Release Notes

McAfee Host Intrusion Prevention 8.0.0 Patch 3 Software

About this release

Thank you for using this McAfee product. This document contains important information about the current release. We strongly recommend that you read the entire document.

Purpose

This release of McAfee® Host Intrusion Prevention provides support for Windows 8 and Windows Server 2012 operating systems **only**.

Although McAfee has thoroughly tested this release, we strongly recommend that you verify this update in test and pilot groups prior to mass deployment. Review the *New features*, *Known issues*, and *Resolved issues* sections for additional information.

For a list of supported environments and latest information for Host Intrusion Prevention 8.0.0 on Microsoft Windows, see KnowledgeBase article KB70778.

Important To install Host Intrusion Prevention on a server, you must purchase a license for Host Intrusion Prevention for Server or a server suite that includes Host Intrusion Prevention for Server (such as Total Protection for Server). You cannot install Host Intrusion Prevention for Desktop on a server. For additional information, contact your McAfee sales or support representative.

Patch version

This Host Intrusion Prevention 8.0.0 release includes two packages:

- **Patch 3** — Updates Host Intrusion Prevention 8.0.0 Patch 2 clients on Windows 8 and Windows Server 2012 systems only.

  Important After upgrading from Patch 2 to Patch 3, you must restart the client system.

- **Repost Patch 3** — Includes full installation for new Windows 8 and Windows Server 2012 systems only.

The **Repost Patch 3** package installs:

- Patch 3 to Windows 8 and Windows Server 2012 systems only
- Patch 2 to all other supported Windows versions

Although the **Repost Patch 3** package includes both Patch 3 and Patch 2, only the appropriate patch is deployed to client systems, depending on the platform.

You can check the appropriate package into the Master Repository on McAfee ePolicy Orchestrator (McAfee ePO) versions 5.0, 4.6, or 4.5.

Refer to KnowledgeBase article KB70760 for the most current Host Intrusion Prevention 8.0 details.

Package date
June 12, 2013

Rating
Patch 3: Mandatory for Windows 8 and Windows Server 2012

Patch 3 supports Windows 8 and Server 2012 operating systems only and, for those systems, the patch is **Mandatory**. McAfee Support requires customers using Windows 8 or Windows Server 2012 systems to apply this patch before being able to provide assistance.

Patch 2: High Priority

McAfee considers this release to be high priority for supported Windows versions other than Windows 8 and Windows Server 2012. Failure to apply a **High Priority** update might result in potential business impact.

See KnowledgeBase article KB51560 for information on ratings.

New features

Here is a list of features included with Patch 3.

Support for Windows 8
This release of Host Intrusion Prevention:

- Uses toast notifications (popup messages) in Metro mode to alert you to messages when Host Intrusion Prevention intercepts unknown network traffic and when IPS events occur.
- Integrates with the Windows Action Center (WAC).
  You can view messages and resolve problems reported by Host Intrusion Prevention from the Security area of the Action Center. For example, the Action Center displays status information on Host Intrusion Prevention Firewall.

Note Patch 3 supports Windows 8 Desktop mode only; it does not support Metro mode.

Support for SQL 2012
This release includes protection for SQL 2012, including changes to the Host Intrusion Prevention client and new signatures in the Host Intrusion Prevention Content release.

Support for Internet Information Services (IIS) 8.0
This release includes protection for IIS 8.0, including changes to the Host Intrusion Prevention client and new signatures in the Host Intrusion Prevention Content release.

Connected standby mode
This release of Host Intrusion Prevention provides support for systems in connected standby mode (also called *Always On Always Connected* or AOAC).

Note AOAC mode is only supported on Windows 8 systems with hardware chips that support AOAC.

AOAC suspended mode

When the system is in AOAC suspended mode, Host Intrusion Prevention buffers log entries — it does not display IPv6 and Debug level notifications. If Host Intrusion Prevention is in learn mode, Host Intrusion Prevention does not display learn mode alerts.

Updated components

This release includes updated versions of the following components:

- HipMgmt Service, which handles Host IPS/MA communication and uses the new MA LPC interface
- VScore components (version 15.1) to support Windows 8/Windows Server 2012
- Updated Visual Studio 2010 C++ runtime libraries, which are installed on client machine if needed
- Solaris package, which includes fixes to the installer

ASLR and DEP features

This release of Host Intrusion Prevention enables the following security features for all Host Intrusion Prevention components:

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)

Resolved issues

Here is a list of issues from this and previous releases of the software that have been fixed.

Issues resolved in this release

These issues were resolved in the Host Intrusion Prevention Patch 3 release.

Important This package includes both Patch 3 and Patch 2. The following resolutions included in Patch 3 apply to Windows 8 and Windows Server 2012 client systems only.

1 **Issue** — A vulnerability allowed for unauthorized privilege escalation by an authenticated user. (Reference: 791162)

Resolution — This update resolves the vulnerability. Refer to online Security Bulletin SB10034 for the most current details.

2 **Issue** — Some VPN clients failed to establish a VPN link when Host Intrusion Prevention 8.0 was installed on the system. (Reference: 771202)

Resolution — Updated the firewall logic to meet certain VPN client requirements.

3 **Issue** — Host Intrusion Prevention Content version 4517 caused Firefox and IE browsers to hang with the API engine. (Reference: 793215)

Resolution — Extended the logic to handle some duplicate Windows notifications.

4 **Issue** — Invalid firewall policies caused Naprdmgr.exe to crash during policy enforcement. (Reference: 798767)

Resolution — Added logic to better handle invalid policies.

5 **Issue** — Firesvc.exe caused high CPU usage. (Reference: 803520)

Resolution — Improved the efficiency of the service.

6 **Issue** — System bugcheck D1 in mfefirek.sys when using Host Intrusion Prevention 8.0 Patch 2 and certain VPN clients. (Reference: 806069)

Resolution — Certain VPN clients exposed a compatibility issue between Microsoft's WFP framework and the McAfee WFP driver. McAfee implemented a workaround in the WFP driver which resolves the issue.

7 **Issue** — DriverVerifier testing caused Mfehidk.sys bugcheck C1 on Microsoft Windows 7. (Reference: 807869)

Resolution — Fixed a buffer overrun issue.

8 **Issue** — Host Intrusion Prevention 8.0 did not register for ownership of firewall categories required for Microsoft DirectAccess. (Reference: 813045)

Resolution — Host Intrusion Prevention now registers for the BootTimeRuleCategory, FirewallRuleCategory, and StealthRuleCategory categories.

9 **Issue** — McTray.exe caused an error at system logon. (Reference: 788146)

Resolution — Fixed some asynchronous RPC issues.

10 **Issue** — Excessive memory usage by NaPrdMgr.exe when Host Intrusion Prevention 8.0 is installed. (Reference: 782946)

Resolution — Fixed a memory leak.

11 **Issue** — Host Intrusion Prevention blocked traffic in a Location Aware Group for Checkpoint VPN. (Reference: 733085)

Resolution — Fixed Location Aware Group matching logic.

12 **Issue** — Host Intrusion Prevention 8.0 fails to parse certain FQDN rules. (Reference: 818082)

Resolution — Fixed the parsing logic to correctly handle all FQDN rules.

13 **Issue** — Host Intrusion Prevention 8.0 causes Windows 8 machines to automatically restart. (Reference: 823785)

Resolution — Updated core components to support Windows 8 and Server 2012.

14 **Issue** — Host Intrusion Prevention 8.0 prevents Windows Firewall from being used. (Reference: 843301)

Resolution — Cleaned up Host Intrusion Prevention registration with Windows Firewall.

15 **Issue** — Explorer crashes when running Host Intrusion Prevention 8 Patch 2. (Reference: 821363)

Resolution — Modified the handling of certain exceptions to avoid the crash.

Issues resolved in Patch 2

These issues were resolved in the Host Intrusion Prevention Patch 2 release.

1 **Issue** — System Bugcheck 7f when using certain third-party VPN clients. (Reference: 716205, 725914)

Resolution — This could occur with the McAfee filter driver due to lost content header information when transmitting through a raw socket on Windows 7. The McAfee filter driver now ensures header information is preserved and forwarded through a raw socket.

2 **Issue** — A process could hang when running Host Intrusion Prevention and certain third-party applications. (Reference: 712198, 705273)

Resolution — When certain third-party applications perform process injections and cause Kernel32.dll to load unexpectedly, a timing issue with the Host Intrusion Prevention buffer overflow engine could result in a corrupt thread state. This potential timing issue is now avoided by using an alternative Windows API function.

3 **Issue** — Checking in a Host Intrusion Prevention 8.0 incremental patch to the evaluation branch in McAfee ePO requires a Host Intrusion Prevention 8.0 full installation package. (Reference: 709188, 727693)

Resolution — Removed an unnecessary incremental patch check-in restriction.

4 **Issue** — VirusScan Enterprise 8.7 Buffer Overflow Protection is disabled after installing Host Intrusion Prevention 8.0 Firewall-only client. (Reference: 697222)

Resolution — Updated the Buffer Overflow interaction logic to correctly handle the Firewall-only client.

5 **Issue** — Firewall rule does not trigger when using the "Allow any signature" option. (Reference: 695368)

Resolution — Fixed the digital signature-matching logic.

6 **Issue** — Upgrading from Host Intrusion Prevention 7.0 to Host Intrusion Prevention 8.0 on an IIS 6 based system leaves the legacy ISAPI filter behind. (Reference: 691280)

Resolution — Removed the legacy ISAPI filter entry and modules when adding new engines.

7 **Issue** — Host Intrusion Prevention 8.0 uninstallation fails if the McAfeeLogs folder has been deleted. (Reference: 648538)

Resolution — Fixed the installer logic to handle the missing McAfeeLogs folder.

8 **Issue** — Host Intrusion Prevention content update does not apply from evaluation or previous branch. (Reference: 708494, 709299)

Resolution — Modified the update logic to update evaluation and previous versions successfully.

9 **Issue** — Services.exe crashes on HcSvc.dll. (Reference: 682442)

Resolution — Restructured the integration with services to avoid the crash.

10 **Issue** — Application list fails to populate when the option "Automatically include network-facing and service-based applications in the application protection list" is enabled. (Reference: 675658)

Resolution — Fixed logic in the Host Intrusion Prevention client to handle list population.

11 **Issue** — Under certain circumstances, Host Intrusion Prevention adds duplicate entries into the access control list. Eventually, this can lead to the list reaching a maximum size and cause policy applications to fail. (Reference: 715967)

Resolution — Host Intrusion Prevention no longer adds duplicate entries.

12 **Issue** — Microsoft SQL 2005 runs out of resources and becomes non-functional. (Reference: 715941, 719013)

Resolution — Modified the working set logic to fix this issue.

13 **Issue** — Microsoft Project might experience latency caused by Host Intrusion Prevention Buffer Overflow Engine. (Reference: 698505, 698680)

Resolution — Optimized the Buffer Overflow Engine detection mechanism for better performance.

14 **Issue** — Host Intrusion Prevention sets IrpStackSize instead of IRPStackSize. (Reference: 708512)

Resolution — Fixed the installer to correctly set the case-sensitive registry key value.

15 **Issue** — Host Intrusion Prevention 8.0 Exclusion parameter "Group Name" does not work properly. (Reference: 688393)

Resolution — Fixed the IPS exception parsing logic to correct this behavior.

16 **Issue** — "Create a firewall application rule for all Ports and protocols" is not honored if there is an existing application rule for specific port or protocol. (Reference: 725733)

Resolution — Fixed the related learn mode logic to correct this behavior.

17 **Issue** — System Bugcheck in mfehidk.sys or HipShieldK.sys when certain third-party tools are installed. (Reference: 699334)

Resolution — Fixed the binary querying logic to correct this behavior.

18 **Issue** — Delayed restart time occurs when Host Intrusion Prevention is installed on Linux RedHat Enterprise. (Reference: 713569)

Resolution — Handle the received SIGTERM signal from the OS and immediately shut down HipClient.

19 **Issue** — Host Intrusion Prevention fails to detect buffer overflow for various CVE vulnerabilities. (Reference: 708803, 667445, 665359, 702042)

Resolution — Added additional protection to cover new vulnerabilities.

20 **Issue** — System Bugcheck after upgrading from Host Intrusion Prevention 7.0 to to Host Intrusion Prevention 8.0. (Reference: 709280)

Resolution — Updated the Host Intrusion Prevention 8.0 installer to help recover from a broken Host Intrusion Prevention 7.0 installation.

21 **Issue** — Wireless connection fails if the system is restarted and the Ethernet cable is not connected. (Reference: 728156)

Resolution — Fixed the boot-time and run-time firewall policies to correct this behavior.

22 **Issue** — McTray crashes randomly. (Reference: 733395)

Resolution — Fixed an RPC issue that was causing this behavior.

23 **Issue** — VPN connections terminate randomly. (Reference: 697716)

Resolution — Updated the stateful firewall logic to properly handle VPN tunnel connections not going through the McAfee NDIS driver.

24 **Issue** — Windows desktop fails to load properly on systems running Host Intrusion Prevention and Blue Coat. (Reference: 736186)

Resolution — Modified the injection logic to handle unexpected scenarios caused by certain third party applications.

25 **Issue** — System hangs after installing Host Intrusion Prevention 8.0.0 Patch 1 and restarting. (Reference: 737277, 765242)

Resolution — Fixed a race condition between Microsoft TCP/IP and the WFP driver to avoid the hang.

26 **Issue** — Some custom signatures fail to match if the executable has been renamed. (Reference: 707321)

Resolution — Implemented an alternative solution to handle related operating system limitations.

27 **Issue** — System hangs when a USB drive is connected. (Reference: 760418)

Resolution — Fixed a potential deadlock issue.

28 **Issue** — Custom IPS signatures report the user information as DOMAIN UNKNOWN / USER UNKNOWN when triggered,

making it impossible to create an exclusion for a specific user. (Reference: 770081)

Resolution — Implemented an alternative solution for gathering domain/user information.

29 **Issue** — Trusted Source blocks incoming ICMP traffic. (Reference: 759077)

Resolution — Re-evaluated the security requirements for ICMP and ICMPv6 and adjusted the Trusted Source logic accordingly.

Issues resolved in Patch 1

These issues were resolved in the Host Intrusion Prevention Patch 1 release.

1 **Issue** — Some systems lose network connectivity during upgrade from Host Intrusion Prevention 7.0 to 8.0. (Reference: 661416)

Resolution — Updated the installer for Host Intrusion Prevention 8.0 to recover from an occasional failure during uninstallation of the Host Intrusion Prevention 7.0 NDIS filter driver.

2 **Issue** — The Host Intrusion Prevention 8.0 upgrade is interrupted, leaving the system with an incomplete installation. (Reference: 664654, 664659)

Resolution — Updated the installer to prevent Host Intrusion Prevention 7.0 from performing a policy enforcement which could interrupt the Host Intrusion Prevention 8.0 installation.

3 **Issue** — Trusted Source lookup causes VPN to fail. (Reference: 666991, 676489)

Resolution — Updated the Firewall component to prevent VPN failure during Trusted Source lookup.

4 **Issue** — BugCheck during the installation of a 3rd party VPN software. (Reference: 670709, 677894, 678618, 689466, 689933, 693416)

Resolution — Updated String operation errors to prevent BugCheck.

5 **Issue** — Security vulnerabilities found in the included Visual C++ 2005 package. (Reference: 678336)

Resolution — Host Intrusion Prevention 8.0 RTW was confirmed not to be affected by the vulnerabilities found in the original Visual C++ 2005 package. Regardless, Patch 1 now includes the updated Microsoft Visual C++ 2005 Service Pack 1 redistributables which include fixes for these vulnerabilities.

6 **Issue** — Host Intrusion Prevention 8.0 causes explorer.exe to hang when enabling a USB external hard drive. (Reference: 683143, 683222)

Resolution — Fixed a deadlock issue to prevent explorer.exe from hanging.

7 **Issue** — Network Performance degrades after installing Host Intrusion Prevention 8.0. (Reference: 659781)

Resolution — Updated internal algorithms to improve network performance.

8 **Issue** — Activity Log tab shows blank entries for Intrusion events on Trusted Networks. (Reference: 678330, 683970, 684963, 688320, 689625, 698629)

Resolution — Added logic to ensure that the signature info is populated.

9 **Issue** — Dynamically learned rule causes policy enforcement failure on McAfee ePO managed systems. (Reference: 682892)

Resolution — Updated string operation errors to prevent failure.

10 **Issue** — Host Intrusion Prevention 8.0 FireTray.exe crashes with an application error. (Reference: 688732)

Resolution — Fixed an error to prevent the failure.

11 **Issue** — Host Intrusion Prevention 8.0 Connection Aware Group is unable to match traffic to the loopback interface on Vista and older operating systems. (Reference: 645792, 649041, 650988, 658430, 666469)

Resolution — Added loopback interface support on Vista and older platforms.

12 **Issue** — IPv6 encapsulated in IPv4 is blocked inside Connection Aware Group rules. (Reference: 647941)

Resolution — Extended FireCore logic to correctly parse this traffic type.

13 **Issue** — Memory leak in mfevtps.exe. (Reference: 668024, 668596, 670452)

Resolution — Resolved a potential issue with Windows DLL to prevent the error.

14 **Issue** — System instability with Host Intrusion Prevention 8.0 installed. (Reference: 660568, 647259, 660979, 663429, 664933, 667040, 667240, 668589)

Resolution — Resolved several issues with Host Intrusion Prevention for enhanced stability.

Installation instructions

Use these instructions to install, verify, and remove this Host Intrusion Prevention 8.0.0 Patch release.

Install the product directly to a client system

Follow these steps to install the package directly to a target client system.

Task

1 Download the appropriate package:

- **Patch 3** — HIP80P3.Zip
- **Repost Patch 3** — HIP80LMLRP3.Zip

2 Extract the patch files to a temporary folder on your hard drive.

3 Disable Host Intrusion Prevention protection with an ePolicy Orchestrator delivered policy or in the local client interface.

4 Double-click the setup file in the temporary folder created in Step 2:

- **Patch 3** — McAfeeHIP_ClientPatch3.exe
- **Repost Patch 3** — McAfeeHIP_ClientSetup.exe

5 Follow the installation wizard instructions.

6 Depending on your package:

- **Patch 3** — Restart the client system after upgrading from Patch 2.

  Important You must restart the client system to restore communication between Host Intrusion Prevention and McAfee Agent. Features that depend on communication with McAfee Agent, such as policy enforcement, content updates, and reporting IPS detections back to McAfee Agent will not work until the client system is restarted.

- **Repost Patch 3** — No need to restart the client system.

  Note Host Intrusion Prevention Repost Patch 3 installation does not require a restart but might cause a brief interruption in network traffic.

7 Enable Host Intrusion Prevention protection.

For more information, see the *Host Intrusion Prevention Installation Guide*.

Deploy the product using ePolicy Orchestrator

Follow these steps to deploy this release to managed systems using ePolicy Orchestrator version 5.0, 4.6, or 4.5.

Task

For option definitions, click ? in the interface.

1 Check the package into the ePolicy Orchestrator Master Repository:

a Select Menu | Software | Master Repository, then click Check In Package.

b Select the Product or Update (.ZIP) package type.

c Click Choose File and select the Host Intrusion Prevention zip package:

- **Patch 3** — HIP80P3.Zip
- **Repost Patch 3** — HIP80LMLRP3.Zip

Important The Repost Patch 3 package replaces the currently checked-in Repost Patch 2 package.

This process might take several minutes to complete.

For more information, see *Checking in packages manually* in the ePolicy Orchestrator online help.

2 Deploy the Patch 3 package to the client systems:

- **Patch 3** — Use a McAfee Agent Product Update client task.

  During an upgrade from Host Intrusion Prevention 7.0, if the 7.0 NDIS fails to uninstall, the installer automatically restarts the system after 10 minutes. To disable the automatic restart, add the BYPASSREBOOT=1 option to the Command line field in the Product Deployment Task. For more information, see KB76609.

  Important After upgrading from Patch 2 to Patch 3, you must restart the client systems.

- **Repost Patch 3** — Use a McAfee Agent Product Deployment client task.

  Important A single Product Deployment task detects the platform and downloads and installs only the appropriate files for that operating system: Patch 3 to Windows 8 and Windows Server 2012 systems only, and Patch 2 to all other supported Windows versions.

3 Restart any client systems that were upgraded from Patch 2 to Patch 3.

Important You must restart the client systems to restore communication between Host Intrusion Prevention and McAfee Agent. Features that depend on communication with McAfee Agent, such as policy enforcement, content updates, and reporting IPS detections back to McAfee Agent will not work until the client system is restarted.

For more information, see the *Host Intrusion Prevention Installation Guide*.

Verify the installation

After installing the Host Intrusion Prevention Patch 3 package, verify that the product installed correctly on the client systems.

Important Releases are not displayed or do not report installed if an error occurred during installation, or if a file did not install correctly.

Task

1 In ePolicy Orchestrator, run the Host IPS: Client Versions query.

For systems with Patch 3 installed, the Client Version (Host IPS) is 8.0.0.2589.

2 Click on the version number to display the system names.

File inventory

Folder name	File name	Version
Program Files\Common Files\McAfee\SystemCore	fwinfo.exe	15.1.0.580
	mfeapfa.dll	15.1.0.580
	mfeavfa.dll	15.1.0.580
	mfefire.exe	15.1.0.580
	mfefwctl.dll	15.1.0.580
	mfehida.dll	15.1.0.580
	mfehidk_messages.dll	15.1.0.580
	mfevtpa.dll	15.1.0.580
Program Files\McAfee\Host Intrusion Prevention	ClientControl.exe	8.0.0.2589
	DebugLog.dll	8.0.0.2589
	FireCL.dll	8.0.0.2589
	FireCNL.dll	8.0.0.2589
	FireComm.dll	8.0.0.2589
	FireCore.dll	8.0.0.2589
	FireEpo.dll	8.0.0.2589
	FireSvc.exe	8.0.0.2589
	FireTray.exe	8.0.0.2589
	HcApi.dll	8.0.0.2589
	HcCode.dll	8.0.0.2589

	HcSql.dll	8.0.0.2589
	HcSvc.dll	8.0.0.2589
	HcThe.dll	8.0.0.2589
	Helper.exe	8.0.0.2589
	HipMgtPlugin.dll	8.0.0.2589
	HipRc.dll	8.0.0.2589
	HipShield.dll	8.0.0.2589
	HpmRegistry.dll	8.0.0.2589
	McAfeeFire.exe	8.0.0.2589
	mcafeewin32guisupportdll.dll	8.0.0.2589
	MngFirecore.dll	8.0.0.2589
	SecCtrFw.exe *	8.0.0.2589
Program Files\McAfee\Host Intrusion Prevention\VSCore\release Program Files (x86)\McAfee\Host Intrusion Prevention\VSCore\release Program Files (x86)\McAfee\Host Intrusion Prevention\VSCore\x64	fwinfo.exe	15.1.0.580
	HipShieldK.sys	8.0.0.2589
	mfeapfa.dll	15.1.0.580
	mfeapfk.sys	15.1.0.580
	mfeavfa.dll	15.1.0.580
	mfeavfk.sys	15.1.0.580
	mfefire.exe	15.1.0.580
	mfefirek.sys	15.1.0.580
	mfefwctl.dll	15.1.0.580
	mfehida.dll	15.1.0.580
	mfehidin.exe	15.1.0.580
	mfehidk.sys	15.1.0.580
	mfehidk_messages.dll	15.1.0.580
	mfendisk.sys	15.1.0.580
	mfenlfk.sys	15.1.0.580
	mfetdi2k.sys	15.1.0.580
	mfevtpa.dll	15.1.0.580
	mfevtps.exe	15.1.0.580

	mfewfpk.sys	15.1.0.580
[Windows]\System32	mfevtps.exe	15.1.0.580
[Windows]\System32\Drivers	mfeapfk.sys	15.1.0.580
	mfeavfk.sys	15.1.0.580
	mfefirek.sys	15.1.0.580
	mfehidk.sys	15.1.0.580
	mfewfpk.sys	15.1.0.580
* New with Patch 3.		

Files specific to 32-bit operating systems

Folder name	File name	Version
Program Files\McAfee\Host Intrusion Prevention	McTrayHipPlugin.dll	8.0.0.2589
	HipMgmt.exe *	8.0.0.2589
	HipMgmtHpr.dll *	8.0.0.2589
* New with Patch 3.		

Files specific to 64-bit operating systems

Folder name	File name	Version
Program Files (x86)\Common Files\McAfee\SystemCore	mfeavfa.dll	15.1.0.580
	mfefwctl.dll	15.1.0.580
	mfehida.dll	15.1.0.580
Program Files (x86)\McAfee\Host Intrusion Prevention	DebugLog.dll	8.0.0.2589
	FireCL.dll	8.0.0.2589
	FireCNL.dll	8.0.0.2589
	FireComm.dll	8.0.0.2589
	FireCore.dll	8.0.0.2589
	FireEpo.dll	8.0.0.2589
	HcApi.dll	8.0.0.2589
	HcCode.dll	8.0.0.2589
	HcSql.dll	8.0.0.2589
	HcThe.dll	8.0.0.2589
	Helper.exe	8.0.0.2589

	HipMgmt.exe *	8.0.0.2589
	HipMgmtHpr.dll *	8.0.0.2589
	HipMgtPlugin.dll	8.0.0.2589
	HpmRegistry.dll	8.0.0.2589
	McTrayHipPlugin.dll	8.0.0.2589
	MngFirecore.dll	8.0.0.2589
* New with Patch 3.		

Remove installation files

You can remove the Host Intrusion Prevention patch remotely from the ePolicy Orchestrator server or directly on the client computer using Windows Add/Remove Programs.

For information, see the *McAfee Host Intrusion Prevention Installation Guide*.

Note This Patch upgrades the McAfee Core files. Because multiple products share these files, removing this patch does not remove the McAfee Core files.

Known issues

For known issues in this product release, refer to KnowledgeBase article KB75919.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under Self Service, access the type of information you need:

To access...	Do this...
User documentation	1 Click Product Documentation. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click Search the KnowledgeBase for answers to your product questions. • Click Browse the KnowledgeBase for articles listed by product and version.