Revision D

McAfee Web Gateway 10.0.x Release Notes

Contents

What's new in the 10.0 release

Releases can introduce new features and enhancements or update platform support.

McAfee® Web Gateway 10.0 is provided as a controlled release. For information about how to install it, see the *McAfee Web Gateway Installation Guide*.

Use of ICAP server supported in Proxy HA mode

When Web Gateway has been set up in Proxy High Availability (HA) mode, use of ICAP servers for processing web traffic can also be configured in this network mode.

For more information, see the *Proxy HA mode* section in the *Proxies* chapter of the *McAfee Web Gateway Product Guide*.

New authentication and encryption methods for SNMP configuration

When users are set up that are allowed to view monitoring information provided under SNMPv3, new methods can be configured for authenticating these users, as well as new methods for encrypting the information.

A hash value for use in authenticating users can now be calculated using one of the following digests in addition to the existing: SHA-224, SHA-256, SHA-384, and SHA-512.

Information can be encrypted using one of these ciphers in addition to the existing: AES-128, AES-192, and AES-256.

The net-snmp package has also been updated.

Due to implementing a solution to an issue with the engine IDs that are provided as part of the SNMP information, existing engine IDs have changed for all Web Gateway appliances that have SNMP configured.

For more information, see the *Event monitoring with SNMP* section in the *Monitoring* chapter of the *McAfee Web Gateway Product Guide*.

New VMware version for virtual appliances

A new version of the VMware that is used when Web Gateway is run as a virtual appliance is now supported. This version is ESXi 7.0.

For more information, see the *System requirements for a virtual appliance* section in the *System requirements* chapter of the *McAfee Web Gateway Installation Guide*.

New Luna client version for use in HSM solution

The version of the Luna client that is used as component when a Hardware Security Module (HSM) solution is implemented to run along with Web Gateway to protect private certificate keys has been updated. The new version is 7.4. The driver that is required for this solution has also been updated.

For more information about the HSM solution, see the *Hardware Security Module* section in the *Web filtering* chapter of the *McAfee Web Gateway Product Guide*.

New version of DLP/CSF filter

The DLP/CSF filter that is used on Web Gateway in preventing data leakage has been updated.

Extraction of DMG files improved

When handling DMG files with unused sectors, the Composite Opener module on Web Gateway no longer extracts these sectors, avoiding unnecessary filling up of the opt partition and memory allocation failures.

Caching of Geo Location lookups improved

Retrieving information on Geo Location through GTI lookups when requests are processed on Web Gateway has been improved by modifying cache behavior.

Range of detected media types extended

A media type that includes what is known as *symbolic* files has been added to the range of types that are detected and can be used in media type filtering rules. This media type is: application/sylk.

Security for HTTPS logon to user interface enhanced

The default TLS version and SSL cipher string have been updated to make HTTPS logon to the Web Gateway user interface even more secure.

More secure algorithms for calculating hash values implemented

Several SSH and other packages with improved algorithms have been implemented on Web Gateway to make calculating hash values that are used for authenticating users more secure.

Additional self-tests run after starting an appliance

Several new self-tests are run after a Web Gateway appliance is started in order to check system integrity and stability. This includes the following tests:

- CPU spike check
- System Crash check
- File integrity check
- MWG service check
- CPU temperature check (on a physical appliance only)
- System Fan check (on a physical appliance only)

The test reports are generated and stored at /opt/mwg/log/debug/mwg-boot-test.log. File integrity failures are reported at /opt/mwg/log/debug/validate.log.

Logging process improved

Additional items related to logging have been implemented on Web Gateway as follows:

- Values of all request and response headers involved in processing web traffic can now be retrieved and stored for use in logging rules.

  Two new properties of the string type have been created, which can be used for this purpose, as well as for others where request and response headers are involved.

- Error logging for calls of /usr/bin/event has been added for the Web Gateway user interface.

  Names of failed processes with their exit values as well as failures to retrieve exit values are now logged.

Resolved issues in update 10.0.2

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

McAfee® Web Gateway 10.0.2 is provided as a controlled release.

For upgrade information, see the *McAfee Web Gateway Installation Guide*. Review also the following additional information.

New VMware version for virtual appliances

A new version of the VMware that is used when Web Gateway is run as a virtual appliance is now supported. This version is ESXi 7.0.

For more information, see the *System requirements for a virtual appliance* section in the *System requirements* chapter of the *McAfee Web Gateway Installation Guide*.

No failover between RADIUS servers

When configuring the RADIUS authentication method for authenticating users, you can set up more than one RADIUS server to run in the process.

Authentication information is retrieved from the first server on the list that is available. It is currently not possible to configure any failover functions for these RADIUS servers.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-1 Vulnerabilities

Reference	Resolution
WP-3024	This Web Gateway release provides an update that supports a secure Remote Procedure Call (RPC) with Netlogon secure channel. This update was implemented to account for a fix that has been made to mitigate the following vulnerability: • CVE-2020-1472 For more information about this vulnerability, see https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472.
WP-2236, WP-3246, WP-3308, WP-3309, WP-3318, WP-3319, WP-3320, WP-3321, WP-3322, WP-3323, WP-3324, WP-3325	This release also includes resolutions relating to other vulnerabilities that were implemented in preceding releases, but were not listed in the release notes then. The following vulnerabilities were involved: • CVE-2017-12652 • CVE-2018-15903 • CVE-2018-20843 • CVE-2019-5094, CVE-2019-5188, CVE-2019-5482 • CVE-2019-11719, CVE-2019-11727, CVE-2019-11756 • CVE-2019-12450 • CVE-2019-14822, CVE-2019-14866 • CVE-2019-17006, CVE-2019-17023, CVE-2019-17498 • CVE-2020-6829 • CVE-2020-8177, CVE-2020-8622, CVE-2020-8623, CVE-2020-8624 • CVE-2020-10754 • CVE-2020-12049, CVE-2020-12243, CVE-2020-12400, CVE-2020-12401, CVE-2020-12402, CVE-2020-12403 • CVE-2020-14779, CVE-2020-14781, CVE-2020-14782, CVE-2020-14792, CVE-2020-14796, CVE-2020-14797, CVE-2020-14803

Resolved issues in update 10.0.1

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

McAfee® Web Gateway 10.0.1 is provided as a controlled release.

For upgrade information, see the *McAfee Web Gateway Installation Guide*.

New VMware version for virtual appliances

A new version of the VMware that is used when Web Gateway is run as a virtual appliance is now supported. This version is ESXi 7.0.

For more information, see the *System requirements for a virtual appliance* section in the *System requirements* chapter of the *McAfee Web Gateway Installation Guide*.

No failover between RADIUS servers

When configuring the RADIUS authentication method for authenticating users, you can set up more than one RADIUS server to run in the process.

Authentication information is retrieved from the first server on the list that is available. It is currently not possible to configure any failover functions for these RADIUS servers.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-2 Network communication

Reference	Resolution
WP-3245	When changing the network mode from Proxy HA to explicit proxy, the usual message that alerts you to restart the appliance after completing the change is again displayed.

Table 2-3 Web filtering and logging

Reference	Resolution
WP-2866	When scanning a file for malware infection leads to a timeout, the error log message includes the full file name again as well as a reference to a Knowledge Base article with further information.
WP-3188	Filtering URLs with SmartMatch lists is no longer impeded by an inflexible cache size, which proved to be a severe restriction when maintaining multiple policies to control web usage of cloud users.
WP-3189	When filtering HTTPS traffic, Web Gateway responds again to a close notification from an HTTPS server by closing the current TLS session immediately.
WP-3191	McAfee-maintained lists for URL blocking that impact system performance due to their huge size, but have also become irrelevant because the blocking is already performed using other methods can be deprecated and removed. The Knowledge Center provides a KB article that explains the procedure.
WP-3228	When HTTPS traffic is filtered, whitelisting based on certificates and hosts also considers the port that listens to requests from the HTTPS server even if it is not the default port.
WP-3238	When updating the Gateway Anti-Malware (GAM) engine, no errors arise anymore from a failure to retrieve certificate revocation lists, which happened due to an invalid URL for a certificate authority.
WP-3291	Excessive CPU usage due to problems with reading file signatures for media type filtering does not occur anymore.

Table 2-4 Vulnerabilities

Reference	Resolution
WP-3236, WP-3309	This Web Gateway release includes CentOS updates that we have applied to MLOS, addressing publicly disclosed CVEs in the open source components, regardless of whether a CVE has been shown to impact customers. The following medium and higher level CVEs (CVSS 3.0 >= 4) were involved: • CVE-2017-15906, CVE-2018-15919, CVE-2019-5482, CVE-2020-8177 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-5 Other

Reference	Resolution
WP-3107	Downloading an ePO extension package or ePO version information can be completed without errors again on Web Gateway.
WP-3137	The core process on Web Gateway fails no longer after responses from a web server are received with and without a response body.
WP-3272	Importing a configuration backup from an older Web Gateway version and restoring it to an upgraded version works again without problems after an empty list of next-hop proxy servers had led to errors and eventually to a failure of the process.

Resolved issues in the 10.0 release

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400).

Resolved issues

JIRA issue numbers are provided in the reference columns of the tables below.

Table 2-6 Network communication

Reference	Resolution
WP-2671	Sending data from director nodes to the virtual IP address of Web Gateway running as proxy does no longer result in connection errors, which had led to infinite loops before.
WP-2705	The *libudns.so* library can be used on Web Gateway again without problems, which had led to a process failures before.
WP-2768	Certificates and private keys for use in secure communication can be updated using the REST interface for Web Gateway without problems now.
WP-2838	Requests for health checks sent under HTTP work as expected now after modifying them to let them use a newer HTTP version.
WP-2840	When static routes are added to the configuration on Web Gateway, processing continues after this had previously halted the process and required a restart.
WP-2875	When a CONNECT request has been received on Web Gateway, non-HTTP data is again forwarded speedily.
WP-2888	CPU load on connections when SSL certificates are sent does no longer become excessive, which had happened before due to bad timing when the sending of a certificate was renegotiated and the request body forwarded at the same time.

Table 2-7 Authentication

Reference	Resolution
WP-1588	When logging on to Web Gateway with NTLM or LDAP as the authentication method, a user can no longer log on more than once if this option is disabled by submitting the user name in lower and upper case spelling.

Table 2-8 Web filtering and logging

Reference	Resolution
WP-2643	When Web Gateway runs with McAfee WGCS in a Hybrid solution, updates to subscribed lists that have been configured for this solution also take effect there, as well as in instances of McAfee WGCS that run in the cloud solely, not being a part of a Hybrid solution then.
WP-2672	Access to a particular badssl website is no longer allowed, which it was occasionally, but constantly blocked by a rule for HTTPS scanning that covers weak key exchange.
WP-2760	A DLP rule for preventing applications from being run out of an Excel spreadsheet works now after it had previously not been able to detect the relevant code string.

Table 2-8 Web filtering and logging *(continued)*

Reference	Resolution
WP-2781	The media type font *.woff2 is detected now by the filtering process and not blocked when a rule for blocking media is enabled where the type cannot be detected.
WP-2782	Files of the Tar type that were blocked because they could not be handled by the opener module on Web Gateway can now be opened and downloaded without problems.
WP-2797	Internal updates of information used by the anti-malware and URL filter modules, which are performed in regular intervals, do not fail anymore, as the inappropriate creation of a zip file, which had led to the failure, is now avoided.
WP-2800	Archives of the OPC type can now be handled by the opener module on Web Gateway.
WP-2829	When an embedded object is received, scanning begins again with the embedding root object, after this order had not been observed for some files before.
WP-2836, WP-2837	Error tolerance has been improved in the process on Web Gateway that handles responses received from the web under HTTP.
WP-2919	When a list of media types is empty, attempts to access it do not lead to a failure of the core process anymore.
WP-2922	Building chains of certificates used for traffic secured under HTTPS no longer fails when a certificate has an invalid extension after a particular change in OpenSSL was also accepted on Web Gateway.
WP-2924	Files that are protected through a password under 7zip, are no longer blocked as corrupted on Web Gateway.

Table 2-9 Vulnerabilities

Reference	Resolution
WP-2578, WP-2775, WP-2777, WP-2948, WP-2962, WP-2790	This Web Gateway release includes CentOS updates that we have applied to MLOS, addressing publicly disclosed CVEs in the open source components, regardless of whether a CVE has been shown to impact customers. The following medium and higher level CVEs (CVSS 3.0 >= 4) were involved: • CVE-2020-1967, CVE-2020-7292, CVE-2020-8616, CVE-2020-8617, CVE-2020-9484 • CVE-2020-10188, CVE-2020-10713, CVE-2020-11022, CVE-2020-14308, CVE-2020-14309, CVE-2020-14310,: CVE-2020-14311, CVE-2020-14556, CVE-2020-14577, CVE-2020-14578, CVE-2020-14579, CVE-2020-14583, CVE-2020-14593, CVE-2020-14621 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-10 Other

Reference	Resolution
WP-2791	The coordinator component on Web Gateway no longer runs into a timeout when downloading updates with zero bytes length, but skips them without passing them on to a filter module.
WP-2817	Failures of the core process that were due to an issue with the Composite Opener no longer occur.
WP-2834	Engine IDs that are part of the information provided under SNMP are no longer identical on all Web Gateway appliances that have SNMP configured.
WP-2852	When multiple administrators access the Web Gateway user interface at the same time, an error message, stating that the object "temporaryIdReplaceBeforeSave" is already locked by a user, is not displayed anymore.
WP-3003	Failures of system list updates that frequently occurred on several Web Gateway appliances running as proxies do not occur anymore.
WP-3140	Increased RAM usage by the core process on a Web Gateway appliance, which had been observed and was due to a memory leak relating to the proxy control settings, has been identified as a problem and fixed.

Rating for update 10.0.2

The rating defines the urgency for installing this update.

Recommended

Mandatory	Critical	High Priority	**Recommended**

- Recommended for all environments. Apply this update at the earliest convenience.
- Not applicable to hotfixes, because a hotfix is only created in response to a business-impacting issue.
- An update that resolves non-severe issues or improves product quality is considered as recommended.

For more information, see KB51560.