Revision C

McAfee Web Gateway 11.1.x Release Notes

Contents

What's new in the 11.1 release

This release introduces new features and enhances existing features.

ℹ McAfee® Web Gateway 11.1 is provided as a controlled release.

For information about how to upgrade to this release, see Upgrading to a new version provided as a controlled release in the *McAfee Web Gateway Installation Guide*.

Radius-based authentication and management of CLI-based administrator accounts

On the Web Gateway user interface, you can as an administrator create CLI-based accounts for other administrators. Each of these accounts works across all the appliances in a cluster or on a standalone appliance. Logon is enabled based on Radius authentication or local authentication depending on the configuration.

For more information, see the *Administrator accounts* chapter of the *McAfee Web Gateway 11.1.x Product Guide*.

Configurable ISTag header parameters for ICAP server responses

You can choose and configure additional parameters for the ISTag header that is sent in responses to the ICAP clients when Web Gateway runs as an ICAP server. The header can also provide information about the version of the web protection policy that is in place on this Web Gateway appliance.

For more information, see the *Proxies* chapter of the *McAfee Web Gateway 11.1.x Product Guide*.

Terminating client connections on the command line interface

You can terminate a client connection by running a command on the command line interface (CLI). The reason for terminating a connection might be that the traffic on this connection consumes too much bandwidth.

Event for removing headers based on wildcard matches

Using the **Header.RemoveAllWildcardMatchingHeaders** event in a rule, you can remove all headers that match a given wildcard from requests and responses sent and received in web traffic that is processed on Web Gateway.

Property for encoding a string under the Base64 method and rendering the result in binary format

Using the **String.Base64EncodeAsBinary** property in a rule, you can have a string encoded under the Base64 method and the result of this encoding turned into a string of binary digits.

Resolved issues in the 11.1.2 release

This release resolves known issue.

For a list of known issues that are currently unresolved, see McAfee Web Gateway 11.x Known Issues (KB94979).

McAfee® Web Gateway 11.1.2 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 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 the 11.1.1 release

This release resolves known issues.

For a list of known issues that are currently unresolved, see McAfee Web Gateway 11.x Known Issues (KB94979).

McAfee® Web Gateway 11.1.1 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 2-2 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.
WP-4450	The mwg-snmp.service unit is available again now after a reboot of Web Gateway.
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 the 11.1 release

This release resolves known issues.

For a list of known issues that are currently unresolved, see McAfee Web Gateway 11.x Known Issues (KB94979).

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-5 Network communication

Reference	Resolution
WP-4255	A check status issue has been fixed. It had happened when a handshake using TLS1.3 connection retries had not worked as expected due to a broken server connection.
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.
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.
WP-3247	The mcelog service is only enabled on physical appliances now and remains disabled on virtual appliances.
WP-4234	Block rules work as expected after the Auth.Username property is filled with values again.

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	A high CPU issue observed in several customer installations of Web Gateway 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.
WP-4384	Luna HSM on 5500-E is running normal after a Web Gateway upgrade to 10.2.5.
WP-4404	Web Gateway 9.2.x and 10.2.x can be successfully upgraded to 10.2.6 and 11.1 when quagga is installed.
WP-3346	SNMP restarts normally after an upgrade to Web Gateway 10.0.
WP-4243	Processing of cluster messages within the notification plugin has been improved.
WP-4232	Connection tracing is off per default.
WP-4280	Failures of the core process do not occur anymore.
WP-4390	Authentication with GetUserAzureGroups is working fine after clearing the cache.
WP-4402	Map.GetStringValue returns the expected value for an existing key-value pair.
WP-4405	OCSP database handling performance is enhanced.

Table 2-8 Vulnerabilities

Reference	Resolution
WP-3335, WP-4131, WP-4159, WP-4197, WP-4237, WP-4259, WP-4279, 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-2019-20892, CVE-2020-15862 • 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-2018-6678 • 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.

Rating for update 11.1.2

The rating defines the urgency for installing this update.

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