About this release

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

McAfee® Web Gateway (Web Gateway) 7.7.0 is provided as a controlled release. It is a major version that includes new features and enhancements 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.
New features and enhancements

This release of the product includes these new features and enhancements.

Additional HSM solutions

Additional solutions are available for using a Hardware Security Module (HSM) to enhance private key security.

You can work with a Hardware Security Module remotely using SafeNet Network HSM, which is provided by an Intel partner (Gemalto), or run an emulation using OpenSSL.

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

Tenant ID configuration

A tenant ID can be configured, which identifies a customer as the owner of a particular instance of Web Gateway and at the same time of other Intel security products that this customer has purchased.

Use the Web Gateway and McAfee® ePolicy Orchestrator® Cloud (McAfee® ePO™ Cloud) interfaces to configure a tenant ID.

For more information, see the Central Management chapter of the McAfee Web Gateway Product Guide.

Cloud sandboxing

A rule set has been created for sending files to the new Cloud Threat Defense product, which provides file sandboxing and analytics, including IoCs, for threat detection and prevention.

Cloud Threat Defense is licensed separately and will be available in the near future.

Improved network protocol handling

Several improvements have been implemented for handling network protocols.

• The HTTP/2 protocol is now available for configuring network communication.
• Several enhancements for configuring inspection of SSL-secured traffic have been implemented.
• The Open SSL 1.0.2j library is now used for processing SSL-secured traffic.

Modified proxy configuration

Proxy configuration using a system console has been improved while some legacy functions are no longer available.

• A proxy that has been configured on the user interface of a Web Gateway appliance for use in performing filter information updates can also be configured for use in performing updates of the MLOS operating system.
• Bandwidth throttling can also be configured for processing web traffic when Web Gateway runs as a proxy in a transparent mode or in proxy HA mode.
• When configuring a destination address for an ICAP client, a fully qualified domain name can be specified instead of an IP address.
• The integrated SOCKS proxy solution that was implemented for an earlier release of Web Gateway no longer includes the option of running a SOCKS Dante proxy.

Migration from a configuration with the SOCKS Dante proxy to one with the modified version of the integrated solution is, however, possible.

• Options for configuring ICQ and Yahoo proxies on Web Gateway have been removed.

Various configuration enhancements
Enhancements have been implemented regarding some configuration tasks.

• When the administrator saves a configuration change on the user interface, an option is provided for storing a comment on the change.

• Two new properties have been added for storing date and time under the UNIX epoch scheme as a string in GMT or ISO format.

• Lists containing web security items that are made available to the administrator are referred to as supplied lists rather than maintained lists on the user interface, as these lists are actually not maintained by Intel.

• Settings for configuring the use of caches on Web Gateway have been modified.

Resolved issues
These issues are resolved in this release of the product. Bugzilla reference numbers are in parentheses.

Network communication

• When Web Gateway was running as a SOCKS proxy using the Kerberos authentication method, a request was not forwarded to the web, as the SOCKS proxy did not accept the authentication handling performed by Kerberos. (1132829)

• When McAfee Client Proxy was used to forward traffic to Web Gateway, the original client IP address could not be matched by any property, as the header that contained the IP address was not correctly decrypted. (1139163)

• Access to a web portal was blocked as the web server sent an expired certificate while a new one had already been registered on Web Gateway. (1140586)

• After a backup and restore had been performed for Web Gateway, the configured rules for handling static routes were no longer observed. (1141680)

• When processing a response sent from a next-hop proxy to Web Gateway, the content length header information was not removed as configured in the rules, which prevented the response from being forwarded to the requesting client. (1144491)

• Web Gateway could not open a TLS connection to a particular web server, which required use of a legacy SHA signature algorithm. A function was implemented for using legacy signatures that allow to establish the SSL connection. (1144894)

• When Web Gateway was running as a SOCKS proxy, including the body size property in the access log prevented log lines from being written. Lines could not be written because the size of the body could not be calculated, which was due to an internal ID that had not been set properly. (1146957)

• When Web Gateway was configured to filter traffic in the FTP over WCCP mode with spoofing enabled for client IP addresses, synchronization requests sent by the active FTP server were ignored on Web Gateway. (1151584)
• When media type filtering was enabled on Web Gateway, processing HTTP traffic led to an internal server error, as Web Gateway deleted some scripts of an unknown script type sent with this traffic. (1152454)

• Static routes that had been configured on Web Gateway were ignored under the Routing Information Protocol and eventually deleted, which was due to a buffer overflow caused by the large number of routes. (1153204)

**Web filtering**

• A space within the file path of a URL caused the URL to be inaccurately categorized. (1131993)

• When the rules in the default rule set for HTML filtering were processed, web objects that were not HTML-related were corrupted during the download, as these rules were also applied to them due to inadequate rule set criteria. (1138608)

• When updates for the Anti-Malware engine were performed on Web Gateway, reinitializing took unusually long, which had an impact on processing requests that required an evaluation of the Antivirus.IsInfected property. (1145537)

• A problem with finding the issuer of a certificate in SSL-secured communication caused the Coordinator subsystem to fail with term signal 6. (1149925)

• A private key for a default certificate authority that was used in a rule set for handling McAfee ePO Cloud requests contained a space, which made its length invalid when decoding was performed for the key prior to encrypting it.

  The key was therefore rejected by the core process, so the configuration could not be saved when changes had been applied. (1150070)

• After being scanned by the ICAP server, files were returned corrupted by Web Gateway, as chunk size information had been destroyed. (1152631)

**Vulnerabilities**

• Web Gateway was not affected by the CVE-2015-2600 vulnerability, which concerned the use of an Open SSH server. A package that was updated to remove this vulnerability has been implemented nevertheless.

  An updated package that addressed the CVE-2016-3115 vulnerability has also been implemented, so Web Gateway is no longer affected by that vulnerability. (1112008)

• Web Gateway was affected by the vulnerability described in the NTP-4.2.8p7 security announcement. After a fix has been implemented, which also covered a number of related vulnerabilities, Web Gateway is not affected anymore. (1137393)

• Web Gateway was affected by the CVE-2016-6515 vulnerability, which allowed the use of passwords with an unrestricted length when OpenSSH was involved. After a fix has been implemented, Web Gateway is not affected anymore. (1156225)

• Web Gateway was affected by the CVE-2016-1762 and several later vulnerabilities, which exposed the libxml2 library. After a fix has been implemented, Web Gateway is not affected anymore. (1159511)
**Miscellaneous**

- When Web Gateway was configured to filter SOCKS traffic, user authentication failed and Web Gateway closed the connection. (1152258)
- No progress page was displayed while downloading a .zip file, as a media type filtering rule was processed before, which required a complete download.
  
  Rule tracing was started to troubleshoot the issue, but failed due to exceeding the limit for the number of rule elements that can be traced simultaneously. (1155082)
- The core process on Web Gateway failed several times when processing a URL due a problem with synchronizing logging threads. (1156628)
- Using a block page to block several requests for web access incorrectly led to an alert call. (1158404)

**Installation instructions**

The requirements for installing this new product version depend on the version that you are currently running.

- **7.3.x to 7.6.x** — You can upgrade to the new version after activating a repository. See Upgrade from 7.3.x or later.

- **7.0.x to 7.2.x** — You can upgrade to the new version after creating a configuration backup. See Upgrade from 7.2.x or earlier 7.x.
  
  Alternatively, you can create a configuration backup, re-image the appliance using an image of the new version, and install the backup.

  ![Tip](https://contentsecurity.mcafee.com/software_mwg7_download)

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

- **6.8.x or 6.9.x** — 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](https://contentsecurity.mcafee.com/software_mwg7_download).

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

**Upgrade from 7.3.x or later**

From a 7.3.x or later version, you can upgrade to the new version after activating a repository.

You can perform the upgrade on the user interface or from a system console.

**Activate the repository**

Activate the repository for the new version from a local system console or work remotely using SSH.

**Task**

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

2. Run the following command:

   ```bash
   mwg-switch-repo 7.7.0
   ```

   You can now 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  When a message informs you that the upgrade has completed, proceed as follows:
   a  Log on to the user interface.
   b  Select Configuration | Appliances, then select your appliance.
   c  On the appliance toolbar, click Reboot.
   When the restart has completed, you can 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  When a message informs you that the upgrade has completed, 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.

Upgrade from 7.2.x or earlier 7.x
When running a 7.2.x version or any earlier 7.x version, create a configuration backup, then use a system console to upgrade to the new version.

The upgrade process includes a major upgrade of the operating system. It takes several steps and more time than usual. If this process fails or is interrupted, you can re-image the appliance using an image of the new version and install the configuration backup.

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.
Task
1. Create a configuration backup.

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

2. From the local system console, or using SSH, log on to the appliance you want to perform the upgrade on.

3. Run the following commands:
   
   ```
   yum upgrade yum yumconf\*
   mwg-dist-upgrade 7.7.0
   ```

   The upgrade to the new version is performed in two phases. After each phase, the appliance restarts automatically.

4. Proceed in one of the following ways to complete the installation:
   
   • 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: KB87762.

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 Reference Guide - Rule Sets Change Log** — Provides a list of changes to existing rule sets and additions of new rule sets for policy configuration on Web Gateway.

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