Release Notes

Revision B

McAfee Firewall Enterprise 8.3.2P03

Contents

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

McAfee® Firewall Enterprise (Firewall Enterprise) version 8.3.2P03 introduces new features, adds enhancements, and resolves issues present in the previous release.

Supported firewall types

Firewall Enterprise supports these firewall types.

- McAfee® Firewall Enterprise appliances
- McAfee® Firewall Enterprise, Virtual Appliance
- McAfee® Firewall Enterprise on Crossbeam X-Series Platforms

These features are not supported on Crossbeam X-Series Platforms for this release:

- Firewall Enterprise Admin Console

  > Use a McAfee® Firewall Enterprise Control Center (Control Center) Management Server to manage Firewall Enterprise on Crossbeam X-Series Platforms.

- Multicast dynamic routing using the PIM-SM protocol
- Hybrid mode (configuring standard and transparent mode on the same firewall)
- Default route failover
- Quality of Service (QoS)

- Transparent (bridged) mode for these configurations:
  - Dual-Box High Availability (DBHA)
  - Multi-application serialization
- DBHA active-active mode

  Active-standby DBHA is supported.

- Crossbeam X-Series Operating System (XOS) features:
  - Virtual Application Processor (VAP) group hide-vlan-header parameter
  - Equal-cost multi-path routing
  - Configuration of the VRRP MAC address

    If you need functionality similar to the VRRP MAC address, Crossbeam recommends configuring a user-defined MAC address on each traffic circuit/interface pair included in the VRRP failover group. See the Crossbeam support knowledge base article 0004069.

Compatible McAfee products

Firewall Enterprise is compatible with the following McAfee products.

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

For more information, see:

- **McAfee firewall products and versions that Firewall Enterprise supports** — KnowledgeBase article KB67462
- **Firewall products and interoperability with Firewall Enterprise** — Technical Note: *Using McAfee Firewall Enterprise with Other McAfee Products*

Requirements

Before you install this version, make sure the Admin Console and Firewall Enterprise requirements are met.

Admin Console requirements

The computer that hosts the Admin Console must meet these requirements.

Table 1-1 Admin Console minimum requirements

Component	Requirements	
Operating system	One of these Microsoft operating systems: • Windows Server 2008 • Windows 7 • Windows 8 These legacy Microsoft operating systems are compatible: • Windows XP Professional • Windows Vista	
Web browser	One of the following: • Microsoft Internet Explorer, version 6 or later • Mozilla Firefox, version 1.0 or later	
Hardware	• 2 GHz x86-compatible processor • 2 GB of memory • 300 MB of available disk space • CD-ROM drive	• 1024 x 768 display • Network card (to connect to your firewall) • USB port

Firewall Enterprise requirements

The firewall must meet these requirements.

Table 1-2 Minimum requirements by Firewall Enterprise type

Firewall type	Platform requirements
Firewall Enterprise appliance	Appliance with a valid support contract: • 1 GB of memory • AMD64-compatible processor
Firewall Enterprise, Virtual Appliance	Virtualization server: • **Hypervisor operating system** — VMware ESX/ESXi version 4.0 or later Firewall Enterprise, Virtual Appliance is installed in 64-bit mode by default. Your system must support Intel VT technology (or equivalent) to run properly in a virtual environment. Before starting the virtual appliance, verify that VT is enabled in your computer BIOS. • **Hardware resources**: • 2 virtual processors • AMD64-compatible processor • 1 GB of memory • 30 GB of free disk space • 2 or more NICs of type e1000 • **Internet connectivity** — The firewall requires a persistent Internet connection to maintain an active license and full functionality.
Firewall Enterprise on Crossbeam X-Series Platforms	Crossbeam X-Series Platform: • **Chassis** — X50, X60, or X80-S • **XOS version** — 9.6.5 and later, 9.7.1 and later, 9.9.x, or 10.0 • **Application Processor Module** — APM-50 or APM-9600 • At least one local disk (RAID 0 and RAID 1 disk configurations are supported; two-disk, non-RAID configurations are not supported) • 12 GB of memory (minimum) • **Network Processor Module** — NPM-50, NPM-86x0, or NPM-96x0 • **CBI package** — MFE-8.3.2-9.mr1.cbi

McAfee EIA requirements

Systems must meet these requirements to install McAfee® Endpoint Intelligence Agent (McAfee EIA).

Table 1-3 McAfee EIA minimum requirements

Component	Requirements
Operating system	One of these 32-bit or 64-bit Microsoft operating systems. • Windows XP Service Pack 2 and later • Windows 2012 • Windows 2012 R2 • Windows 8.1 • Windows 7 • Windows Server 2003 Service Pack 1 and later • Windows Server 2003 R2 Service Pack 1 and later • Windows Server 2008 • Windows Server 2008 R2
Hardware	• 2 GHz x86-compatible processor • 2 GB of memory • 300 MB of available disk space • 1024 x 768 display • Network card (to connect to your firewall) • One of the following: • USB port • CD-ROM drive
Other McAfee products	McAfee EIA deployment requires: • McAfee® Endpoint Intelligence Manager (McAfee EIM) version 2.2.0 • McAfee® ePolicy Orchestrator® (ePolicy Orchestrator) version 4.6.5, 5.x, and later • McAfee Agent version 4.8.0 patch 2 or later

Product resources

You can find additional information by using these resources.

Table 1-4 Product resources

Firewall type	Platform requirements
Online Help	Online Help is built into Firewall Enterprise. Click **Help** on the toolbar or from a specific window.
McAfee Technical Support ServicePortal	Visit support.mcafee.com to find: • Product documentation • KnowledgeBase • Product announcements • Technical support • Product installation files • Upgrades and patches For information about the Firewall Enterprise support life cycle, visit www.mcafee.com/us/support/support-eol.aspx.
Product updates	Visit support.mcafee.com and click the **Downloads** tab to get the latest Firewall Enterprise patches.

New features

This release of the product includes these new features.

Policy troubleshooting

The aconn command has been added as a policy troubleshooting tool to help you identify whether a connection is matching or skipping policy rules.

Enhancements

This release of the product includes these enhancements.

vMotion support

Virtual firewalls can be relicensed for the VMware vMotion feature.

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.

Admin Console

- Improves the port display for custom applications (909748)
- Allows customers to set the interface timeout value (937437)
- Displays IPv4 and IPv6 addresses in the **Blackholed IPs** window (961650)
- Changes Admin Console to core in /var/run/acd instead of a user's home directory (959910)

ARP

- Clears the arp cache for IPfilter and socket sessions when routes change (938420)

Audit and reporting

Improves:

- Handling of SmartFilter audits on Control Center-managed firewalls (901011)
- Logcheck processing if audit files are not present (931963)

Authentication

Improves:

- Handling of rechecks for Active Passport (917381)
- Active Passport processing when using external groups (934209)
- Authentication lockout handling (950185)

Configuration backup and restore

- Improves config restore handling of zero-byte named.conf files (955141)

Crossbeam

- Improves reporting of IPv6 status on Crossbeam X-Series Platforms (948570)

Daemons

- Improves efficiency of the utt_client (898466)

Disaster recovery

- Improves reliability of disaster recovery media (847203)

FIPS

- Adjusts certificate permissions in FIPS mode (938123)
- Allows Ciphers configuration while in FIPS mode (limited to FIPS certified algorithms) (954165)

High Availability

- Improves handling of:
  - Multicast traffic in HA pairs (819931)
  - Pending SNMP trap messages when HA pair members shut down (935104)
  - Large configurations when creating HA pairs (942030)
  - Interface change notifications during HA failover (945400)
- Clears the local IP cache as part of failover processing (950536)

Kernel

Improves:

- NAT and redirect support in IP Filter (837675)
- FTP connection tracking when using NAT (953807)

OpenSSL

- Adds a unique string to OpenSSL, see KB81790 (963047)

Other

- Adds ability to load Geo-Location updates from a file on the firewall (958335)
- Provides Global Threat Intelligence query statistics (961583)

Policy

- Improves:
  - Handling of rule name changes (928776)
  - Renaming of application groups (959566)
- Relaxes port validation for port agile applications (948934)

Proxy

- **HTTP**

Adds HTTP proxy improvements to:

  - HTTP proxy SSL content inspection (920910)
  - Sending of AV scanned POST requests to slow servers (938722)

- **H.323** — Improves handling of audio and video capabilities in H.323 connections (959014)
- **Oracle** — Improves Oracle proxy session handling during policy updates (895900)
- **SSL** — Adds SSL proxy improvements to increase SSL scanning stability (881316)

Routing

- Adds support for TCP-MD5 authentication to BGP (943292 and 943294)
- Improves route validation (954494)

Sendmail

Updates SID filter to whitelist domain names with trailing '.' (956802)

Servers

Improves SNMP stability (919975)

VPN

Improves:

- IPsec VPN processing (930647)
- Handling of IPsec Security Associations (961582)

Vulnerabilities - Common Vulnerabilities and Exposures (CVE)

OpenSSH

Addresses these CVEs:

- CVE-2014-2532 (956794)
- CVE-2014-2653 (958125)

OpenSSL

Addresses these CVEs:

- CVE-2014-0076 (956795)
- CVE-2014-0160 Heartbleed (959936, 961229)
- CVE-2010-5298 (961851)

Routing — Imports a change for CVE-2013-0149 to ease future maintenance; Firewall Enterprise is not vulnerable to CVE-2013-0149 (903973)

Installation instructions

You can perform a new installation or upgrade your firewall to 8.3.2P03.

> **Before you begin**
>
> If your firewall is at version 8.3.2 or 8.3.2P01, review these articles related to your installation path.
>
> - 8.3.2 to 8.3.2P03
>   - Patch 8.3.2P01 — KB79949
>   - Patch 8.3.2P02 — KB81115
> - 8.3.2P01 to 8.3.2P03 — Patch 8.3.2P02 — KB81115
>
> The DSCP pass-through feature was released with version 8.3.2P02; for more information, see KB81115 and the product guide.

Tasks

- *Perform a new installation* on page 9
  Installing version 8.3.2P03 on your firewall requires several high-level steps.
- *Upgrade a firewall* on page 10
  Follow the appropriate upgrade method for your firewall type.

Perform a new installation

Installing version 8.3.2P03 on your firewall requires several high-level steps.

Task

1. If you are installing over an existing firewall configuration, create a configuration backup.
2. Download the Firewall Enterprise software.
3. Download the appropriate documentation.
   - *McAfee Firewall Enterprise Product Guide*, version 8.3.2P03
   - *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*, version 8.3.x
   - *McAfee Firewall Enterprise Control Center Release Notes*, version 5.3.2P02 and *McAfee Firewall Enterprise Control Center Product Guide*, version 5.3.2

   > If your firewall is managed by Control Center, it must be at version 5.3.2P02 or later to manage firewalls at version 8.3.2P03.
4. Install the Management Tools.
5. Download and install the software.

Upgrade a firewall

Follow the appropriate upgrade method for your firewall type.

- **Standalone or HA cluster** — See the *McAfee Firewall Enterprise Product Guide*, version 8.3.2P03.
- **Control Center-managed firewall or HA cluster** — See the *McAfee Firewall Enterprise Control Center Release Notes*, version 5.3.2P02 and *McAfee Firewall Enterprise Control Center Product Guide*, version 5.3.2.

  > If your firewall is managed by Control Center, it must be at version 5.3.2P02 or later to manage firewalls at version 8.3.2P03.

- **Crossbeam X-Series Platforms firewall** — See the *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*, version 8.3.x.

Known issues

For a list of known issues in this product release, see this McAfee KnowledgeBase article: KB79061.

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

Every McAfee product has a comprehensive set of documentation.

McAfee Firewall Enterprise documentation includes:

Typical documents

- *McAfee Firewall Enterprise Product Guide*
- *McAfee Firewall Enterprise Release Notes*
- *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*
- *McAfee Firewall Enterprise Command Line Interface Reference Guide*
- Technical Note — *Using McAfee Firewall Enterprise with other McAfee products*
- Application Note — *Configuring Department of Defense Common Access Card Authentication on McAfee Firewall Enterprise*

Hardware

- *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*
- *McAfee Firewall Enterprise, Virtual Appliance Installation Guide*
- *McAfee Firewall Enterprise, Virtual Appliance Evaluation for Desktop Installation Guide*
- *McAfee Firewall Enterprise Quick Start Guide*

- *McAfee Firewall Enterprise Hardware Guide, models S4016, S5032, S6032, and S7032*
- *McAfee Firewall Enterprise Hardware Guide, models S1104, S2008, and S3008*

Certification

- *McAfee Firewall Enterprise Common Criteria Evaluated Configuration Guide*
- *McAfee Firewall Enterprise FIPS 140-2 Configuration Guide*
- *McAfee Firewall Enterprise FIPS 140-2 Level 2 Kit Installation Guide, S Models*

McAfee
An Intel Company