Revision W

McAfee Web Gateway 9.2.x Release Notes

Contents

What's new in the 9.2 release

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

> McAfee® Web Gateway 9.2 was initially provided as a controlled release and is now provided as a main release. The transition was made when update 9.2.2 was released.

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

Rule set to run next-hop proxies for cloud use

A rule set is provided on-premise for running next-hop proxies that can be enabled for cloud use.

For more information, see the *Next-hop proxies* section in the *Supporting functions* chapter of the *McAfee Web Gateway Product Guide*.

Rule to allow bypassing for MMCS traffic

A new rule has been added to an on-premise rule set that implements bypassing of HTTPS scanning. The rule applies if a connection originates from a mobile system using McAfee Mobile Cloud Security (MMCS) and the site that is involved is whitelisted.

For more information, see the *HTTPS scanning* section in the *Web filtering* chapter of the *McAfee Web Gateway Product Guide*.

More media types supported for filtering

To the media types that are detected and can be filtered on Web Gateway have been added:

- *application/dns-message*
- *application/step*

For more information on media type filtering, see the *Media type filtering* section in the *Web filterrng* chapter of the *McAfee Web Gateway Product Guide*.

File opener improved

The file opener on Web Gateway shows an improved behavior now with support for TTF fonts in PDF files.

For more information on file opening, see the *File opening* section in the *Supporting functions* chapter of the *McAfee Web Gateway Product Guide*.

Transparent Bridge mode restored

After resolving stability issues that had occurred in previous product versions, the Transparent Bridge mode has been restored as an option for setting up Web Gateway in a local network.

For more information, see the *Transparent Proxy ...* sections in the *Proxies* chapter of the *McAfee Web Gateway Product Guide*.

Options for CTD removed from user interface

The Tenant Info settings, which could be used to configure Cloud Threat Detection (CDT) on Web Gateway, have been removed from the user interface.

Number of concurrent client connections increased on WBG-5xxx-D appliances

Web Gateway has been improved to handle an increased number of concurrent connections on one appliance. This adds to the value of the appliance through better scalability.

The increase applies to a standard configuration where the solution known as *normal forward proxy* runs on Web Gateway. It does not apply when you have set up, for example, a *High Availability (HA) proxy* solution.

The following increase has been measured:

- WBG-5000-D could handle 10% more client connections, resulting in 55,000 concurrent connections
- WBG-5500-D could handle 101% more client connections, resulting in 100,500 concurrent connections

For more information, see the *Advanced settings (for proxies)* section in the *Proxies* chapter of the *McAfee Web Gateway Product Guide*.

New administrator roles for use in troubleshooting

New role options have been implemented for administrators who perform troubleshooting on Web Gateway.

For more information, see the *Administrator role settings* section in the *Administrator accounts* chapter of the *McAfee Web Gateway Product Guide*.

Monitoring of response times on GTI server connections

When queries are sent from a Web Gateway appliance to a Web Gateway appliance to a Global Threat Intelligence (GTI) server to retrieve information about URL categories and reputation scores, response times can be monitored.

Log messages are written when response times increase as well as when they return to normal.

For more information, see the *URL Filter settings* section in the *Web filterrng* chapter of the *McAfee Web Gateway Product Guide*.

More granular monitoring of system resources

Usage of system resources on a Web Gateway appliance can be monitored in a more granular way using the new - *S threads-short* command when creating core files for tracing the mwg-core process.

When this command delivers output, threads are identified by short names, so excessively CPU consuming threads and other that cause problems can be detected more easily.

ENA adapter supported

The Elastic Network Adapter (ENA) is now supported on Web Gateway for AWS instance types that also support it. This means that a particular kernel-crash dump feature is available for troubleshooting when running Web Gateway on those instance types.

To these have been added the C5 and M5 instance types.

What's new in update 9.2.13

This release introduces several enhancements.

Kerberos authentication with improved logging

When the Kerberos authentication method is used, error logging has been improved, for example, by writing client IP addresses in the log.

More Visio media types detected

More media types relating to Microsoft Visio can be detected in media type filtering, for example, files with extension VSDX and content type *application/vnd.ms-visio.drawing.main+xm* or with extension VSTX and content type *application/vnd.ms-visio.template.main+xmlmore*.

Handling of HTTP2 statistics improved

HTTP2 statistics, which are also shown on the Web Gateway dashboard, are provided under the Simple Network Management Protocol (SNMP) to be read by an external SNMP manage poll.

What's new in update 9.2.12

Releases can introduce new features and enhancements.

Enhancements have been introduced as follows in this release.

More efficient handling of WebSwing user interface

For users working with the WebSwing version of the user interface, the individual IP addresses of their client systems are recorded in the audit log when requests come in from these clients. The common 127.0.0.1 address is no longer in use here.

This address had been logged for all users due the role as a remote desktop that WebSwing took from the point of view of the Java user interface.

A commercial WebSwing version has also been implemented to overcome some limitations of the open source versions.

Resolved issues in update 9.2.19

This release resolves known issue.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.19 is provided as a main release and archived.

For upgrade information, see the Upgrading to a new version provided as a main release of the *McAfee Web Gateway Installation Guide*.

Resolved issue

JIRA issue number is provided in the reference column below.

Table 2-1 Vulnerabilities

Reference	Resolution
WP-4554	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-2022-0778 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 9.2.18

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.18 is provided as a main release and archived.

For upgrade information, see the Upgrading to a new version provided as a main release of the *McAfee Web Gateway Installation Guide*.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-2 Network communication

Reference	Resolution
WP-4451	The Bond interface is brought up with the appliance and Static Routes settings are restored correctly after a full restore of Web Gateway.

Table 2-3 Other

Reference	Resolution
WP-4134	A password for an update proxy user is escaped properly again, after this had not worked and caused yum to treat the user name as the name of the proxy server.
WP-4350	A URL path encoding issue that involved subscribed lists has been resolved.
WP-4331	A 502 error that occurred when working with the AWS admin page has been resolved.
WP-4408	Java 1.8.0 openjdk is working normally.
WP-4440	An admin user can again log onto Web Gateway using NTLM authentication successfully.

Table 2-3 Other *(continued)*

Reference	Resolution
WP-4444	Files are no longer detected as missing for Web Gateway nodes because of incorrect reference handling.
WP-4518	High memory usage on a Web Gateway appliance does not occur anymore.

Table 2-4 Vulnerabilities

Reference	Resolution
WP-4347, WP-4416	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-2021-41617 • CVE-2021-4008, CVE-2021-4009, CVE-2021-4010 CVE-2021-4011 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 9.2.17

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

ⓘ McAfee® Web Gateway 9.2.17 is provided as a main release and archived.

For upgrade information, see the Upgrading to a new version provided as a main release of the *McAfee Web Gateway Installation Guide*.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-5 Network communication

Reference	Resolution
WP-3263	Traffic redirected to Web Gateway in Transparent Router mode is processed again.
WP-4255	A check status issue that happened when a handshake using TLS1.3 connection retries had not worked as expected due to a broken server connection has been fixed.
WP-4268	POST commands running while HTTP tunneling is enabled do not lead to a failure of the core process on Web Gateway anymore.
WP-4278	After deleting the haproxy.cfg manually, the haproxy functions work as expected.
WP-4328	Port redirection issues that occurred with range entries have been fixed.

Table 2-6 Web filtering and logging

Reference	Resolution
WP-3963	Web Gateway accepts incoming connections and continues to operate, which did not work after opening a corrupted .rar file.
WP-4061	Malicious Reputations use the ATD block template again.
WP-4156	Invalid logon error "Session restricted to another IP" has been fixed.
WP-4270	Web Gateway now recognizes a Python 3.py script as python type,
WP-4271	TAR archives with Pax extended headers are recognized as allowed and no longer blocked.
WP-4279	System preference for an HTML-based user interface has been removed from the logon screen, so the Java-based user interface is available on the same terms.

Table 2-6 Web filtering and logging *(continued)*

Reference	Resolution
WP-4330	PDF files are no longer blocked as corrupted media type when the "Block Corrupted MediaTypes" option is enabled under the Composite Opener.
WP-4369	A limit can be set to the compression ratio again after this had not been possible due to adding the "Body.MediaTypeFromHeader | Does not equal | <empty>" rule.
WP-4385	Logs can again be sent by SFTP.

Table 2-7 Other

Reference	Resolution
WP-3069	Bandwidth service is running normal after a Web Gateway upgrade.
WP-4071	High memory usage on a Web Gateway appliance does not occur anymore.
WP-4294	MWG High CPU issue observed in multiple customer deployments has been fixed.
WP-4345	High memory usage when handling HTTP2 traffic does no longer occur.
WP-4379	An end-of-life version of log4j 1.x is not used anymore.

Table 2-8 Vulnerabilities

Reference	Resolution
WP-3335, WP-4131, WP-4159, WP-4237, WP-4259, WP-4329, WP-4348, WP-4355, WP-4376, WP-4407, WP-4421	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-2021-43527 • CVE-2021-35556, CVE-2021-35567, CVE-2021-35561, CVE-2021-35565, CVE-2021-35564, CVE-2021-35578, CVE-2021-35550, CVE-2021-35559, CVE-2021-35586, CVE-2021-35588, CVE-2021-35603 • CVE-2021-42574, CVE-2021-42694 • CVE-2021-20271 • CVE-2021-37750 • CVE-2021-22945, CVE-2021-22946, CVE-2021-22947 • CVE-2021-42373, CVE-2021-42373, CVE-2021-42374, CVE-2021-42375, CVE-2021-42376, CVE-2021-42377, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42383, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386 • CVE-2020-8927 • CVE-2021-44228, CVE-2021-45046 • CVE-2021-45105, CVE-2021-44832 • CVE-2021-4034 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 9.2.16

This release resolves known issue.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.16 is provided as a main release and archived.

For upgrade information, see the Upgrading to a new version provided as a main release of 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.

JIRA issue numbers are provided in the reference columns below.

Resolved issue

JIRA issue number is provided in the reference column below.

Table 2-9 Vulnerabilities

Reference	Resolution
WP-4355	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-2021-44228 • CVE-2021-45046 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 9.2.15

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.15 is provided as a main release and archived.

For upgrade information, see the Upgrading to a new version provided as a main release of 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.

JIRA issue numbers are provided in the reference columns below.

Table 2-10 Network communication

Reference	Resolution
WP-3710	Web Gateway now supports intermediary headers in messages from HTTP2 -capable servers, so an HTTP2_PROTOCOL_ERROR no longer occurs here.
WP-4073	Bindings between protocol addresses and link layer addresses are established successfully while using an HTML GUI.

Table 2-11 Web filtering

Reference	Resolution
WP-3663	Web Gateway successfully retrieves reports from McAfee® Advanced Threat Defense regarding .zip files after sending a status query to Advanced Threat Defense.
WP-4158	The time consumed during a transaction can be retrieved again as a value for the **Timer.TimeInTransaction** property when Web Gateway is running as a proxy under TCP or the SOCKS protocol.
WP-4164	Files are no longer detected as corrupted under CPIO.

Table 2-12 Vulnerabilities

Reference	Resolution
WP-3806, WP-4203	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-2021-31535 • CVE-2021-25214 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-13 Other

Reference	Resolution
WP-3247	The mcelog service will only be enabled on physical appliances now and will remain disabled on virtual appliances.

Resolved issues in update 9.2.14

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.14 is provided as a main release and archived.

For upgrade information, see the Upgrading to a new version provided as a main release of 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.

JIRA issue numbers are provided in the reference columns below.

Table 2-14 Logging on

Reference	Resolution
WP-4043	Admins can log on to the Web Gateway user interface again from external accounts.

Table 2-15 Log files

Reference	Resolution
WP-4022	The rsyslog daemon had kept the /var/log/haproxy/ haproxy-info_1.log file open until all disk space had been filled up on a Web Gateway appliance. This has been fixed now and log rotation works fine again.

Table 2-16 Vulnerabilities

Reference	Resolution
WP-3792, WP-4003, WP-4021, WP-4058, WP-4067	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-2020-25649 • CVE-2021-2369, CVE-2021-2388 • CVE-2021-3520 • CVE-2021-3711, CVE-2021-3712 • CVE-2021-30640 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 9.2.13

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.13 is provided as the current main release.

For upgrade information, see the Upgrading to a new version provided as a main release of 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 2-17 Network communication

Reference	Resolution
WP-1455	POST commands run while HTTP tunneling is enabled do not lead to a failure of the core process on Web Gateway anymore.
WP-3689	When users browse streaming sites under HTTP2, the /opt/mwg/temp folder on Web Gateway is not filled up with temp files anyrmore, which had happened due to a problem with range headers in the communication between server and client.
WP-3810	When a director node is not working as a scanner in a Proxy High Availability (Proxy HA) configuration, the proxy on Web Gateway listens to other scanning nodes again.

Table 2-18 Web filtering and logging

Reference	Resolution
WP-3072	Only errors relating to the user interface are logged in the mwg.ui.errors log, whereas unexpected errors, such as error 143 and others, are not logged anymore.
WP-3658	When uncategorized URLs are blocked, events are successfully synchronized for two Trusted Source properties, which had not worked properly before, as an unexpected event had been added.
WP-3751	Upgrade packages for Web Gateway can be downloaded, which had not been possible because the PGP key files inside these packages were blocked as encrypted media types.
WP-3811	Requests to retrieve CRL and OSCP information about the status of certificates used for secure communication are forwarded, which had not worked in a next-hop proxy chain with two Web Gateway appliances.
WP-3903	Log file pushing works again after logging a switch to a supported repository version with mwg-switch repo, which had failed before, as no permission to read the log files was reported as an error.
WP-3904	Infinite loops, which caused threads to hang and resulted in problems with high CPU and memory load, are no longer created when zip archives are scanned.

Table 2-19 Vulnerabilities

Reference	Resolution
WP-3580, WP-3656, WP-3815, WP-3878, WP-3882, WP-3934, WP-3935, WP-3936, WP-3999	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-2016-3674 • CVE-2017-7957 • CVE-2019-10208 • CVE-2020-24489, CVE-2020-25111, CVE-2020-25112, CVE-2020-25113, CVE-2020-25648, CVE-2020-25694, CVE-2020-25695, CVE-2020-26217 • CVE-2021-3472 • CVE-2021-21341, CVE-2021-21342, CVE-2021-21343, CVE-2021-21344, CVE-2021-21345, CVE-2021-21346, CVE-2021-21347, CVE-2021-21348, CVE-2021-21349, CVE-2021-21350, CVE-2021-21351 • CVE-2021-22876, CVE-2021-22890, CVE-2021-22901 • CVE-2021-25217 • CVE-2021-27219 • CVE-2021-32027 • CVE-2021-33909 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 9.2.12

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.12 is provided as the current main release.

For upgrade information, see the Upgrading to a new version provided as a main release of 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 2-20 Network communication

Reference	Resolution
WP-2823	Long-running web socket connections last again as expected after terminating prematurely before and the configured timeout is observed.
WP-3440	When Web Gateway runs in Proxy High Availability (Proxy HA) mode, log files are rotated in a suitable manner preventing overflow of the Proxy HA log and spilling over into other partitions, which had happened before.
WP-3529	When stickiness is configured for forwarding requests for web access from a client to a particular next-hop proxy, this is observed again after not having worked properly before.
WP-3585	A certificate for secure connections can be removed along with its certificate chain and a new certificate implemented without the old chain still showing up in vulnerability scans.
WP-3787	When static routes are configured, the tool tip message no longer suggests that the field for the gateway IP address might be left empty, which is actually not allowed here.

Table 2-21 Vulnerabilities

Reference	Resolution
WP-3484, WP-3744, WP-3745, WP-3746, WP-3747, WP-3793, WP-3800	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-2020-12321 • CVE-2020-25684, CVE-2020-25685, CVE-2020-25686 • CVE-2020-36221, CVE-2020-36222, CVE-2020-36223, CVE-2020-36224, CVE-2020-36225, CVE-2020-36226, CVE-2020-36227, CVE-2020-36228, CVE-2020-36229, CVE-2020-36230 • CVE-2021-2161, CVE-2021-2163 • CVE-2021-20305 • CVE-2021-25215, CVE-2021-25216 • CVE-2021-27135 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 9.2.11

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.11 is provided as a main 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 2-22 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 2-23 Web filtering

Reference	Resolution
WP-3666	Traffíc originating from use of the Facebook Messenger app is appropriately recognized as Facebook Chat in application filtering on Web Gateway.
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 2-24 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 9.2.10

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

> McAfee® Web Gateway 9.2.10 is provided as a main 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 2-25 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 2-26 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 2-27 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 update 9.2.9

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.9 is provided as a main 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 2-28 Network communication

Reference	Resolution
WP-3303	When Web Gateway runs as a web proxy in Proxy High Availability (HA) mode, processing requests for web access that come in from clients under FTP, the virtual IP address (VIP) sent initially to a client used to be replaced with a different VIP upon directing the request to a scanning node in passive FTP mode, which caused the process to fail, as the client was unaware of the changed VIP. The VIP now used by a Web Gateway appliance when connecting as director node to an appliance that runs as scanning node in passive FTP mode is the one that is configured as VIP of the Virtual Router Redundancy Protocol (VRRP) interface. When more than one VIP is configured for this interface, the most recently added is used. This applies to a Proxy HA as well as to a Transparent Router setup.
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, but can be based on information sent with the GET request.
WP-3487	In a Proxy High Availability (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.

Table 2-29 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 being sent with the cookies.

Table 2-30 Web filtering

Reference	Resolution
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 2-31 Vulnerabilities

Reference	Resolution
WP-2326, WP-3443	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-2020-0548 CVE-2020-0549 • CVE-2020-8169 CVE-2020-8177 CVE-2020-8231 CVE-2020-8234 CVE-2020-8285 CVE-2020-8286 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-32 Other

Reference	Resolution
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-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-3545	Offline upgrades to new Web Gateway versions using mwg-update do not fail anymore.

Resolved issues in update 9.2.8

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.8 is provided as a main 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 2-33 Network communication

Reference	Resolution
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-3441	When a file copy fails in a Web Gateway cluster, the error message that is created is also logged, which had not happened 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 High Availability (HA) Proxy process anymore unless the settings for this process have also changed.

Table 2-33 Network communication *(continued)*

Reference	Resolution
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 HA Proxy 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 in the authentication process.

Table 2-34 Web filtering and quota management

Reference	Resolution
WP-2308	Processing regular expressions no longer uses a cache that locked traffic to inhibit multi-thread access, which had impacted performance after the adoption of Blue Coat policies on Web Gateway, but relies on the memory functions of the operating system instead.
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 and required a second attempt.

Table 2-35 Vulnerabilities

Reference	Resolution
WP-3426, WP-3427, WP-3307, 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-2019-19126, CVE-2019-20907 • CVE-2020-14345, CVE-2020-14346, CVE-2020-14356, CVE-2020-14361, CVE-2020-14362 • CVE-2021-3156, CVE-2021-23885 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-36 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.

Resolved issues in update 9.2.7

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.7 is provided as a main 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 2-37 Network communication

Reference	Resolution
WP-3109	When enabling WCCP with L2 transparent redirection after running Web Gateway in Transparent Router mode with virtual IP spoofing before, receiving and sending web traffic over a passive FTP connection is no longer impeded by some retained Transparent Router settings.
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.

Table 2-38 Web filtering and logging

Reference	Resolution
WP-3074	Warnings that could be seen in rsyslog after starting Web Gateway are not shown 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.

Table 2-39 Vulnerabilities

Reference	Resolution
WP-3342, WP-3379	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-2019-17498 • CVE-2020-1971 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Resolved issues in update 9.2.6

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.6 is provided as a main 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 2-40 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 9.2.5

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

ℹ McAfee® Web Gateway 9.2.5 is provided as a main 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 2-41 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 2-42 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-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 2-43 Vulnerabilities

Reference	Resolution
WP-2986, 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, CVE-2020-10713 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-44 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 update 9.2.4

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.4 is provided as a main 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*.

Retrieval of GTI information for URL filtering improved

Several enhancements have been implemented for the automatic GTI airgap mode to optimize and improve it for use in URL filtering.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-45 Web filtering and logging

Reference	Resolution
WP-2874	When log file pushing is configured, the log file manager no longer rejects path information that consists of a slash or is empty, but accepts it and uses the root directory to push log files there.
WP-2916	Log file rotation works now even when interfaces that are matched by the log file manager to IP addresses contain dots in their names.
WP-3074	A syslog warning that appeared when an additional listener was running together with the default listener for the rsyslog service is not triggered anymore after several lines have been modified or removed in the files that were involved in the process.

Table 2-46 Vulnerabilities

Reference	Resolution
WP-2789, WP-3138	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-2020-1968, CVE-2020-11022 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-47 Other

Reference	Resolution
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-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.

Resolved issues in update 9.2.3

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.3 is provided as a main release.

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

New appliance hardware

The WBG-5000-E and WBG-5500-E models of the appliance hardware are now available as platforms for running Web Gateway as a physical appliance. The new models are shipped with version 8.2.8 of the Web Gateway appliance software preinstalled.

Documentation is provided for these new models explaining their port assignments and several hardware-related tasks, for example, adding fiber NICs.

For more information, see the latest version of the *McAfee 9.2.x Hardware Guide*.

Information about incidents added

The documentation for Web Gateway provides also information about the meaning and several parameters of incidents. Values for origin and severity of incidents occurring with the SSOS and CASB filters that were missing from the existing documentation have now been added.

For more information, see the latest version of the *McAfee 9.2.x Interface Reference Guide*.

HSM firmware upgrade

If you are using a Thales hardware component for running a Hardware Security Module (HSM) with Web Gateway, make sure that you are also using the appropriate firmware.

The Web Gateway repository provides nfast-driver version 12.40 for running the Thales HSM component.

If your monitor and module firmware does not support this driver version, you must obtain the required firmware version from Thales and perform a firmware upgrade before upgrading to a new Web Gateway version.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-48 Network communication

Reference	Resolution
WP-2531	When Web Gateway runs in Proxy High Availability (HA) mode, ICAP traffic can be processed in addition to traffic going on under HTTP and FTP.
WP-2768	Certificates and private keys for use in secure communication can be updated using the REST interface for Web Gateway without problems now.

Table 2-49 Web filtering and logging

Reference	Resolution
WP-2546	When handling DMG files with unused sectors, the opener module on Web Gateway no longer extracts these sectors, avoiding unnecessary filling up of the opt partition and memory allocation failures.
WP-2910	Error logging for calls of /usr/bin/event has been added for the Web Gateway user interface..
WP-2924	Files that are protected through a password under 7zip, are no longer blocked as corrupted on Web Gateway.

Table 2-50 Vulnerabilities

Reference	Resolution
WP-2948	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-2020-14556, 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 2-51 Other

Reference	Resolution
WP-1032	An upgrade of the SafeNet/Luna client that runs with Web Gateway in a Hardware Security Module (HSM) solution has been completed.
WP-2835	To prevent failures when processing XML documents, a new library package has been imported.
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.

Resolved issues in update 9.2.2

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.2 is provided as a main release.

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

New appliance hardware

The WBG-5000-E and WBG-5500-E models of the appliance hardware are now available as platforms for running Web Gateway as a physical appliance. The new models are shipped with version 8.2.8 of the Web Gateway appliance software preinstalled.

Documentation is provided for these new models explaining their port assignments and several hardware-related tasks, for example, adding fiber NICs.

For more information, see the latest version of the *McAfee 9.2.x Hardware Guide*.

Information about incidents added

The documentation for Web Gateway provides also information about the meaning and several parameters of incidents. Values for origin and severity of incidents occurring with the SSOS and CASB filters that were missing from the existing documentation have now been added.

For more information, see the latest version of the *McAfee 9.2.x Interface Reference Guide*.

HSM firmware upgrade

If you are using a Thales hardware component for running a Hardware Security Module (HSM) with Web Gateway, make sure that you are also using the appropriate firmware.

The Web Gateway repository provides nfast-driver version 12.40 for running the Thales HSM component.

If your monitor and module firmware does not support this driver version, you must obtain the required firmware version from Thales and perform a firmware upgrade before upgrading to a new Web Gateway version.

Resolved issues

JIRA issue numbers are provided in the reference column of the table below.

Table 2-52 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	Use of the *libudns.so* library on Web Gateway does not lead to a process failure anymore.
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, while 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 2-53 Web filtering

Reference	Resolution
WP-2581	URLs can now be resolved through DNS queries even when requests for retrieving service groups originate from a SHN client.
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.
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-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-2851	The **Body.IsSupportedByOpener** property is no longer set to an invalid value when unsupported files of the Tar type are processed.
WP-2855	Media of the .slk type is properly detected on Web Gateway after it had previously not been identified correctly or not detected at all.

Table 2-54 Vulnerabilities

Reference	Resolution
WP-1585, WP-2864, WP-2932	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-2019-1551, CVE-2019-11091, CVE-2019-12126, CVE-2019-12127, CVE-2019-12130 • CVE-2020-13934, CVE-2020-13935 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-55 Other

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.
WP-2817	Failures of the core process that were due to an issue with the Composite Opener do not occur anymore.

Resolved issues in update 9.2.1

This update resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

McAfee® Web Gateway 9.2.1 is provided as a controlled release.

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

HSM firmware upgrade

If you are using a Thales hardware component for running a Hardware Security Module (HSM) with Web Gateway, make sure that you are also using the appropriate firmware.

The Web Gateway repository provides nfast-driver version 12.40 for running the Thales HSM component.

If your monitor and module firmware does not support this driver version, you must obtain the required firmware version from Thales and perform a firmware upgrade before upgrading to a new Web Gateway version.

Resolved issues

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

Table 2-56 Web filtering

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 SSL scanning that covers weak key exchange.
WP-2781	The media type font *.woff2 is detected now by the filtering process and not blocked when a rule for blocking media where the type cannot be detected is enabled.
WP-2797, 2798	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.

Table 2-57 Vulnerabilities

Reference	Resolution
WP-2578, WP-2728, WP-2740, WP-2775, WP-2777	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 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-58 Other

Reference	Resolution
WP-2817	Failures of the core process that were due to an issue with the Composite Opener do not occur anymore.

Resolved issues in the 9.2 release

This release resolves known issues.

For a list of currently unresolved known issues, see McAfee Web Gateway 9.x Known Issues (KB92141).

HSM firmware upgrade

If you are using a Thales hardware component for running a Hardware Security Module (HSM) with Web Gateway, make sure that you are also using the appropriate firmware.

The Web Gateway repository provides nfast-driver version 12.40 for running the Thales HSM component.

If your monitor and module firmware does not support this driver version, you must obtain the required firmware version from Thales and perform a firmware upgrade before upgrading to a new Web Gateway version.

Resolved issues

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

Table 2-59 Network communication

Reference	Resolution
WP-2300	When decrypted traffic is monitored, source ports are no longer set to zero, but retain their original values.
WP-2325	When a proxy is set up on Web Gateway to run in High Availability mode, processing web traffic is no longer slow and long running connections do not occur anymore.
WP-2389	When Web Gateway has been configured to run as a High Availability proxy, web traffic is not forwarded to a wrong listener address anymore, which had caused faulty processing of web security rules.
WP-2495	When a Web Gateway appliance is restarted, it immediately rejoins a Windows Domain that it had been joined to before, which had been delayed due to an authentication issue.
WP-2569	The **Command.Name** property and the User-Agent header fields no longer remain empty, but are again filled with values when incoming requests are processed.
WP-2644	A package that contains the proper version of a particular OpenSSLlibrary is now used on Web Gateway after use of a different version had led to issues.

Table 2-60 Authentication

Reference	Resolution
WP-2457	When user information is retrieved for authentication under LDAPS, using a converted value as a placeholder in the search string works again as expected.
WP-2693	When log files are auto-pushed with SCP, authentication using a public key for SSH-secured communication works now even if no password is submitted with the user name.

Table 2-61 Web filtering and logging

Reference	Resolution
WP-2066	When anti-malware filtering is performed, no errors originating from the AntiVirus filter module appear in the mwg-core error logs anymore, which had happened before due to issues with opening archive files.
WP-2282	A certificate chain for the user interface that could not be imported is made available again for importing when SSL-secured traffic is processed.
WP-2337	When a destination IP address in a URL that a user requests access to is logged on Web Gateway, the 255.255.255.255 address is no longer written into the access log in addition to the correct address.
WP-2373	Auto-pushing can be performed again without problems to move access log files to an SFTP server.
WP-2441	When customer-subscribed lists are downloaded, the option for ignoring certificate warnings is recognized again, which had temporarily not worked and caused downloads to fail.
WP-2459	When the web security policy on Web Gateway is extended to the cloud, requests are no longer blocked without providing a value for the block reason, which had led to allowing requests where they should have been blocked.
WP-2500	When a prefix has been configured for Syslog events,*mwg* is no longer shown instead as prefix in these events, which had happened due to a Java code issue.
WP-2602	In a list that is used for application control on Web Gateway and stored in a database for items related to Layer 7, several relevant domain names have been added.
WP-2675	Password-protected 7-zip archives that were created using the BCJ2 filter are correctly detected as encrypted and not marked as corrupted when they are not.
WP-2685	Under application control on Web Gateway, the ADRM application is no longer inappropriately marked as High Risk.

Table 2-62 Vulnerabilities

Reference	Resolution
WP-2348, WP-2545, WP-2556, WP-2638, WP-2651, WP-2690	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-2015-2716 • CVE-2018-1116, CVE-2018-1311, CVE-2018-10360, CVE-2018-10916, CVE-2018-18066, CVE-2018-18751, CVE-2018-20852 • CVE-2019-5436, CVE-2019-5953, CVE-2019-6465, CVE-2019-6477, CVE-2019-9924, CVE-2019-13232, CVE-2019-16056, CVE-2019-17041, CVE-2019-17569 • CVE-2020-1935, CVE-2020-1938, CVE-2020-2754, CVE-2020-2755, CVE-2020-2756, CVE-2020-2757, CVE-2020-2773, CVE-2020-2781, CVE-2020-2800, CVE-2020-2803, CVE-2020-2805, CVE-2020-2830, CVE-2020-5208, CVE-2020-10531 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-63 Other

Reference	Resolution
WP-2289	System lists can be updated again without problems, which occurred when updates were attempted several times, as it had not been recorded that updating job had already been done.
WP-2295	Threads are removed again after having been processed on Web Gateway, which had not worked previously and led to a failure of the core process after reaching the maximum number of threads allowed per process.
WP-2407	Website content that users request under HTTP2 is properly displayed by Web Gateway again with no spaces left blank unintentionally anymore.
WP-2533	The /opt partition of the appliance system is no longer filled up and the mwg-core temp file does not increase excessively anymore when large downloads are performed, which had impacted performance and happened due to problems with handling size limits.

Rating for update 9.2.19

The rating defines the urgency for installing this update.

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