

McAfee Firewall Enterprise Control Center 5.3.2 Patch 2

Contents

- ▶ *About this release*
- ▶ *Enhancements*
- ▶ *Resolved issues*
- ▶ *Installation instructions*
- ▶ *Known issues*
- ▶ *Additional information*
- ▶ *Find product documentation*


About this release

McAfee® Firewall Enterprise Control Center (Control Center) version 5.3.2 Patch 2 provides support for McAfee® Firewall Enterprise version 8.3.2.P03 (8.3.2.3) and earlier (8.x.x and 7.0.1.03 Patch H08). The system must be on version 5.3.2 to install the 532P02 patch.

This release introduces enhancements and resolves issues present in the previous release.

You can find additional information by using the resources listed in the table.

Table 1-1 Product resources

Component	Requirements
Help	Online Help is built into Control Center. Click Help on the toolbar or from a specific window.
McAfee Technical Support ServicePortal	Visit support.mcafee.com to find: <ul style="list-style-type: none"> • Product documentation • KnowledgeBase • Product announcements • Technical support • Product installation files • Upgrades and patches <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  For information about the Control Center support life cycle, refer to http://www.mcafee.com/us/support/support-eol.aspx. </div>
Product updates	Visit support.mcafee.com and click on the Downloads tab to get the latest McAfee Firewall Enterprise Control Center patches.

Compatible McAfee products

Control Center version 5.3.2 Patch 2 is compatible with the following McAfee products:

- McAfee® Firewall Enterprise
- McAfee® ePolicy Orchestrator® Extension
- McAfee® Logon Collector
- McAfee® Endpoint Intelligence Agent (McAfee EIA)

For the latest information about the McAfee firewall products and versions that interoperate with Control Center, see KnowledgeBase article [KB67462](#).

Enhancements

This release of the product includes these enhancements.

Controlled access with SELinux

Security-Enhanced Linux (SELinux) in Control Center enables you to support access control security policies. This acts as another layer of security and hardens the Control Center system.

By default, when you install Control Center 5.3.2 Patch 2 or upgrade from earlier versions to 5.3.2 Patch 2, SELinux is enabled. As a root user, you can modify and check the SELinux settings.



You can't disable SELinux on Control Center.

SELinux can be either in `Permissive` or `Enforcing` mode. The default `Enforcing` mode enables and enforces SELinux policies to restrict access and log actions. The `Permissive` mode enables SELinux, but does not enforce the security policy. It only allows to warn and log actions.

Backup and restore for High Availability

This patch release supports backup and restore for a High Availability pair. You can take a backup from the High Availability pair and restore the pair without having to break the pair.

On a standalone Control Center system, when you perform a backup and restore, the system restores automatically. However, for a High Availability pair, you need to enter the login password to restore the High Availability pair successfully.



While restoring the backup on an HA pair, use the same user credentials on which the HA backup was initially taken.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in earlier releases, see the Release Notes for the specific release.

- Control Center must support BGP using TCP with MD5 authentication. The earlier manual VPNs must be preserved when new VPNs are applied. (951039)
- Control Center must remove support for Firewall Profiler and Firewall Reporter. (882708)
- Firewall Enterprise can uninstall 8.3.2.3 without uninstalling the related `ccmd` package. (965108)

Installation instructions

You can install Control Center on a physical or virtual appliance. You can upgrade from Control Center version 5.2.x to 5.3.2 for these appliances.

If you are upgrading from 5.2.x or 5.3.0, refer to the *McAfee Firewall Enterprise Control Center Installation and Migration Guide* 5.3.0 and 5.3.1 to upgrade to 5.3.1, and then upgrade to Control Center 5.3.2. Once 5.3.2 is installed, download and install the 532P02 patch.



If you are on Control Center 5.3.2, you must install 5.3.2.P02 to manage 8.3.2.P03 firewalls.



Once you upgrade to Control Center 5.3.2, you have to re-register all the firewalls and clusters, and retrieve **Firewall Dialog Information** to enable communication between Control Center and Firewall Enterprise.

For more details, refer to the *McAfee Firewall Enterprise Control Center Installation and Migration Guide*.



To uninstall Firewall Enterprise 8.3.2.3 patch, first uninstall the ccmd 8.3.2CC5.3.20406 package and then uninstall the Firewall Enterprise 8.3.2.3 patch.


Hardware appliance requirements

Before you install 5.3.2, make sure the Control Center Client application and Management Server requirements are met.

Client application requirements

The computer that hosts the Control Center Client application must meet these requirements.

Table 4-1 Client application minimum requirements

Component	Requirements
Operating system	<p>One of the following Microsoft operating systems:</p> <ul style="list-style-type: none"> • Windows Server 2008 • Windows Server 2003 • Windows 7 • Windows 8 Professional • Windows Vista • Windows XP Professional with SP2 or later
Web browser	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer, version 6 or later • Mozilla Firefox, version 1.0 or later
Hardware	<ul style="list-style-type: none"> • 3.0 GHz Intel Pentium 4 processor or higher • System memory <ul style="list-style-type: none"> • Windows Server or Windows XP — 3 GB (2 GB minimum) • Windows Vista, Windows 7, or Windows 8 — 4 GB (3 GB minimum) • 150 MB of available disk space • CD drive • Network card (with access to network hosting the Management Server) • USB port (for USB drive) • USB drive formatted in MS-DOS (hereinafter <i>configuration USB drive</i>) <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p> You must provide a configuration USB drive; the USB drive provided by McAfee cannot be used to store the configuration file.</p> </div> <ul style="list-style-type: none"> • 1280 x 1024 display (1024 x 768 minimum) • Keyboard and mouse • Network cables

Management Server requirements

Control Center 5.3.0 and later use the McAfee® Linux Operating System 2.1.0 64-bit version (hereinafter MLOS).

Table 4-2 Management Server minimum requirements




Component	Requirements
Hardware	<ul style="list-style-type: none"> • Examples: <ul style="list-style-type: none"> • C1015 • C2050

Virtual appliance requirements

The McAfee® Firewall Enterprise Control Center, Virtual Appliance runs on the VMware ESX 4.1 update 2 or later hypervisor operating system, providing flexible security for your virtual environment.

To run Control Center, Virtual Appliance, the following requirements must be met.

Table 4-3 System requirements

Component	Requirements
Control Center, Virtual Appliance	
VMware server	VMware ESX version 4.1 update 2 or later  Make sure that VT (Virtual Technology) is enabled in your computer BIOS.
Hardware	<ul style="list-style-type: none">• Any server-class type hardware. Examples:<ul style="list-style-type: none">• Dell R910• Dell R610
CPU	One virtual processor
Memory	1 GB minimum (Recommended 2 GB)
Drives	150 GB of available disk space  Hard drive space is thin provisioned. 150 GB is the maximum amount of disk space the virtual machine requires. A minimal installation uses approximately 5 GB of disk space and increase as needed.  For a VMDK installation, we recommend that you select thin provisioning.
Control Center Client application	
Operating system	One of the following Microsoft operating systems: <ul style="list-style-type: none">• Windows XP Professional• Windows Vista• Windows Server 2003• Windows 7• Windows Server 2008• Windows 8 Professional
Monitor	1024 x 768 or higher
Network interface card	Access to the network hosting your Control Center, Virtual Appliance
Browser	<ul style="list-style-type: none">• Microsoft Internet Explorer, version 6 or later• Mozilla Firefox, version 1.0 or later

Known issues

For known issues in this product release, refer to KnowledgeBase article [KB79057](#).

Additional information

This section provides details for Heartbleed and McAfee Host IPS related KnowledgeBase articles.

For the Heartbleed fix and details for Control Center, refer to KnowledgeBase article [KB81699](#).

For details on Host Based Security System (HBSS) for McAfee Host IPS, refer to KnowledgeBase article [KB81908](#)

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

- 1 Go to the McAfee ServicePortal at <http://support.mcafee.com> and click **Knowledge Center**.
- 2 Enter a product name, select a version, then click **Search** to display a list of documents.

Product documentation

McAfee Firewall Enterprise Control Center documentation set includes the following:

Typical documents

- *McAfee Firewall Enterprise Control Center Release Notes*
- *McAfee Firewall Enterprise Control Center Product Guide*
- *McAfee Firewall Enterprise Control Center Online Help*

Hardware

- *McAfee Firewall Enterprise Control Center Hardware Product Guide, C Models*
- *McAfee Firewall Enterprise Control Center Installation and Migration Guide*
- *McAfee Firewall Enterprise Control Center Installation USB Drive Product Note*
- *McAfee Firewall Enterprise Control Center Quick Start Guide*

Certification

- *McAfee Firewall Enterprise Control Center Common Criteria Evaluated Configuration Guide*
- *McAfee Firewall Enterprise Control Center FIPS 140-2 Configuration Guide*
- *McAfee Firewall Enterprise Control Center FIPS 140-2 Level 2 Kit Installation Guide*

Copyright © 2014 McAfee, Inc. Do not copy without permission.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

0B00