



McAfee®

Email Gateway 7.0.2

Release Notes for McAfee® Email Gateway

Version 7.0

Patch 7.0.2

Copyright © 2012 McAfee, Inc.

All Rights Reserved

About this release

Thank you for using our software. This file contains important information about this release. We strongly recommend that you read the entire document.

[About this release](#)

[Purpose](#)

[Packaging](#)

[Rating](#)

[Resolved issues](#)

[Additional functionality \(total: 15, new: 15\)](#)

[Vulnerabilities \(total: 10, new: 4\)](#)

[High severity issues \(total: 6, new: 4\)](#)

[Medium severity issues \(total: 43, new: 31\)](#)

[Low severity issues \(total: 67, new: 62\)](#)

[Issues list](#)

[Issues resolved in previous releases](#)

[Additional information](#)

[Incremental update package](#)

[Installation requirements](#)

[Superseded releases](#)

[Actions on installation](#)

[External components installed by this package](#)

[Files included with this package](#)

[Installation steps](#)

[After installation](#)

[Removing this package](#)

[Installable images](#)

[Superseded releases](#)

[Notices](#)

[Copyright](#)

[Trademark attributions](#)

[License information](#)

[License Agreement](#)

Purpose

This release addresses the issues shown in the [Resolved issues](#) section below.

Packaging

This release is available in the form of:

- an [incremental update package](#)
- a set of [installable images](#)

Rating

This release addresses critical issues. McAfee strongly recommends implementing this release at your earliest opportunity.

Severity of issues listed below is based on these definitions:

- **High**
a critical issue which should be addressed as soon as possible, if necessary outside a planned maintenance schedule.
- **Medium**
an issue which should be addressed at the earliest opportunity, normally as part of a planned maintenance schedule.
- **Low**
a non-critical issue, advisable to address as part of planned maintenance.

Resolved issues

Additional functionality (total: 15, new: 15)

Additional functionality in this release:

[f_753960](#), [f_755637](#), [f_758141](#), [f_759501](#), [f_762436](#), [f_766563](#), [f_769073](#), [f_770973](#),
[f_771755](#), [f_778066](#), [f_778293](#), [f_778530](#), [f_778711](#), [f_779123](#), [f_782518](#)

Vulnerabilities (total: 10, new: 4)

Vulnerabilities newly addressed in this release:

[f_713692](#), [f_759635](#), [f_764456](#), [f_769711](#)

Vulnerability fixes included from previous releases:

[f_765419](#), [f_781825](#), [f_788824](#), [f_789886](#), [f_759607](#), [f_753669](#)

High severity issues (total: 6, new: 4)

High severity issues newly addressed in this release:

[f_753960](#), [f_759635](#), [f_769711](#), [f_771755](#)

High severity fixes included from previous releases:

[f_788824](#), [f_759607](#)

Medium severity issues (total: 43, new: 31)

Medium severity issues newly addressed in this release:

[f_739701](#), [f_754025](#), [f_754883](#), [f_754884](#), [f_754900](#), [f_755637](#), [f_756072](#), [f_759030](#),
[f_759501](#), [f_761923](#), [f_762815](#), [f_764456](#), [f_766563](#), [f_769073](#), [f_770973](#), [f_771763](#),
[f_773085](#), [f_778066](#), [f_778293](#), [f_778530](#), [f_778711](#), [f_779123](#), [f_780481](#), [f_780499](#),
[f_782518](#), [f_787944](#), [f_789833](#), [f_792627](#), [f_792860](#), [f_793512](#), [f_793707](#)

Medium severity fixes included from previous releases:

[f_792650](#), [f_765419](#), [f_765437](#), [f_766131](#), [f_788869](#), [f_789643](#), [f_789886](#), [f_764326](#),
[f_774667](#), [f_777245](#), [f_758342](#), [f_753669](#)

Low severity issues (total: 67, new: 62)

Low severity issues newly addressed in this release:

[f_636159](#), [f_713692](#), [f_727123](#), [f_731359](#), [f_742363](#), [f_743455](#), [f_751989](#), [f_753567](#),
[f_753633](#), [f_753671](#), [f_754508](#), [f_754894](#), [f_754899](#), [f_756031](#), [f_756116](#), [f_756765](#),
[f_756777](#), [f_756784](#), [f_756898](#), [f_757206](#), [f_757621](#), [f_758141](#), [f_758349](#), [f_758355](#),
[f_758398](#), [f_759403](#), [f_760297](#), [f_762377](#), [f_762436](#), [f_763533](#), [f_763748](#), [f_765250](#),
[f_765303](#), [f_767982](#), [f_771889](#), [f_772506](#), [f_773306](#), [f_773470](#), [f_773477](#), [f_773650](#),
[f_773943](#), [f_774658](#), [f_774988](#), [f_775001](#), [f_775280](#), [f_775588](#), [f_780241](#), [f_781285](#),
[f_782867](#), [f_782889](#), [f_782895](#), [f_782898](#), [f_782899](#), [f_783417](#), [f_783666](#), [f_784392](#),

[f_785422](#), [f_785570](#), [f_786680](#), [f_787730](#), [f_791861](#), [f_800921](#)

Low severity fixes included from previous releases:

[f_781825](#), [f_789113](#), [f_754010](#), [f_778492](#), [f_764779](#)

Issues list

- Feature [f_753960](#)
 - Description:
The Secure Web Delivery feature has been enhanced to support pull messages in the Blade and Cluster environment.
Please refer to KnowledgeBase article [KB76059](#) for more information.
 - Severity: High
- Feature [f_759635](#)
 - Description:
ISSUE: Vulnerabilities [CVE-2012-0053](#), [CVE-2012-0031](#), [CVE-2012-0021](#) were reported against the apache version used by the appliance.
RESOLUTION: The apache package has been updated to address the problem.
Please refer to KnowledgeBase article [KB76079](#) for more information.
 - Severity: High
- Feature [f_769711](#)
 - Description:
ISSUE: The appliance uses HTTPS for secure access to the user interface. An HTTPS connection to the appliance may be subject to SSL vulnerability [CVE-2011-3389](#), allowing a blockwise chosen-boundary attack (BCBA, also known as "BEAST") if a cipher suite that uses a block cipher, such as AES, is negotiated during the SSL handshake.
RESOLUTION: The appliance is now configured to always use a stream cipher, RC4, if the client software supports it.
Please refer to KnowledgeBase article [KB75874](#) for more information.
 - Severity: High
- Feature [f_771755](#)
 - Description:
The password management on the appliance has been modified to allow the minimum number of different characters in a password to be configured by the user.
Please refer to KnowledgeBase article [KB76050](#) for more information.
 - Severity: High
- Feature [f_788824](#)
 - Description:
ISSUE: Vulnerability [VU#118913](#) (covering [CVE-2012-1766](#), [CVE-2012-1767](#), [CVE-2012-1768](#), [CVE-2012-1769](#), [CVE-2012-1770](#), [CVE-2012-1771](#), [CVE-2012-1772](#), [CVE-2012-1773](#), [CVE-2012-3106](#), [CVE-2012-3107](#), [CVE-2012-3108](#), [CVE-2012-3109](#), [CVE-2012-3110](#)) was reported against the Oracle Outside In library used on the appliance.
RESOLUTION: The Outside In library has been updated to address the problem.
Please refer to KnowledgeBase article [KB75864](#) for more information.
 - Previously addressed by [7.0h788861](#), [7.0h793047](#).
 - Severity: High
- Feature [f_759607](#)
 - Description:
Multiple security vulnerabilities in the appliance user interface were resolved, including a bypass of authentication controls.
Please refer to KnowledgeBase article [KB75077](#) for more information.
 - Previously addressed by [7.0h759601](#), [7.0h778488](#), [7.0h788861](#), [7.0h793047](#).
 - Severity: High
- Feature [f_739701](#)
 - Description:
The appliance has the ability to log email SPF events to syslog. The syslog format for SPF events has been changed to incorporate the full SPF result in the log message.
Please refer to KnowledgeBase article [KB74083](#) for more information.

- Severity: Medium
- Feature f_754025
 - Description:

ISSUE: The appliance is able to display the status of the Out of Band management interface on the dashboard. An issue with the monitoring service was causing an error status to be displayed when the interface was disabled and disconnected.

RESOLUTION: The monitoring service has been modified to correctly display the state of the Out of Band management interface when it is disabled and disconnected.

Please refer to KnowledgeBase article [KB75376](#) for more information.
 - Severity: Medium
- Feature f_754883
 - Description:

ISSUE: The appliance offers the facility to filter email using the McAfee Global Threat Intelligence (GTI) message reputation service. With GTI message reputation checking enabled on the appliance, it was possible that email attachments could get corrupted under certain circumstances due to an incorrect length calculation.

RESOLUTION: The length calculation has been corrected.

Please refer to KnowledgeBase article [KB74681](#) for more information.
 - Severity: Medium
- Feature f_754884
 - Description:

ISSUE: The appliance has the facility to use a pool of addresses when making outbound connections to deliver email. In a cluster deployment the address pool was not being used when selecting an outbound address, hence connections were being made using the physical address of the master appliance.

RESOLUTION: The outbound connection routine has been modified to use an address from the outbound address pool.

Please refer to KnowledgeBase article [KB74680](#) for more information.
 - Severity: Medium
- Feature f_754900
 - Description:

ISSUE: The appliance has a facility for Bounce Address Tag Validation (BATV) on email, validating and stripping BATV tags on replies to emails that were originally tagged by the appliance. However, BATV tag validation and stripping was done only when the sender address was null (with mail from set to <>, as is usual with a bounced email). If the sender address was not null, BATV tags were not validated or stripped.

RESOLUTION: It is now possible to configure BATV in such a way that tagged addresses for incoming emails are validated and stripped even if the sender address is not null.

Please refer to KnowledgeBase article [KB73687](#) for more information.
 - Severity: Medium
- Feature f_755637
 - Description:

The appliance now has the ability to bypass all scanning and traffic interception for transparent mode TLS connections.

Please refer to KnowledgeBase article [KB76077](#) for more information.
 - Severity: Medium
- Feature f_756072
 - Description:

ISSUE: The appliance supports configuration import from previous versions. An error in the migration module caused an incomplete migration under certain circumstances when restoring a version 5.5 configuration. This caused the "System->Logging, Alerting and SNMP settings" page to issue an error.

RESOLUTION: The error in the migration module has been corrected.

Please refer to KnowledgeBase article [KB74977](#) for more information.
 - Severity: Medium
- Feature f_759030
 - Description:

ISSUE: The auto-update facility on the appliance has the capability to generate

notification events via email and SNMP when new update packages are available to install. It was not possible to enable these notifications via the user interface.

RESOLUTION: The base configuration has been updated to correct this.

Please refer to KnowledgeBase article [KB75339](#) for more information.

- Severity: Medium
- Feature f_759501
 - Description:

The appliance can now continuously generate and send email traffic to itself in the VMTrial edition. Test email traffic can be used to test policies, and to see how detections and mail flow are reported within the appliance user interface. Continuous test email generation is enabled from the user interface Troubleshooting pages on the VMTrial appliance.

Please refer to KnowledgeBase article [KB76053](#) for more information.
 - Severity: Medium
- Feature f_761923
 - Description:

ISSUE: The appliance uses the Apache HTTP server to provide the user interface. Apache version information was being unnecessarily included in HTTP response headers and error documents.

RESOLUTION: The Apache configuration has been changed remove the version data.

Please refer to KnowledgeBase article [KB76199](#) for more information.
 - Severity: Medium
- Feature f_762815
 - Description:

ISSUE: The appliance can synchronize LDAP attributes to its local cache, and can verify email addresses against the cached data. An issue in the cache system prevented the validation of recipients with multiple email address entries.

RESOLUTION: The appliance cache system has been updated to ensure multiple email address attributes are handled correctly.

Please refer to KnowledgeBase article [KB76274](#) for more information.
 - Severity: Medium
- Feature f_764456
 - Description:

ISSUE: Vulnerabilities [CVE-2012-0884](#), [CVE-2012-1165](#), [CVE-2012-2110](#), [CVE-2012-2131](#), [CVE-2012-2333](#) were reported against the OpenSSL version used by the appliance.

RESOLUTION: The OpenSSL package has been updated to address the problem.

Please refer to KnowledgeBase article [KB74898](#) for more information.

Please refer to KnowledgeBase article [KB75312](#) for more information.

Please refer to KnowledgeBase article [KB75334](#) for more information.
 - Severity: Medium
- Feature f_766563
 - Description:

The appliance can now be configured to notify the administrator when the Engine and DAT updates have not been performed for a specified period of time.

Please refer to KnowledgeBase article [KB76061](#) for more information.
 - Severity: Medium
- Feature f_769073
 - Description:

The appliance can now apply the existing recipient aliasing functionality to [RFC 822](#) email headers.

Please refer to KnowledgeBase article [KB76080](#) for more information.
 - Severity: Medium
- Feature f_770973
 - Description:

The appliance user interface has been enhanced to include the facility to export and import the contents of lists throughout.

Please refer to KnowledgeBase article [PD23757](#) for more information.
 - Severity: Medium
- Feature f_771763

- Description:
ISSUE: The appliance can deliver mail to an onward server whilst the client is still connected. An issue with the SMTP proxy was intermittently causing the client connection to be dropped when the onward server sent an unexpected response.
RESOLUTION: The SMTP proxy has been modified to correctly handle unexpected responses from the onward server.
Please refer to KnowledgeBase article [KB76013](#) for more information.
 - Severity: Medium
- Feature f_773085
 - Description:
ISSUE: The appliance can be configured to use SPF to authenticate the sender of an email. Events for SPF could not be enabled and disabled independently, and were not configurable for the syslog and SNMP channels.
RESOLUTION: The user interface has been updated to allow SPF event generation to be controlled independently for the syslog and SNMP channels.
Please refer to KnowledgeBase article [KB75337](#) for more information.
 - Severity: Medium
- Feature f_778066
 - Description:
The appliance favorite reports can now be exported as a CSV format file.
Please refer to KnowledgeBase article [KB76078](#) for more information.
 - Severity: Medium
- Feature f_778293
 - Description:
The results of a Message Search can now be exported as a CSV format data file.
Please refer to KnowledgeBase article [KB76051](#) for more information.
 - Severity: Medium
- Feature f_778530
 - Description:
The appliance can now be configured to raise an alert when the number of messages in the email queues exceed certain thresholds.
Please refer to KnowledgeBase article [KB76074](#) for more information.
 - Severity: Medium
- Feature f_778711
 - Description:
The appliance can now be configured to report the names of email attachments in Message Search.
Please refer to KnowledgeBase article [KB76275](#) for more information.
 - Severity: Medium
- Feature f_779123
 - Description:
The appliance now allows the administrator to revert the Anti-Virus DAT to a previously installed version. NOTE: This operation should only be attempted if advised by McAfee Technical support.
Please refer to KnowledgeBase article [KB76081](#) for more information.
 - Severity: Medium
- Feature f_780481
 - Description:
ISSUE: The appliance supports auto updating from FTP. An issue in the FTP update script was preventing updates occurring when an FTP proxy server was in use.
RESOLUTION: The FTP update script has been modified to correctly handle transfer through an FTP proxy.
Please refer to KnowledgeBase article [KB75888](#) for more information.
 - Severity: Medium
- Feature f_780499
 - Description:
ISSUE: The appliance can be configured to periodically backup configuration to an FTP server. An issue in the FTP upload script caused the FTP upload to fail when the FTP credentials contained certain special characters.
RESOLUTION: The FTP upload script has been modified to correctly handle special characters in the FTP credentials.

- Please refer to KnowledgeBase article [KB75671](#) for more information.
 - o Severity: Medium
- Feature f_782518
 - o Description:

The appliance now supports importing of lists that can be exported from MEG6 HF8. The supported lists are TLS domains, Internal Servers and Domain & User groups.

Please refer to KnowledgeBase article [KB76052](#) for more information.
 - o Severity: Medium
- Feature f_787944
 - o Description:

ISSUE: The appliance user interface allows the administrator to search and display the details of messages that have been processed by the appliance. An issue in the SMTP proxy was causing the message size of a modified email to be displayed incorrectly.

RESOLUTION: The SMTP proxy has been modified to log the correct size of a modified message.

Please refer to KnowledgeBase article [KB76028](#) for more information.
 - o Severity: Medium
- Feature f_789833
 - o Description:

ISSUE: The appliance is able to archive and transfer syslog files to an external server. An issue in the transfer script was causing an incomplete file to be transferred to the external server under certain circumstances.

RESOLUTION: The transfer script has been corrected to ensure the archive transfer is completed before termination.

Please refer to KnowledgeBase article [KB76031](#) for more information.
 - o Severity: Medium
- Feature f_792627
 - o Description:

ISSUE: The appliance encryption feature can be configured to allow email recipients to construct replies to secure messages using the Secure Web Mail Client (SWMC) interface. An issue in the code which attaches files to messages caused the original file path to be exposed in the email.

RESOLUTION: The attachment code has been corrected, and now does not expose the file path.

Please refer to KnowledgeBase article [KB76041](#) for more information.
 - o Severity: Medium
- Feature f_792860
 - o Description:

ISSUE: The appliance includes Secure Web Delivery. When a user receives a secure message for the first time, they receive a notification that an account has been created. An issue in the Secure Web Delivery library was causing an unread message notification to be sent to the recipient.

RESOLUTION: The issue in the Secure Web Delivery library has been corrected to ensure unread message notifications are not sent until the appropriate configured time.

Please refer to KnowledgeBase article [KB76049](#) for more information.
 - o Severity: Medium
- Feature f_793512
 - o Description:

ISSUE: The appliance can be configured to detect file-based Denial of Service attempts. An issue in the decomposition engine was causing certain Excel spreadsheet files to be detected as a Denial of Service attempt.

RESOLUTION: The decomposition engine has been upgraded.

Please refer to KnowledgeBase article [KB76040](#) for more information.
 - o Severity: Medium
- Feature f_793707
 - o Description:

ISSUE: The appliance has a quarantine facility that allows end users to manage their quarantine via an email quarantine digest. When configured for operation in

certain languages an issue in the quarantine management interface was causing email subject lines to display incorrectly.

RESOLUTION: The quarantine management interface has been modified to correctly encode subject lines.

Please refer to KnowledgeBase article [KB76107](#) for more information.

- Severity: Medium
- Feature f_792650
 - Description:

ISSUE: The appliance has a web-mail user interface for viewing secure emails. Some emails read using this Secure Web Mail Client were not registered as having been read. Such emails continued to be shown as unread in the mailbox list, and any read-receipts requested were not sent.

RESOLUTION: The cause was found to be an address parsing error, which has been corrected.

Please refer to KnowledgeBase article [KB75965](#) for more information.
 - Previously addressed by 7.0h793047.
 - Severity: Medium
- Feature f_765419
 - Description:

ISSUE: Vulnerabilities [CVE-2012-0554](#), [CVE-2012-0555](#), [CVE-2012-0556](#), [CVE-2012-0557](#) were reported against the Oracle Outside In library used on the appliance.

RESOLUTION: The Outside In library has been updated to address the problem.

Please refer to KnowledgeBase article [KB75342](#) for more information.
 - Previously addressed by 7.0h788861, 7.0h793047.
 - Severity: Medium
- Feature f_765437
 - Description:

ISSUE: The appliance offers content scanning into the text of certain file types by means of a third party plugin. There was an issue in this plugin which resulted in the SMTP proxy failing with a segmentation violation when particular attachment files were scanned.

RESOLUTION: The third party plugin has been updated to handle these files.

Please refer to KnowledgeBase article [KB74024](#) for more information.

Please refer to KnowledgeBase article [KB75180](#) for more information.

Please refer to KnowledgeBase article [KB75251](#) for more information.
 - Previously addressed by 7.0h788861, 7.0h793047.
 - Severity: Medium
- Feature f_766131
 - Description:

ISSUE: The appliance has the facility to filter images in email for unacceptable content. It was found that some small images, logos and icons, were incorrectly blocked.

RESOLUTION: The configuration for the image filtering algorithm has been modified to prevent small images being incorrectly blocked.

Please refer to KnowledgeBase article [KB75458](#) for more information.
 - Previously addressed by 7.0h788861, 7.0h793047.
 - Severity: Medium
- Feature f_788869
 - Description:

ISSUE: The appliance offers content scanning into the text of certain file types by means of a third party plugin. The plugin was found to perform poorly on some Microsoft Excel files, impeding email traffic.

RESOLUTION: The third party plugin has been updated to handle these files.

Please refer to KnowledgeBase article [KB75866](#) for more information.
 - Previously addressed by 7.0h788861, 7.0h793047.
 - Severity: Medium
- Feature f_789643
 - Description:

ISSUE: The appliance offers secure web access to email for users. Due to fixed limits in some versions of Internet Explorer, some users were unable to access the secure email web interface.

RESOLUTION: The user interface configuration has been adjusted to mitigate the problem.

Please refer to KnowledgeBase article [KB75887](#) for more information.

- Previously addressed by 7.0h788861, 7.0h793047.
- Severity: Medium
- Feature f_789886
 - Description:
ISSUE: Vulnerability [CVE-2012-1033](#) was reported against the BIND version used on the appliance.
RESOLUTION: The BIND package has been updated to address the problem.
Please refer to KnowledgeBase article [KB75889](#) for more information.
 - Previously addressed by 7.0h788861, 7.0h793047.
 - Severity: Medium
- Feature f_764326
 - Description:
ISSUE: The appliance has a web-mail user interface for composing secure emails. Due to a file encoding issue affecting the Internet Explorer browser, attempts to add attachments to emails were failing with an error message "There was a problem communicating with the Secure Web Mail system".
RESOLUTION: The encoding of the file upload has been modified to parse correctly in Internet Explorer.
Please refer to KnowledgeBase article [KB75476](#) for more information.
 - Previously addressed by 7.0h778488, 7.0h788861, 7.0h793047.
 - Severity: Medium
- Feature f_774667
 - Description:
ISSUE: The appliance has a web-mail user interface for viewing secure emails. An issue with the interpretation of the 'Content-ID' MIME header in messages composed by some mail clients, prevented the display of email attachments in the web-mail client.
RESOLUTION: The code used to interpret message headers for the web-mail client has been modified to correctly identify attachments.
Please refer to KnowledgeBase article [KB75630](#) for more information.
 - Previously addressed by 7.0h778488, 7.0h788861, 7.0h793047.
 - Severity: Medium
- Feature f_777245
 - Description:
ISSUE: The appliance has a web-mail user interface for viewing secure emails. An issue with the interpretation of the MIME type of the message body was causing calendar invitations to be displayed as raw text.
RESOLUTION: The user interface has been modified to display unrecognized textual parts of an email as attachments.
Please refer to KnowledgeBase article [KB75623](#) for more information.
 - Previously addressed by 7.0h778488, 7.0h788861, 7.0h793047.
 - Severity: Medium
- Feature f_758342
 - Description:
ISSUE: The appliance has the facility to change or compare email addresses using LDAP data. The targetAddress attribute provided by some LDAP servers was not correctly processed.
RESOLUTION: The LDAP targetAddress attribute is now handled correctly.
Please refer to KnowledgeBase article [KB75091](#) for more information.
 - Previously addressed by 7.0h758342, 7.0h778488, 7.0h788861, 7.0h793047.
 - Severity: Medium
- Feature f_753669
 - Description:
ISSUE: Vulnerability [CVE-2003-1418](#) was reported against the Apache version used by the appliance.
RESOLUTION: The Apache configuration used on the appliance has been updated to address the problem.
Please refer to KnowledgeBase article [KB74962](#) for more information.

- Previously addressed by 7.0h753669, 7.0h759601, 7.0h778488, 7.0h788861, 7.0h793047.
 - Severity: Medium
- Feature f_636159
 - Description:

ISSUE: The appliance has a facility to produce reports of detections. Due to an error in the reporting database module, a policy name change was not being reflected in the generated reports

RESOLUTION: The reporting database module has been corrected to ensure the policy name is updated when necessary.

Please refer to KnowledgeBase article [KB74909](#) for more information.
 - Severity: Low
- Feature f_713692
 - Description:

ISSUE: Vulnerability [CVE-2011-3368](#) was reported against the apache version used by the appliance.

RESOLUTION: The apache package has been updated to address the problem.

Please refer to KnowledgeBase article [KB74003](#) for more information.
 - Severity: Low
- Feature f_727123
 - Description:

ISSUE: The appliance offers the ability to configure primary and secondary actions when a scanner triggers. One of these is the ability to reroute the email to a different MTA instead of the default routing path. A user interface problem in the Anti-Spam and Content Settings prevented this action from taking effect.

RESOLUTION: The User Interface has been updated to allow emails to be rerouted correctly.

Please refer to KnowledgeBase article [KB73655](#) for more information.
 - Severity: Low
- Feature f_731359
 - Description:

ISSUE: On some hardware platforms the appliance uses the MegaCli tool to monitor RAID status. MegaCli was logging debug output in the /root directory which could fill the disk space.

RESOLUTION: MegaCli tool invocation is changed so that it no longer outputs debug logs.

Please refer to KnowledgeBase article [KB73840](#) for more information.
 - Severity: Low
- Feature f_742363
 - Description:

ISSUE: The appliance can be configured to display the status of a connected UPS device. Due to an error in the UPS monitoring script, when a UPS device connected to the appliance by USB cable was running on battery, the appliance was failing to display the status.

RESOLUTION: The UPS monitoring script has been corrected to acquire the UPS status accurately.

Please refer to KnowledgeBase article [KB74851](#) for more information.
 - Severity: Low
- Feature f_743455
 - Description:

ISSUE: The appliance allows configuration of per-domain SMTP relays. Due to incorrect validation of relay names entered in the user interface it was possible for an invalid DNS configuration to be saved, which would prevent DNS working on the appliance and block email flow.

RESOLUTION: The relay validation in the user interface has been corrected.

Please refer to KnowledgeBase article [KB76075](#) for more information.
 - Severity: Low
- Feature f_751989
 - Description:

The appliance supports status monitoring via SNMP. The SNMP support has been enhanced to clearly indicate the state values using an enumerated INTEGER type in

- the MIB file.
Please refer to KnowledgeBase article [KB75432](#) for more information.
- o Severity: Low
- Feature f_753567
 - o Description:
ISSUE: The appliance can update its spam engine over FTP. When configured to use an FTP proxy the appliance was unable to update due to an issue with the spam engine update script.
RESOLUTION: The spam engine update script has been corrected to work with FTP proxies
Please refer to KnowledgeBase article [KB74719](#) for more information.
 - o Severity: Low
- Feature f_753633
 - o Description:
ISSUE: The appliance can be configured to detect Corrupted and Encrypted email content and reports showing only such detections can be selected in the user interface. Due to an error in the reporting module the reports would incorrectly show nothing, because the appliance was failing to correctly log these detections to the database.
RESOLUTION: The error in the reporting module has been corrected.
Please refer to KnowledgeBase article [KB74814](#) for more information.
 - o Severity: Low
- Feature f_753671
 - o Description:
ISSUE: The appliance is able to generate a report of the current configuration. The configuration report generator was including information not applicable to the MEG software, and missing some information relating to the LDAP configuration.
RESOLUTION: The configuration report generator has been updated to no longer include the "User, Groups and Services" section. The LDAP configuration is now included.
Please refer to KnowledgeBase article [KB76076](#) for more information.
 - o Severity: Low
- Feature f_754508
 - o Description:
ISSUE: The appliance offers the facility to utilise syslog to output log messages. An error in the appliance configuration monitor script was preventing changes to the appliance hostname from being reflected in the syslog output.
RESOLUTION: The configuration monitor now applies the hostname change to the syslog module.
Please refer to KnowledgeBase article [KB74359](#) for more information.
 - o Severity: Low
- Feature f_754894
 - o Description:
ISSUE: The appliance offers a quarantine digest feature to send a summary of quarantined email to users. In a cluster environment the quarantine digest settings were not being synchronized due to an error in the synchronization module.
RESOLUTION: The error in the synchronization module has been corrected.
Please refer to KnowledgeBase article [KB74852](#) for more information.
 - o Severity: Low
- Feature f_754899
 - o Description:
ISSUE: The appliance offers the ability to quarantine emails to the off box McAfee Quarantine Manager (MQM). When a user or administrator releases a quarantined email stored on MQM it is sent to the appliance for delivery. If the email could not be delivered and the Directory Harvesting configuration was set to quarantine, these emails were incorrectly stored on the appliance, rather than being sent back to MQM.
RESOLUTION: The appliance quarantine functionality has been updated to ensure that when configured to use MQM, all quarantined emails are correctly sent off box.
Please refer to KnowledgeBase article [KB73663](#) for more information.
 - o Severity: Low
- Feature f_756031

- Description:

ISSUE: The appliance database has built in retention limits for events and delivery status, in both age and number of items. The age limits cannot be changed, but were incorrectly exposed in the user interface.

RESOLUTION: Text boxes for entering retention limits in days for events and delivery status in database have been removed.

Please refer to KnowledgeBase article [KB74089](#) for more information.
 - Severity: Low
- Feature f_756116
 - Description:

ISSUE: The appliance has the ability to synchronize with a LDAP directory server at regular intervals. Due to an issue with the schedule generation script it was not possible to disable the directory synchronization.

RESOLUTION: The issue in the directory synchronization schedule generation script has been corrected.

Please refer to KnowledgeBase article [KB75341](#) for more information.
 - Severity: Low
- Feature f_756765
 - Description:

ISSUE: The message search feature can display details of the messages that have been processed by the appliance. Under certain circumstances, the subject line of alert emails was displayed incorrectly due to an error in the email generation module.

RESOLUTION: The email generation module has been modified to ensure the correct subject line is generated for message search.

Please refer to KnowledgeBase article [KB74978](#) for more information.
 - Severity: Low
- Feature f_756777
 - Description:

ISSUE: The appliance dashboard has the facility to display the number of recipients queued for email delivery. Under certain circumstances the dashboard was displaying an incorrect number of queued recipients due to an issue in a database procedure.

RESOLUTION: The database procedure has now been corrected to correctly report the number of queued recipients.

Please refer to KnowledgeBase article [KB75004](#) for more information.
 - Severity: Low
- Feature f_756784
 - Description:

ISSUE: The appliance keeps a deferred queue of emails which cannot be delivered immediately. In some circumstances emails could appear in the deferred queue with a "0: Not Attempted" status. This could happen when the SMTP response from the onward MTA included an invalid UTF-8 byte sequence, or when one onward MTA was unresponsive for an email with multiple recipients.

RESOLUTION: These cases are now handled correctly.

Please refer to KnowledgeBase article [KB73847](#) for more information.
 - Severity: Low
- Feature f_756898
 - Description:

ISSUE: The appliance can selectively authenticate email recipients. A user interface issue affecting Internet Explorer prevented the correct display of the protocol preset recipient authentication checkbox.

RESOLUTION: The user interface code has been updated to ensure correct value is displayed in all supported browsers.

Please refer to KnowledgeBase article [KB76066](#) for more information.
 - Severity: Low
- Feature f_757206
 - Description:

ISSUE: The appliance user interface can restrict access to certain pages by the creation of custom roles. Due to an issue in the access control code, certain combinations of role privileges caused the user interface to become unresponsive when a user logged in and attempted to access some pages.

RESOLUTION: The access control code has been modified to correctly handle all combinations of role privileges.

Please refer to KnowledgeBase article [KB75194](#) for more information.

- Severity: Low
- Feature f_757621
 - Description:

ISSUE: The appliance features Bounce Address Tag Validation (BATV), and the ability to limit the length of email addresses. Due to an error in the address length calculation, the address local part length was being incorrectly calculated when BATV was enabled, resulting in a '501 Syntax error - Badly formatted address.' SMTP response under certain circumstances.

RESOLUTION: The address length calculation algorithm has been corrected to function correctly when BATV is enabled.

Please refer to KnowledgeBase article [KB75092](#) for more information.
 - Severity: Low
- Feature f_758141
 - Description:

ISSUE: The appliance uses various third party packages to assist in malware scanning. On occasions malfunctions in these packages can result in excessive scan times, adversely affecting appliance throughput.

RESOLUTION: A watchdog timer has been implemented to forcibly terminate scanning of any item after a configurable time limit.

Please refer to KnowledgeBase article [KB75044](#) for more information.
 - Severity: Low
- Feature f_758349
 - Description:

ISSUE: The appliance user interface can be configured to time out after a period of inactivity. An issue with inactivity detection, affecting only Internet Explorer, was causing the timeout to occur regardless of activity.

RESOLUTION: The activity detection code has been updated to function correctly in all browsers.

Please refer to KnowledgeBase article [KB75378](#) for more information.
 - Severity: Low
- Feature f_758355
 - Description:

ISSUE: The appliance can send notifications when the state of a network interface changes. Due to an issue with the monitoring service, email alerts reporting a change in state of the network interfaces were sometimes issued when configuration was applied.

RESOLUTION: The monitoring service has been modified to persist the state of the network interfaces during configuration application.

Please refer to KnowledgeBase article [KB75464](#) for more information.
 - Severity: Low
- Feature f_758398
 - Description:

ISSUE: The appliance can add a disclaimer to email messages passing through the appliance. An issue in an upgrade script caused configured disclaimers to be incorrectly removed from system configuration.

RESOLUTION: The upgrade script has been corrected to retain email disclaimers.

Please refer to KnowledgeBase article [KB75165](#) for more information.
 - Severity: Low
- Feature f_759403
 - Description:

ISSUE: The appliance monitors the state of the application software and can be configured to send alerts when an application fails. An issue in the proxy application which was triggered when the policy split event was issued, was causing the proxy application to fail on a regular basis.

RESOLUTION: The proxy application code has been corrected to ensure the application does not fail when the policy split event is issued

Please refer to KnowledgeBase article [KB75655](#) for more information.
 - Severity: Low
- Feature f_760297

- Description:

ISSUE: The appliance supports an out-of-band network interface for management purposes. The interface uses a firewall to allow only management connections on the interface. Due to an error in the firewall configuration code, connections with the ePO agent on the appliance were being disallowed.

RESOLUTION: The firewall configuration code has been corrected to allow ePO agent connections.

Please refer to KnowledgeBase article [KB75111](#) for more information.
 - Severity: Low
- Feature f_762377
 - Description:

ISSUE: The appliance can generate a scheduled report which includes information regarding the direction of email flow. An error in the string mapping file was causing inbound messages to be displayed as outbound

RESOLUTION: The error in the string mapping file has been corrected.

Please refer to KnowledgeBase article [KB75105](#) for more information.
 - Severity: Low
- Feature f_762436
 - Description:

Network interface status is now visible in the Troubleshooting/Hardware status pages of the user interface.

Please refer to KnowledgeBase article [KB76058](#) for more information.
 - Severity: Low
- Feature f_763533
 - Description:

ISSUE: The appliance offers a feature that allows the administrator to import or enter a list of recipients who are permitted to receive email via the appliance. Email address validation of permitted recipient email addresses was incorrectly disallowing use of a wildcard in the domain part of the email address.

RESOLUTION: Corrected the error in the email address validation for permitted recipient email address to allow the use of wildcards in the domain part.

Please refer to KnowledgeBase article [KB74043](#) for more information.
 - Severity: Low
- Feature f_763748
 - Description:

ISSUE: The appliance has the ability to generate scheduled reports. Due to an issue in the report generation module, scheduled reports generated with certain filters resulted in an empty report.

RESOLUTION: The report generation module has been updated to correctly return results for all filters.

Please refer to KnowledgeBase article [KB75066](#) for more information.
 - Severity: Low
- Feature f_765250
 - Description:

ISSUE: The appliance user interface features a dashboard which displays the status of the appliance and reports appliance activity over a period of time. An issue in a database query which provides data to the dashboard was causing significant delays, so making the user interface unresponsive.

RESOLUTION: The database query has been modified to alleviate the performance issue.

Please refer to KnowledgeBase article [KB75938](#) for more information.
 - Severity: Low
- Feature f_765303
 - Description:

ISSUE: The appliance is able to monitor the state of the SNMP service. An issue with the monitoring service was causing the SNMP state to be incorrectly reported when the community name was set to something other than 'public'.

RESOLUTION: The monitoring service has been updated to report the state of SNMP correctly when the community name has been modified by the user.

Please refer to KnowledgeBase article [KB75637](#) for more information.
 - Severity: Low

- Feature f_767982
 - Description:

ISSUE: The appliance can archive system logs to an external FTP or SSH server. Due to an issue in archive scripts, when the remote account credentials contained certain characters the data transfer operation failed.

RESOLUTION: The transfer script has been modified to correctly handle all characters in the credentials.

Please refer to KnowledgeBase article [KB75431](#) for more information.
 - Severity: Low
- Feature f_771889
 - Description:

ISSUE: The appliance allows the administrator to change the password from the console graphical configuration wizard. An issue in the script that applies configuration was preventing the application of the new password until the next reboot.

RESOLUTION: The configuration application script has been corrected to apply the password change immediately.

Please refer to KnowledgeBase article [KB75575](#) for more information.
 - Severity: Low
- Feature f_772506
 - Description:

ISSUE: The appliance user interface has the facility to show itemized reports of detections, with links to show more detail on specific viruses. Due to an error in the report generation, when viewing itemized reports, clicking a link with a virus name containing non-ASCII characters would cause errors to be displayed in the user interface

RESOLUTION: The error in the report generation has been corrected.

Please refer to KnowledgeBase article [KB75126](#) for more information.
 - Severity: Low
- Feature f_773306
 - Description:

ISSUE: The appliance supports upgrade and configuration import from EWS version 5.6. An issue in the configuration migration script was preventing the Maximum Mail Size Anti-Spam configuration from being imported during an upgrade.

RESOLUTION: The migration script has been corrected to import all Anti-Spam settings during an upgrade.

Please refer to KnowledgeBase article [KB76065](#) for more information.
 - Severity: Low
- Feature f_773470
 - Description:

ISSUE: The appliance can include charts in scheduled Email reports. Under certain circumstances scheduled Email reports have bar charts incorrectly displayed due to an error in the chart rendering library.

RESOLUTION: The chart rendering library code has been corrected.

Please refer to KnowledgeBase article [KB75299](#) for more information.
 - Severity: Low
- Feature f_773477
 - Description:

ISSUE: The appliance allows creation of sub-policies to manage a subset of traffic in POP3 configuration. An error in the user interface code was preventing customization of Protected File settings when new policies were created.

RESOLUTION: The user interface has been corrected to generate Protected File settings for sub-policies in POP3.

Please refer to KnowledgeBase article [KB75278](#) for more information.
 - Severity: Low
- Feature f_773650
 - Description:

ISSUE: The appliance has a facility to customize the headers and footers of generated alerts. Due to an issue in the user interface code the footer text could not be removed.

RESOLUTION: The user interface code has been modified to allow the footer text to be removed.

Please refer to KnowledgeBase article [KB75302](#) for more information.

- Severity: Low
- Feature f_773943
 - Description:
ISSUE: The appliance policy settings allow the administrator to configure any number of compliance rules per policy. When viewed with Internet Explorer, the user interface was not displaying the vertical scroll bar when the number of rules overflowed a single page.
RESOLUTION: The user interface code has been corrected to display the vertical scroll bar when necessary.
Please refer to KnowledgeBase article [KB75633](#) for more information.
 - Severity: Low
- Feature f_774658
 - Description:
ISSUE: The appliance includes reporting, which allows administrators to filter and display events from a specific period of time. When viewed using Internet Explorer the filter interface displayed the default category as 'Viruses', rather than 'All'.
RESOLUTION: The user interface has been modified to correctly display the default value for the reporting category.
Please refer to KnowledgeBase article [KB75632](#) for more information.
 - Severity: Low
- Feature f_774988
 - Description:
ISSUE: The appliance user interface includes a dashboard which displays the status of the appliance and reports appliance activity over a period of time. The user interface code was handling certain error conditions incorrectly, causing a failure to load the dashboard.
RESOLUTION: The user interface code has been correct to handle error conditions gracefully.
Please refer to KnowledgeBase article [KB75698](#) for more information.
 - Severity: Low
- Feature f_775001
 - Description:
ISSUE: The appliance allows the administrator to import certificates for encryption services. The appliance user interface was not giving any feedback to the administrator when the certificate was successfully imported.
RESOLUTION: The user interface has been modified to confirm the success of the import to the administrator.
Please refer to KnowledgeBase article [KB75834](#) for more information.
 - Severity: Low
- Feature f_775280
 - Description:
ISSUE: The appliance allows an administrator to configure a list of relay hosts for delivery of mail to specific domains. An issue in the user interface was allowing the entry of invalid addresses into the Domain Routing lists.
RESOLUTION: The user interface has been updated to correctly validate input into the Domain Routing lists.
Please refer to KnowledgeBase article [KB75556](#) for more information.
 - Severity: Low
- Feature f_775588
 - Description:
ISSUE: The appliance has a quarantine facility that allows end users to manage their quarantine via an email quarantine digest. When configured for operation in certain languages an issue in the quarantine management interface was preventing the user from releasing quarantined items from the email digest.
RESOLUTION: The quarantine management interface has been updated has been updated to correctly handle release requests in all languages.
Please refer to KnowledgeBase article [KB76124](#) for more information.
 - Severity: Low
- Feature f_780241
 - Description:

ISSUE: The appliance administrator can configure the appliance to send bounce messages (also known as Non-Delivery Reports or NDRs) from any email sender. An issue in the bounce generation code caused the customized sender information to be used as the envelope sender of a message, contrary to [RFC 5321](#).

RESOLUTION: The bounce generation code has been modified to ensure the envelope sender of a bounce message has the null address.

Please refer to KnowledgeBase article [KB75746](#) for more information.

o Severity: Low

• Feature f_781285

o Description:

ISSUE: The appliance allows an administrator to create new users to manage the appliance. An error in the data transfer encoding routines was preventing a user with a username containing non-ASCII characters from logging in.

RESOLUTION: The data transfer routines have been modified to correctly handle non-ASCII characters.

Please refer to KnowledgeBase article [KB75695](#) for more information.

o Severity: Low

• Feature f_782867

o Description:

ISSUE: The appliance allows customization of LDAP queries. Due to a user interface issue, any attempt to remove the secondary LDAP query caused it to be reset to the default value.

RESOLUTION: The user interface code has been corrected to ensure that secondary LDAP queries can be removed.

Please refer to KnowledgeBase article [KB76060](#) for more information.

o Severity: Low

• Feature f_782889

o Description:

ISSUE: The appliance can generate reports showing detections made in emails. An issue in the report generator handling of escape sequences resulted in events failing to appear in the reports.

RESOLUTION: The report generator has been modified to correctly handle escape sequences.

Please refer to KnowledgeBase article [KB75622](#) for more information.

o Severity: Low

• Feature f_782895

o Description:

ISSUE: The appliance supports interception of HTTP and HTTPS connections. It has the ability to sustain these connections during a restart of services. An error in the handling of the restart could eventually result in the appliance running out of memory.

RESOLUTION: Long lived connections are now handled correctly.

Please refer to KnowledgeBase article [KB72806](#) for more information.

o Severity: Low

• Feature f_782898

o Description:

ISSUE: The appliance supports full management by McAfee ePolicy Orchestrator (ePO). An issue in the ePO management interface was causing files to build up on the appliance filesystem and eventually filling the disk completely.

RESOLUTION: An ePO management interface script has been corrected to ensure temporary files are removed after use.

Please refer to KnowledgeBase article [KB76123](#) for more information.

o Severity: Low

• Feature f_782899

o Description:

ISSUE: The appliance can send scheduled reports via email. It can be configured to send the report from any specified user. An issue with the user interface email address validation was preventing the postmaster address being specified as the sender of the scheduled report.

RESOLUTION: The user interface email address validation has been corrected to accept the postmaster address.

Please refer to KnowledgeBase article [KB75740](#) for more information.

- Severity: Low
- Feature f_783417
 - Description:

ISSUE: The appliance uses a database to store events generated by mail traffic flowing through the appliance. Under certain circumstances the database may be temporarily unavailable. An issue with the event queue was causing events logged whilst the database was unavailable to be discarded.

RESOLUTION: The event queue management has been modified to ensure events logged whilst the database is unavailable are retained.

Please refer to KnowledgeBase article [KB76038](#) for more information.
 - Severity: Low
- Feature f_783666
 - Description:

ISSUE: The appliance can be configured to add a custom disclaimer to email messages. An issue in the user interface code was preventing the display of the HTML disclaimer in Internet Explorer.

RESOLUTION: The user interface code has been changed to ensure the HTML disclaimer is displayed in Internet Explorer.

Please refer to KnowledgeBase article [KB76006](#) for more information.
 - Severity: Low
- Feature f_784392
 - Description:

ISSUE: The appliance Minimum Escalation Report generates a data file which is used to diagnose issues on the appliance. An issue in the report generation script was preventing the NTP test from running.

RESOLUTION: The report generation script has been modified allow the NTP test to run correctly.

Please refer to KnowledgeBase article [KB76125](#) for more information.
 - Severity: Low
- Feature f_785422
 - Description:

ISSUE: Multiple security vulnerabilities have been reported against the sudo version used on the appliance.

RESOLUTION: The sudo package has been upgraded to address the problem.

Please refer to KnowledgeBase article [KB75944](#) for more information.
 - Severity: Low
- Feature f_785570
 - Description:

ISSUE: The appliance includes logging and reporting, which can be used by an administrator to determine the status of messages handled by the appliance. An issue in the event database was preventing the logging of events from virtual hosts with names containing non-ASCII characters.

RESOLUTION: The event database handler has been updated to correctly parse virtual host names containing non-ASCII characters.

Please refer to KnowledgeBase article [KB76030](#) for more information.
 - Severity: Low
- Feature f_786680
 - Description:

ISSUE: The appliance can upload syslog data to an external server. Due to an issue in the upload script, if incorrect credentials were specified for the external server, the syslog archive file was deleted and the data lost.

RESOLUTION: The upload script has been modified to preserve syslog archives if the upload failed.

Please refer to KnowledgeBase article [KB75999](#) for more information.
 - Severity: Low
- Feature f_787730
 - Description:

ISSUE: The appliance can be configured to issue email alerts when services on the appliance have failed. An issue with the health monitoring application was causing repeated notifications of the gti_feedback service restarting.

RESOLUTION: The health monitoring application has been corrected to accurately

determine the state of the gti_feedback service.

Please refer to KnowledgeBase article [KB76019](#) for more information.

- Severity: Low
- Feature f_791861
 - Description:
ISSUE: The appliance can issue events in the ArcSight Common Event Format. An omission in the event generation code prevented Anti-Relay events from being issued in the Common Event Format.
RESOLUTION: The event generation code has been corrected to allow Anti-Relay events in Common Event Format.
Please refer to KnowledgeBase article [KB75869](#) for more information.
 - Severity: Low
- Feature f_800921
 - Description:
ISSUE: The appliance has the ability to display the status on installed certificates. Due to an error in translation to German, an incorrect string was being displayed on the status icon.
RESOLUTION: The translation has been corrected.
Please refer to KnowledgeBase article [KB76260](#) for more information.
 - Severity: Low
- Feature f_781825
 - Description:
ISSUE: Vulnerability [CVE-2012-1667](#) was reported against the BIND version used on the appliance.
RESOLUTION: The BIND package has been updated to address the problem.
Please refer to KnowledgeBase article [KB75745](#) for more information.
 - Previously addressed by 7.0h788861, 7.0h793047.
 - Severity: Low
- Feature f_789113
 - Description:
ISSUE: The appliance has the facility to filter images in email for unacceptable content. Some valid images with small color depth were being incorrectly detected as corrupt.
RESOLUTION: The image analysis software interface has been changed to correct the problem.
Please refer to KnowledgeBase article [KB75865](#) for more information.
 - Previously addressed by 7.0h788861, 7.0h793047.
 - Severity: Low
- Feature f_754010
 - Description:
ISSUE: The appliance can send quarantine digest emails to users allowing them to release their quarantined emails. The digest generation algorithm was not distinguishing between email addresses with different case, causing digests to be incorrectly generated and failure to release certain emails.
RESOLUTION: Mails can now be released from a digest message regardless of the case of the email address.
Please refer to KnowledgeBase article [KB74855](#) for more information.
 - Previously addressed by 7.0h778488, 7.0h788861, 7.0h793047.
 - Severity: Low
- Feature f_778492
 - Description:
ISSUE: The appliance can use Sender Policy Framework (SPF) to determine the authenticity of an email sender. Under certain circumstances, an error in the SPF parsing code caused the 'include' statement to be incorrectly interpreted.
RESOLUTION: The Sender Policy Framework (SPF) code has been modified to correctly interpret the 'include' statement.
Please refer to KnowledgeBase article [KB75047](#) for more information.
 - Previously addressed by 7.0h778488, 7.0h788861, 7.0h793047.
 - Severity: Low
- Feature f_764779
 - Description:

ISSUE: The appliance uses the Linux kernel. A bug in the Linux kernel could have caused it to hang when a leap second was inserted.

RESOLUTION: The appliance Linux kernel has been updated to prevent the problem.

Please refer to KnowledgeBase article [KB75268](#) for more information.

- Previously addressed by 7.0h764779.
- Severity: Low

Issues resolved in previous releases

For information on issues resolved in earlier releases not included above, consult their release notes:

- Patch 7.0.1 (see KnowledgeBase article [KB74045](#))

Additional information

This release was built on 2012-11-07.

For updated information on this release see the KnowledgeBase article [KB75327](#).

This release was tested with anti-virus engine version 5400, DATs version 6830 and later. McAfee strongly recommends that the appliance is always kept up to date with the latest anti-virus components to achieve the highest possible security.

Incremental update package

The incremental update package may be installed on a running appliance with the least possible disruption of service.

In due course this package, or one superseding it, will be made available for download and install with the appliance auto-update system. For information on using auto-update refer to KnowledgeBase article [KB74923](#).

Installation requirements

You must have the following McAfee Email Gateway software installed on the appliance you intend to update with this package:

- Version 7.0
- Patch 7.0.1

Superseded releases

This package incorporates and supersedes the following earlier releases:

- Hotfix 7.0h753669
- Hotfix 7.0h758342
- Hotfix 7.0h759601
- Hotfix 7.0h764779
- Hotfix 7.0h778488
- Hotfix 7.0h788861
- Hotfix 7.0h793047

Actions on installation

At the end of the installation process the following actions will occur automatically:

- The user interface will log off.
- The appliance will reboot.

External components installed by this package

CMA version 4.6.0 release 2918.3
 The McAfee Agent
 intel-syscfg version 5.0.1 release 25x2.6.27.57x9.0.23.scm
 Intel Syslinux BIOS configuration utility
 libpng version 1.2.49 release 1.mfe1
 A library of functions for manipulating PNG image format files
 net-snmp version 5.3.0.1 release 2
 Tools and servers for the SNMP protocol
 net-snmp-utils version 5.3.0.1 release 2
 The tooAutoReqProvls and binaries from the Net-SNMP package.
 rsync version 3.0.9 release 201209171900
 rsync
 openssl version 0.9.8x release 201209171900
 Secure Sockets Layer and cryptography libraries and tools
 sudo version 1.7.4p5 release mfe
 rpm-sudo
 mcafee-eSCM version 4.4 release 7093
 The McAfee eSCM content scanning framework
 mcafee-eSCM-enginetest version 4.4 release 7093
 An engine test tool for the McAfee eSCM content scanning framework
 mcafee-eSCM-spam version 4.4 release 7093
 McAfee eSCM content scanning framework
 mcafee-eSCM-support version 4.4 release 7093
 rpm-mcafee-eSCM-support
 mcafee-eSCM-urfilter version 4.4 release 7093
 McAfee eSCM content scanning framework
 mimepp version 1.3 release 7093
 The MIME++ Library
 xerces13 version 1.3 release 7093
 The run-time libraries for Xerces 1.3
 libspf version 1.0.0 release 201202182000_133
 An SPF library
 bind version 9.7.3 release 201202182000_135
 The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server
 bind-libs version 9.7.3 release 201202182000_135
 Libraries used by the BIND DNS packages
 bind-utils version 9.7.3 release 201202182000_135
 Utilities for querying DNS name servers

Files included with this package

This package consists of archive file called MEG-7.0.2-2301.114.zip, which contains the following files:

```

7.0.2-2301.114/ftrs/f_731359/postscript
7.0.2-2301.114/ftrs/f_736878/postscript
7.0.2-2301.114/ftrs/f_778488/postscript
7.0.2-2301.114/rpms/CMA-4.6.0-2918.3.i386.rpm
7.0.2-2301.114/rpms/bind-9.7.3-201202182000_135.i386.rpm
7.0.2-2301.114/rpms/bind-libs-9.7.3-201202182000_135.i386.rpm
7.0.2-2301.114/rpms/bind-utils-9.7.3-201202182000_135.i386.rpm
7.0.2-2301.114/rpms/intel-syscfg-5.0.1-25x2.6.27.57x9.0.23.scm.i386.rpm
7.0.2-2301.114/rpms/libpng-1.2.49-1.mfe1.i386.rpm
7.0.2-2301.114/rpms/libspf-1.0.0-201202182000_133.i386.rpm
7.0.2-2301.114/rpms/mcafee-eSCM-4.4-7093.i386.rpm
7.0.2-2301.114/rpms/mcafee-eSCM-enginetest-4.4-7093.i386.rpm
7.0.2-2301.114/rpms/mcafee-eSCM-spam-4.4-7093.i386.rpm
7.0.2-2301.114/rpms/mcafee-eSCM-support-4.4-7093.i386.rpm
7.0.2-2301.114/rpms/mcafee-eSCM-urfilter-4.4-7093.i386.rpm
7.0.2-2301.114/rpms/mimepp-1.3-7093.i386.rpm
7.0.2-2301.114/rpms/net-snmp-5.3.0.1-2.i386.rpm
7.0.2-2301.114/rpms/net-snmp-utils-5.3.0.1-2.i386.rpm
7.0.2-2301.114/rpms/openssl-0.9.8x-201209171900.i386.rpm
7.0.2-2301.114/rpms/rsync-3.0.9-201209171900.i386.rpm
7.0.2-2301.114/rpms/sudo-1.7.4p5-mfe.i386.rpm
7.0.2-2301.114/rpms/vmware-open-vm-tools-kmod-modules-8.3.7-381511x2.6.27.57x9.0.23.scm.i386.rpm
7.0.2-2301.114/rpms/webshield-CfgMgr-Converter-Base-9.0-201209171900.i386.rpm
7.0.2-2301.114/rpms/webshield-CfgMgr-Converter-MigrationAid-9.0-201209171900.i386.rpm
7.0.2-2301.114/rpms/webshield-CfgMgr-Converter-Native-9.0-201209171900.i386.rpm
  
```

7.0.2-2301.114/rpms/webshield-CfgMgr-Converter-System-9.0-201209171900_103.i386.rpm
 7.0.2-2301.114/rpms/webshield-CfgMgr-schema-Native-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-SAFE_config-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-UI_backend-9.0-201209171900_109.i386.rpm
 7.0.2-2301.114/rpms/webshield-WebMailClient-9.0-201209171900_101.i386.rpm
 7.0.2-2301.114/rpms/webshield-Web_UI-9.0-201209171900_109.i386.rpm
 7.0.2-2301.114/rpms/webshield-apache-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-appliance-kernel-2.6.27.57-9.0.23.scm.i386.rpm
 7.0.2-2301.114/rpms/webshield-autoupdate-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-base-xmlconfig-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-comp-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-ePO-9.0-201209171900_109.i386.rpm
 7.0.2-2301.114/rpms/webshield-ePO-extension-9.0-201209171900_109.i386.rpm
 7.0.2-2301.114/rpms/webshield-encryption-9.0-201209171900_102.i386.rpm
 7.0.2-2301.114/rpms/webshield-files-9.0-201209171900_103.i386.rpm
 7.0.2-2301.114/rpms/webshield-fips-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-gls-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-help-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-inv-cloud-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-inv-pop3-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-inv-smtp-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-kernel-9.0-201209171900_101.i386.rpm
 7.0.2-2301.114/rpms/webshield-l10n-9.0-201209171900_109.i386.rpm
 7.0.2-2301.114/rpms/webshield-libconfig-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-libsconfig-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-management-common-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-mtafiles-9.0-201209171900_109.i386.rpm
 7.0.2-2301.114/rpms/webshield-offboxstorage-9.0-201209171900_114.i386.rpm
 7.0.2-2301.114/rpms/webshield-reports-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-resiliency-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-resiliency-sb-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-retryer-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-siteadvisor-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-smg-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-smtp-retryer-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-snmp-9.0-201209171900_101.i386.rpm
 7.0.2-2301.114/rpms/webshield-testmode-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-tqmd-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-ui-9.0-201209171900_101.i386.rpm
 7.0.2-2301.114/rpms/webshield-ups-9.0-201209171900.i386.rpm
 7.0.2-2301.114/rpms/webshield-utils-9.0-201209171900_101.i386.rpm
 7.0.2-2301.114/rpms/webshield-variants-9.0-201209171900_104.i386.rpm
 7.0.2-2301.114/rpms/xerces13-1.3-7093.i386.rpm
 7.0.2-2301.114/updata/package.xml
 validate/filelist.txt
 validate/md5sum.txt
 validate/version

Installation steps

In the case of a virtual appliance it may be useful to take a snapshot of the appliance before installing the package.

To install this package:

1. Create a temporary directory on your hard disk, and download the zip file provided by McAfee to a computer on your network that can access the McAfee Email Gateway appliance.
2. Open your Internet browser, and browse to the McAfee Email Gateway appliance.

If installing on a Content Security Blade Server, go first to the Failover Management blade to do the following steps, then repeat them on the Management blade (the content scanning blades will be updated automatically).

If installing on an appliance cluster the steps must be done on all the appliances in the cluster, starting with the Failover Management appliance, then the Management appliance, then the remainder.

3. When prompted, log on to the appliance by typing your username and password.
4. On the navigation bar, select **System | Component Management | Package Installer**.
5. Under **Manual Package Install**, click **Update from file**. In the **Import package** window, click **Browse**, find the location of the file "MEG-7.0.2-2301.114.zip", click **Open**, and then click **OK**.

A popup window appears displaying the package description and a notice that the appliance will restart after installation. Click **OK** to install the package.

Upon completion of the installation the [actions noted above](#) will be performed automatically.

6. Clear the browser cache before logging on to the interface again. If the browser cache is not cleared, the interface will not behave correctly.
7. After installation, log on to the user interface and click **About the appliance** to check that "7.0.2-2301.114" is displayed.

After installation

- If you plan to use the MEG-7.0.2-2301.114.zip archive file again, keep it available on your computer. Otherwise, delete the file after successful installation. If you re-install your McAfee Email Gateway version 7.0 software, we recommend that you re-install this release.

Removing this package

To remove this package from your McAfee Email Gateway appliance, you need to reinstall McAfee Email Gateway version 7.0. An alternative, for a virtual appliance, is to revert to a previous snapshot. Please note that all other hotfixes or patches installed on the appliance would also be removed in the process.

Installable images

Installable images are available for the various types of appliance. For information on installing these images refer to KnowledgeBase article [KB71956](#).

When using this method to upgrade an existing appliance, there is an option to install software while retaining the existing operational data (option 2 on the install menu). This option is available where one of the following compatible versions is already installed:

- This release or any [superseded releases](#), but not any later release other than hotfixes
- Version 5.6 with 5.6p1 or later releases

Superseded releases

This package incorporates and supersedes the following earlier releases:

- Version 7.0
- Patch 7.0.1
- Hotfix 7.0h753669
- Hotfix 7.0h758342
- Hotfix 7.0h759601
- Hotfix 7.0h764779
- Hotfix 7.0h778488
- Hotfix 7.0h788861
- Hotfix 7.0h793047

Notices

Copyright

Copyright © 2012 McAfee, Inc. All Rights Reserved

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

Trademark attributions

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

License information

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Copyright © 2012 McAfee, Inc. All Rights Reserved