Release Notes

Revision A

McAfee Web Gateway 7.5.2.8

Contents

About this release

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

McAfee® Web Gateway (Web Gateway) 7.5.2.8 is provided as a main release. It is a maintenance version that includes two enhancements of the rule set system and resolves issues present in previous versions.

> ! If you have implemented a bonding configuration, which was available as an unsupported feature before the release of Web Gateway 7.5.2, remove any settings of this configuration before upgrading to this new version. Otherwise you risk creating an unstable state on the appliance.
>
> After the upgrade, you can again implement network interface bonding as described in the *System configuration* chapter of the *McAfee Web Gateway Product Guide.*.

Enhancements

This release of the product includes two enhancements.

A rule set has been added and another changed as follows in the rule set system of Web Gateway.

- **Gateway Anti-Malware with TIE (Library rule set) – New**

  This rule set provides several rules in addition to the rules in the **Gateway Anti-Malware** default rule set. These rules integrate anti-malware filtering as performed by the filtering functions on Web Gateway with information retrieved from a TIE server.

- **SSL Scanner (Default rule set) – Changed**

  A new embedded rule set has been inserted into this rule set with two rules that were previously contained in a different embedded rule set. The rules were moved because one of them caused an inappropriate skipping of a following embedded rule set while still in its old position.

  > The inappropriate skipping occurred in the following versions:
  >
  > - 7.5.2.6 and 7.5.2.7 (if these versions had been newly installed)
  > - Any upgrade from 7.5.2.6 or 7.5.2.7 (if these versions had been newly installed)

For more information, see the *McAfee Web Gateway Rule Sets Change Log*.

Resolved issues

The following issues are resolved in this release of the product.

> Bugzilla reference numbers are in parentheses.

Network communication

- Blocking ports on the eth0 interface did not work when network protection was configured, due to a fault in the iptables part of the system configuration file. (1129925)
- When Web Gateway was configured to run in transparent router mode, a failure of the core process occurred. (1130282)
- A conditional DNS reverse lookup failed for IP addresses with a /12 subnet due to faulty code that did not read the netmask properly. (1130571)
- Client requests that had been sent using persistent HTTPS connections were not answered on several Web Gateway appliances. This was due to a problem with obtaining certificates from the relevant web server, which closed the connection before the call for certificate verification had been completely processed. (1133332)
- Performing a forward and reverse DNS lookup for a progress page on the same connection at the same time caused the core process to fail with term signal 11. (1135466)

Web filtering

- The core and anti-malware processes failed on Web Gateway, as progress indication started when scanning the requested web object was already finished. (1125664)
- Accessing a particular URL caused the core process Web Gateway to fail, as the settings for SSL scanning contained an incorrectly specified cypher parameter. (1129537)

Miscellaneous

- After logging off from the user interface, the detachment process took an unusually long time to complete. Logging on again while this process was still going on resulted in a null-pointer error message. (1118477)
- A scheduled policy synchronization with SaaS Web Protection failed several times on Web Gateway and synchronization had to be performed manually. (1120953)
- When a time range was configured for the **DateTime.Time** property, a blocking message was incorrectly displayed to the user for a minute at every full hour. (1129697)
- When a rule that used a log handler event was copied on the user interface of Web Gateway, an inappropriate error message was displayed. (1133026)
- When a change had been made to a customer-maintained subscribed list on one node in Central Management, synchronization failed and the list was not updated on another node. (1133848)
- Web Gateway was affected by the CVE-2016-2105 to CVE-2016-2109 and the CVE-2016-2176 vulnerabilities, which exposed several weaknesses regarding memory, encryption, and other OpenSSL functions. After suitable fixes have been implemented, Web Gateway is not affected anymore. (1134653)
- When setting up Web Gateway as a virtual appliance with VMware, the vmhgfs module was missing and could not be loaded. (1138248)

Installation instructions

The requirements for installing Web Gateway 7.5.2.8 on an appliance depend on the version you are currently running.

- When running an earlier 7.5.x, a 7.4.x, or a 7.3.x version, you can immediately upgrade to the new version. See *Perform an upgrade*.
- When running a 7.2.x or any earlier 7.x version:

  1. Create a configuration backup.

     Use the options provided under **Troubleshooting** | **Backup/Restore** on the user interface to create the backup.

  2. Upgrade to the new version. See *Perform an upgrade*.

     The upgrade process includes a major upgrade of the operating system. It takes several steps and more time than usual.

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

  Alternatively, you can:

  1. Create a configuration backup.
  2. Re-image the appliance using an image of the new version and install the configuration backup.

- When running a 6.8.x or 6.9.x version, you must re-image the appliance using an image of the new version.

Download an image of the new version from the download page of the McAfee Content & Cloud Security Portal at https://contentsecurity.mcafee.com/software_mwg7_download.

For more information about re-imaging, see the *McAfee Web Gateway Installation Guide*.

Perform an upgrade

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

Upgrade on the user interface

You can work with the options of the user interface to perform the upgrade.

Task

1. Select **Configuration | Appliances**.

2. On the appliances tree, select the appliance you want to perform the upgrade on.

   The appliance toolbar appears on the upper right of the tab.

3. Click **Update Appliance Software**.

   The upgrade to the new version is performed. The upgrade process also logs you off from the user interface.

4. Proceed in one of the following ways to complete the installation.

   - When upgrading from an earlier 7.5.x, a 7.4.x, or a 7.3.x version:

     1. Wait until a message informs you that the upgrade has completed and a logon button appears.

     2. Log on to the user interface again.

     3. Select **Configuration | Appliances**, then select your appliance.

     4. On the appliance toolbar, click **Reboot**.

     When the restart has completed, a logon button appears. You can now log on to the user interface again and start working with the new version.

   - When upgrading from a 7.2.x or any earlier 7.x version:

     The appliance restarts automatically after each of the two upgrade phases that are performed.

     When the second restart has completed, a logon button appears. You can now log on to the user interface again and start working with the new version.

Upgrade from a system console

You can upgrade from a local system console or remotely using SSH.

Task

1. Log on to the appliance you want to perform the upgrade on.

2. Run the following commands:

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

   ```
   yum upgrade
   ```

   The upgrade to the new version is performed.

3. Proceed in one of the following ways to complete the installation:
   - When upgrading from an earlier 7.5.x, a 7.4.x, or a 7.3.x version:

     Wait until a message informs you that the upgrade has completed, then run the following command:

     ```
     reboot
     ```

     When the restart has completed, a logon prompt appears. You can now log on to the user interface and start working with the new version.

   - When upgrading from a 7.2.x or any earlier 7.x version:

     The appliance restarts automatically after each of the two upgrade phases that are performed.

     - If you are using a local system console:

       When the second restart has completed, a logon prompt appears. You can now log on to the user interface and start working with the new version.

     - If you are using SSH:

       When the appliance restarts after the first upgrade phase, you are disconnected and the second upgrade phase begins.

       After this phase has completed, including the automatic restart, you can log on to the user interface and start working with the new version.

       The following command lets you view messages about the upgrade progress:

       ```
       tail -F /opt/mwg/log/update/mlos2.upgrade.log
       ```

       When you see that the upgrade has completed, press **Ctrl+C** to stop the process. You can now log on to the user interface and start working with the new version.

Known issues

For known issues in this product release, see this Knowledge Center article: KB82983.

Find product documentation

On the **ServicePortal**, you can find information about a released product, including product documentation, technical articles, and more.

Task

1. Go to the **ServicePortal** at https://support.mcafee.com and click the **Knowledge Center** tab.
2. In the **Knowledge Base** pane under **Content Source**, click **Product Documentation**.
3. Select a product and version, then click **Search** to display a list of documents.

Product documentation

Every McAfee product has a comprehensive set of documentation. For Web Gateway, this includes the following:

- *McAfee Web Gateway Product Guide* — Describes the features and capabilities of Web Gateway, providing an overview of the product, as well as detailed instructions on how to configure and maintain it
- *McAfee Web Gateway Installation Guide* — Describes how to set up Web Gateway, as well as several devices that can be run with the product
- *McAfee Web Gateway Quick Start Guide* — Describes high-level steps for setting up a Web Gateway version that is shipped as pre-installed appliance software on a hardware platform

  This document is shipped in printed format with the pre-installed software and the hardware.

  > The current version of Web Gateway is not shipped as pre-installed software, so there is no *McAfee Web Gateway Quick Start Guide* for this version.

- *McAfee Web Gateway SSO Catalog* — Provides a list of the cloud applications and services that are supported by Web Gateway with preconfigured connectors or connector templates