



McAfee[®] Email Gateway 7.0.1

Release Notes for McAfee[®] Email Gateway

Version 7.0

Patch 7.0.1

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 \(total: 4, new: 4\)](#)

[Vulnerabilities \(total: 6, new: 6\)](#)

[High severity issues \(total: 2, new: 2\)](#)

[Medium severity issues \(total: 8, new: 8\)](#)

[Low severity issues \(total: 16, new: 16\)](#)

[Issues list](#)

[Additional information](#)

[Incremental update package](#)

[Installation requirements](#)

[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[Superseded releases](#)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: 4, new: 4)

Additional functionality in this release:

[f_724578](#), [f_724584](#), [f_731901](#), [f_736380](#)

Vulnerabilities (total: 6, new: 6)

Vulnerabilities newly addressed in this release:

[f_719593](#), [f_728405](#), [f_731938](#), [f_735407](#), [f_737110](#), [f_738324](#)

High severity issues (total: 2, new: 2)

High severity issues newly addressed in this release:

[f_724523](#), [f_731901](#)

Medium severity issues (total: 8, new: 8)

Medium severity issues newly addressed in this release:

[f_724528](#), [f_724578](#), [f_724584](#), [f_728405](#), [f_731938](#), [f_732570](#), [f_735407](#), [f_736380](#)

Low severity issues (total: 16, new: 16)

Low severity issues newly addressed in this release:

[f_719593](#), [f_723233](#), [f_724662](#), [f_726522](#), [f_727762](#), [f_728115](#), [f_732047](#),
[f_732682](#), [f_733059](#), [f_733650](#), [f_734235](#), [f_735591](#), [f_736375](#), [f_736753](#),
[f_737110](#), [f_738324](#)

Issues list

- Feature f_724523
 - Description:
ISSUE: The Intel 3300 and 3400 appliances offer remote console access via the Intel RMM3 module. When applying unrelated changes through the appliance GUI the default gateway for the RMM3 module was being reset to default.
RESOLUTION: The appliance's configuration system has been updated to ensure that the correct network settings are applied to the RMM3 module.
Please refer to KnowledgeBase article [KB73536](#) for more information.
 - Severity: High
- Feature f_731901
 - Description:
The McAfee Email Gateway now supports Secure Web Mail PUSH functionality on Blade and Cluster deployments
Please refer to KnowledgeBase article [KB74634](#) for more information.
 - Severity: High
- Feature f_724528
 - Description:
ISSUE: Some appliances provide an Out of Band Management (OOB) interface separate from the main network interfaces. When the main data network interfaces were set to use fiber the OOB interface link media settings would be lost, including forced link speed and duplex settings.
RESOLUTION: The OOB interface settings are now retained correctly.
Please refer to KnowledgeBase article [KB73510](#) for more information.
 - Severity: Medium
- Feature f_724578
 - Description:
The appliance can now be configured to utilise Forward Confirmed reverse DNS (FCrDNS) to authenticate email senders.
Please refer to KnowledgeBase article [KB74633](#) for more information.
 - Severity: Medium
- Feature f_724584
 - Description:
The appliance can now be configured to attempt TLS delivery of an email in preference to content encryption via S/MIME, PGP, or Secure Web Delivery.
Please refer to KnowledgeBase article [KB74152](#) for more information.
 - Severity: Medium
- Feature f_728405
 - Description:
ISSUE: Vulnerability [CVE-2011-4313](#) 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 [KB73711](#) for more information.
 - Severity: Medium
- Feature f_731938
 - Description:
ISSUE: Vulnerabilities [CVE-2011-4108](#), [CVE-2011-4109](#), [CVE-2011-4576](#), [CVE-2011-4577](#), [CVE-2011-4619](#), [CVE-2012-0027](#) were reported against the openssl version used on the appliance.
RESOLUTION: The openssl package has been updated to address the problems.
Please refer to KnowledgeBase article [KB73822](#) for more information.
 - Severity: Medium
- Feature f_732570

- Description:
ISSUE: On appliances using some Intel hardware the network interfaces would stop sending and receiving traffic after an unpredictable period of time. When this occurs, the only solution was to reboot the appliance. This was recorded in the system log as a NETDEV WATCHDOG timeout message.
RESOLUTION: The appliance kernel boot parameters have been updated to prevent the problem on the affected platforms.
Please refer to KnowledgeBase article [KB73823](#) for more information.
- Severity: Medium
- Feature f_735407
 - Description:
ISSUE: Vulnerabilities [CVE-2011-4516](#), [CVE-2011-4517](#), and [CVE-2012-0110](#) 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 [KB73960](#) for more information.
 - Severity: Medium
- Feature f_736380
 - Description:
The appliance previously offered the ability for end users to manage their quarantined email via an email digest on their desktop computer. This functionality has now been added for Blackberry devices. Configuration on the appliance is through the backend configuration.
Please refer to KnowledgeBase article [KB73935](#) for more information.
 - Severity: Medium
- Feature f_719593
 - Description:
ISSUE: Vulnerability [CVE-2009-0688](#) was reported against the cyrus-sasl version installed on the appliance.
RESOLUTION: The cyrus-sasl package was not used on the appliance and has been removed.
Please refer to KnowledgeBase article [KB74087](#) for more information.
 - Severity: Low
- Feature f_723233
 - Description:
ISSUE: The Japanese translation of "Make deobfuscated content available to other scanners" in the user interface was incorrect.
RESOLUTION: The translation has been corrected.
Please refer to KnowledgeBase article [KB74094](#) for more information.
 - Severity: Low
- Feature f_724662
 - Description:
ISSUE: The appliance allows configuration of per-domain SMTP relays. Adding a DNS relay with a trailing '.' caused an invalid DNS configuration to be saved resulting in DNS not responding on the appliance.
RESOLUTION: The appliance code has been modified to handle entries that end with a '.' correctly.
Please refer to KnowledgeBase article [KB73785](#) for more information.
 - Severity: Low
- Feature f_726522
 - Description:
ISSUE: The appliance stores its configuration on the /config partition. Occasionally, when the power was lost and the appliance was unable to shut down gracefully, one or more of the configuration files could be corrupted.
RESOLUTION: Changes have been made to the way the configuration files are written to disk to prevent corruption should the appliance experience sudden

power loss.

Please refer to KnowledgeBase article [KB73654](#) for more information.

- Severity: Low
- Feature f_727762
 - Description:

ISSUE: The appliance allows configuration of per-domain SMTP relays. When a large number of SMTP relays was present, incorrect configuration was being saved by the GUI resulting in emails being queued with the message '442 No Delivery Mechanism Available'.

RESOLUTION: The GUI implementation has been modified to ensure large number of relays are saved correctly.

Please refer to KnowledgeBase article [KB73671](#) for more information.
 - Severity: Low
- Feature f_728115
 - Description:

ISSUE: The appliance can be monitored using SNMP version 1 trap managers. When configured in bridge mode the appliance was incorrectly using a LAN1 or LAN2 IP address, rather than the correct Bridge IP address.

RESOLUTION: The appliance hosts file has been updated to ensure that when in bridge mode the correct IP address will be used in the SNMP trap messages.

Please refer to KnowledgeBase article [KB73535](#) for more information.
 - Severity: Low
- Feature f_732047
 - Description:

ISSUE: The appliance offers the ability to configure virtual hosts, each with its own virtual IP address. When virtual hosts were used in a cluster or on a blade server, the virtual host IP address was not immediately usable by clients when the master failed and the failover took over.

RESOLUTION: The appliance now communicates to the network to update the ARP cache upon failover, allowing virtual hosts to continue to work without delay.

Please refer to KnowledgeBase article [KB73482](#) for more information.
 - Severity: Low
- Feature f_732682
 - Description:

ISSUE: The appliance offers a quarantine digests feature which periodically notifies end users of their emails which have been quarantined. Quarantine digests were not being generated because the user interface failed to enable the feature due to an incorrect configuration mapping.

RESOLUTION: The configuration mapping has been corrected in the user interface.

Please refer to KnowledgeBase article [KB73886](#) for more information.
 - Severity: Low
- Feature f_733059
 - Description:

ISSUE: The appliance can be configured to validate email recipients against an LDAP database. The appliance was failing to validate the secondary email address when the LDAP cache feature was enabled because the secondary email address was omitted from the LDAP cache.

RESOLUTION: Secondary email addresses are now added to the LDAP cache.

Please refer to KnowledgeBase article [KB73885](#) for more information.
 - Severity: Low
- Feature f_733650
 - Description:

ISSUE: The appliance offers the administrator the option to allow non-RFC characters in the domain part of the email address. By default the appliance

rejects messages with such addresses. When they were allowed, some of these non-RFC characters caused the SMTP proxy to abort.

RESOLUTION: The SMTP proxy has been updated to support any non-RFC characters in the domain part of an email address.

Please refer to KnowledgeBase article [KB73552](#) for more information.

- Severity: Low
- Feature f_734235
 - Description:

ISSUE: The appliance has the ability to display a full log of a conversation from the Email message search page. After a period of time the log files are archived to conserve storage. An error in the user interface code was occasionally preventing the archived conversation logs from being located resulting in a '404 not found' response.

RESOLUTION: The error has been corrected to ensure the log file is reliably located.

Please refer to KnowledgeBase article [KB74101](#) for more information.
 - Severity: Low
- Feature f_735591
 - Description:

ISSUE: The appliance has the facility to send notification to recipients as a result of user specified conditions. When creating the notification email the appliance was including all of the original recipients on the "To" header including BCC (blind copy) recipients of the original email.

RESOLUTION: Notification email generation has been modified to show only the intended recipient of the notification email.

Please refer to KnowledgeBase article [KB74086](#) for more information.
 - Severity: Low
- Feature f_736375
 - Description:

ISSUE: The appliance offers the administrator the option to allow non-RFC characters in the domain part of the email address. By default the appliance rejects these messages. Some of these non-RFC characters resulted in the SMTP proxy aborting.

RESOLUTION: The SMTP proxy has been updated to support the nonRFC characters in the domain part of the email address.

Please refer to KnowledgeBase article [KB73605](#) for more information.
 - Severity: Low
- Feature f_736753
 - Description:

ISSUE: The appliance offers the ability to display an HTML report of the configuration. Delivery settings such as "Relay List" and "Fallback Relay List" were not present in the Configuration Report.

RESOLUTION: Delivery settings have been added to the Configuration Report.

Please refer to KnowledgeBase article [KB72797](#) for more information.
 - Severity: Low
- Feature f_737110
 - Description:

ISSUE: Vulnerability [CVE-2011-3348](#) was reported against the mod_proxy_ajp module when used with mod_proxy_balancer in certain configurations for the Apache version on the appliance.

RESOLUTION: The mod_proxy_ajp and mod_proxy_balancer modules were not used on the appliance and have been removed.

Please refer to KnowledgeBase article [KB74084](#) for more information.
 - Severity: Low
- Feature f_738324

- Description:
ISSUE: Vulnerability [CVE-2011-4849](#) was reported against the use of cookies without the secure flag in https.
RESOLUTION: All cookies created by the appliance user interface have the secure flag set.
Please refer to KnowledgeBase article [KB74088](#) for more information.
- Severity: Low

Additional information

This release was built on 2012-03-14.

For updated information on this release see the KnowledgeBase article [KB74045](#).

This release was tested with anti-virus engine version 5400, DATs version 6615 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

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 2156.4
The McAfee Agent
intel-syscfg version 5.0.1 release 25x2.6.27.57x9.0.20.scm
Intel Syslinux BIOS configuration utility
javascript-yui3 version 3.4.1 release 201202182000
JavaScript and CSS library
mshyperv version 2.1 release 201202182000
Microsoft Hypervisor support
perl-Digest-HMAC version 1.02 release 201105061900
Perl extension Digest::HMAC
perl-Digest-SHA version 5.61 release 201111082000
Perl extension Digest::SHA

perl-Digest-SHA1 version 2.12 release 201105061900
Perl extension Digest::SHA1
mcafee-eSCM version 4.4 release 6713
The McAfee eSCM content scanning framework
mcafee-eSCM-enginetest version 4.4 release 6713
An engine test tool for the McAfee eSCM content scanning framework
mcafee-eSCM-spam version 4.4 release 6713
McAfee eSCM content scanning framework
mcafee-eSCM-urfilter version 4.4 release 6713
McAfee eSCM content scanning framework
mimepp version 1.3 release 6713
The MIME++ Library
xerces13 version 1.3 release 6713
The run-time libraries for Xerces 1.3
bind version 9.7.3 release 201202182000
The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server
bind-libs version 9.7.3 release 201202182000
Libraries used by the BIND DNS packages
bind-utils version 9.7.3 release 201202182000
Utilities for querying DNS name servers
libidn version 1.18 release 201202182000
Internationalized Domain Name support library
openssl version 0.9.8s release 201202182000
Secure Sockets Layer and cryptography libraries and tools

Files included with this package

This package consists of archive file called MEG-7.0.1-2151.108.zip, which contains the following files:

```
7.0.1-2151.108/ftrs/f_721881/postscript
7.0.1-2151.108/ftrs/f_721881/prescript
7.0.1-2151.108/ftrs/f_724523/postscript
7.0.1-2151.108/ftrs/f_732570/postscript
7.0.1-2151.108/rpms/CMA-4.6.0-2156.4.i386.rpm
7.0.1-2151.108/rpms/bind-9.7.3-201202182000.i386.rpm
7.0.1-2151.108/rpms/bind-libs-9.7.3-201202182000.i386.rpm
7.0.1-2151.108/rpms/bind-utils-9.7.3-201202182000.i386.rpm
7.0.1-2151.108/rpms/drac4fixup-1.0.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/intel-syscfg-5.0.1-25x2.6.27.57x9.0.20.scm.i386.rpm
7.0.1-2151.108/rpms/javascript-yui3-3.4.1-201202182000.i386.rpm
7.0.1-2151.108/rpms/libidn-1.18-201202182000.i386.rpm
7.0.1-2151.108/rpms/mcafee-agc-2.0-297mfe.i386.rpm
7.0.1-2151.108/rpms/mcafee-eSCM-4.4-6713.i386.rpm
7.0.1-2151.108/rpms/mcafee-eSCM-enginetest-4.4-6713.i386.rpm
7.0.1-2151.108/rpms/mcafee-eSCM-spam-4.4-6713.i386.rpm
7.0.1-2151.108/rpms/mcafee-eSCM-support-4.4-6713.i386.rpm
7.0.1-2151.108/rpms/mcafee-eSCM-urlfilter-4.4-6713.i386.rpm
7.0.1-2151.108/rpms/mimepp-1.3-6713.i386.rpm
7.0.1-2151.108/rpms/mshyperv-2.1-201202182000.i386.rpm
7.0.1-2151.108/rpms/openssl-0.9.8s-201202182000.i386.rpm
7.0.1-2151.108/rpms/perl-Digest-HMAC-1.02-201105061900.i386.rpm
7.0.1-2151.108/rpms/perl-Digest-SHA-5.61-201111082000.i386.rpm
7.0.1-2151.108/rpms/perl-Digest-SHA1-2.12-201105061900.i386.rpm
7.0.1-2151.108/rpms/vmware-open-vm-tools-kmod-modules-8.3.7-381511x2.6.27.57x9.0.20.scm.i386.rpm
7.0.1-2151.108/rpms/webshield-CfgMgr-Converter-MigrationAid-9.0-201202182000_103.i386.rpm
7.0.1-2151.108/rpms/webshield-CfgMgr-Converter-Native-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-CfgMgr-Converter-System-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-SAFE_config-9.0-201202182000_103.i386.rpm
7.0.1-2151.108/rpms/webshield-UI_backend-9.0-201202182000_103.i386.rpm
7.0.1-2151.108/rpms/webshield-WebMailClient-9.0-201202182000_107.i386.rpm
7.0.1-2151.108/rpms/webshield-Web_UI-9.0-201202182000_103.i386.rpm
7.0.1-2151.108/rpms/webshield-apache-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-appliance-kernel-2.6.27.57-9.0.20.scm.i386.rpm
7.0.1-2151.108/rpms/webshield-autoupdate-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-base-xmlconfig-9.0-201202182000.i386.rpm
```

7.0.1-2151.108/rpms/webshield-branding-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-comp-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-ePO-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-ePO-extension-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-encryption-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-files-9.0-201202182000_106.i386.rpm
7.0.1-2151.108/rpms/webshield-fips-9.0-201202182000_103.i386.rpm
7.0.1-2151.108/rpms/webshield-gls-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-help-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-installer-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-inv-cloud-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-inv-pop3-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-inv-smtp-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-kernel-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-l10n-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-libconfig-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-libidentity-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-libsconfig-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-management-common-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-mtafiles-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-reports-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-resiliency-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-resiliency-sb-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-retryer-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-siteadvisor-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-smtp-retryer-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-snmp-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-storage2-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-tqmd-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-tqmd-mgmt-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-ui-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-utils-9.0-201202182000.i386.rpm
7.0.1-2151.108/rpms/webshield-variants-9.0-201202182000_104.i386.rpm
7.0.1-2151.108/rpms/xerces13-1.3-6713.i386.rpm
7.0.1-2151.108/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-7.0.1-2151.108.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 "7.0.1-2151.108" is displayed.

After installation

- If you plan to use the MEG-7.0.1-2151.108.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

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