Release Notes

Revision B

McAfee Firewall Enterprise 8.3.2

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 8.3.2 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
- McAfee® Firewall Enterprise on CloudShield CS-4000 platforms

Unsupported features 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 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.
- 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.

Unsupported features on CloudShield CS-4000 platforms

When installed on CS-4000 platforms, some features are not supported on Firewall Enterprise.

- High Availability (HA)
- Sendmail
- Admin Console

  Firewall Enterprise must be managed using Control Center.
- Link aggregation and interface redundancy
- PPPoE
- USB disaster recovery and USB installation
- VCD and alternate slice

Installation options

These installation options are available.

- **New installation** — Re-image a firewall using installation media.
- **Upgrade** — Upgrade a firewall.

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® 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 XP Professional • Windows Vista • Windows 7 • Windows 8
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

Firewall Enterprise on CloudShield CS-4000 platforms	CloudShield CS-4000 platform: • **MC-CPOS server** — version 5.1 • **Chassis Management Module** — CMM-100 • **1/10G Ethernet Integrated Switch Module** — ISM-800 or ISM-XVR • **Content Processing Accelerator** — CPA-1000

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 above • Windows 7 • Windows Server 2003 Service Pack 1 and above • Windows Server 2003 R2 Service Pack 1 and above • 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 product	McAfee EIA deployment requires: • McAfee® ePolicy Orchestrator® (ePolicy Orchestrator) version 4.6.5 and later • McAfee Agent version 4.8.0 patch 1 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 mysupport.mcafee.com to find: • Product documentation • KnowledgeBase • Product announcements • Technical support For information about the Firewall Enterprise support life cycle, visit www.mcafee.com/us/support/support-eol.aspx.
Product updates	Visit go.mcafee.com/goto/updates to download the latest Firewall Enterprise patches.
Product installation files	1 Go to www.mcafee.com/us/downloads. 2 Provide your grant number, then navigate to the appropriate product and version.

New features

This release of the product includes these new features.

Administrator read-only role

The read-only role is now available for administrator accounts. Administrators can view all system information and run reports, but they cannot commit changes to any area of the firewall.

Firewall self-diagnosis

You can configure the firewall to identify, alert, or terminate processes that monopolize the CPU.

Only the processes managed by daemond can be terminated.

Enhancements

This release of the product includes these enhancements.

Application field in the audit

Where application detection is incomplete, the **Application** field now includes session begin and end events in the firewall audit. This reduces the number of application audit events labeled as unknown TCP, UDP, or other protocol.

FIPS update

These updates are supported and comply with FIPS 140.2 requirements.

- SHA2 hash function
- Enforcement of new algorithm and key size
- Larger asymmetric keys
- OpenSSL

URL filtering solution

McAfee® SmartFilter® (SmartFilter) remote management has been deprecated, and many of its features are incorporated in Firewall Enterprise.

USG IPv6 update

These updates comply with USGv6 requirements.

- The firewall can selectively block IPv6 packets based on next header values and other options.
- ICMP can be sent over IPv6 addresses.
- The firewall can block tunnels, such as IPv4 within IPv6 addresses.

File reputation in the audit

When McAfee EIA is enabled, the firewall can now audit executable file connections based on metadata sent by McAfee EIA and checked against McAfee® Global Threat Intelligence™ (McAfee GTI). An overall confidence score is calculated. The administrator can also manage an executable file classification list on the firewall. The firewall can be configured to respond to executable files with a malicious or unknown reputation.

On load-sharing or DBHA pairs, file reputation information is sent to the member that has established DTLS with the endpoint host.

AV and driver updates

- The firewall is compatible with the McAfee 5600 AV engine.
- The E1000 network interface drivers support Intel 1Gb Ethernet chipsets.
- The IX network interface drivers support Intel 10Gb Ethernet chipsets.

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.

This release includes over 250 resolved issues. The main resolutions are included here.

Admin Console

- Fixes an issue in cf_cmd parsing of key cache lifetime (839731)
- Resolves **Banner** window errors when clicking X (871901)
- Fixes an issue with the **Reset Default Route** button not working to restore the default route when change tickets were turned on (877606)
- Fixes an issue where the High Availability Monitor Link Status setting was enabled even though it was configured as disabled (886920)
- Resolves an issue with the Dashboard reporting more interfaces than are configured (888125)

Applications

- Resolves an issue where application discovery with a packet filter causes traffic to stop (793115)
- Resolves an issue where HTTPS was identified as NetBIOS NS (874603)
- Fixes an issue related to SmartFilter processing for late binding applications (835929)
- Resolves an issue of certain traffic allowed through the firewall irrespective of a deny rule (878000)

Audit/Reporting

- Resolves an issue where certain reports are not generated correctly using the cf reports command (791516)
- Fixes a traceback error message when navigating to the **Applications** window after startup (820011)

- Fixes an issue with the **Audit Viewing** window where the previous audit could not be viewed after an upgrade (876940)
- Resolves an issue where the policy report failed with a message, ordinal not in range (128) (881257)

Authentication

- Fixes an issue with the LDAP authenticator password appearing in clear text on the firewall policy report (880728)
- Fixes an authentication issue for the Remote Desktop Protocol (878299)

Configuration Subsystem

- Fixes an issue when adding IPv6 objects using the cf command, which caused those objects to expand (781579)
- Corrects an issue with the SmartFilter audit configuration that was giving a validation error in the Control Center Client (814030)

Daemons

- Resolves an issue where acld ran hot (100 percent of a thread) when followed by any configuration change (844163)
- Resolves an issue where the Admin Console took a long time pushing endpoint intersections to the firewall (892359)
- Resolves a continuous restart of auditdbd (892633)

HA

Fixes an issue in an HA master/slave configuration where changes made when the slave is the primary were overwritten when the master became the primary again (872194)

Kernel

- Resolves a buffer overflow issue in the igb and ixgbe drivers when the network comes up from a down state (842448)
- Fixes a kernel panic in an HA cluster (800247)
- Resolves an issue on Crossbeam X-Series Platforms where an APM becomes unresponsive (821304)
- Fixes a kernel panic with IP filter when a firewall is in an HA cluster (844905)
- Fixes a kernel panic when only one member of an HA cluster was defined and no cable was plugged in the heartbeat interface (895594)

Policy

- Improves the rule compiler performance for configurations that have hundreds of overlapping rules using authentication (838511)
- Resolves an issue where URL categories in the outbound rule do not work in the SSL rule (840497)
- Fixes an issue where McAfee GTI-enabled rules that were pushed from Control Center did not enable an implicit rule on the firewall, which is a McAfee GTI requirement (850210)

- Resolves an issue where the Deny and Drop rules did not match the traffic for addresses on the firewall (874124)
- Resolves an issue where policies cannot be changed when the policy contains a large number of IP address-based endpoints (884451)

Proxy

- **FTP**
  - Resolves an issue where the FTP completion message, "226 File sent OK," was not getting forwarded through the FTP proxy (790497)
  - Fixes an issue where the firewall received a bad port command in an FTP exchange and continued the connection (845335)
- **H323** — Fixes a NAT-related issue (832056)
- **HTTPS**
  - Fixes a memory leak in the HTTP proxy related to chunk encoding (763710)
  - Resolves an issue where HTTP proxy was blocking traffic due to the URL length even when the URL control was disabled (785424)
  - Fixes an issue with the HTTP proxy where the SmartFilter block page didn't display images every time (793585)
  - Resolves an issue where the non-transparent HTTP proxy waited until the AAAA timeout before completing an IPv4 connection (824999)
  - Fixes an auditing issue in an error scenario (840881)
  - Fixes an issue with HTTP multi-part boundary header processing (883218)
  - Fixes an issue where an HTTP request was sent to the wrong destination (891252)
- **ICMP** — Resolves an issue with the continuous restart and coring of the Ping proxy (845340)
- **SIP** — Fixes multiple issues in SIP proxy that were causing call establishment failures (851291)
- Fixes incorrect TCP timestamp information when TCP options were negotiated during session startup but not used during the session (875675)
- Fixes a download issue with the McAfee® Email and Web Security Spam update (818081)
- Resolves an issue with an unexpected response from the proxy and the AV scan (794847)

Servers

Resolves an issue where the DHCP Relay agent stops relaying messages (800976)

System

- Updates the number of default AV scanners in firewalls with 2 GB RAM (795512)
- Fixes an issue in the SmartFilter processing of late binding applications (875686)

VPN

Improves the stability of the IKE server when external authenticators are used (764894)

Installation instructions

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

Tasks

- *Perform a new installation* on page 10
  Install version 8.3.2 on your firewall.
- *Upgrade a firewall* on page 12
  Select the appropriate upgrade method for your firewall type.

Perform a new installation

Install version 8.3.2 on your firewall.

Tasks

- *Create a configuration backup* on page 10
  If you are installing over an existing firewall configuration, McAfee recommends that you create a configuration backup.
- *Download Firewall Enterprise software* on page 10
  Download the version 8.3.2 software.
- *Download Firewall Enterprise documentation* on page 11
  Download documentation necessary for the planning and setup process.
- *Install the Management Tools* on page 11
  Install the Management Tools on a Windows-based computer.

Create a configuration backup

If you are installing over an existing firewall configuration, McAfee recommends that you create a configuration backup.

When you perform a new installation on your firewall, all configuration and log information is removed. Backing up the configuration files lets you quickly restore a firewall. For instructions on creating a configuration backup, see the *McAfee Firewall Enterprise Product Guide*.

Download Firewall Enterprise software

Download the version 8.3.2 software.

Task

1 Go to http://www.mcafee.com/us/downloads.

2 Enter your grant number, then navigate to the appropriate product and version.

3 Download the appropriate files.

- **Firewall Enterprise appliance** — Download the installation CD image (.iso) file or USB image (.zip) file.

  

  Select the USB image file if your appliance does not have a CD drive.

- **Firewall Enterprise, Virtual Appliance** — Download the virtual image (.zip) file.
- **Firewall Enterprise on Crossbeam X-Series Platforms** — Download the Crossbeam installer (.cbi) file.

- **Firewall Enterprise on CloudShield CS-4000 Platforms** — Download the CPA-V template (.zip) file.
- **Management Tools** — If your firewall is not managed by Control Center, download the McAfee Firewall Enterprise Admin Console executable (.exe) file or CD image (.iso) file.

Select the CD image file if you want to create a CD for use in installing the Management Tools.

4 [Firewall Enterprise appliances only] Create physical installation media using the downloaded installation files.
   - Write the .iso file to a CD.
   - If you downloaded the USB image file, write the image to a USB drive. See the KnowledgeBase article KB69115 for instructions.

Download Firewall Enterprise documentation

Download documentation necessary for the planning and setup process.

Task

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

2 Under **Self Service**, click **Product Documentation**.

3 Select the appropriate product and version.

4 Download the *McAfee Firewall Enterprise Product Guide*.

5 For non-appliance platforms, download the appropriate documentation for your platform.
   - *McAfee Firewall Enterprise, Virtual Appliance Installation Guide*
   - *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*
   - *McAfee Firewall Enterprise on CloudShield CS-4000 Platforms Installation Guide*

Install the Management Tools

Install the Management Tools on a Windows-based computer.

The Management Tools include:

- **Quick Start Wizard** — Creates the initial configuration for the firewall
- **Admin Console** — Manages the firewall

Firewall Enterprise Management Tools are version-specific. You cannot connect to a version 8.x firewall using an older version of the Admin Console. However, you can have multiple versions of Management Tools that co-exist on the same Windows-based computer.

Task

1 Start the installation process:
   - If you downloaded the .exe file, locate the file on your computer, then double-click it.
   - If you downloaded the CD image (.iso) file and used it to create a CD, insert the CD into the appropriate drive.

   The welcome window appears.

2 Follow the on-screen instructions to complete the setup program.

McAfee recommends using the default settings.

Consider installing an SSH client on your computer. Use the SSH client to provide secure command line access to the firewall.

Upgrade a firewall

Select the appropriate upgrade method for your firewall type.

Before you begin

- Your firewall must be at version 8.3.1.
- [Virtual appliances only] Your system must support Intel VT technology (or equivalent). Verify that VT is enabled in your computer BIOS.

If you have a 32-bit hardware appliance that does not support 64-bit processing, an upgrade to version 8.3.2 is not supported.

Tasks

- *Upgrade a standalone firewall or HA cluster* on page 13
  Use the Admin Console to upgrade a standalone firewall or HA cluster
- *Upgrade a Control Center-managed firewall or HA cluster* on page 16
  Use Control Center to upgrade managed firewalls and clusters.
- *Upgrade a firewall on a Crossbeam X-Series Platform* on page 17
  Upgrade Firewall Enterprise on a Crossbeam X-Series Platform.

Preparing your policy

Firewall Enterprise has enhanced policy validation to detect policy and rule configuration issues that could lead to indeterminate or incorrect policy enforcement of network traffic.

The updated policy validation checks for SNMP host or domain objects and agent port conflicts can cause existing policy configurations to fail when upgrading, causing the patch installation to fail.

Select one of these methods to review your policy.

Table 5-1 Policy review options

Review your policy before upgrading	Review your policy while upgrading
Take precautionary steps to prevent upgrade failure. • Verify that no SNMP Agent rules are using host or domain objects as endpoints. • Verify that there are no port conflicts between rule agents in each zone. Port conflicts occur when there are multiple policy rules that make use of different applications representing the same traffic but with different agent properties in the same zone. A common example is SSH traffic. A generic custom application (resolving to the HTTP proxy) on TCP port 22 cannot be used in the same zone as the SSH application (resolving to the SSH Proxy). With complex policy configuration, it might be more efficient to attempt the upgrade and resolve the affected rules identified in the package log.	Prepare for extended downtime to run the upgrade and validate the policy. 1 Run the upgrade. 2 Resolve the policy validation failures in the package or patch log, and modify the identified policy rules. 3 Complete the patch installation.

Upgrade a standalone firewall or HA cluster

Use the Admin Console to upgrade a standalone firewall or HA cluster

To upgrade an HA cluster, upgrade the secondary/standby firewall first, then upgrade the primary firewall.

Tasks

- *Create a configuration backup* on page 13
  If you are installing over an existing firewall configuration, McAfee recommends creating a configuration backup.
- *Download the package on a firewall with Internet access* on page 14
  If your firewall has Internet connectivity, use the Admin Console to download the patch.
- *Manually load the package on a firewall without Internet access* on page 14
  If your firewall is not connected to the Internet, use a web browser to download the package, then manually load the package on the firewall.
- *Install the upgrade package* on page 15
  Install the upgrade package on your firewall. This package also includes a separate Admin Console update.
- *Verify the installation* on page 15
  Verify that the software is installed on your firewall.
- *Perform patch rollback* on page 16
  If the installed patch does not work to your satisfaction, you can use the Rollback feature to restore the firewall to a previous state.

Create a configuration backup

If you are installing over an existing firewall configuration, McAfee recommends creating a configuration backup.

When you perform a new installation on your firewall, all configuration and log information is removed. Backing up the configuration files lets you quickly restore a firewall.

See the *McAfee Firewall Enterprise Product Guide* for complete details.

Download the package on a firewall with Internet access

If your firewall has Internet connectivity, use the Admin Console to download the patch.

Downloading the patch moves it from the McAfee FTP site to the firewall but does not install it.

Task

For option definitions, press **F1** or click **Help** in the interface.

1 Select **Maintenance** | **Software Management**.

2 Click the **Manage Packages** tab.

3 Display the available packages.

   a Click **Check for Updates**. When the operation is complete, a pop-up window appears.

   b Click **OK**. Packages appear in the table with a status of *Available*. These packages are available for downloading from the McAfee FTP site.

To configure this action to occur automatically, use the **Download Packages** tab.

4 Select the upgrade package, then click **Download**. Click **Yes** to confirm.

   A success message appears, and the package status changes to *Loaded*.

Manually load the package on a firewall without Internet access

If your firewall is not connected to the Internet, use a web browser to download the package, then manually load the package on the firewall.

Task

1 Use a web browser to download the upgrade package.

   a Go to go.mcafee.com/goto/updates.

   b Scroll down to the McAfee Firewall Enterprise **Upgrades and Patches** entry for the current version, then click **Download**.

   c Enter a valid Firewall Enterprise serial number, then click **Submit**.

   d Click **Download Patch**.

2 Place the upgrade file where the firewall can access it. Choose one of these options:

- **Local FTP site** — Place the package on an FTP site that the firewall has access to.
- **HTTPS website** — Place the package on an HTTPS website that the firewall has access to.
- **CD** — Place the package in a /packages directory on a CD, then insert the CD into the firewall CD drive.
- **Directory on the firewall** — Use SCP to copy the package to the /home directory of your firewall administrator account.

To transfer files to the firewall using SCP, SSH access must be enabled on the firewall.

3 In the Admin Console, select **Maintenance** | **Software Management**, then click the **Download Packages** tab.

For option descriptions, click Help.

4 Click **Perform Manual Load Now**. The **Manual Load** window appears.

5 Specify where the upgrade package is stored.

a From the **Load packages from** drop-down list, select the appropriate method to load the package.

- **FTP** — Package is on a local FTP site
- **HTTPS** — Package is on an HTTPS website
- **CD-ROM** — Package is contained on a CD you created
- **File** — Package is copied to your home directory on the firewall

b In the **Packages** field, type `8.3.2`.

c Complete the remaining fields.

d Click **OK**. A confirmation message appears.

6 Click **Yes**. The firewall loads the package from the specified location. When the operation is complete, a message appears.

7 Click **OK**.

8 Verify that the patch loaded on your firewall.

a Click the **Managed Packages** tab.

b Verify that the **Status** column for the package shows *Loaded on <date>*.

Install the upgrade package

Install the upgrade package on your firewall. This package also includes a separate Admin Console update.

The firewall will restart during the patch installation.

Task

For option definitions, press **F1** or click **Help** in the interface.

1 Select **Maintenance** | **Software Management**.

2 Click the **Manage Packages** tab.

3 Select the version from the list of packages, then click **Install**.

4 Select **Install now**, then click **OK**.

A warning appears stating that the firewall will restart after the patch is installed.

5 Click **Yes**.

The package is installed, then an error message appears stating that the connection to the server has been lost.

6 Click **OK**.

The Admin Console is disconnected and the firewall restarts.

Verify the installation

Verify that the software is installed on your firewall.

Task

For option definitions, press **F1** or click **Help** in the interface.

1. Reconnect the Admin Console to the firewall.
2. Select **Maintenance** | **Software Management**.
3. In the **Manage Packages** tab, verify that the **Status** column for the version shows *Installed*.
   - If the patch status is still *Loaded*, call technical support.
   - You can also click **View Package Details** or **View Log** to see information about the installation.

The patch is now installed.

Perform patch rollback

If the installed patch does not work to your satisfaction, you can use the Rollback feature to restore the firewall to a previous state.

If you use the Rollback feature, any configuration changes made after the patch was installed are lost. Therefore, rolling back is a recommended recovery option for only a short time after a patch installation.

A rollback always requires a restart.

Task

For option definitions, press **F1** or click **Help** in the interface.

1. Select **Maintenance** | **Software Management**.
2. Click the **Rollback** tab.
3. Click **Rollback Now**, or select **Schedule Rollback for** to schedule a time for the rollback.

Upgrade a Control Center-managed firewall or HA cluster

Use Control Center to upgrade managed firewalls and clusters.

Do not use the Firewall Enterprise Admin Console to install a patch directly on a managed firewall.

Follow these steps to upgrade your CloudShield CS-4000 platform firewall.

Task

1. Upgrade your Control Center to version 5.3.2 or later; see the *McAfee Firewall Enterprise Control Center Release Notes*, version 5.3.2.
2. Use Control Center to upgrade the managed firewall to version 8.3.2; see the *McAfee Firewall Enterprise Control Center Product Guide*.

Upgrade a firewall on a Crossbeam X-Series Platform

Upgrade Firewall Enterprise on a Crossbeam X-Series Platform.

Tasks

- *Upgrade Control Center* on page 17
  Upgrade Control Center to version 5.3.2 or later; see the *McAfee Firewall Enterprise Control Center Release Notes*.
- *Upgrade or install your Crossbeam X-Series Platform* on page 17
  Make sure you are running a supported version of XOS.
- *Install the Firewall Enterprise CBI package* on page 17
  Download the Firewall Enterprise CBI package and load it on your Crossbeam X-Series Platform.

Upgrade Control Center

Upgrade Control Center to version 5.3.2 or later; see the *McAfee Firewall Enterprise Control Center Release Notes*.

Upgrade or install your Crossbeam X-Series Platform

Make sure you are running a supported version of XOS.

Select one of these options:

- Upgrade to the latest 9.6.x or 9.7.1 or later version of XOS.
- Perform a new installation of the latest 9.9.x version of XOS.

See the *Crossbeam XOS Configuration Guide*.

Install the Firewall Enterprise CBI package

Download the Firewall Enterprise CBI package and load it on your Crossbeam X-Series Platform.

This procedure updates the Firewall Enterprise CBI that is present on the CPM, which is used to provision new VAPs. Performing this procedure will not modify firewall VAPs that are already installed.

Task

1. Download the Firewall Enterprise CBI package.
   a. In a web browser, navigate to www.mcafee.com/us/downloads.
   b. Enter your grant number, then navigate to the appropriate product and version.
   c. Download the Crossbeam installer (.cbi) file for the version.
2. Transfer the .cbi file to the /crossbeam/apps/archive directory on each X-Series CPM.
3. Run the following command for the firewall VAP group:

   ```
   CBS# application-upgrade mfe vap-group <VAP_group_name>
   ```

4. Accept the prompts.

Known issues

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

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

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 on CloudShield CS-4000 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 S4016, S5032, S6032, and S7032 Hardware Guide*
- *McAfee Firewall Enterprise S1104, S2008, and S3008 Hardware Guide*

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*

B00