prepare for Maximum
   - Maximum
   - Warning
3. **IPS Rules.** Defines exceptions, signatures, and application protection rules; displays events and client rules. This multiple-instance policy is a profile of settings with one or more policies. Preset policies:
   - (McAfee Default)
Host Intrusion Prevention policies (continued)

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

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

   Preset policies:
   - Minimal (McAfee Default)
   - Learning Starter
   - Client High
   - Client Medium
   - Server High
   - Server Medium

3. Quarantine Options. Turns quarantine mode on or off.
   Preset policies:
   - Disabled (McAfee Default)

   Preset policies:
   - (McAfee Default)

Application Blocking policies
The Application Blocking feature contains two policies that manage applications that you allow to run with other applications (known as application creation) or bind with other applications (known as application hooking).

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

2. Application Blocking Rules. Defines application blocking rules that prevent unknown and unwanted applications from running or binding with other applications. It also displays client rules. Preset policies:
   - (McAfee Default)
“Out-of-the-box” and advanced protection

Basic protection
Host Intrusion Prevention ships with a set of default policies 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.

How protection works
As soon as the default policies are applied to the agents, intrusion prevention protection is in effect as long as the agent is running on a client. Communication with the ePO server is required for policy and content updates and monitoring.

Advanced protection
For advanced protection, switch from the default IPS policies to stronger preset policies, or create custom policies.

Manual tuning
- For IPS protection, monitor events for false positives and create rules for exceptions or trusted application 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.

For details on applying new policies, see the appropriate chapters in the Host Intrusion Prevention Product Guide.

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, all of which appear in the ePO console.
- Promote appropriate client rules to administrative policy rules to prevent IPS events from occurring and numerous client rules from being created.
- 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.
Always up-to-date

Content updating
The ePO database contains security content data, including signatures, which is displayed in Host Intrusion Prevention policies.

Updates are handled by a content update package, which contains version information and updating scripts. At check-in, the package version is compared to the most recent content in the database. If the package is newer, content data is extracted and stored. This new content is then passed to agents at the next agent-server communication.

To add update packages manually:
1. Download the content update package from McAfee.
2. Select the Repository in the ePO console tree and click Check in package.
3. Click Next, then select Products or updates.
4. Click Next, then enter the full path for the PkgCatalog.z file.
5. Click Next, then click Finish.

Sending content updates to agents
Communicate the updates to agents by scheduling an update task or by sending an immediate agent wakeup call. An agent can also request updates.

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

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

To have an agent request an update:
(Valid only if an ePO agent icon appears in the client computer system tray.)
- Right-click the ePO icon in the system tray and select Update Now.

Checking in update packages automatically or manually
Create an ePO server task that automatically downloads and checks in content update packages to the ePO Repository, or download an update package and check it in manually.

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

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

Host Intrusion Prevention content updates must be checked into the ePO Repository for distribution to agents. Host Intrusion Prevention agents can obtain updates only through communication with the ePO server.
Getting information

What product documentation is available?

**Host Intrusion Prevention 6.0**
*Installation/Configuration Guide* (PDF format)
- Installation and upgrade instructions
- Basic deployment instructions

*Product Guide* (PDF format)
- Product introduction
- Detailed instructions for configuring and using the software.
- Information on deployment.
- Recurring tasks.
- Operating procedures.

*Online Help* (Context-sensitive help topics accessible by clicking Help on a Host Intrusion Prevention dialog box or toolbar.)
- Reference information.
- Procedures.
- All information found in the product guide

*Release Notes* (Text file format)
- Known issues in the current release.
- Resolved issues since the last release.
- Last-minute changes to the product or its documentation.

**ePolicy Orchestrator 3.6**
*Installation Guide* (PDF format)
- Installation instructions for the database and product in a production environment.
- Clustering instructions, for use with Microsoft Clustering Services.

*Product Guide* (PDF format)
- Procedures on setting up and customizing the software.
- Detailed information about the options in the product.

*Reporting Guide* (PDF format)
- Procedures on running reports.
- Reference information for report and query templates.

*Online Help* (Context-sensitive help topics accessible by clicking Help on an ePolicy Orchestrator dialog box or toolbar.)
- Reference information.
- Procedures.
- Database maintenance.
- All information found in the product guide and reporting guide.

*Release Notes* (Text file format)
- Known issues in the current release.
- Resolved issues since the last release.
- Last-minute changes to the product or its documentation.

How do I contact technical support?

**Home Page**
http://www.mcafeesecurity.com/us/support/technical_support

**KnowledgeBase Search**
http://knowledgemap.nai.com/

**McAfee Technical Support ServicePortal**
(Logon credentials required)
https://mysupport.mcafeesecurity.com

Copyright © 2006 McAfee, Inc. All Rights Reserved.

DBN-001-EN

700-1287-00

mcafee.com