Revision D

McAfee Web Gateway 10.1.x Release Notes

Contents

What's new in the 10.1 release

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

> McAfee® Web Gateway 10.1 is provided as a controlled release.

For information about how to upgrade to this release, see the McAfee Web Gateway Installation Guide.

File Uploads and Downloads

Download file blocking prevents files from being transferred from the RBI session down to the client machine.

Upload file blocking prevents files from being transferred from the RBI session up to the internet.

More flexible proxy setup

An additional method is available for setting up Web Gateway in Proxy High Availability (Proxy HA) mode.

Unicast packets can be used instead of Multicast packets, which are not allowed in a public cloud environment, to support a failover in a Proxy HA setup. A Keepalived daemon can be configured for this purpose on a system console that is connected to Web Gateway.

For more information about setting up proxies, see the *Proxies* chapter of the *McAfee Web Gateway Product Guide*.

Improved IP address handling

Limitations to the handling of IP addresses on Web Gateway have been removed.

- When a user logs on from a client to the Web Gateway user interface, the client IP address is recorded in the audit log, rather than a Web Gateway address that would be taken for the original address.
- A new environment variable has been introduced that enables progress pages to work on Points of Presence (PoPs), where Web Gateway cannot use its inbound IP address for communication.

Improved web filtering

An improvement has been implemented in the filtering process that protects your network against threats arising from web usage.

Different timeouts can be configured when long-running anti-malware jobs scan web objects for infections.

For more information about anti-malware scanning, see the *Web filtering* chapter of the *McAfee Web Gateway Product Guide*

HSM hardware upgrades

New versions of hardware components for the Hardware Security Module (HSM) solution are available and upgrades have been completed in order to adapt Web Gateway to working with the new hardware.

- The new nShield HSM cards and the nShield HSM appliance are supported.
- The HSM agent on Web Gateway has been upgraded.
- The LUNA network HSM engine has been upgraded to use a new OpenSSL version.

> You cannot implement these upgrades in an HSM solution that you are already using on your own. See KB94202 for more information and guidance.

For general information about working with an HSM solution, see the *Web filtering* chapter of the *McAfee Web Gateway Product Guide*

More supportive user interface

New functions have been implemented on the Web Gateway user interface for the benefit of the admin.

- An incident is created and an alert displayed on the dashboard when a Web Gateway license has been disabled.
- The appliance hardware model that a particular instance of the Web Gateway appliance software runs on is displayed on the user interface.
- When an admin has submitted invalid credentials for the user interface, a different admin can log on without being blocked during the time the other admin has to wait before new credentials are accepted.

Enhanced SNMP monitoring

SNMP monitoring on Web Gateway is enhanced. Review the settings named max characters for clipboard copy.

Web Gateway offers the option to send SNMP v3 traps. A separate trap sink can now be configured for traps sent under this protocol version.

For more information about event monitoring with SNMP, see the *Monitoring* chapter of the *McAfee Web Gateway Product Guide*

Extended logging

The range of activities that are logged on Web Gateway has been extended.

More logs that record activities relating to the user interface are now available providing feedback for troubleshooting purposes.

For more information about logging, see the *Monitoring* chapter of the *McAfee Web Gateway Product Guide*

Resolved issues in update 10.1.2

This release resolves known issues.

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

McAfee® Web Gateway 10.1.2 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 Network communication

Reference	Resolution
WP-3274	More than 15 ports can be specified for a port redirection rule, which had not worked before, but is handled now by creating additional IP tables.
WP-3639	In a Proxy High Availability (Proxy HA) setup only one node is shown with active director status at a time, whereas two were shown before even though only one had really been acting as director node.

Table 2-2 Web filtering

Reference	Resolution
WP-3674	When a block rule is configured in URL filtering, it blocks requests matching the blocking criteria and is no longer impacted by requests originating under the Periodic Rule Engine Trigger, which had stopped the request cycle before this block rule could be processed.

Table 2-3 Other

Reference	Resolution
WP-3591	A timeout that is set for deleting content stored under a PD storage rule is observed and the content deleted completely, which had only worked for parts of the content before.
WP-3694	A missing nscd package is now included in upgrading Web Gateway, which avoids an upgrade failure due to nscd dependencies that cannot be met preventing also glibc and other dependent upgrades.

Resolved issues in update 10.1.1

This release resolves known issues.

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

McAfee® Web Gateway 10.1.1 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 2-4 Network communication

Reference	Resolution
WP-3540	When Web Gateway runs as proxy, a virtual IP address can be configured and used as the proxy IP address, which had not worked as expected.
WP-3631	When several Web Gateway appliances run in Proxy High Availability (Proxy HA) network mode, the load balancer distributes work load only to ports on nodes that have been entered in the scanner table whereas all ports in the HTTP proxy table had been considered before due to a faulty line in a configuration file.

Table 2-5 Authentication and web filtering

Reference	Resolution
WP-3555	After sending a connect request to a domain controller for authentication under NTLM, Web Gateway checks the size of the response and reads the data as expected after having thrown an out-of-range exception before, which was due to an unsuccessful attempt to read the hardcoded response length from the buffer.
WP-3612	When user group information is evaluated for authentication purposes in a cluster of Web Gateway appliances, Chinese characters in the name of a user group are read without problems everywhere in the cluster. This had not worked before, as these characters were read properly on one cluster node, but when group names were distributed to other nodes running as proxies, authentication failed because these characters could not be read there.
WP-3617	Encrypted files that are processed on Web Gateway are detected and blocked under a rule that is configured after having been allowed before or blocked not as encrypted, but due to their file types, which were mistakenly recognized as unknown.

Table 2-6 Vulnerabilities

Reference	Resolution
WP-3445, WP-3483, WP-3527, WP-3528, WP-3547, WP-3584, WP-3589, WP-3611	This Web Gateway release includes updates addressing publicly disclosed CVEs, 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-2019-25013 • CVE-2020-8625 • CVE-2020-10029, CVE-2020-10543, CVE-2020-10878 • CVE-2020-12723 • CVE-2020-14347, CVE-2020-14360, CVE-2020-14372 • CVE-2020-25632, CVE-2020-25647, CVE-2020-25712 • CVE-2020-27749, CVE-2020-27779 • CVE-2020-29573 • CVE-2021-3347, CVE-2021-3449, CVE-2021-3450 • CVE-2021-20225, CVE-2021-20233 • CVE-2021-23839, CVE-2021-23840, CVE-2021-23841 • CVE-2021-25329 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in the 10.1 release

This release resolves known issues.

The resolved issues are described in this section. For a list of currently unresolved known issues, see McAfee Web Gateway 10.x Known Issues (KB93400). Review also the following additional information.

HSM firmware upgrade

If the Hardware Security Module (HSM) firmware you are using is not compatible with the new 12.60 HSM driver version, you must obtain the required firmware version from the vendor and perform a firmware upgrade before upgrading to a new version of the Web Gateway appliance software. The vendor is Entrust.

For more information about working with an HSM solution on Web Gateway, see the *Web filtering* chapter of the *McAfee Web Gateway Product Guide*

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-7 Network communication

Reference	Resolution
WP-1651	When Global Threat Intelligence (GTI) information is retrieved for URL filtering on Web Gateway, the GTI server no longer closes the connection prematurely after recognizing a TCP window full status.
WP-3227	When several instances of Web Gateway are running as proxies in a proxy chain, a request for a certification revocation list (CRL) that a client sends to the first proxy in the chain is checked on this proxy and forwarded to the proxy where the list resides, which had not been done before and caused a failure to process the request.
WP-3262	When a next-hop proxy is used in processing requests for web access that have HTTPS scanning applied to them on Web Gateway, the web server IP address is included in the response to the client that sent the request after having been overwritten with the ext-hop proxy IP address before.
WP-3314	RX packets are not dropped anymore, but forwarded when coming in through the eth0 and eth1 network interfaces on Web Gateway.
WP-3345	When overriding an outbound source IP address is configured on Web Gateway, this works as expected now after having caused a complete standstill of traffic processing before.
WP-3367	When web traffic is processed on Web Gateway under HTTPS, it is no longer determined already with the CONNECT request how to route the traffic, for example, over a next-hop proxy. The routing can also be based now on information sent with the GET request.
WP-3441	When a file copy fails in a Web Gateway cluster, the error message that is created is also logged, which had not been done before.
WP-3447	When a configuration rollback is performed in a Web Gateway cluster after a file copy failure, there is no restart of the Proxy High Availability (Proxy HA) process anymore unless the settings for this process have also changed.
WP-3464	Cluster nodes no longer reject configuration changes that are distributed across the cluster, which used to happen and trigger a storage rollback that caused a restart of the functions of the Proxy High Availability (Proxy HA) network mode.
WP-3477	A secure channel can be set up again on Web Gateway to Microsoft Windows Server 2008 when it is acting as a Domain Controller (DC) in the authentication process.
WP-3487	In a Proxy High Availability (Proxy HA) setup with two Web Gateway appliances running as director and scanning nodes, web traffic is forwarded to a next-hop proxy under FTP without problems, which had occurred when the Fully Qualified Domain Name (FQDN) had been configured for the next-hop proxy address, The issue was irrespective of the network mode that had been set up for Web Gateway.
WP-3556	When processing web requests on Web Gateway includes retrieving a value for a property relating to the Sky High Network (SHN) services, connecting to the SHN destination is no longer repeated for each request after this destination has been found not to be available, which reduces latency in the process.

Table 2-8 Authentication

Reference	Resolution
WP-3375	When a timeout occurs on a connection to an NTML authentication server, a log entry is written into an authentication log.
WP-3455	When SAML with cookie authentication is configured on Web Gateway, web access using a Chrome browser is no longer impeded by a problem with handling SameSite attributes for cookies after suitable attributes are now sent with the cookies.

Table 2-9 Web filtering, quota management, and logging

Reference	Resolution
WP-2308	Processing regular expressions no longer uses a cache that locked traffic to inhibit multi-thread access, but relies on the memory functions of the operating system instead. Use of this cache had impacted performance after the adoption of Blue Coat policies on Web Gateway.
WP-2537	When a request for activating a coaching session has been allowed on Web Gateway, the session can be started immediately, which had failed occasionally requiring a second attempt.
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 (KB) article with further information.
WP-3074	Warnings that could be seen in rsyslog after starting Web Gateway are not shown anymore.
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-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.
WP-3316	Files in rtf format are no longer erroneously considered corrupted and therefore blocked when handled by the File Opener, which had happened due to an inadequately implemented boundary check.
WP-3359	When .eml files are tested, they can pass again, as they are no longer blocked by media type filtering on Web Gateway, which had happened after the files had mistakenly been recognized as corrupted archives.
WP-3398	An archive that contains a large text file can be downloaded and extracted, which had failed before due to being mistakenly recognized as corrupted on Web Gateway.

Table 2-10 Vulnerabilities

Reference	Resolution
WP-2326, WP-3236, WP-3246, WP-3306, WP-3307, WP-3308, WP-3309, WP-3318, WP-3319, WP-3320, WP-3321, WP-3322, WP-3323, WP-3324, WP-3325, WP-3342, WP-3379, WP-3426, WP-3427, WP-3443, WP-3444, WP-3452, WP-3475	This Web Gateway release includes updates addressing publicly disclosed CVEs, 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-2016-5766 • CVE-2017-12652 • CVE-2018-15903, CVE-2018-15919 • CVE-2018-20843 • CVE-2019-5094, CVE 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-2019-19126 • CVE-2019-20907 • CVE-2020-548, CVE-2020-549 • CVE-2020-1971 • CVE-2020-6829 • CVE-2020-8169, CVE-2020-8177, CVE-2020-8231, CVE-2020-8234, CVE-2020-8285, CVE-2020-8286, CVE-2020-8622, CVE-2020-8623, CVE-2020-8624, CVE-2020-8625, CVE-2020-8626 • CVE-2020-10754 • CVE-2020-12049, CVE-2020-12243, CVE-2020-12400, CVE-2020-12401, CVE-2020-12402, CVE-2020-12403 • CVE-2020-14345, CVE-2020-14346, CVE-2020-14356, CVE-2020-14361, CVE-2020-14362, CVE-2020-14363, CVE-2020-14779, CVE-2020-14781, CVE-2020-14782, CVE-2020-14792, CVE-2020-14796, CVE-2020-14797, CVE-2020-14803 • CVE-2021-3156 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-11 Other

Reference	Resolution
WP-1366	When running as a virtual machine on an Azure platform, Web Gateway no longer submits an outdated token to be authenticated, which had required a restart of the core process to complete the authentication successfully.
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 or 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.

Table 2-11 Other *(continued)*

Reference	Resolution
WP-3340	RAM usage no longer increases excessively on some Web Gateway appliances that were running as nodes on a Point of Presence (POP) after a memory leak occurring in a library used for authentication purposes had been fixed.
WP-3389	An upload to a web server works as expected under HTTP2 after having produced an error due a problem with a response Web Gateway received from the web server.
WP-3390	Credentials submitted on McAfee® Web Gateway Cloud Service (McAfee® WGCS) in order to connect to MVISION Unified Cloud Edge, are no longer rejected, which had happened due to a low timeout value.
WP-3411	File download with data trickling works as expected when two Web Gateway appliances run in a proxy chain, where a timeout had occurred before due to a problem with handling internal error messages.
WP-3455	When a Chrome browser is used for web access on Web Gateway with cookie authentication enabled, images and frames are loaded again, which had failed due to a changed setting in Chrome for accepting the cookies that are required for loading these objects.
WP-3513	When Web Gateway runs in a hybrid setup with McAfee WGCS and McAfee® Client Proxy, cookie authentication works again for access to web sites under HTTP, after redirection using the original URL had failed due to a problem with a special character in the URL.
WP-3545	Offline upgrades to new Web Gateway versions using mwg-update do not fail anymore.

Rating for update 10.1.2

The rating defines the urgency for installing this update.

This update is recommended for all environments. Apply it at the earliest convenience.