Release Notes

Revision A

McAfee Web Gateway

7.2.0.3

This document provides information about the McAfee® Web Gateway 7.2.0.3 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

Enhancement

Resolved issues

Known issues

Installation

About this release

McAfee Web Gateway version 7.2.0.3 is provided as a main release. It is a maintenance version that introduces an enhancement and resolves issues present in previous versions.

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

Enhancement

The following enhanced feature is included in this release.

Feedback script with additional output

The feedback.sh script was enhanced to create additional output for the *iptables* command.

Output was limited to the information provided when running the command with the *-L* parameter. It includes now also the *verbose* information that is made available when using the *-v* parameter. This provides additional information on the interfaces used in the communication.

Feature Modification Request 799495 had been entered for this enhancement in Bugzilla.

Resolved issues

The following issues have been resolved in this release. (Bugzilla reference numbers are in parentheses.)

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

- 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)
- 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)
- After a CONNECT request had been acknowledged by a next-hop proxy, more CONNECT requests were sent from an appliance to the next-hop proxy, instead of returning a 502 message to the client that had originally sent the CONNECT request. (786163).
- 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)
- A Cannot Connect message was sent from several appliances to their clients and users had to restart services to get access to the web, which was caused by inappropriate use of properties in rules for DNS lookups. (794139)

Quota and coaching issues

- When time quota restrictions had been configured, users were intermittently not given any session time at the beginning of the working day and session lengths were shorter than configured. (765193)
- When quota restrictions for web access were enabled, clicking the Continue button did not allow users to continue with their sessions, and the coaching page was still displayed. (779302)
- 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)

Web filtering issues

- 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. (794122)
- While media type filtering was performed for an .eot file, the core process failed with term signal 11. (798706)

- After a CONNECT request had been acknowledged by a next-hop proxy, more CONNECT requests were sent from an appliance to the next-hop proxy, instead of returning a 502 message to the client that had originally sent the CONNECT request. (786163).

Other issues

- Storing a certificate chain in the file for the server certificate when configuring the client context settings led to an error which made it impossible to edit the configuration and save the changes anymore. (792720, 792891)
- 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)
- 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)
- Authentication failed on an FTP connection when proxy authentication had been configured and a particular syntax was used for submitting the proxy password and other information. (802546)

Known issues

For known issues in this product release, refer to KnowledgeBase article KB76395.

Installation

Complete the following procedures to install version 7.2.0.3 of the McAfee Web Gateway software on your appliance.

Overview

What is required to install version 7.2.0.3 depends on the version you are currently running.

Note: If you have been testing a beta version, you need to remove this version first. See *Remove a beta version*.

- If you are running version 7.2.0.2 or a lower 7.x.x.x version, you can upgrade to the new version. See *Perform an upgrade*.
- 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*.

Remove a beta version

To remove a beta version before installing the new version:

1. Make sure you have another repository configuration installed.
2. Log on to the appliance from a system console using SSH.
3. Run the following two commands:

   ```
   yum clean all
   ```

   ```
   yum remove yumconf-beta
   ```

The beta version is removed from your appliance.

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.

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:

   ```
   reboot
   ```

For support information, visit mysupport.mcafee.com.