Release Notes

Revision A

McAfee Firewall Enterprise Control Center 5.3.2

Contents

About this release

McAfee® Firewall Enterprise Control Center (Control Center) version 5.3.2 provides support for McAfee® Firewall Enterprise version 8.3.2 and earlier (8.x.x and 7.0.1.03 Patch H08).

This release introduces new features, 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	Help is built into the Control Center Client application and the Initialization Tool. Press **F1** from a specific window or page or click **?** on the title bar.
McAfee Technical Support ServicePortal	Visit mysupport.mcafee.com to find: • Product announcements • Product documentation • Technical support • KnowledgeBase

Table 1-1 Product resources *(continued)*

Component	Requirements
Product updates	Visit go.mcafee.com/goto/updates to download the latest McAfee Firewall Enterprise Control Center patches.
Product installation files	1 Go to www.mcafee.com/us/downloads. 2 Enter your grant number and download McAfee Firewall Enterprise Control Center installation files.

ℹ For information about the Control Center support life cycle, refer to http://www.mcafee.com/us/support/support-eol.aspx.

Compatible McAfee products

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

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

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

New features

This release of the product includes this new feature.

Computing executable file reputation

McAfee® Endpoint Intelligence Agent (hereinafter Endpoint Intelligence Agent or McAfee EIA) analyzes different characteristics of executable files and associated libraries (dlls) to determine an endpoint application's trust. You can also use reputation sources like McAfee® Global Threat Intelligence™ (McAfee GTI) file reputation and host reputation from McAfee EIA to compute executable file reputation. The reputations help to derive an overall malware confidence level for an executable file.

ℹ You have to enable Endpoint Intelligence Agent to use this capability. Executable file reputation is supported only on 8.3.2 firewalls and later.

Control Center enables you to create new or modify retrieved executable reputation objects for a firewall and apply them across firewalls in the network. From the **Dashboard | Summary** page, access firewall audit entries related to Endpoint Intelligence Agent.

Overall malware confidence for an executable file

The overall malware confidence level for an executable file is determined using reputations from various sources.

Overall malware confidence is calculated from these elements:

- **GTI Reputation** — Reputation of the executable received from Global Threat Intelligence. When Global Threat Intelligence is enabled, the risk level in the database is reported back to the firewall: very low, low, medium, high, very high, or unknown.
- **Host Reputation** — Reputation of the executable received from Endpoint Intelligence Agent in the endpoint information. McAfee EIA on the host assigns the executable file MD5 a risk level rating: very low, low, medium, high, very high, or unknown.
- **Executable Reputation** — Reputation computed using the classification list (whitelisted and blacklisted). When the classification list is enabled, the executable file is compared to the imported trusted list or manual executable entries.

The reputations and overall confidence level are displayed on the **Dashboards | Summary** page.

Firewall response

Once Firewall Enterprise gets the overall confidence for an executable file, it can take action. Firewall Enterprise can use executable file reputation to create a whitelist or blacklist database for auditing, and generate alerts and reports for whitelisted, blacklisted, new, and unknown executables detected in the network. You can create malware rules, define attack responses, and view and analyze firewall audits.

Refer to the *McAfee Firewall Enterprise Control Center Product Guide* for more details.

Enhancements

This release of the product includes these enhancements.

SHA2 support

Control Center supports SHA2 digest algorithms and enforces new key size rules and supports larger asymmetric key lengths. Moving from SHA1 to SHA2 also helps us to adhere to FIPS 140-2 Level 1 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-57 and NIST SP 800-78 requirements and in turn improves the security posture of our systems.

High Availability optimization

In High Availability deployments, there have been past cases of accidental switchover. The Client application displays a dialog for users to select the **Switchover to Secondary Server** checkbox and click **Switchover** to make users doubly aware of a switchover.

For High Availability issues, the logs are more detailed and help the McAfee technical support team to troubleshoot and resolve issues faster.

IPv6 support for CAC, SNMP, and SSH

The CAC (Common Access Card) Authentication Warder now supports IPv6. By default, the CAC authenticator is enabled for IPv6 when used on an IPv6-enabled interface. IPv6 endpoints can also be used on explicit CAC authenticator policy rules.

SNMP agent and trap functionality is updated in these areas:

- **IPv6 support** — The SNMP agent supports IPv6 for agent requests and Trap destinations. You can enable IPv6 support for SNMP by specifying IPv6 source and destination endpoints on SNMP policy rules or by using **<Any>**. You can also add new IPv6 trap destinations.
- **Agent binding** — The SNMP agent enhancements allow a single agent instance to handle SNMP requests for multiple zones. There are no longer any policy restrictions for creating SNMP agent rules in multiple zones or specifying multiple zones on a single SNMP Agent rule.
- **Agent startup** — The SNMP agent always starts on the firewall to ensure consistent SNMP trap delivery, even if it does not accept SNMP agent requests.

SSH functionality is updated in these areas:

- **IPv6 support** — The SSH client and server is updated to support IPv6. To enable IPv6 support in the SSH server, policy rules can be specified with IPv6 endpoints or that use **<Any>** for source or destination.
- **Agent binding** — The address binding algorithm is updated, allowing the SSH server to properly bind to any IPv4 and IPv6 addresses configured in rules. You can manually override the bind behavior by specifying ListenAddress directives in the sshd_config.

IPv6 extension headers

By default, IPv6 extension headers are not passed. For 8.3.2 firewalls, you can specify in filters the extension headers and options you want to allow over IPv6. This enhancement complies to United State government (USG) IPv6 standards.

Read Only Administrator

The **Admin Read Only** accounts are better for corporate security and compliance requirements. This user role allows an administrator to view all system information, as well as create and run audit reports. An administrator with read-only privileges cannot commit changes to any area of the firewall.

McAfee Firewall Enterprise ePolicy Orchestrator extension

The McAfee Firewall Enterprise 5.3.2 ePolicy Orchestrator extension supports Dashboard reporting support for Firewall Enterprise resources (from Control Center), firewall statistics, and firewall internal host mapping (Firewall Enterprise). This extension version does not support Firewall Profiler.

Control Center version 5.3.2 is compatible with McAfee Firewall Enterprise ePolicy Orchestrator extension, version 5.3.2. This release is supported on McAfee ePolicy Orchestrator versions 4.6.0 to 5.0.1.

> ℹ For more details, refer to the *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide.*

> ! For Endpoint Intelligence Agent 2.0.0 and Network Integrity Agent 1.0.1 policy and configuration management, refer to the *Endpoint Intelligence Management 2.0.0 Help Extension* documentation.

Performance and stability improvements

These are the enhancements to improve performance and stability.

- **Database tuning** — The database system has been tuned to take advantage of available memory.
- **Log configuration** — The system is configured to log slow queries and the log patterns are improved to help log analysis.

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.

- Fixes an issue where you can perform a switchover when you are not assigned a role for High Availability. (885435)
- Resolves the `OutOfMemoryError with GC overhead limit exceeded` error when **Apply / Validate** is performed for a large policy. (893519)
- Provides you the option to set up shared buffers and working memory in the `postgresgl.conf` file based on the total RAM available during an installation or upgrade. (900175)
- Fixes an issues where Control Center allows users to connect to update servers through HTTP proxies, but it does not allow configuration of user name and password for these proxies. (779219)
- Resolves an issue where tooltips were not displayed for new and updated alerts. (883873)
- Fixes an issue where alert popups are immovable. (883876)
- Rectifies an issue where a blank screen is displayed when you click **View Event in Audit** from the **Monitor | Alerts** page. (883881)
- Provides a **File** option on the **Control Center | Control Center updates | Upload to Server** page to copy a file from the Management Server to a specified location. (885265)

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 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*.

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 5-1 Client application minimum requirements

Component	Requirements
Operating system	One of the following Microsoft operating systems: • Windows Server 2008 • Windows Server 2003 • Windows 7 • Windows 8 Professional • Windows Vista • Windows XP Professional with SP2 or later
Web browser	One of the following: • Microsoft Internet Explorer, version 6 or later • Mozilla Firefox, version 1.0 or later
Hardware	• 3.0 GHz Intel Pentium 4 processor or higher • System memory • 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 *configuration USB drive*) You must provide a configuration USB drive; the USB drive provided by McAfee cannot be used to store the configuration file. • 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 5-2 Management Server minimum requirements

Component	Requirements
Hardware	• Examples: • 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 5-3 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	• Any server-class type hardware. Examples: • 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: • Windows XP Professional • Windows Server 2003 • Windows Server 2008 • Windows Vista • Windows 7 • Windows 8 Professional
Monitor	1024 x 768 or higher
Network interface card	Access to the network hosting your Control Center, Virtual Appliance
Browser	• 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 more details about the release.

Clearing old alerts

Currently **Purgedata** cleans up alerts based on the settings in the `/usr/local/dcserver/conf/purgedata.properties` file as shown in the following examples. There is an additional **Priority** option that cleans all the open, orphan, and closed alerts based on the set priority.

##
##########

Examples of possible values

```
#activealerts=1 - deletes the active alerts older then 1 day #
#activealerts=1d - deletes the active alerts older then 1 day #
#activealerts=1h - deletes the active alerts older then 1 hour #
#activealerts=never - doesn't delete the active alerts #
```

##
######

```
activealerts=1
orphanalerts=1
closedalerts=1
```

##
######

Examples of possible values with additional priority setting

```
#activealerts=1 - deletes the active alerts older then 1 day #
#activealerts=1d - deletes the active alerts older then 1 day #
#activealerts=1h - deletes the active alerts older then 1 hour #
#activealerts=never - doesn't delete the active alerts #
#priority=1 - priority of the active alerts #
```

#priority should be between 1 and 5 #

#"1-Critical", "2-High", "3-Medium", "4-Low", "5-Warning" #

##
######

```
activealerts=30d
priority=2
orphanalerts=1
closedalerts=1
```

The default value of priority is set to **High** and cleans up alerts that are older than 30 days. Since this is configurable, if you don’t want to clean up active alerts, you can modify this setting.

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.

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*