Release Notes

Revision A

McAfee Web Gateway

7.3

This document provides information about the McAfee® Web Gateway 7.3 appliance software.

You can find more information at the following locations:

- **Help** — Help is built into McAfee Web Gateway. Click the Help icon in the upper right corner of the user interface.
- **Support** — Visit mysupport.mcafee.com to find product documentation, announcements, and support.

In this document ...

About this release

McAfee Web Gateway version 7.3 is provided as a controlled release. It introduces new features and enhancements, and resolves issues present in previous releases.

For information on setting up and administering an appliance, see the *McAfee Web Gateway Product Guide* at mysupport.mcafee.com.

New and enhanced features

The following new and enhanced features are included in this release.

Setup wizard

A setup wizard guides you in setting up the appliance after you have logged on for the first time.

Guidance is provided for the following two activities:

- Import a license
- Initially download filtering modules and patterns for malware recognition

We do not recommend using the option to perform additional administration activities before the modules and patterns are downloaded.

For more information, see the *Setup* chapter of the *McAfee Web Gateway Product Guide*.

Organized rule set library

Organization of the rule set library on the appliance has been improved by grouping the rule sets into a small number of rule set categories and displaying them on the user interface accordingly.

For example, rule sets that deal with URL filtering, such as the URL Filtering rule set or the Global Whitelist rule set, appear now in the *URL Filter* category, rule sets dealing with authentication matters appear in the *Authentication* category, and so on.

For each rule set, a description has also been added.

For more information, see the *Rules* chapter of the *McAfee Web Gateway Product Guide*.

Seamless MCIM authentication

The McAfee Web Gateway appliance can be configured to work as one of the services that perform user authentication for McAfee® Cloud Identity Manager (MCIM).

The two web security products work together in a single-sign-on authentication process, where McAfee Web Gateway handles the authentication and the user is spared the effort of authenticating to both security products.

For more information, see the *Authentication* chapter of the *McAfee Web Gateway Product Guide*.

Payload Heuristics

Virus and malware filtering on the appliance has been enhanced to support the highly efficient heuristics known as Payload Heuristics, which are applied by one of the anti-malware modules.

A watermark is added to a URL if it serves as a link to an executable file or other types of media. The watermark is removed before the URL is passed on to the appropriate web server.

For more information, see the *Web Filtering* chapter of the *McAfee Web Gateway Product Guide*.

More granular error messages for virus and malware filtering

Information on errors in virus and malware filtering is provided in a more granular manner, as three messages for specific errors have been added, covering the following error situations:

- Timeout occurred
- Update prevents filtering
- Scanning failed

The general message for internal errors in virus and malware filtering has been kept.

For more information, see the *Configuration lists* chapter of the *McAfee Web Gateway Product Guide*.

IFP support

The proxy functions on the appliance have been extended to include settings for implementing an IFP (Internet Filtering Protocol) proxy. Using this proxy, URL filtering can be performed on requests to web access that are submitted under this protocol.

Filtering activities for IFP requests are displayed on the dashboard of the user interface. Connection tracing can also be performed for these activities.

For more information, see the *Web Filtering* chapter of the *McAfee Web Gateway Product Guide*.

Application control for individual functions

Application control can now be configured to block one or more individual functions of an application, without blocking the complete application.

For more information, see the *Web Filtering* chapter of the *McAfee Web Gateway Product Guide*.

Localization of user message templates

Message templates for informing users about their web access requests are now available in the following languages: English, French, Spanish, German, Italian, Japanese, Chinese (Simplified), and Chinese (Traditional).

For more information, see the *User messages* chapter of the *McAfee Web Gateway Product Guide*.

Additional options for the REST interface

The internal REST (Representational State Transfer) interface enables you to complete administration activities on the appliance without being logged on to its user interface.

In addition to already existing options, the following can now be performed:

- Configure policy settings
- Configure action and engine settings
- Handle complex lists more comfortably
- Enable, disable, move, delete, import, and export rule sets
- Trigger automatic yum updates and engine updates
- Perform manual engine updates

For more information, see the *REST interface* chapter of the *McAfee Web Gateway Product Guide*.

Upgrade to MLOS2

The version of the operating system on the McAfee Web Gateway appliance has been upgraded to MLOS2 (McAfee Linux Operation System 2).

This version is also used by other Linux-based McAfee security products, for example, by McAfee Email Gateway, which reduces learning effort for administrators who are responsible for two or more of these products.

For more information, see the *Introduction* of the *McAfee Web Gateway Product Guide*.

G8 blade server support

The range of blade servers that can be used for McAfee Web Gateway to run on has been extended to include Romley-based HP G8 blade servers.

For more information, see the *Blade server* chapter of the *McAfee Web Gateway Product Guide*.

Email Gateway to Web Gateway migration tool

A tool is provided to assist you with migrating from McAfee® Email and Web Security to McAfee Web Gateway.

The tool uses a backup of a McAfee Email and Web Security configuration to migrate settings and lists to make them available to the McAfee Web Gateway rules while McAfee Email and Web Security rules are not migrated.

Resolved issues

The following issues have been resolved since the release of McAfee Web Gateway 7.2. (Bugzilla reference numbers are in parentheses.)

Issues with headers, routing, and other protocol-related matter

- Processing requests under HTTP failed several times when the web cache was used and HTTP tunneling enabled. (761760)
- When an IP address could not be resolved, a *Virus found* message was displayed to the user instead of an *Unresolvable* message due to internal problems with reading long IP address lists containing addresses in both IPv4 and IPv6 format. (762213)
- When a Yahoo proxy had been set up, all traffic, including authentication and keep-alive messages, was directed to port 80 instead to 5050, which had been configured for the logon server settings. (767472)
- Filtering a request for accessing an FTP site that submitted a logon name with an empty password string resulted in returning an error message to the client. (769148)
- When an FTP proxy had been set up, DNS queries were performed unnecessarily for requests that did not include a URL, so no host name was specified. (770446)
- When assignment by mask had been selected as the load distribution method in a configuration with two WCCP services and IP spoofing, data packets were not routed accordingly. (770831)
- Incorrect reading of a long DNS name for a domain controller prevented an appliance from joining a Windows domain. (776420)
- Downloading a file failed at first attempt, as the processing of the response header caused a problem for a particular browser. (777300)
- In a configuration where active FTP was used for the server connection, a timeout that occurred while sending a data command led to a failure of the core process. (782339)

- When a client tried to connect to different Yahoo servers, the server IP addresses that were sent from the appliance to the client were not changed accordingly, which led to issues with authentication and SSL scanning. (785431)
- When a rule with the event for HTTP tunneling was enabled, the connection to a client was closed after receiving the first request, although the client had more requests to send and asked to keep the connection alive. (793606)
- When trying to load a block page into a browser, the .css file for this page was blocked, which was due to the failure of the appliance to send an appropriate Content-Type header with the response to the client request for sending the file. (798684)

List handling issues

- Lists that were the parameters of the URL.Host.BelongsToDomains property were not shown as being used by the property when a search for referring objects was performed. (771623)
- When a change to a parent directory had been performed by a web server in a configuration with an FTP over HTTP proxy, the name of the parent directory was not displayed together with the LIST information due to a synchronization problem. (771626)
- After configuring a filter for displaying list entries on the user interface and deleting this filter again, clicking another list and going back to the first list caused the filter to be set to "Type to filter content" while no list entries were displayed. (776449)
- After editing a subscribed list file by deleting all its content, it was not possible to save the file. (784763)
- Entries in subscribed lists that contained the special characters <, >, and & were not processed correctly, but led to error messages about unexpected close tags and unavailability of a preview. (785335)

Authentication and administrator role issues

- When working with a self-configured administrator role, it was not possible to import rule sets from the library. (760629)
- After upgrading to version 7.2, authenticating a user by the eDirectory authentication method was not possible. (766632)

Web filtering issues

- CPU usage went up to 100 percent on an appliance due to an endless loop in virus and malware filtering. This was partly caused by an incorrect use of a cached value for a property involved in the filtering. (739047)
- Use of the Antimalware.Proactive.Probability property in an error template caused the core process to fail with term signal 11. (751874)
- When large text files were uploaded to the web using POST requests, filtering them led to a failure of the core process due to problems with memory allocation that was performed for an internal re-encoding. (761397)
- When the appliance was configured as an ICAP server in REQMOD mode with Squid on the ICAP client, enabling the SafeSearch function did not lead to the expected results in filtering requests. (780909)
- An application filtering rule that had been configured to block particular applications specified on a list also blocked other applications that were not listed. (770126)
- Inappropriate use of the StreamDetector.Probability property in a rule led to a failure of the rule engine. (771102)
- An internal URL filtering error caused a failure of the proxy functions on an appliance in a Central Management configuration, as some files were erroneously overwritten when updates were performed. (772349)

- Malformed URLs in requests could not be processed properly and attempts of forwarding the requests resulted in an endless loop. (774166)
- Performance was low with high CPU usage and load averages when processing an anti-malware rule set with rules that let the scanning modules be called more often than necessary. (782326)
- A rule that exempted particular URLs from further filtering, using also the values of the AntiMalware.VirusNames property, was not processed properly, and access to web objects was prevented by a blocking rule later in the rule set due to a problem with the anti-malware queue. (794172)
- While media type filtering was performed for an .eot file, the core process failed with term signal 11. (798706)

Issues with SSL-secured communication

- A very long common name could not be retrieved from an SSL certificate, which resulted in sending an unnecessary certificate warning to the user. (761576)
- The list of certificate authorities could not be saved and new certificate authorities could not be added when the list contained invalid entries that could not be internally validated. (767487)
- A next-hop proxy that was configured for use in fetching a certificate was ignored and the location of the certificate was directly accessed. (775025)
- In a configuration with X509 proxy authentication and SSL scanning only on the client side, no client certificate was sent from the appliance to the server. (787325)
- Storing a certificate chain in the file for the server certificate when configuring the client context settings led to an error of the rule engine, which made it impossible to edit rules anymore. (792720)
- Storing a certificate chain in the file for the server certificate when configuring the client context settings made it impossible to save configuration changes anymore or to access websites under HTTP. (792891)

Logging and tracing issues

- When an archive with a very high number of members was downloaded, rule tracing for the rules processed in the embedded object cycles led to a memory shortage and a failure of the core process. (762721)
- When an SNMP trap was sent upon an event, a message string that had been added by the user was not sent with the trap. (765946)
- Errors concerning the synchronization of nodes in a Central Management configuration were logged after some configuration changes had been applied although the synchronization actually went fine. (770436)
- A change applied to the order of rule sets by dragging and dropping the relevant icon on the user interface was not recorded in the audit log. (777079)
- When a reverse DNS lookup based on the client IP address was performed, the server name was not retrieved and written into a log file. (782334)

Other issues

- The core process failed several times a day on multiple appliances in a Central Management configuration. (753717)
- When a next-hop proxy was down in a configuration with persistent client connections, attempts to connect to the proxy were not continued after one to three unsuccessful attempts had been made. (761994)

- When an archive with a very high number of members was downloaded, rule tracing for the rules processed in the embedded object cycles led to a memory shortage and a failure of the core process. (762721)
- After editing the fallback template for user messages in HTML format within the Template Editor, the preview showed not the edited content, but the default English template version. (765206)
- Configuring a property for a block page using the Template Editor caused problems when selecting the option for most recently used settings, as this option is not available for configuring rules and other configuration jobs. (765231)
- When configuring a property using the Template Editor, the search button could not be used for selecting a property. (765233)
- The MegaSAS.log file increased in size unexpectedly in the root partition of an appliance when the RAID status was checked by a monitoring daemon using a command tool. (765744)
- When an appliance update was performed on the user interface, the progress bar showed an unwanted jumping behavior. (772833)
- Searching for "Google" unspecifically on the user interface of an appliance produced fewer results than a specific search for this term. (773040)
- When a user name contained an apostrophe in a configuration with authentication and a welcome page, the user could not proceed beyond the welcome page due to a browser problem. (779689)
- A list of domains that was used by the URL.Host.BelongsToDomains property, and displayed on the user interface with this property, could not be immediately accessed by clicking on it. (783047)
- When performing a Google search in configuration where coaching was implemented, the user could not proceed beyond the coaching page due to a problem with reading a user name that contained a particular special character. (784115)
- Access to the user interface was not possible and an error message was displayed when an internal server error occurred. (784502)
- Creating rule criteria with particular tagged terms resulted in unexpected behavior of the rule criteria section on the user interface, such as ignoring the entered rule criteria and letting the section become inaccessible. (796161)
- The feedback script used in troubleshooting failed to perform after it had been started from the command line using a particular command syntax. (797999)

Known issues

For known issues in this product release, refer to KnowledgeBase article KB76291.

Installation

Complete the following procedures to install version 7.3 of the McAfee Web Gateway software on your appliance.

Overview

What is required to install version 7.3 depends on the version you are currently running.

- If you have been testing one of the two 7.3 beta versions, you can upgrade to the new version. See *Perform an upgrade*.
- If you are running version 7.2 or any other 7.x.x version:
  - Create a configuration backup.

    Use the options provided under **Troubleshooting | Backup/Restore** on the user interface to create the backup.
  - Install a repository for the new version. See *Install a repository*.
  - Upgrade to the new version. See *Perform an upgrade*.

    The upgrade process includes a major upgrade of the operating system. It will take several steps and more time than usual. When the upgrade has been successfully performed, the appliance restarts to complete the process.

    If the upgrade process fails or is interrupted, you can still re-image the appliance using an image of the new version and install the configuration backup.

  Alternatively, you can:

  - Create a configuration backup.
  - Re-image the appliance using an image of the new version and install the configuration backup.
- If you are running a 6.8.x or 6.9.x version, you need to re-image the appliance using an image of the new version.

Download an image of the new version from:

https://contentsecurity.mcafee.com/software_mwg7_download

For more information on re-imaging, see the *McAfee Web Gateway Product Guide*.

Install a repository

To install a repository for the new version:

1. Log on the the appliance from a system console using SSH.
2. Run the following command:

   ```
   yum install yumconf-7.3.0-mwg
   ```

You can now upgrade to the new version.

Perform an upgrade

You can upgrade to the new version on the user interface or from a system console.

Upgrade on the user interface

To upgrade on the user interface:

1. Select **Configuration | Appliances**.
2. On the appliances tree, select the appliance you want to upgrade.

   The appliance toolbar appears on the upper right side of the tab.
3. Click **Update Appliance Software**.

   The new version is installed on your appliance.
4. Click **Reboot** to complete the upgrade (only when upgrading from a 7.3 beta version).

   When upgrading from version 7.2 or another 7.x.x version, the appliance restarts automatically after the upgrade process has been successfully performed.

Upgrade from a system console

To upgrade from a system console:

1. Log on to the appliance using SSH.
2. Run the following two commands:

   ```
   yum upgrade yum yumconf\*
   ```

   ```
   yum upgrade
   ```

   The new version is installed on your appliance.
3. Run the following command to complete the upgrade (only when upgrading from a 7.3 beta version):

   ```
   reboot
   ```

   When upgrading from version 7.2 or another 7.x.x version, the appliance restarts automatically after the upgrade process has been successfully performed.