Release Notes

McAfee® Firewall Enterprise (*Sidewinder*®)

version 7.0.1.03

This document provides information about McAfee® Firewall Enterprise (*Sidewinder*®) version 7.0.1.03, including download and installation instructions.

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

Table 1 Product resources

Resource	Location
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
Product updates	Visit go.mcafee.com/goto/updates to download the latest Firewall Enterprise patches.
Product installation files	**1** In a web browser, navigate to www.mcafee.com/us/downloads. **2** Provide your grant number, then navigate to the appropriate product and version.

In this document ...

About this release

Firewall Enterprise version 7.0.1.03 enhances Common Access Card authentication, High Availability, and SNMP. This release also resolves issues present in the previous release.

Firewall Enterprise version 7.0.1.03 will be supported for one year after the next feature release.

Note: At this time, there is no upgrade option available from version 7.0.1.03 to version 8.x. However, McAfee intends to release this upgrade path in the future.

Supported firewall types

Any Firewall Enterprise at version 7.0.1.02 can be upgraded to version 7.0.1.03. The following firewall types are supported:

- McAfee® Firewall Enterprise appliances
- McAfee® Firewall Enterprise, Virtual Appliance
- McAfee® Firewall Enterprise on Riverbed Services Platform

Compatible McAfee products

Firewall Enterprise version 7.0.1.03 is compatible with the following McAfee products:

- McAfee® Firewall Enterprise Control Center
- McAfee® Firewall Profiler
- McAfee® Firewall Reporter

Note: To find the latest information on the McAfee firewall products and versions that Firewall Enterprise supports, refer to KnowledgeBase article KB67462.

Requirements

Before you install version 7.0.1.03, 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 2 Admin Console minimum requirements

Component	Requirements
Operating system	• Microsoft Windows Server 2008 • Windows Server 2003 • Windows 7 • Windows Vista • Windows XP Professional
Web browser	• Microsoft Internet Explorer version 6 or later • Mozilla Firefox version 1.0 or later
Hardware	• 1 GHz x86-compatible processor • 512 MB of system memory • 300 MB of available disk space • CD-ROM drive • 1024 x 768 display • Network card • USB port

Firewall Enterprise requirements

The firewall must meet these requirements.

Table 3 Minimum requirements by type

Firewall type	Platform requirements
Firewall Enterprise appliance	D model appliance or later with a valid support contract
Firewall Enterprise, Virtual Appliance	Virtualization server that meets the following requirements: • **Hypervisor operating system** — VMware ESX/ESXi version 4.0 or later • **Hardware resources**: • Two virtual processors • 512 MB of memory • 28 GB of drive space Note: If you plan to use features such as virus scanning or sendmail, increase the allocated memory to 1024 MB. • **Internet connectivity** — The firewall requires a persistent Internet connection to maintain an active license and full functionality.
Firewall Enterprise on Riverbed Services Platform	Riverbed Steelhead appliance that meets the following requirements: • RiOS version 6.0 or later • RSP version 6.0 or later installed and licensed • Available RSP slot • 512 MB of free memory • 28 GB of free disk space

Enhancements

Firewall Enterprise version 7.0.1.03 provides the following enhancements.

Common Access Card

Provides the following enhancements to Common Access Card (CAC) authentication:

- Certificate validation of CAC credentials
- Certificate status checking using OCSP (Online Certificate Status Protocol)

  Note: Certificate status checking by means of certificate revocation lists (CRLs) for CAC credentials is not supported.

High Availability

Reduces cluster firewall restarts caused by HA configuration changes

SNMP agent

Enhancements include:

- Full support for SNMP version 3
- Support for SHA (authentication) and AES (privacy) attributes for SNMP v3 users

Note: SNMP v3 authentication and encryption uses localized secret keys. These keys are configured with the authentication algorithm, password, and privacy password for each user. For security reasons, the plain text password is not stored on the firewall. As a result, whenever the authentication algorithm changes, you must re-enter the password or create a new password. Consider this to avoid authentication errors when you attempt to access the agent and when authenticated traps are sent.

Resolved issues

This release resolves the following issues.

Admin Console

- Resolves issues on the High Availability window:
  - Removes prompts to restart cluster firewalls after modifying certain non-heartbeat interface parameters
  - Addresses configuration issues for heartbeat verification
  - Fixes Auto-Recover On Reconnect functionality
  - Resolves faild errors when adding a new interface and HA cluster promotion
- Resolves a faild error after saving policy with Control Center
- Resolves issues that caused services to fail on load-sharing HA cluster firewalls
- Corrects the memory usage calculation on the Dashboard
- Corrects miscellaneous Firewall Policy Report issues
- Resolves Admin Console connectivity and response issues
- Fixes validation of password changes and permissions
- Resolves performance issues when viewing and modifying policy
- Fixes a problem that prevented selected generic proxy instance from being restarted
- Fixes an issue that prevented configuration backups from being saved to a remote system
- Fixes an issue that caused the Service Status window to display incorrect status for multiple services while restarting a service
- Fixes a configuration issue for the SunRPC proxy timeout value
- Fixes a problem for adminro users that displayed an incorrect mask for subnet network objects
- Fixes a problem that caused an error when opening the TrustedSource window
- Fixes a problem that prevented Admin Console from working with certificates of long key lengths

Audit and Reporting

- Fixes incorrect auditing of TCP “reset out of window”
- Resolves an issue that could cause an incorrect packet filter rule name to be audited
- Improves auditing for DNS queries
- Corrects an issue that prevented the firewall from sending syslog data to a server in a different subnet
- Improves the SmartFilter® warning mechanism for malicious file downloads
- Resolves a problem that prevented correct auditing of SNMP proxy traffic
- Enhances Syslog facilities
- Adds LCB information to the configuration change reports
- Enhances auditing for traffic that originates from the firewall
- Resolves a problem that prevented the firewall from pushing policy to McAfee® Firewall Profiler during initial configuration

- Prevents the administrator from disabling auditd and acld because both daemons are required to audit traffic
- Resolves a problem that caused the cf reports command to show incorrect data
- Corrects an error when exporting audit data to XML format
- Updates the man page for the acat_acls utility
- Enhances acat to include rule names for proxies when converting to webtrends
- Improves error reporting from cf proxy when restarting an agent
- Resolves an issue that caused the password entered to be shown in audit after the maximum retries was reached
- Fixes a problem that caused cf export transfers to fail
- Resolves an issue that caused rollaudit to repeatedly compress the same file
- Enhances audit to log RAID events
- Fixes zombie file issues that occur after rolling the audit
- Addresses audit errors during virus scanning configuration changes

Authentication

- Resolves CAC authenticator issues:
  - Corrects support for ASN.1
  - Resolves HTTPS issues on load-sharing High Availability clusters
  - Resolves a problem that caused CAC to audit incorrectly while trying to get a one-time password
  - Fixes a problem that caused CAC authentication to fail for SSHD
- Resolves a problem that prevented valid logon attempts when entering emergency maintenance mode
- Resolves a problem that caused user to change password using Admin Console
- Fixes a problem that caused OCSP to give incorrect response
- Fixes a problem that prevented the firewall from passing traffic when a client sent HTTP traffic in non-transparent mode with an authentication request

Configuration backup

- Addresses configuration backup and rollback issues
- Fixes a problem that prevented configuration backups from being saved to USB
- Resolves a problem that causes the Admin Console to hang while a configuration backup is being saved

Firewall-hosted DNS

- Resolves named-internet restart issues
- Adds cryptography and Dnssec Lookaside Validation (DLV) support

High Availability

- Resolves an ARP flush issue during HA promotion and deletion
- Improves handling of traffic when the cluster firewall passing the traffic is restarted
- Resolves a policy synchronization issue between cluster firewalls
- Addresses policy translation issues
- Resolves FTP failover issues
- Resolves issues during failover releases from one cluster firewall to another
- Resolves policy creation, configuration synchronization, and connectivity issues
- Fixes a kernel lock ordering issue on load-sharing HA clusters
- Resolves a problem that could cause the primary firewall in a peer-to-peer cluster to restart unexpectedly
- Resolves faild invalid region errors
- Resolves cluster creation and demotion issues for peer-to-peer HA clusters
- Resolves an issue registering a secondary firewall with the primary
- Corrects cluster IP, remote ping test, and IP aliases issues
- Corrects MAC address validation
- Enhances auditing for errors when modifying cluster interfaces
- Resolves issues with unmonitored interfaces and HA-related failover address information
- Enhances status details for interfaces in the output of the cf failover status command
- Addresses issues related to gratuitous ARP
- Fixes a problem that caused firewall-hosted DNS (BIND) to run on a secondary firewall even though transparent DNS was configured
- Replicates zone data files across HA cluster firewalls

IPS

- Corrects miscellaneous IPS issues
- Improves IPS performance
- Uploads PCRE IPS signature files to Control Center
- Fixes a problem that prevented custom IPS signatures from being uploaded to Control Center during policy retrieve

Miscellaneous

- Resolves health monitor issues for appliance model S2008
- Addresses memory and partition issues
- Corrects issues related to packaging, tapered scripts, and licensing
- Resolves a problem that caused the ccfwadmin user to be in more than one role after registering to Control Center
- Fixes a problem that caused NICID command to shut down the interfaces on exit
- Corrects an error when modifying the hardware device on an IPv6 interface in router mode

- Fixes a problem that caused default route learned through ospfd to disappear after adding a static route
- Addresses various scanner issues
- Corrects netstat and systat traffic report statistics
- Corrects a FIN after window data corruption issue
- Addresses a kernel page fault during latency test
- Fixes forced kernel core dump generation using break sequence from the serial console
- Fixes an issue that prevented a static route from being added when a disabled interface was configured for the same subnet
- Fixes netstat -rn output overflows for “Use” value
- Resolves a buffer overrun in IPV6 route lookup
- Fixes stateless NAT and redirection for IPv4
- Corrects an issue that prevented the IP TTL from being decremented, causing network slowdowns
- Fixes the output of the netstat -ni command

Packet filter

- Adds support for source port NAT with redirection
- Resolves a checksum error for the FTP packet filter with NAT or redirection enabled
- Allows multicast and TTL=1 traffic in transparent packet filter mode
- Corrects a packet filter rule issue for burbs with indexes larger than 32
- Fixes an issue that caused packet filter absorb rules for server services to allow other types of traffic

Policy

- Allows netmaps to be used in stateless bidirectional rules
- Resolves a problem that prevented firewall from handling DNS host objects with more than 36 addresses
- Resolves VLAN configuration and validation issues
- Resolves configuration issues for rules and Application Defenses
- Resolves issues related to GRE traffic
- Removes the length limit for custom FTP commands
- Resolves an issue that caused a rule remnant to prevent firewall from being re-registered to Control Center
- Fixes a problem that caused renaming netgroup objects to fail

Proxies

- Corrects socket mating issues
- Resolves an acld performance degradation
- Corrects issues with cleaning up TCP connections
- Corrects an issue that increased the time required to restart proxy services

Citrix proxy

Corrects audit issues

FTP proxy

Corrects handling of some FTP commands

H323 proxy

- Resolves issues with invalid packets
- Corrects issues with transparent interfaces
- Supports neighbor gatekeepers

HTTP proxy

- Resolves redirect and HTTPS issues for non-transparent HTTP
- Resolves issues with TrustedSource™
- Corrects miscellaneous issues related to multipart headers, virus scanning, HTTP timers, tokens, and long URLs
- Addresses memory and performance degradation issues
- Corrects handling of FTP over HTTP/1.0
- Corrects an error caused by the combination of Passport and verbose ACL auditing
- Addresses HTTPS issues with VeriSign certificates

Oracle proxy

Corrects an issue that caused transparent connections to be denied

Ping proxy

Resolves issues with ICMP echo replies on load-sharing High Availability clusters

SIP proxy

Corrects handling of some SIP headers

SNMP proxy

- Corrects performance degradation caused by configuration changes
- Fixes an SNMP proxy hang that occurs after policy push

SMTP proxy

- Resolves issues with malformed “from” headers
- Corrects issues with SMTP commands such as size and bdat
- Resolves issues related to buffering, percent hack, memory overwrite, and transparent mail

SSH proxy

- Resolves a performance degradation issue with weak SSH keys
- Corrects issues related to X11 forwarding, large file transfer, and transparent interfaces

Sun RPC proxy

Corrects idle timeout behavior

Security updates

- Addresses FreeBSD security advisories
- Addresses CVE-2009-0696, CVE-2009-4022, CVE-2010-0097, CVE-2010-3613, VU#418861, and VU#360341 for firewall-hosted DNS (BIND)
- Resolves CVE-2010-0405 for bzip2
- Resolves CVE-2010-4180 for sendmail
- Addresses VU#435052 for HTTP
- Resolves a DHCP client vulnerability
- Addresses CPNI-957037 for Open SSH
- Resolves CVE-2010-2948 and CVE-2010-2949 for bgpd in Quagga
- Resolves CVE-2009-3563 for NTP

SNMP agent

Resolves an SNMPv3 authentication issue in FIPS mode

VPN

- Adds a method to allow administrators to view the VPN passwords
- Fixes a problem that caused the firewall to perform NAT-T when NAT-T was disabled
- Fixes an issue that caused lookup of INFO_V2 exchange state to fail
- Fixes a problem that prevented traffic from going over the VPN tunnel

Known issues

For information about known issues for Firewall Enterprise version 7.0.1.03:

1. Visit mysupport.mcafee.com.
2. Log on with your user ID and password. The ServicePortal homepage appears with a welcome message at the top.
   - If you do not have an account but have received a grant number:
     - In the User Login section, click **New User**.
     - Complete the information and follow the prompts to set up your account.
   - If you do not have an account or grant number, contact Customer Service.
3. In the Self Service section, click **Search the KnowledgeBase**. The KnowledgeBase welcome page appears.
4. In the Ask a Question section, type **KB71899**, then click **Ask**. The KnowledgeBase article appears with any known issues.

Upgrade from version 7.0.1.02 to 7.0.1.03

Select the upgrade method that is appropriate for your firewall type.

- *Upgrade a standalone firewall or HA cluster*
- *Upgrade a Control Center-managed firewall or HA cluster*

Note: Your firewall must be at version 7.0.1.02 to upgrade to version 7.0.1.03 as described in this section.

Upgrade a standalone firewall or HA cluster

Use the Admin Console to upgrade a standalone firewall or HA cluster to version 7.0.1.03. Perform these tasks in order:

1. *Create a configuration backup*
2. *Download the 7.0.1.03 package*
3. *Install the 7.0.1.03 package*
4. *Update the Admin Console*
5. *Verify the installation*

Note: To upgrade a High Availability cluster, upgrade the secondary/standby firewall first, then upgrade the primary firewall.

Create a configuration backup

McAfee recommends that you create a configuration backup before upgrading. Backing up the configuration files lets you quickly restore a firewall.

For instructions on creating a configuration backup, refer to the *McAfee Firewall Enterprise Administration Guide*.

Download the 7.0.1.03 package

Perform the appropriate procedure to download the 7.0.1.03 package.

- If your firewall has Internet connectivity, follow the steps under *Download the package using the Admin Console*.
- If your firewall does not have Internet connectivity, follow the steps under *Manually load the package*.

Download the package using the Admin Console

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

To download the patch from the network:

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.

   Tip: To configure this action to occur automatically, use the Download Packages tab.
4. Select the **7.0.1.03** package, then click **Download**. Click **Yes** to confirm.

   A “successfully loaded” message appears, and the package status changes to *Loaded*.

Manually load the package

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.

1. Use a web browser to download the 7.0.1.03 package.
   - a Go to go.mcafee.com/goto/updates.
   - b Scroll down to the McAfee Firewall Enterprise Upgrades and Patches entry for version 7.0.1.03, then click **Download**.
   - c Enter a valid Firewall Enterprise serial number, then click **Submit**.
   - d Click **Download Patch** for version 7.0.1.03.
2. Place the 7.0.1.03 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-ROM drive.
   - **Directory on the firewall** — Use SCP to copy the package to the /home directory of your firewall administrator account.

     Note: 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. The Download Packages tab appears.

   Tip: For option descriptions, click **Help**.
4. Click **Perform Manual Load Now**. The Manual Load window appears.
5. Specify where the 7.0.1.03 package is stored.
   - a From the **Load packages from** drop-down list, select the appropriate method to load the package.
     - **FTP** — Select if you placed the package on a local FTP site
     - **HTTPS** — Select if you placed the package on an HTTPS website
     - **CDROM** — Select if you created a CD that contains the package
     - **File** — Select if you copied the package to your home directory on the firewall
   - b In the **Packages** field, type **7.0.1.03**.
   - c Complete the remaining fields as appropriate.
   - 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 7.0.1.03 is loaded on your firewall.
   - a Click the **Manage Packages** tab.
   - b Verify that the Status of the 7.0.1.03 package is *Loaded on <date>*.

Install the 7.0.1.03 package

Perform this procedure to install the 7.0.1.03 package on your firewall. This package also includes a separate Admin Console update.

Note: The firewall will restart during the patch installation.

To install this patch on your firewall from the Admin Console:

1. Select **Maintenance | Software Management**.
2. Click the **Manage Packages** tab.
3. Select **7.0.1.03** 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.

Update the Admin Console

After the firewall restarts, update the Admin Console by connecting to the firewall.

1. Reconnect the Admin Console to the firewall.

   A message appears prompting you to install an Admin Console update.
2. Click **Yes**.

   The Admin Console update downloads, then a message appears asking if you want to install the package now.
3. Click **Yes**.

   The Admin Console closes and the InstallShield Wizard window appears.
4. Click **Next**.

   A progress bar appears while the Admin Console update installs. When the installation completes, the Update Complete window appears.
5. Click **Finish**. The Admin Console opens.

Verify the installation

After the Admin Console update completes, verify that version 7.0.1.03 is installed on your firewall.

1. Reconnect the Admin Console to the firewall.
2. Select **Maintenance | Software Management**.
3. On the Manage Packages tab, verify that the status for **7.0.1.03** is *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.

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.

Caution: 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.

Note: A rollback always requires a restart.

To restore the firewall to a previous state:

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 firewalls managed by Control Center.

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

1. Upgrade your Control Center to version 5.1.2 or later. For instructions, see the *McAfee Firewall Enterprise Control Center Release Notes*.
2. Use Control Center to upgrade the managed firewall to version 7.0.1.03. For instructions, see the *McAfee Firewall Enterprise Control Center Product Guide*.

For support information, visit mysupport.mcafee.com.

700-3292A00