Revision E

McAfee Web Gateway 11.0.x Release Notes

Contents

What's new in the 11.0 release

This release introduces new features and enhances existing features.

McAfee® Web Gateway 11.0 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*.

Download of lists maintained under MVISION Unified Cloud Edge for on-prem web policy

You can download lists of user names, user groups, and other web objects that are maintained under MVISION Unified Cloud Edge for the on-prem policy that you set up on Web Gateway

The lists are continually synchronized. When enabling the download on Web Gateway, you set the synchronization interval.

This download feature is a part of a Hybrid solution that allows you to filter web traffic using both Web Gateway and MVISION Unified Cloud Edge.

For more information, see Synchronize lists for your web policy when using a Hybrid solution in the *McAfee Web Gateway Product Guide*.

Secure net-hop proxy for securing traffic to MVISION Unified Cloud Edge

You can set up a secure next-hop proxy on Web Gateway to ensure traffic going to MVISION Unified Cloud Edge is secure.

The traffic follows the TLS protocol. A certificate is presented at the initial handshake from the server side whereas Web Gateway uses the authentication method that is enabled by Client Proxy to authenticate to MVISION Unified Cloud Edge.

For more information, see Set up a secure next-hop proxy to secure traffic on a Hybrid connection in the *McAfee Web Gateway Product Guide*.

Use of keywords to filter lists with Azure Active Directory group names

When searching lists of user groups stored in an Azure Active Directory, you can use a keyword to filter the search result. You can create lists of keywords and use more than one in a search.

For more information, see Azure Directory settings in the *McAfee Web Gateway Product Guide*.

SmartMatch optimization

Performance has been optimized for SmartMatch lookups by improving the handling of partial matches in URL lists.

For more information, see the entry on the **URL.SmartMatch** property under Properties — U in the *McAfee Web Gateway Product Guide*.

Improved detection of CPIO application type

Applications of the *application/x-cpio* type are properly recognized through improving the methods for their detection, which had only relied on checking the file header before and caused incorrect further treatment, for example, being rated as corrupt by the file opener.

New locations for storing cloud access log data

New options available when choosing the country or region where cloud access log data are stored, including Canada, United Kingdom, United Arab Emirates, and Singapore.

For more information, see Cloud Access Log Data Residency settings in the *McAfee Web Gateway Product Guide*.

Recognition of intermediary HTTP2 headers

When receiving web traffic from servers that support HTTP2 on the connection to Web Gateway, headers with status code 1xx are recognized by Web Gateway as intermediary headers preceding the main headers and processed accordingly.

Improved handling of HTTP2 statistics

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.

For more information about how to configure this protocol, see Event monitoring with SNMP in the *McAfee Web Gateway Product Guide*.

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 efficient troubleshooting methods

More efficient methods are used now to identify customers, clients, and connections relating to high load or overload issues in temp files on Web Gateway.

Resolved issues in update 11.0.2

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 11.0.2 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*.

Resolved issue

JIRA issue number is provided in the reference column below.

Table 2-1 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 11.0.1

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 11.0.1 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*.

Resolved issues

JIRA issue numbers are provided in the reference columns below.

Table 2-2 Web filtering

Reference	Resolution
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.

Table 2-3 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 the 11.0 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 2-4 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-3637	When the NTLM authentication method is applied, submitting user names in the User Principal Name (UPN) format does not lead to a failure of the authentication process anymore.
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.
WP-4073	When using the IP Neigh network tool for troubleshooting on a Web Gateway appliance with an HTML-based user interface, bindings between protocol and link layer addresses are displayed again.

Table 2-5 Authentication

Reference	Resolution
WP-3637	When the NTLM authentication method is applied, submitting user names in the User Principal Name (UPN) format does not lead to a failure of the authentication process anymore.

Table 2-6 Web filtering

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-3663	When running Advanced Threat Defense (ATD) to scan web traffic, a previous detection of malware can be reused, which had not worked for a zip file due to incorrectly querying md5 information.
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-3904	Infinite loops that were created on some occasions when zip archives were scanned, causing threads to hang and resulting in problems with high CPU and memory load, do no longer occur.

Table 2-7 Vulnerabilities

Reference	Resolution
WP-3468, WP-3580, WP-3656, WP-3765, WP-3792, WP-3806, WP-3815, WP-3878, WP-3882, WP-3934, WP-3935, WP-3936, WP-3999, WP-4003, WP-4021, WP-4058, WP-4067, 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-2016-3674 • CVE-2017-7957 • CVE-2017-11610 • CVE-2019-10208, • CVE-2020-15250 • CVE-2020-24489 • CVE-2020-25111, CVE-2020-25112, CVE-2020-25113, CVE-2020-25648, CVE-2020-25649, CVE-2020-25694, CVE-2020-25695 • CVE-2020-26217 • CVE-2021-2369, CVE-2021-2388 • CVE-2021-3472 • CVE-2021-3520 • CVE-2021-3711, CVE-2021-3712 • 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-2021-25214, CVE-2021-25217 • CVE-2021-27219 • CVE-2021-30640 • CVE-2021-31535 • CVE-2021-32027 • CVE-2021-33909 For more information about these CVEs and their impact, see the Red Hat CVE portal.

Table 2-8 Other

Reference	Resolution
WP-2686	Documents containing Austrian IBAN numbers are detected with the Data Loss Protection (DLP) functions on Web Gateway even if spaces between number groups are omitted.
WP-3951	An issue that caused the core process on a Point-of-Presence (PoP) for Web Gateway to fail has been resolved.
WP-3998	An issue that caused the core process on Web Gateway running as a node in a cluster to fail has been resolved.
WP-4010	The latest KVM build for the Oracle Cloud Infrastructure (OCI) that Web Gateway runs with can be downloaded again.

Table 2-8 Other *(continued)*

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