

Common Criteria Evaluated Configuration Guide

Revision B

McAfee® Email Gateway 7.0.1

Appliances

COPYRIGHT

Copyright © 2012 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS

McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

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.

Contents

	About this guide	5
1	Preparing the Common Criteria environment	7
	Additional McAfee documentation	7
	Key networking terms	8
	Hardware and software requirements	10
	Appliance hardware	10
	Virtual appliance software	10
	Appliance software	10
	Administration computer software	10
	TOE environment guidelines	11
2	Installing and configuring the McAfee Email Gateway Appliance	13
	Pre-installation tasks	13
	Check the shipment	13
	Review the documentation	13
	Prepare the environment	14
	Install the appliance	14
	Configure the appliance	14
	Configure your model 4000, 4500, 5000, or 5500 appliance	14
	Configure a virtual appliance	15
	Configure McAfee Email Gateway on a blade server	15
	Setup Wizard	15
	Final notes	16
3	Maintaining a TOE configuration	17
	Overview of Dashboard features	17
	Overview of Reports features	17
	Overview of the Email menu	18
	Overview of the System menu	18
	Appliance management	19
	User management	19
	Logs, alerts, and SNMP	19
	About alerts	20
	Settings	21
	Event log settings	21
	Component management	24
	Setup Wizard	24
	Troubleshooting features	24
	ePolicy Orchestrator management	24
	Configure additional settings for Common Criteria	24
	Configure the audit of Common Criteria specific events	25
	Export audit logs	26

About this guide

This guide describes requirements and guidelines for installing, configuring, and maintaining a McAfee® Email Gateway (hereinafter Email Gateway) appliance to comply with Common Criteria evaluation standards. If your organization's security policy requires the Email Gateway appliance to match the Common Criteria Target of Evaluation (TOE) configuration, carefully follow the instructions in this document.

Any guidance provided in this document supercedes that given in the McAfee Email Gateway documentation.

For more information about Common Criteria, McAfee, Inc., and McAfee Email Gateway appliances evaluation level requirements, visit:

- www.commoncriteriaportal.org
- mysupport.mcafee.com

1

Preparing the Common Criteria environment

Common Criteria represents the effort to develop criteria for evaluation of information technology (IT) security products. The criteria and evaluation standards are broadly used and respected within the international community. Many organizations require that their security products be CC certified.

The McAfee® Email Gateway Appliance and software version 7.0.1 have been submitted for Common Criteria certification at Evaluation Assurance Level 2 (EAL 2+).

Contents

- ▶ [Additional McAfee documentation](#)
- ▶ [Key networking terms](#)
- ▶ [Hardware and software requirements](#)
- ▶ [TOE environment guidelines](#)

Additional McAfee documentation

This guide applies to the McAfee Email Gateway Appliances and software version 7.0.1 and provides the specific parameters and requirements for setting up and maintaining an Email Gateway Appliance run in a Common Criteria TOE configuration.

Use this guide in conjunction with the following reference materials to implement and administer your appliance TOE configuration.

- *McAfee Email Gateway Appliance 7.0.1 Security Target*



Specific identification and build information for the TOE will be added when they become available.

- *McAfee Email Gateway 7.0 Appliances Installation Guide* (meg_700_ig_app_7003349A00_en-us.pdf)
- *McAfee Content Security Blade Server 7.0 System Installation Guide* (meg_700_ig_csbs_7003359A00_en-us.pdf)
- *McAfee Email Gateway version 7.0 Quick Start Guide* (meg_700_qsg_7003380A00_en-us.pdf)
- *McAfee Content Security Blade Server Quick Start Guide, version 7.0.0* (csbs_70_qs_7003392A00_en-us.pdf)
- *McAfee Email Gateway 7.0 Virtual Appliance Installation Guide* (meg_700_ig_va_7003349A00_en-us.pdf)
- *McAfee Email Gateway 7.0 Appliances Administrators Guide* (meg_701_ag_7003319B00_en-us.pdf)

- *McAfee Email Gateway 7.0 Appliance Help*; online Help is included in the McAfee Email Gateway Appliance version 7.0.
- *McAfee Email Gateway Release Notes, version 7.0 Patch 7.0.1* (meg-7.0.1-2151.150.readme.en-us.pdf)

Key networking terms

The following table provides definitions of key terms related to McAfee Email Gateway Appliances.

Table 1-1 Definitions

Term	Description
appliance	Within the context of this document, the term <i>appliance</i> is synonymous with TOE — the combination of hardware and software that is described within the TOE boundary.
blacklist	A list of email addresses or domains you created that the anti-spam module will always treat as spam. When the application detects an incoming message from an address or domain on the blacklist, it immediately assigns a high score to that message.
content filtering	A process that uses rules to detect undesirable content, such as offensive words, in email messages.
Cyrus IMAP software	The Cyrus IMAP (Internet Message Access Protocol) software provides access to personal mail and system-wide bulletin boards through the IMAP protocol.
data loss prevention	Refers to systems that identify, monitor, and protect data in use (for example, endpoint actions), data in motion (for example, network actions), and data at rest (for example, data storage) through deep content inspection and contextual security analysis of transactions (attributes of originator, data object, medium, timing, recipient/destination, and so on).
Denial of Service (DoS)	A means of attack against a computer, server, or network that disrupts the ability to respond to legitimate connection requests. A denial-of-service attack overwhelms its target with false connection requests, so that the target ignores legitimate requests.
denied connection	The term used by the TOE to denote traffic dropped in response to matching a Denial of Service prevention policy as defined and configured by the TOE administrator.
directory harvest attack (DHA)	An attack on an email server that uses a script to identify and gather valid email addresses; used by spammers.
explicit proxy mode	In explicit proxy mode, some network devices must be set up to explicitly send traffic to the appliance. The appliance then works as a proxy, processing the traffic on behalf of these network devices.
heuristic analysis	A method of scanning that looks for patterns or activities that are virus-like, to detect new or previously undetected viruses.
ICAP	Internet Content Adaptation Protocol.
image filtering	A method of scanning that searches for inappropriate images in email traffic and performs a designated action on discovery
IMAP	Internet Message Access Protocol
keylogger	A computer program that captures the keystrokes of a computer user and stores them.

Table 1-1 Definitions *(continued)*

Term	Description
network user	An unauthenticated remote user or process sending information to the workstation through a network protocol; this role only has the authority to send information through the appliance from either the Internet or the internal network.
packers	Compression tools that compress files and change the binary signature of the executable. They can be used to compress Trojans and make them harder to detect.
Perl DBI	Perl DBI (database interface) is a database interface for the Perl programming language. It is used within the McAfee Email Gateway Appliance in the logging subsystem for the purposes of accessing the database housing audit records.
phishing	This category includes sites that typically arrive in hoax email established only to steal user account information. These sites falsely represent themselves as legitimate company websites in order to deceive and obtain user account information that can be used to perpetrate fraud or theft.
POP3	Post Office Protocol 3
potentially unwanted programs (PUPs)	A program that performs some unauthorized (and often harmful or undesirable) acts such as viruses, worms, and Trojan horses.
quarantine	Enforced isolation of a file or folder — for example, to prevent infection by a virus or to isolate a spam email message — until action can be taken to clean or remove the item.
scanning engine	The mechanism that drives the scanning process.
signature	The description of a virus, malware, or attack methodology.
SMTP 250 command	Requested mail action okay, completed.
spam score	A rating system used to indicate the likelihood that an email message contains spam. The higher the score allocated to a message, the more likely it is to be spam.
spyware	This category includes URLs that download software that covertly gathers user information through the user's Internet connection, without his or her knowledge, usually for advertising purposes. This might be considered a violation of privacy and might have bandwidth and security implications.
transparent mode	In either transparent router mode or transparent bridge mode, the communicating devices are unaware of the intervention of the appliance — the appliance's operation is transparent to those devices.
Trojan	An application that either pretends to have, or is described as having, a set of useful or desirable features, but actually contains a damaging payload. Trojan horses are not technically viruses because they do not replicate.
virtual appliance	A virtual machine image designed to run on a virtualization platform.
virus	An application that is capable of replicating with little or no user intervention, and the replicated program(s) also replicate further.
whitelist	A list of email addresses or domains you created that the anti-spam module treats as non-spam. When the anti-spam module detects an incoming message from an address or domain on the whitelist, it immediately assigns a high negative score to that message.
worm	A virus that spreads by creating duplicates of itself on other drives, systems, or networks.

Hardware and software requirements

Follow these guidelines for supported hardware and software.

For more information about downloading the software, see *Task - Download the installation software* in either the *McAfee Email Gateway 7.0 Appliances Installation Guide* or the *McAfee Email Gateway 7.0 Virtual Appliance Installation Guide*.

Appliance hardware

Use any of these appliances in clusters:

- Email Gateway Appliance for the 4000 platform
- Email Gateway Appliance for the 4500 platform
- Email Gateway Appliance for the 5000 platform
- Email Gateway Appliance for the 5500 platform
- Content Security Blade Server M3 chassis
- Content Security Blade Server M7 chassis

You can use the M3 and M7 blade enclosures to house combinations of the following blades.



You can use the M7 single-phase power, M7 DC power, M7 three-phase international, M7 DC international, and M3 single-phase AC blade enclosures.

- **Management** — At least one management blade must be present within any single blade enclosure.
- **Scanning** — Two or more scanning blades must be present within any single blade enclosure. At least one must be configured to be an *email* scanning blade.

Virtual appliance software

VMware vSphere 4.1 or later

Appliance software

Use any of these McAfee Email Gateway version 7.0.1 software packages.

Table 1-2 Software ISO files

Software	ISO files
Email Gateway Appliance	McAfee-MEG7.0.1-2151.152.iso (models 4000, 4500, 5000, and 5500)
Content Security Blade Server	McAfee-MEG7.0.1-2151.152.iso (M3 or M7)
Email Gateway Virtual Appliance	McAfee-MEG7.0.1-2151.152.VMbuy.iso McAfee-MEG7.0.1-2151.152.VMbuy_ESX.zip McAfee-MEG7.0.1-2151.152.VMtrial.zip McAfee-MEG7.0.1-2151.152.VMbuy_vCenter.zip (for VMware vSphere 4.1 or later)

Administration computer software

The administration computer is used to access the user interface.

The administration computer must be general purpose, running Microsoft Internet Explorer 7.0 or later, or Mozilla Firefox 3.6 or later.

The web browser must be configured as follows:

- HTTPS with Secure Socket Layer (SSL) version 3.0 or Transport Layer Security (TLS) version 1 encryption, using RC4 with 128-bit cryptographic key size, or 3DES with 112-bit cryptographic key size



SSLv2 and SSLv1 protocols must be explicitly disabled and cleartext not permitted for the connection with the TOE user interface.

- ActiveX enabled

TOE environment guidelines

You must adhere to these security objectives in the TOE operating environment as specified in *McAfee Email Gateway 7.0.1 Security Target*.

- The administrators of the appliance must review all associated documentation and guidance before installing and managing the device. Administration of the Email Gateway Appliance requires a base of knowledge in networking and traffic management. The administrator is responsible for ensuring that qualified personnel complete all tasks described herein and in references.
- The location of the appliance should protect it from casual access by unauthorized personnel, and provide physical protection appropriate for the deployment.
- Administrators of the appliance must ensure that the appliance is not used for any purpose other than its primary function to perform content scanning of email. Do not install non-TOE software on the appliance.
- Administrators of the appliance must ensure that all DAT signature files and scanning engine update files provided by the anti-virus vendor are installed on the appliance(s) to maintain the currency of the scanning signature files.
- The administrator management computer must be kept free from malware or other malicious software.
- Administrators of the appliance must apply the guidance provided in [Install the appliance](#) on page 14 to ensure that all traffic between the TOE and administration computer for administrator sessions is protected with SSL v3.0/TLS v1.0.
- Administrators of the appliance must perform regular checks to ensure the cached DNS entries on the network devices are not misdirecting the update requests sent to McAfee.
- The management information exchanged between instances of the McAfee Email Gateway in a cluster must be protected from unauthorized interception and eavesdropping.

2

Installing and configuring the McAfee Email Gateway Appliance

Verify the required information for installing and configuring the appliance in compliance with Common Criteria standards.

Contents

- *Pre-installation tasks*
- *Install the appliance*
- *Configure the appliance*

Pre-installation tasks

Use this information to supplement the installation instructions found in the documentation referenced below.

You can find a list of the available guides at [Additional McAfee documentation](#) on page 7.

Check the shipment

Verify the secure delivery of the McAfee Email Gateway Appliance and software version 7.0.1.

Use the following steps to ensure you have received the correct appliance model:

Task

- 1 Verify that all components listed on the packing slip are included and undamaged.
- 2 Ensure the tamper seals on the Email Gateway Appliance and on all supplied software packages are intact.

Review the documentation

Review all associated documentation and guidance before installing, configuring, and managing the appliance.

As Administrator, you must have knowledge of networking and traffic management, since you are responsible for ensuring that qualified personnel complete all tasks described in this guide and additional reference material.

Prepare the environment

Provide an environment where the Email Gateway Appliance is both physically and operationally secure.

Task

- 1 Install the McAfee Email Gateway Appliance in a secure location that provides the same level of physical protection as used for the assets the appliance protects.
- 2 Limit access to administrator personnel as defined in the *McAfee Email Gateway Appliance 7.0.1 Security Target*.
- 3 Ensure that networks and domains are secure, separate, dedicated, available, and established for the administration system with access to the appliance.
- 4 Ensure that traffic cannot bypass the appliance by IT network design.

Install the appliance

Follow the instructions provided in the installation guide or quick start guide for the appliance you are installing.

- Ensure the appliance is installed according to the specifications in this document.
- Hardware and software must comply with the TOE configuration requirements specified in [Hardware and software requirements](#) on page 10.

See the list of documents in [Additional McAfee documentation](#) on page 7.

Configure the appliance

Follow the initial configuration steps for your specific setup.

See the list of documents in [Additional McAfee documentation](#) on page 7.

Configure your model 4000, 4500, 5000, or 5500 appliance

Follow the appropriate documentation to configure Email Gateway Appliance hardware platforms.

Task

- 1 Consult Chapter 1, *Preparing to Install* in the *McAfee Email Gateway 7.0 Appliances Installation Guide* to review concepts of use.
- 2 Follow the instructions in Chapter 2, *Installing the McAfee Email Gateway appliance* in the *McAfee Email Gateway 7.0 Appliances Installation Guide* for information about installation and configuration. Note the following specific instructions:
 - Complete the *Installing the software* section to ensure you install McAfee Email Gateway Appliance software version 7.0.
 - Follow the guidance in *Using the Configuration Console* to enter the appliance name, appropriate network address, gateway, and DNS values for your network. DNS will populate these details, if they are available, and you can confirm or amend them.

- Select the required operational mode.
- Select option **K** to enable FIPS mode.



Additional details about the options available in the configuration console can be found in *Performing a Standard Setup* in Chapter 2 of the *McAfee Email Gateway 7.0 Appliances Installation Guide*.

- 3 Log on to the appliance and use the Setup Wizard to complete the remaining configuration tasks.

Configure a virtual appliance

Consult the *McAfee Email Gateway 7.0 Virtual Appliance Installation Guide* for required information.

Task

- 1 Consult the *Preparing to Install* section to review use concepts.
- 2 Complete the configuration using the *Installing the McAfee Email Gateway Virtual Appliance* section.
- 3 Select option **K** to enable FIPS mode.

Configure McAfee Email Gateway on a blade server

Consult the *McAfee Content Security Blade Server 7.0 System Installation Guide* for required information to configure an M3 or M7 blade server chassis.

Task

- 1 Consult the *Preparing to Install* section to review the concepts of use.
- 2 Follow the instructions in the *Connecting and configuring the blade server* section.
 - a When you install the software, ensure that McAfee Email Gateway software version 7.0.1 is installed on the device.
 - b Follow the guidance for entering the device name, appropriate network address, gateway, and DNS values for your network. DNS will populate these details, if they are available, and you can confirm or amend them. Select the required operational mode.
 - c Select option **K** to enable FIPS mode.
- 3 Log on to the device and use the Setup Wizard to complete the remaining configuration tasks.

Setup Wizard

Use the Setup Wizard to complete the initial configuration.

Each of the installation guides describe how to access the Setup Wizard, which starts automatically the first time the administrator connects to the appliance IP address and logs on to the appliance's user interface.

For more information about the Setup Wizard, see *Using the Configuration Console* provided in the *McAfee Email Gateway 7.0 Appliance Installation Guide* or online Help.



There is a standard setup wizard and a custom setup wizard. The standard installation has fewer steps and is intended for transparent bridge mode. The custom installation allows selection of the operating mode.

For information specific to your appliance, see the following sections in the corresponding guide:

- *Using the Configuration Console* in the *McAfee Email Gateway 7.0 Appliance Installation Guide*.
- *Installing the Virtual Appliance on vSphere* in the *McAfee Email Gateway 7.0 Virtual Appliance Installation Guide*.
- *Using the Configuration Console* in the *McAfee Content Security Blade Server 7.0 System Installation Guide*.
- Follow the guidance in the *Performing a Standard Setup* section of the *McAfee Email Gateway 7.0 Appliance Installation Guide*, noting the following:
 - Potentially Unwanted Programs — This option should be clicked to activate PUP scanning.
 - Current Password/New Password — The new password should include alphabetic characters with either numeric or special characters, and must be at least six characters in length.
 - Time settings — Enter the correct time and click **Set now**. NTP Servers should not be configured for use, because this connection is not encrypted.

Final notes

Pay attention to the following installation and initial configuration notes:

- Any references to upgrading the appliance software made in the documentation (other than DAT signature files and associated scanning engine patches) do not apply to the TOE, and might result in a non-compliant state.
- If you re-install the software, you must repeat the entire configuration process to ensure compliance with the TOE configuration.
- When installation and initial configuration are completed, complete the remaining administrator settings tasks and the deployment process using instructions in this guide.

3

Maintaining a TOE configuration

Additional administrative tasks must be performed to set up Email Gateway to meet the TOE configuration.

A list of the available documentation for Email Gateway can be found at [Additional McAfee documentation](#) on page 7 in this guide.

Review the supplemental information corresponding to installation instructions in the *McAfee Email Gateway 7.0 Administrators Guide*.

Contents

- *Overview of Dashboard features*
- *Overview of Reports features*
- *Overview of the Email menu*
- *Overview of the System menu*
- *Logs, alerts, and SNMP*
- *Component management*
- *Setup Wizard*
- *Troubleshooting features*
- *ePolicy Orchestrator management*
- *Configure additional settings for Common Criteria*

Overview of Dashboard features

No further guidance is necessary in addition to that provided in the *McAfee Email Gateway Appliances 7.0 Administrators Guide*.

Overview of Reports features

The table below provides information you will need when you set up the reporting features.


Table 3-1 Reports features

Feature	Guidance
Types of reports	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Administrators Guide</i> .
Scheduled reports	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Administrators Guide</i>
Email reports	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Administrators Guide</i>
System reports	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Administrators Guide</i>

Overview of the Email menu

The table below provides information you will need when you set up items from the email menu.

Table 3-2 Email menu

Menu item	Guidance
Life of an email message	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Appliances Administrators Guide</i> .
Email configuration	The use of DKIM for signing of outgoing email (as detailed in the DKIM signing subsection) is not supported in the TOE. Therefore, this feature should not be enabled.
Email policies	Using LDAP for group-based policies is not supported in the TOE because the security of the external LDAP servers cannot be assured. Therefore, LDAP groups should not be configured in policy groups (as discussed in the Scanning Policies - Add Policy... portion of the Email Scanning Policies subsection).
DLP and compliance overview	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Administrators Guide</i> .
Encryption	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Administrators Guide</i> .
Certificate management	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Administrators Guide</i> .
Group management	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Administrators Guide</i> .
Add directory service wizard	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Administrators Guide</i> .
Quarantine configuration	<p>The use of an off-box McAfee Quarantine Manager (MQM) is supported in the TOE; however, functionality provided by the MQM is not within the scope of the TOE. An administrator might select to send all quarantined messages to an MQM, rather than use on-box storage of the quarantined messages. However, as the MQM does not form part of the TOE, there are no claims associated with the analysis and management of quarantined email by the MQM, and it is the responsibility of the administrator to obtain the necessary assurance in the behavior of this external component and the protection of the communication between the appliance and the MQM.</p> <div>  <p>It is necessary to use the MQM as an external database of quarantined email for the M3 and M7 blade servers because the blade servers do not support storing this volume of data.</p> </div>

Overview of the System menu

This section provides additional information you need when setting up features from the system menu.

Appliance management

The table below provides guidance for configuring features used in managing your appliance.

Table 3-3 Appliance management

Feature	Guidance
Time and date	To maintain compliance with the TOE configuration NTP Servers should not be configured. The administrator should set the time and date manually, and ensure it is checked regularly to adjust any time drift. The connection between the TOE and NTP servers does not support encryption.
Application management remote access	The use of SSH and out-of-band management for remote access is not supported in the TOE. Therefore, these features should not be enabled.
Load balancing	An additional role, Scanning Appliance Administrator , becomes available if load balancing is enabled. However, this role is not relevant to operation in accordance with the evaluated configuration.

User management

The table below provides guidance to assist you in configuring and managing users

Table 3-4 Users

Feature	Guidance
Directory services menu (authentication groups)	Directory services is not supported in the evaluated configuration because the security of the external directory servers cannot be assured. Therefore, this feature should not be enabled.
Web user authentication menu (authentication groups)	Web user authentication (through RADIUS, Kerberos, NTLM, LDAP, or Microsoft Active Directory) is not supported in the TOE because the security of the external authentication servers cannot be assured. Therefore, these features should not be enabled.
Policy groups menu	Specifying LDAP groups for policies based on group membership is not supported in the TOE because the security of the external LDAP servers cannot be assured. Therefore, LDAP groups should not be configured in policy groups.
Role-based user accounts	The password requirements for user accounts and roles to adhere to the TOE are as follows: <ul style="list-style-type: none">• Minimum length of six characters• Include either numeric or special characters
Virtual hosting	No further guidance is necessary in addition to that provided in the <i>McAfee Email Gateway 7.0 Appliances Administrators Guide</i> .

Logs, alerts, and SNMP

This section provides additional information to help you configure and manage logs and alerts.



All relevant logs are contained within the Message logs and the System logs.

The Message logs include the following information for each event recorded:

- Date/time
- Sender
- Source IP address
- Properties

- Recipient
- Status/category
- Size

The System logs include the following information for each event recorded:

- Date/time
- Gateway name
- Gateway component related to the event
- Details of the event
 - Event ID
 - Identity of subject initiating the event
 - Outcome

Here is an example System log:

```
Sep 5 11:24:56 scmgateway : Application='update-xmlconf', Event  
Id='220010', Event String='Finished applying new configuration', Reason='',  
Appliance IP='10.1.1.108', Local  
Time='2012-09-05_11:24:49_UTC_(+0000)', UTC Time  
='2012-09-05_11:24:49', AdminIP='10.1.1.15', AdminUser='admin'
```

About alerts

You can configure the appliance to send an email message to an administrator when specified events are detected. To use this option, you must enable it in the TOE.

To enable this option, select **System | Logging, Alerting and SNMP | Email Alerting** and select **Enable email alerting**. You can then configure the events that will result in sending an email message to an administrator through the user interface.

In the TOE, you must select the following event types:

- Anti-virus events
- Anti-spam and phish events
- Content filter and compliance events
- URL filter events
- System Log events

You must enter the message and administrator details. Select **System | Logging, Alerting and SNMP | Email Alerting** and enter the appropriate information in the **Alert Settings** field.

Settings

This table provides additional information for configuring alerts and logging.

Table 3-5 Settings

Setting	Guidance
SNMP alert settings	SNMP is not supported in the evaluated configuration due to the inherent weaknesses in this protocol. All SNMP alerting and monitoring functionality can be achieved using other features of the appliance. Therefore, SNMP features should not be enabled.
SNMP monitor settings	SNMP is not supported in the evaluated configuration due to the inherent weaknesses in this protocol. All SNMP alerting and monitoring functionality can be achieved using other features of the appliance. Therefore, SNMP features should not be enabled.
System log settings	Extended syslog features for ArcSight and Splunk are not supported in the evaluated configuration. Therefore, these features should not be enabled.
Logging configuration	To enable generation of the audit records specified in <i>McAfee Email Gateway Appliance 7.0 Security Target</i> for the TOE, configure the audit event settings as detailed in Event log settings on page 21.

Event log settings

To generate proper audit records for the TOE, you must configure the relevant log settings, as shown in the following table:

Table 3-6 Event settings

Event type	Setting type	Navigation path	High severity event setting
Success or failure in logging on to the user interface	User interface settings	System Logging, Alerting and SNMP Logging Configuration Non-proxy Settings User Interface Settings , then select Advanced	<ul style="list-style-type: none"> • 220000 — User logon
Success or failure in logging on to configuration changes	User interface settings	System Logging, Alerting and SNMP Logging Configuration Non-proxy Settings User Interface Settings , then select Advanced	<ul style="list-style-type: none"> • 220009 — Applying new configuration • 220010 — Finished applying new configuration • 220011 — Configuration changed
Identification of virus, malware or spyware	SMTP settings	System Logging, Alerting and SNMP Logging Configuration SMTP Settings , then select Detection Events Advanced	<ul style="list-style-type: none"> • 180000 — Anti-virus engine detection
	POP3 settings	System Logging, Alerting and SNMP Logging Configuration POP3 Settings , then select Detection Events Advanced	<ul style="list-style-type: none"> • 180000 — Anti-virus engine detection

Table 3-6 Event settings *(continued)*

Event type	Setting type	Navigation path	High severity event setting
Detection events	SMTP settings	System Logging, Alerting and SNMP Logging Configuration SMTP Settings , then select Detection Events Advanced	<ul style="list-style-type: none"> • 180002 — Anti-spam classification • 180004 — MIME format detection • 180010 — Compliance detection • 180014 — Image analyzer detection • 180016 — Avira anti-virus engine detection • 180017 - Authentium anti-virus engine detection • 50013 — Sender authentication; permit/deny information
	POP3 settings	System Logging, Alerting and SNMP Logging Configuration POP3 Settings , then select Detection Events Advanced	<ul style="list-style-type: none"> • 180002 — Anti-spam classification • 180004 — MIME format detection • 180014 — Image analyzer detection • 180016 — Avira anti-virus engine detection • 180017 — Authentium anti-virus engine detection
Action taken to remove or mitigate virus, malware, or spyware	SMTP settings	System Logging, Alerting and SNMP Logging Configuration SMTP Settings , then select Detection Events Advanced	<ul style="list-style-type: none"> • 180005 — Scan actions
	POP3 settings	System Logging, Alerting and SNMP Logging Configuration POP3 Settings , then select Detection Events Advanced	<ul style="list-style-type: none"> • 180005 — Scan actions
Network-level communication events	SMTP settings	System Logging, Alerting and SNMP Logging Configuration SMTP Settings , then select Advanced events for Communication Events	<ul style="list-style-type: none"> • 19001 — SSL certificate conversation failed • 19003 — SSL certificate initialization failed • 50053 — Using encrypted delivery for email
Protocol processing events	SMTP settings	System Logging, Alerting and SNMP Logging Configuration SMTP Settings , then select All events for Protocol Events	<ul style="list-style-type: none"> • 19000 — Protocol conversation

Table 3-6 Event settings *(continued)*

Event type	Setting type	Navigation path	High severity event setting
	POP3 settings	System Logging, Alerting and SNMP Logging Configuration POP3 Settings , then select All events for Protocol Events	<ul style="list-style-type: none"> • 19000 — Protocol conversation
Unsuccessful attempt to scan traffic or message	SMTP settings	System Logging, Alerting and SNMP Logging Configuration SMTP Settings , then select Communication Events Advanced	<ul style="list-style-type: none"> • 180007 — Scanner failed
	POP3 settings	System Logging, Alerting and SNMP Logging Configuration POP3 Settings , then select Communication Events Advanced	<ul style="list-style-type: none"> • 180007 — Scanner failed
Hardware and software appliance settings, including TOE Security Function (TSF) settings	System settings, system events	System Logging, Alerting and SNMP Logging Configuration Non-proxy Settings System events Advanced	<ul style="list-style-type: none"> • 210011 — MA state has changed • 210101 — Anti-virus update has made changes • 210103 - Anti-virus update failed • 210104 — Anti-virus update interrupted • 210111 — Anti-spam engine update has made changes • 210113 — Anti-spam engine update failed • 210114 — Anti-spam engine update interrupted • 210125 — Anti-spam rules update succeeded after a series of failures • 210126 — Anti-spam update failing repeatedly • 210500 — Package update
	System settings, user interface events	System Logging, Alerting and SNMP Logging Configuration Non-proxy Settings User interface events Advanced	<ul style="list-style-type: none"> • 220003 — Appliance date changed • 220006 — Appliance configuration saved • 220012 — User accounts/roles modified • 220160 — Log to file archival
	Web Mail Client user events	System Logging, Alerting and SNMP Communication Events Advanced	<ul style="list-style-type: none"> • 50061 — Web Mail Client login

Component management

This table provides additional information for configuring specific components of your system.

Table 3-7 Components

Component	Guidance
Update status	The appliance administrator must ensure that signature (DAT) files and scanning engine updates provided by McAfee for the appliance are installed promptly upon release. Settings within the appliance will allow for automatic updating upon signature file release. This function must be enabled for the TOE. To enable this option, select System Component Management Update Status and set the Scheduled entry for each type of component. The administrator is responsible for performing regular checks to ensure that the local DNS cache has not been subject to a DNS poison attack.
Package installer	Use of this feature to apply hotfixes and patches will result in the appliance running non-certified firmware.
ePolicy Orchestrator	Management by ePolicy Orchestrator® is not supported in the TOE.

Setup Wizard

Email Gateway setup wizards guide you through appliance configuration.

Email Gateway provides two setup wizards:

- **Standard Setup Wizard** — Has fewer steps and is intended for setting up the appliance in Transparent Bridge mode
- **Custom Setup Wizard** — Allows selection of the operating mode

Troubleshooting features

No further guidance is necessary in addition to that provided in the *McAfee Email Gateway 7.0 Administrators Guide*.

ePolicy Orchestrator management

In the TOE, interoperability with ePolicy Orchestrator is not supported.

Configure additional settings for Common Criteria

You must configure additional settings to audit SSL and HTTPS connections and enable the Web Mail Client audit trail, and to upload the audit logs over SSH.

Tasks

- [Configure the audit of Common Criteria specific events on page 25](#)
Follow this process to configure the auditing of failed SSL connections, the creation and/or termination of HTTPS connections, and enabling the Web Mail Client audit trail.
- [Export audit logs on page 26](#)
Follow this process to export audit logs over SSH.

Configure the audit of Common Criteria specific events

Follow this process to configure the auditing of failed SSL connections, the creation and/or termination of HTTPS connections, and enabling the Web Mail Client audit trail.

Some of the required configuration is not available through the user interface.

Task

- 1 Back up the appliance configuration.
 - a Navigate to **System | System Administration | Configuration Management**.
 - b Select **Backup Configuration** to save the ZIP file to disk.
- 2 On the workstation, extract the ZIP file.



It is important to preserve the directory structure of the ZIP file.

- 3 Use WordPad to open the file config\channels.xml from the folder.

The file opens.

- 4 Locate the line: `<EventGroup enabled="yes" name="SystemEvents">`.
- 5 Immediately underneath that line add the lines:

```
<Event id="220050" enabled="yes" default="yes"/>
<Event id="220051" enabled="yes" default="yes"/ >
<Event id="50061" enabled="yes" default="yes"/>
```

- 6 Locate the following near the beginning of the file:

```
<xsl:value-of select="@app"/>
```

- 7 Immediately underneath that line, add the following lines:

```
<xsl:if test="Info [@name=username]/text()">
  <xsl:text>',Username='</xsl:text>
  <xsl:value-of select="Info [@name='username']/text()"/>
</xsl:if>
```

- 8 Save the updated file in text format.
- 9 Use WordPad to open the file config\ui-logging.xml from the folder.

The file opens

- 10 Locate the line:

```
<Group name="ui" level="1" default="1"/>
```



The level attribute may contain a different value (such as "3"). This is allowed.

- 11 Immediately underneath that line add the line: .

```
<Event id="220051" group="ui" enabled="yes" default="yes" level="1"/>
```

- 12 Save the updated file in text format.
- 13 Use WordPad to open the file config\smtp-logging.xml from the folder.

The file opens.

14 Locate the line beginning: `<Event id="50059"`. Update the entry to read:

```
<Event id="50061" group="detection" enabled="yes" default="no" subgroup="generic"
level="1" high-volume="yes"/>
```

15 Save the updated file in text format.

16 Recreate the ZIP file from the root directory of the extracted ZIP file.

17 On the user interface, navigate to **System | System Administration | Configuration Management**.

18 Select **Restore From File**.

19 Browse to the modified ZIP file, and select **Import Config**.

20 Apply your changes.

SSL failure events, creation/termination of HTTPS connections, and Web Mail Client events will be logged in `/var/log/messages`, with the event id 220050, 220051 and 50061, respectively. You can view the logs by navigating to **System | Logging, Alerting and SNMP | System Log Settings** and selecting **View the system logs**.

Export audit logs

Follow this process to export audit logs over SSH.

Task

1 Navigate to **System | Logging, Alerting and SNMP | System Log Settings**.

2 Scroll down the page, and select **System Log Archive**.

3 Select **Transfer via SSH**.

The audit logs are exported.

Index

A

- alerts [19](#)
 - email [20](#)
- appliance
 - hardware [10](#)
 - management [19](#)
 - software [10](#)
- appliance configuration [14](#)

B

- blade server configuration [15](#)

C

- component management [24](#)
- configuration
 - appliance [14](#)
 - blade server [15](#)
 - virtual appliance [15](#)

D

- dashboard [17](#)
- definitions
 - key terms [8](#)
- documentation
 - additional MEG 7.0 [7](#)
 - review [13](#)

E

- email menu [18](#)
- environment, operating [11](#)
- ePolicy Orchestrator [24](#)
- event log [21](#)

H

- hardware, appliance [10](#)

I

- installation
 - appliance [14](#)

K

- key terms [8](#)

L

- logging
 - alerts [20](#)
 - event settings [21](#)
 - settings [21](#)
- logs [19](#)

M

- management
 - appliance [19](#)
 - component [24](#)
 - ePolicy Orchestrator [24](#)
 - users [19](#)

O

- operating environment
 - guidelines [11](#)
 - preparation [14](#)

P

- pre-installation [13](#)
 - documentation review [13](#)
 - environment preparation [14](#)
 - shipment check [13](#)

R

- reporting [17](#)

S

- setup wizard [15](#), [24](#)
- SNMP [19](#)
- software
 - administration computer [10](#)
 - appliance [10](#)
 - virtual appliance [10](#)
- SSL connections
 - auditing [24](#)
 - uploading audit logs [24](#)

system menu [18](#)

T

troubleshooting [24](#)

U

users, managing [19](#)

V

virtual appliance configuration [15](#)

