



Product Guide

McAfee Security for Microsoft Exchange 8.5.0

COPYRIGHT

Copyright © 2014 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS

McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure 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.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

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 MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface	7
About this guide	7
Audience	7
Conventions	7
Using this guide	8
Find product documentation	8
1 Introduction	9
What's new in this release	9
Product features	11
Why do you need MSME	13
Threats to your organization	13
How MSME protects your Exchange Server	14
How emails are scanned	16
Scanning inbound emails	16
Scanning outbound emails	17
Scanning internal emails	18
2 Installation and configuration	19
Pre-installation	19
System requirements	20
Supported Microsoft Exchange Server roles	21
Package contents	21
Installation	22
Install the software using setup wizard	22
Install the McAfee Anti-spam add-on manually	24
Perform a silent installation	25
Upgrade a standalone deployment	26
Post-installation	28
Quick setup	28
Cluster deployment	29
Test your installation	31
3 Dashboard	33
Statistical information of detected items	33
Detections	34
Scanning	38
Graph	38
Product versions and updates	39
Update information	39
Schedule a software update	40
Product information	40
Licenses	41
View recently scanned items	41
On-Demand scan and its views	42

View on-demand scan tasks	43
Create on-demand scan task	44
Status reports	46
View status report tasks	46
Schedule a new status report	47
Status report email notifications	48
Configuration reports	49
View configuration report tasks	49
Schedule a new configuration report	50
Configuration report email notifications	52
Graphical reports	52
View graphical report using simple search filters	52
Using advanced search filters	53
4 Detected items	57
Manage quarantined data	57
Detection types	58
Available primary search filters	60
Search filter comparison chart	62
Additional search options	63
Search detected items	64
Actions that you can take on quarantined items	65
5 Policy Manager	69
Policy Manager menu options	70
Policy categories to handle threats	70
Policy Manager views	71
Master policy and subpolicy	72
Create subpolicies	72
Core scanners and filters	74
Scanners and filters comparison chart	75
List all scanners and filters for a selected policy	77
Adding a scanner or filter	78
Create new rule for specific users	79
Actions you can take on detections	79
Shared Resource	81
Configure scanner settings	81
Configure alert settings	82
Create an alert	83
Configure DLP and compliance rules	85
Configure file filtering rules	88
Configure time slots	89
Manage core scanner settings for a policy	90
Configure anti-virus scanner settings	91
Configure DLP and compliance scanner settings	93
Configure file filtering settings	95
Configure mail URL reputation settings	96
Configure anti-spam settings	99
Configure anti-phishing settings	102
Manage filter settings for a policy	103
Configure corrupt content settings	103
Configure protected content settings	104
Configure encrypted content settings	104
Configure signed content settings	105
Configure password-protected file settings	105
Configure mail size filtering settings	106

Configure scanner control settings	107
Configure MIME mail settings	108
Configure HTML file settings	110
Manage miscellaneous settings for a policy	111
Configuring alert message settings	111
Configuring disclaimer text settings	112
6 Settings and diagnostics	115
On-Access settings	117
Microsoft Virus Scanning API (VSAPI) settings	118
Background scan settings	119
Transport scan settings	120
On-Demand settings	120
Configure mailbox exclusion settings	121
Examples of using wildcards for mailbox exclusions	123
Notification settings	123
Configure notification settings	124
Edit notification template	125
Notification fields that you can use	126
Enable product health alerts	126
Anti-spam settings	128
Detected items settings	129
Quarantine using McAfee Quarantine Manager	129
Quarantine using the local database	131
User interface preferences settings	132
Configure dashboard settings	132
Configure graph and chart settings	133
Diagnostics settings	133
Configure debug log settings	133
Configure event logging settings	135
Configure product log settings	136
Configure error reporting service settings	137
View product logs	138
Configure DAT settings	139
Import and export configuration settings	139
Export your existing MSME configuration	140
Import configuration from another MSME server	140
Import a sitelist	141
Configure anti-spam proxy settings	141
7 Program maintenance	143
Modify the installation	143
Repair the installation	143
Restore default settings	144
Purge and optimize	144
Uninstall the software	145
8 Integrating MSME with ePolicy Orchestrator	147
Prerequisites	147
Check in the MSME package	148
Install the MSME extension	148
Migrate policies from older versions	148
Deploy the MSME software to clients	149
Set up the McAfee Anti-spam software	150
Check in the McAfee Anti-spam package	150
Deploy the McAfee Anti-spam add-on	151

Manage policies	151
Create or modify policies	152
Assign policies	152
Create and schedule tasks	153
Schedule automatic updates	153
Schedule an on-demand scan	154
Schedule to send status report	155
Schedule to send configuration report	156
Schedule a task to purge the old DAT files	156
Queries and reports	157
Predefined queries	157
Custom query filters	158
Run a default query	159
Filter events	159
Configure automatic responses	160
Remove the software	161
Remove the McAfee Anti-spam software from clients	161
Remove the client software	162
Remove the software extension	162
9 Troubleshooting	165
Default Vs. Enhanced configuration settings	165
Important registry keys	166
10 Frequently asked questions	167
General	167
Installation	168
Policy Manager	168
Settings and diagnostics	169
McAfee Anti-Spam add-on component	170
Regular Expressions (regex)	171
A Using McAfee Security for Microsoft Exchange Access Control	173
B SiteList Editor	175
Configure sitelist repository settings	176
Configure sitelist proxy settings	178
Index	181

Preface

This guide provides the information you need for all phases of product use, from installation to configuration to troubleshooting.

Contents

- ▶ *About this guide*
- ▶ *Find product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience





McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses these typographical conventions and icons.

<i>Book title, term, emphasis</i>	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
User input, code, message	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Using this guide

This guide will take you through the installation process and help you understand the various features of McAfee Security for Microsoft Exchange 8.5.0.

To do this...	Look here...
Learn how the software works, product features and how emails are scanned.	Chapter 1, Introduction
Plan and perform your desired type of installation such as standalone, silent, cluster or upgrading from an older version.	Chapter 2, Installation and configuration
Get information about the system health through dashboards and graphical reports. Schedule on-demand scans, status reports, and configuration reports.	Chapter 3, Dashboard
View information about all email messages containing potential threats that are detected and quarantined by the software.	Chapter 4, Detected Items
Configure or manage different policies and actions to determine how different types of threats are treated when detected.	Chapter 5, Policy Manager
Plan and configure the software settings to best suit the security for your Microsoft Exchange server.	Chapter 6, Settings and Diagnostics
Perform maintenance tasks such as repair, modify, remove or restore the software. Also perform purge and optimization tasks to improve the database utilization.	Chapter 7, Program maintenance
Manage your McAfee Security for Microsoft Exchange server using an ePolicy Orchestrator server to manage the policies and product specific tasks.	Chapter 8, Integrating McAfee Security for Microsoft Exchange with ePolicy Orchestrator
Determine and troubleshoot issues while using the software.	Chapter 9, Troubleshooting
Get answers to common situations that you might encounter when installing or using the product.	Chapter 10, Frequently asked questions
Allow or deny access to the McAfee Security for Microsoft Exchange user interface for specific users or groups.	Appendix A, Using the McAfee Security for Microsoft Exchange Access Control
Configure sitelists that specify the location from where automatic updates are downloaded.	Appendix B, SiteList Editor

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

- 1 Go to the McAfee ServicePortal at <http://support.mcafee.com> and click **Knowledge Center**.
- 2 Enter a product name, select a version, then click **Search** to display a list of documents.

1

Introduction

McAfee® Security for Microsoft Exchange (MSME) protects your Microsoft Exchange server from various threats that could adversely affect the computers, network, or employees.

MSME uses advanced heuristics against viruses, unwanted content, potentially unwanted programs, and banned file types or messages. It also scans:

- Subject line and body of the email messages
- Email attachments (based on file type, file name, and file size)
- Text within the email attachments
- URLs in the email body

The software also includes the McAfee Anti-Spam add-on that protects your Exchange server from spam and phishing emails.

Contents

- ▶ [What's new in this release](#)
- ▶ [Product features](#)
- ▶ [Why do you need MSME](#)
- ▶ [How MSME protects your Exchange Server](#)
- ▶ [How emails are scanned](#)



What's new in this release

McAfee Security for Microsoft Exchange has increased its protection profile to provide the best protection for your Microsoft Exchange servers.

Here is a list of new features included with this release of the product:

Feature	Description
Protection from malicious URLs	When enabled, MSME scans each URL in the email body, gets the reputation score of the link, compares the score to the defined threshold, and takes appropriate action according to the configuration.
Exchange server support	Support for Microsoft Exchange Server 2013 SP1.
No dependency on anonymous logon permission	MSME does not require anonymous logon permission anymore in exchange receive connector for notification.
Additional communication channels to quarantine the detected items	In addition to the existing quarantine mechanism (local database and RPC channels), MSME provides HTTP and HTTPS channels to communicate with McAfee® Quarantine Manager (MQM) server. These stateless connections make sure that the software communicates with the MQM server seamlessly.

Feature	Description
DLP rules in all supported locale	Allows you to define DLP rules in all supported locales. You can also view and edit the dictionaries of other supported locales. The supported locales are Chinese Simplified, English, French, German, Japanese, and Spanish.
Management of on-demand (MSMEODUser) user account	Allows you to modify the on-demand user password credentials and synchronize them with the LDAP server using the interface.
Exclusion of subfolders and public folders from scanning	Provides the option to exclude mailbox subfolders and public folders from on-access scanning (VSAPI scanning). You can also configure these exclusions from ePolicy Orchestrator.
IP whitelisting	Provides the option to whitelist the known legitimate IP address that is refused by the IP reputation threshold settings.
Monitoring the scanner process to avoid high RPC issue	Uses the watch process approach to monitor the high RPC issue that happens due to additional time taken to scan specific sample files. Corrective action is taken according to the policy settings.
Mail size filtering	Allows you to configure the mail size filtering for On-Access policy and Gateway policy separately.
Restricted files in .zip format	Provides option to allow or block restricted files such as .exe files that come as a password-protected .zip file.
Scan failure scenario	Allows you to configure actions for scan failure due to generic failure or product failure.
Proxy server	Allows you to configure proxy servers to get IP reputation, message reputation, and URL reputation database.
Support for 7-Zip archive file scanning	Supports 7-Zip file scanning on all scanners and filters.
Compatibility with ePolicy Orchestrator FIPS (Federal Information Processing Standard) mode	Compatible with ePolicy Orchestrator, which is installed in FIPS mode. You can use the same ePolicy Orchestrator to manage MSME.
Viewing on-demand scan status in ePolicy Orchestrator	View the status of scheduled on-demand scan tasks in ePolicy Orchestrator. For managed systems, on-demand scanning events are generated with the details such as start time, end time, number of items scanned, and number of items quarantined. Events are generated whether the on-demand scan is initiated by the local system or initiated from ePolicy Orchestrator.
Viewing on-demand scan completion percentage in ePolicy Orchestrator	View the percentage of the on-demand scan task completion status in ePolicy Orchestrator, when the scanning is initiated from ePolicy Orchestrator. You can view the on-demand scanning percentage in the Threat Event Log page in the Threat source URL column.
Purge old DAT using scheduled tasks from ePolicy Orchestrator	Allows you to purge the old DAT files from managed systems using scheduled tasks.

Feature	Description
McAfee stack upgrade	<p>Bundled with newer versions of these components:</p> <ul style="list-style-type: none"> • McAfee Agent • McAfee Content Scanning Engine • McAfee Anti-Spam Engine • PostgreSQL 9.3 database <p> When upgrading the PostgreSQL database, your existing data is migrated to 9.3 supported schema. Depending on the database size, the installer might take additional time to complete the update.</p>
Enhanced alert notification for detected items	<p>Categorizes the detected items based on the reason for blocking, instead of repeating the reason for each item.</p>
Browser enhancements	<ul style="list-style-type: none"> • Support for new browsers: <ul style="list-style-type: none"> • Microsoft Internet Explorer 8.0, 9.0, 10.0, and 11.0 • Mozilla Firefox 29.x and 30.x • Google Chrome 35 <p> Make sure that you disable the pop-up blocker in the browser settings to access the product web interface.</p>

Product features

The main features of MSME are described in this section.

- **Protection from viruses** — Scans all email messages for viruses and protects your Exchange server by intercepting, cleaning, and deleting the viruses that it detects. MSME uses advanced heuristic methods and identifies unknown viruses or suspected virus-like items and blocks them.
- **Protection from spam** — Helps you save bandwidth and the storage space required by your Exchange servers by assigning a spam score to each email message as it is scanned and by taking pre-configured actions on those messages.
- **Protection from phishing** — Detects phishing emails that fraudulently try to obtain your personal information.
- **Protection from malicious URLs** — Protects your system from malicious URLs. When enabled, MSME scans each URL in the email body, gets the reputation score of the link, compares the score with the defined threshold, and takes appropriate action according to the configuration.
- **Capability to detect packers and potentially unwanted programs** — Detects packers that compress and encrypt the original code of an executable file. It also detects potentially unwanted programs (PUPs), that are software programs written by legitimate companies to alter the security state or privacy state of a computer.
- **Content filtering** — Scans content and text in the subject line or body of an email message and an email attachment. MSME supports content filtering based on regular expressions (regex).
- **File filtering** — Scans an email attachment depending on its file name, type, and size of the attachment. MSME can also filter files containing encrypted, corrupted, password-protected, and digitally signed content.

- **DLP and compliance** — Ability to ensure that email content is in accordance with your organization's confidentiality and compliance policies. Pre-defined compliance dictionaries include:
 - Addition of 60 new DLP and Compliance dictionaries
 - Support for industry specific compliance dictionaries — HIPAA, PCI, Source Code (Java, C++ etc.)
 - Improvements to existing phrase based detections.
 - Reduced false positives, due to enhanced capabilities in detecting non-compliant content, based on the Threshold score and in combination with the maximum term count (occurrence).

Customize policies for content security and Data Loss Prevention (DLP).

- **IP reputation** — A method of detecting threat from email messages based on the sending server's IP address. IP Reputation Score reflects the likelihood that a network connection poses a threat. IP reputation leverages on McAfee Global Threat Intelligence (GTI) to prevent damage and data theft by blocking the email messages at the gateway based on the source IP address of the last email server. MSME processes the message before it enters the organization by rejecting or dropping the connection based on the IP reputation score.
- **Advanced On-Demand scan** — Ability to perform granular-level on-demand scan on Exchange Server 2010 & 2013, resulting in faster on-demand scans. You can schedule on-demand scans based on these filters; Subject, Attachments, Sender/Recipient/CC, Mail Size, Message ID, Unread items, and Time duration.
- **Background scanning** — Facilitates scanning of all files in the information store. You can schedule background scanning to periodically scan a selected set of messages with the latest engine updates and scanning configurations. In MSME, you can exclude mailboxes that you don't want to be scanned.
- **Product Health Alerts** — These are notifications on the status of the product's health. You can configure and schedule these alerts.
- **Integrate with McAfee ePolicy Orchestrator 4.6, 5.0, or 5.1** — Integrates with ePolicy Orchestrator 4.6, 5.0, or 5.1 to provide a centralized method for administering and updating MSME across your Exchange servers. This reduces the complexity of, and the time required to, administer and update various systems.
- **Web-based user interface** — Provides a user-friendly web-based interface based on DHTML.
- **Policy Management** — The **Policy Manager** menu option in the product user interface lists different policies you can set up and manage in MSME.
- **Centralized scanner, filter rules, and enhanced alert settings** — Using scanners, you can configure settings that a policy can apply when scanning items. Using File Filtering rules, you can set up rules that apply to a file name, file type, and file size.
- **On-demand/time-based scanning and actions** — Scans email messages at convenient times or at regular intervals.
- **Multipurpose Internet Mail Extensions (MIME) scanning** — A communications standard that enables you to transfer non-ASCII formats over protocols (such as SMTP) that support only 7-bit ASCII characters.
- **Quarantine management** — You can specify the local database to be used as a repository for quarantining infected email messages. You can choose to store quarantined messages on your own server running McAfee Quarantine Manager, which is called the *Off-box quarantine*.
- **Auto-update of virus definitions, Extra DATs, anti-virus and anti-spam engine** — Regularly provides updated DAT files, anti-virus scanning engine, and anti-spam engine to detect and clean the latest threats.

- **Retention and purging of old DATs** — Retain old DAT files for periods you define or purge them as needed.
- **Support for Site List editor** — Specify a location from which to download automatic updates for MSME.
- **Support for Small Business Server** — MSME is compatible with Small Business Servers.
- **Detection reports** — Generates status reports and graphical reports that enable you to view information about detected items.
- **Configuration reports** — Summarizes product configuration such as information about the server, version, license status and type, product, debug logging, on-access settings, on-access policies, and gateway policies. You can specify when your server needs to send the configuration report to the administrator.
- **Denial-of-service attacks detection** — Detects additional requests or attacks flooding and interrupting the regular traffic on a network. A denial-of-service attack overwhelms its target with false connection requests, so that the target ignores legitimate requests. MSME considers these three scenarios as Denial-of-service attacks:
 - Scanning time exceeds the defined time
 - Nested level exceeds the defined level
 - Expandable file size limit for archived files exceeds the defined size
- **Advanced notifications** — Forward the quarantined emails for compliance audit to multiple users, based on the detection category.
- Support for VMware workstation 7.0 or later, and VMware ESX 5.5.

Why do you need MSME

Your organization is vulnerable to many threats that can affect its reputation, employees, computers, and networks.

- The reputation of an organization can be affected by the loss of confidential information or through an abuse that can lead to legal action.
- Electronic distractions and unrestricted use of email and the Internet can affect the productivity of employees.
- Viruses and other potentially unwanted software can damage computers, making them unusable.
- Uncontrolled use of various types of files on your networks can cause performance problems for your entire organization.

Threats to your organization

Learn about various threats that could affect an organization.

Type of threat	Description
Reputation of a company	An unguarded or ill-informed remark by an employee might cause legal problems, unless it is covered by a disclaimer.
Spam (unsolicited email)	Unsolicited commercial email messages are the electronic equivalent of spam or junk mail. Often they contain advertisements that are not expected by the recipients. Although it is more of a nuisance than a threat, spam can degrade the performance of your network.
Large email messages	Large email messages or messages that contain numerous attachments can slow down the performance of email servers.

Type of threat	Description
Mass-mailer viruses	Although they can be cleaned like any other virus, they can spread rapidly and quickly degrade the performance of your network.
Email messages from unwanted sources	Disgruntled ex-employees and unscrupulous individuals who know the email addresses of your employees can cause distress and distraction by sending unwanted emails.
Non-business use of email	If most employees use recipient email addresses not within their organization, such emails are likely to be for personal or non-business use.
Loss of company-confidential information	Employees might disclose confidential information related to unreleased products, customers or partners.
Offensive language	Offensive words or phrases can appear in email messages and attachments. Besides causing offense, they can provoke legal action too.
Transfer of entertainment files	Large video or audio files intended for entertainment might reduce your network performance.
Inefficient file types	Some files use large amounts of memory and can be slow to transfer, but alternatives are often available. For example, GIF and JPEG files are much smaller than their equivalent BMP files.
Transfer of large files	Transferring large files can reduce your network performance.
Denial-of-service attack	A deliberate surge of large files can seriously affect the performance of your network, making it unusable to its legitimate users. While scanning large size compressed files, MSME considers three parameters for DOS attack: <ul style="list-style-type: none"> • Scanning time for compressed files exceeds the threshold. • The nested levels of compressed files are identified. For example, a compressed .zip file contains another compressed files inside, and continues expanding with more compressed files. • The expandable size limit of archived files exceeds the threshold.
Pornographic text	Vulgar language or terms must not be used in emails.
Viruses and other potentially unwanted software	Viruses and other potentially unwanted software can quickly make computers and data unusable.
Corrupt or encrypted content	This type of content cannot be scanned. Appropriate policies must be specified to handle it.

How MSME protects your Exchange Server

Learn how MSME protects your exchange server by accessing all email messages that reach the exchange server, and emails that are read from and written to the mailbox.

Protecting your Microsoft Exchange server

MSME uses the virus scanning interface of your Exchange server to gain full access to all email messages that are being read from, and written to the mailbox of the Exchange server.

- The anti-virus scanning engine compares the email message with all the known virus signatures stored in the DATs.
- The content management engine scans the email message for banned content as specified in the content management policies in MSME.

If these checks find any viruses or banned content within the email message, MSME takes the specified action. If no items are detected, MSME passes the information back to the virus-scanning interface to complete the original message request within Microsoft Exchange.

Real-time detection

MSME integrates with your Exchange server and works in real time to detect and delete viruses or other harmful or unwanted code. It also helps you maintain a virus-free environment by scanning the databases on your Exchange server. Each time an email message is sent to or received from a source, MSME scans the email message to compare it with a list of known viruses and suspected virus-like behavior and intercepts and cleans the infected file before it spreads. It can also scan content within the email message (and its attachments), using rules and policies defined in the software.

Scanning of email messages

- The anti-spam, anti-virus, and the content management engines scan the email messages and provide the result to MSME before the content is written to the file system or read by the Microsoft Exchange users.
- The anti-virus and the anti-spam scanning engines compare the email message with all the known signatures stored in the currently installed virus definition files (DATs) and anti-spam rules. The anti-virus engine also scans the message using selected heuristic detection methods.
- The content management engine scans the email message for banned content as specified in the content management policies running within the software. If there are no viruses, banned/unwanted content in the email message, MSME passes the information back to Microsoft Exchange. In case of a detection, MSME takes actions as defined within its configuration settings.

How scanning works

- Central to your MSME are the scanning engine and DAT files. The engine is a complex data analyzer. The DAT files contain a great deal of information including thousands of different drivers, each of which contains detailed instructions on how to identify a virus or a type of virus.
- The scanning engine works with the DAT files. It identifies the type of the item being scanned and decodes the content of that object to understand what the item is. It then uses the information in the DAT files to search and locate known viruses. Each virus has a distinctive signature. There is a sequence of characters unique to a virus and the engine searches for that signature. The engine uses a technique called heuristic analysis to search for unknown viruses. This involves analyzing the object's program code and searching for distinctive features typically found in viruses.
- Once the engine has confirmed the identity of a virus, it cleans the object to the extent possible. For example, it removes an infected macro from an attachment or deletes the virus code in an executable file.

What and when to scan?

- The threat from viruses can come from many directions such as infected macros, shared program files, files shared across a network, email messages and attachments, floppy disks, files downloaded from the Internet, and so on. Individual McAfee Security anti-virus software products target specific areas of vulnerability. We recommend a multi-tiered approach to provide the full range of virus detection, security, and cleaning capabilities that you require.
- MSME provides a range of options that you can further configure according to the demands of your system. These demands will vary depending on when and how the component parts of your system operate and how they interact with each other and with the outside world, particularly through emails and Internet access.
- You can configure or enable various actions that allow you to determine how your MSME server should deal with different items and what actions it should take on detected or suspicious items.

How emails are scanned

MSME scans an email differently based on whether it is an inbound, outbound, or internal email.

Each time an email message is sent to or received from a source, MSME scans it comparing it with a list of known viruses and suspected virus-like behavior. MSME can also scan for content within the email message using rules and policies defined within the software.

When MSME receives an email, it scans in this order:

- 1 IP address, spam or phish
- 2 Corrupt or encrypted content
- 3 File filter
- 4 Content scanning (DLP and Compliance)
- 5 Anti-virus
- 6 Mail URL reputation

Even though emails are scanned in this order, if an item is detected first by the file filtering scanner, it will still be scanned for anti-virus before being quarantined.



Detecting an email based on the source IP address is possible when you enable the IP reputation feature in MSME. This feature is available when you install the McAfee Anti-Spam component.

Scanning inbound emails

Step-by-step information on what happens to an email that reaches your organization and how MSME scans it to determine if the email is clean or infected.

The task described below is narrated assuming a situation in your organization, where you have installed MSME on all these roles:

- Edge Transport
- Hub Transport
- Mailbox

If you don't have an Exchange server on the Edge or Hub Transport role, MSME will ignore the steps related that role.

Task

- 1 The SMTP stack hosted by `EdgeTransport.exe` on Edge role receives the email.
- 2 MSME Transport Agent (McAfeeTxAgent) scans the email for spam, phish or mail size.



If you have installed the McAfee Anti-Spam add-on component and enabled the IP reputation feature, emails will be scanned based on the source IP address by the Transport IP Agent (McTxIPAgent).

- 3 If there is detection, it is dropped, else it is returned to the SMTP stack.
- 4 If the email is clean, McAfeeTxRoutingAgent processes it.
- 5 MSME receives the same stream and scans for File filtering, Content scanning and Anti-virus (AV) scanning.
- 6 If there is a detection, action is taken as per product configuration.
- 7 MSME stamps the email with AV stamp as per Microsoft specifications.
- 8 The email is now sent to Exchange Hub server role.
- 9 SMTP stack hosted by `EdgeTransport.exe` on Hub server role, receives the email.

- 10 MSME Transport Agent (McAfeeTxAgent) scans the email for spam, phish or mail size. Only in case of EdgeSync (Edge and Hub server), the session is authenticated where anti-spam scanning is skipped. In this case, Originator check is used for session authentication.
- 11 If there is detection, the email is dropped, else it is returned back to the SMTP stack.
- 12 If the email is clean, McAfeeTxRoutingAgent processes it and checks for AV stamp (if any).
- 13 If AV stamp is present, it checks and compares with the stamp MSME forms with engine/DAT on Hub server role.
- 14 If the stamp is different, MSME receives the same stream and scans for File filtering, Content scanning and Anti-virus scanning.
- 15 On Transport, MSME looks for AV stamp whereas on VSAPI, Exchange Store does this work and MSME will not receive a scan call if AV stamp matches.
- 16 If there is a detection, an action is taken as per product configuration.
- 17 MSME stamps the email with AV stamp as per Microsoft specifications.
- 18 The email is routed to Exchange Mailbox server role.
- 19 Exchange store receives the mail and before saving it to its database, checks for the AV stamp.
- 20 If AV stamp matches, it saves the item without scanning.
- 21 If AV stamp does not match, Exchange store calls VSAPI (Virus Scanning API) and scans the email.
- 22 If there is detection, the email is replaced or deleted as per product configuration.

Scanning outbound emails

Step-by-step information on what happens to an email that goes out of the organization and how MSME scans it, to determine if the email is clean or infected.

Task

- 1 The end-user sends an email to an external user, using the email client.
- 2 Exchange store receives the email and scans it in the Outbox folder.
- 3 If there is detection, it is replaced or deleted as per the product configuration and if replaced it is submitted to Transport queue.
- 4 SMTP stack hosted by `EdgeTransport.exe` on Hub server role, receives the email.
- 5 MSME Transport Agent (McAfeeTxRoutingAgent) scans the email for File filtering, Content scanning, then Anti-Virus scanning and also disclaimer addition.
- 6 If there is detection, it is dropped or replaced and appropriately returned to the SMTP stack.
- 7 If the email is clean, it is returned to SMTP stack for further routing.
- 8 If the email is routed to Edge server role from this Hub server, then:
 - a SMTP stack hosted by `EdgeTransport.exe` on Edge server role, receives the email.
 - b MSME Transport Agent (McAfeeTxRoutingAgent) checks for AV stamp (if any).
 - c If AV stamp is present, it checks and compares with the stamp MSME forms with engine/DAT on Edge server role.

- d If the stamp is different then, MSME receives the same stream and scans for File filtering, Content scanning, then Anti-virus scanning.
 - e If there is a detection, action is taken as per product configuration.
 - f MSME stamps the email with AV stamp, as per Microsoft specifications on Edge server role.
- 9 Now the email is returned to SMTP stack, hosted by `EdgeTransport.exe` on Edge server role for further routing.

Scanning internal emails

Step-by-step information on what happens to an email that is sent within the organization and how MSME scans it, to determine if the email is clean or infected.

Task

- 1 The end-user sends an email to an internal user, using the email client.
- 2 Exchange store receives the email and scans it in the Outbox folder.
- 3 If there is detection, it's replaced or deleted as per the product configuration and if replaced it is submitted to Transport queue.
- 4 SMTP stack hosted by `EdgeTransport.exe` on Hub server role, receives the email.
- 5 MSME Transport Agent (McAfeeTxRoutingAgent) scans the email for File filtering, Content scanning, then Anti-virus scanning.
- 6 If there is detection, it is dropped or replaced and appropriately returned to the SMTP stack.
- 7 MSME stamps the email with AV stamp, as per Microsoft specifications on Hub server role.
- 8 If the email is clean, it is returned to SMTP stack for further routing.
- 9 The Exchange Mailbox server receives the email.
- 10 Exchange store checks for AV stamp and if it matches, the email will not be sent to MSME scanning for VSAPI, else the email is scanned for Anti-Virus, File filtering and Content Scanning by VSAPI.

2

Installation and configuration

Select the option to install and use your MSME software, which best suits your requirements.

Installation type		Description
Standalone	Wizard-based	When using the wizard-based setup file, select one of these options per your requirements: <ul style="list-style-type: none">• Typical — Configured for all standard features except the McAfee Anti-Spam add-on. You can install the McAfee Anti-spam add-on separately at a later stage.• Complete — Configured for all standard features with the McAfee Anti-Spam add-on that provides protection against Spam or Phish attacks.• Custom — Configure using the advanced options to customize your setup.
	Silent	Install the software without any user interaction or prompts. Modify and run the <code>Silent.bat</code> file that allows you to record selections for the installation process.
ePolicy Orchestrator-managed		Deploy MSME in ePolicy Orchestrator environment to allow centralized policy management and enforcement on your Microsoft Exchange Servers.



You can also deploy MSME to a Microsoft Exchange Server cluster. This deployment requires certain post-installation configuration tasks.

See also

[Cluster deployment on page 29](#)

Contents

- ▶ [Pre-installation](#)
- ▶ [Installation](#)
- ▶ [Post-installation](#)

Pre-installation



Use this information to prepare for the MSME installation.

Contents

- ▶ [System requirements](#)
- ▶ [Supported Microsoft Exchange Server roles](#)
- ▶ [Package contents](#)

System requirements

Make sure that your server meets these requirements.

Component	Requirement
Operating system	<ul style="list-style-type: none"> • Microsoft Windows 2008 Standard/Enterprise Server SP2 (64-bit) • Microsoft Windows 2008 Standard/Enterprise Server R2 (64-bit) • Microsoft Windows 2012 Standard/Enterprise Server (64-bit) • Microsoft Windows 2012 Standard/Enterprise Server R2 (64-bit)
Microsoft Exchange Server	<ul style="list-style-type: none"> • Microsoft Exchange Server 2007 SP3 • Microsoft Exchange Server 2010 SP2 • Microsoft Exchange Server 2013 SP1
Browser	<ul style="list-style-type: none"> • Microsoft Internet Explorer version 8.0, 9.0, 10.0, and 11.0. • Mozilla Firefox 29.x and 30.x • Google Chrome 35 <p> Make sure that you disable the pop-up blocker in the browser settings.</p>
Processor	<ul style="list-style-type: none"> • Intel x64 architecture-based processor that supports Intel Extended Memory 64 technology (Intel EM64T) • AMD x64 architecture-based processor with AMD 64-bit technology
Memory	<p> The memory requirement to install MSME is the same as Microsoft Exchange Server requirement. For more information, see the <i>Microsoft Exchange</i> website.</p> <p>Microsoft Exchange Server 2007</p> <ul style="list-style-type: none"> • Minimum — 2 GB RAM • Recommended — 4 GB RAM <p>Microsoft Exchange Server 2010</p> <ul style="list-style-type: none"> • Minimum — 4 GB RAM • Recommended — 4 GB RAM for a single role and 8 GB for multiple roles <p>Microsoft Exchange Server 2013</p> <ul style="list-style-type: none"> • Minimum — 8 GB RAM • Recommended — 8 GB RAM
Disk space	Minimum: 740 MB
Network	10/100/1000-Mbps Ethernet card
Screen resolution	1024 x 768
McAfee management software	<ul style="list-style-type: none"> • McAfee ePolicy Orchestrator 4.6 • McAfee ePolicy Orchestrator 5.0 • McAfee ePolicy Orchestrator 5.1

Component	Requirement
McAfee Agent	<ul style="list-style-type: none"> McAfee Agent 4.6 or later.
Upgrade path	<ul style="list-style-type: none"> McAfee Security for Microsoft Exchange 7.6 Patch 1 Rollup 2 McAfee Security for Microsoft Exchange 8.0



To view updated system requirements, see [KB76903](#).

Supported Microsoft Exchange Server roles

The MSME installation depends upon the role selected for the Microsoft Exchange Server installation.

These roles are supported for the various versions of Microsoft Exchange Servers:

- Microsoft Exchange Server 2007 and 2010:
 - Edge Transport Server — Runs in the perimeter outside a domain and provides message hygiene and security. It is installed on a standalone server that is not a member of an Active Directory domain.
 - Hub Server — Handles all mail flow inside the organization, applies transport rules, and delivers messages to a recipient's mailbox in an Active Directory domain.
 - Mailbox Server — Holds the Exchange databases containing the user mailboxes.
 - An installation with a dual role of Mailbox with Hub.
- Microsoft Exchange Server 2013 and 2013 SP1
 - MBX Server — Holds the dual role of Mailbox with Hub.
 - Edge Transport Server. (only for Microsoft Exchange Server 2013 SP1)

Package contents

The software package contains the files necessary to install and set up the software as required.

Unzip the MSMEv85_x64.ZIP archive, to find these directories.

Folder	Content
Standalone	Contains the files required to perform a standalone installation of the product: <ul style="list-style-type: none"> Setup_x64.exe — Setup file to install the software using a wizard. Silent.bat — Record file to install the software without any prompts or wizard.
ePO	Contains installation and configuration files required for managing the product using ePolicy Orchestrator. <ul style="list-style-type: none"> ePO_Extension_XX: Contains the product extensions for all locales in their respective locale folders. For example, ePO_Extension_EN. MSME_Deployment_x64_xxxx.zip: Deployment package to deploy the software on the managed clients. MSME_AS_Deployment_xxxx.zip: Deployment package to deploy the McAfee Anti-spam component on to the managed clients. MSMEePOUpgrade.zip: Contains the executable file required to migrates policies from MSME 7.6.x, or 8.0 to MSME 8.5 in an upgrade. MSME85REPORTS.zip: Extension to add MSME reporting interface such as dashboards, queries.

Folder	Content
Manual	Contains the product guide in PDF format for all locales.
Readme	Contains the product release notes in HTML format for all locales.
AntiSpam	Contains <code>ASAddon_x64.exe</code> to install the McAfee Anti-Spam add-on component.



MSME installer includes McAfee Agent 4.8 Patch 2. The agent collects and sends information between the ePolicy Orchestrator server and repositories, and manages installations across the network.

Installation

MSME is installed in a compatible environment with features depending on your requirement.

MSME can be installed on a standalone server or integrated with ePolicy Orchestrator.



Make sure that you have the Windows administrator credentials to install the product. This account must be a Domain administrator and these credentials are required to launch the product installer.

See also

[Integrating MSME with ePolicy Orchestrator on page 5](#)

Contents

- ▶ [Install the software using setup wizard](#)
- ▶ [Install the McAfee Anti-spam add-on manually](#)
- ▶ [Perform a silent installation](#)
- ▶ [Upgrade a standalone deployment](#)


Install the software using setup wizard


Install the software on a system where Microsoft Exchange Server 2007, 2010, or 2013, is installed. In Microsoft Exchange Server 2007 and 2010, MSME executes Transport Scanning for the Edge transport and Hub transport roles, and VirusScan API for the Mailbox role (based on the roles configured).

Task

- 1 As an administrator, log on to the system where Microsoft Exchange Server is installed.
- 2 Create a temporary directory on your local drive.
- 3 Download the archived software package and extract it to the temporary directory you created.
- 4 From the setup folder, double-click `setup_x64.exe` (this is the setup application for a 64-bit operating system).
- 5 Select a language from the drop-down list, then click **OK**.
- 6 In the **Preparing to Install** screen, the installation wizard is prepared and all required installation files are extracted. When the process is complete, the **Welcome** screen appears. Click **Next**.
- 7 The **Exchange Server Role Detection** screen lists the roles selected during the Microsoft Exchange Server installation. Click **Next**.

- 8 Select an installation type, then click **Next**.
 - **Typical** — Commonly used features are installed with Web-based Product Configuration. The McAfee Anti-Spam add-on is not installed.
 - **Complete** — (Recommended) Web based product configuration and McAfee Anti-Spam add-on are installed. If the node is cluster aware, the required cluster setup components and services are also installed.
 - **Custom** — (Recommended only for advanced users) Select which application features you want to install and where to install. If you select this type of installation, a dialog box displays the features you can install. To change the destination folder for the installation files, click **Change**.
- 9 Accept the terms in the license agreement, then click **Next**.
- 10 In the **Additional Configuration Settings** screen, complete these options, then click **Next**.
 - a Select **Import existing configuration** to import the MSME configuration from an existing installation in the same or a different system. This configuration setting is saved as a .cfg file. To import this configuration, click **Import**, browse to the .cfg file, then click **Open**.

 You must have already exported a configuration file from the product interface.
 - b Under **Select Quarantine mechanism**, select a location to store all quarantined items, then complete the options for the location you selected.
 - c If you select **Local Database**, click **Browse** to change the default location (optional). If you select **McAfee Quarantine Manager**, type the IP address of the McAfee Quarantine Manager server, the port number, and the callback port number. Make sure that the McAfee Quarantine Manager server is up and is available for quarantining.
 - **RPC** — Remote Procedure Call (RPC) is a communication mechanism that requires uninterrupted connection to communicate with McAfee Quarantine Manager server. If the network connection is not available, processes such as quarantine and release are interrupted.
 - **HTTP** — A stateless communication mechanism to communicate with McAfee Quarantine Manager server. If there is a communication issue with McAfee Quarantine Manager server, the items are stored in the local database until the connection is restored. MSME tries to send the quarantined items to McAfee Quarantine Manager three times. If all three attempts fail, a product log entry is created and the item is stored in the local database.
 - **HTTPs** — A secured HTTP communication mechanism where the data is transferred in encrypted format.

 McAfee recommends that you use HTTP/HTTPs communication channel because stateless connections make sure that the software can communicate with McAfee Quarantine Manager seamlessly.
 - d Under **Administrator Email address**, type the email address to which all notifications, configuration reports, and status reports must be sent.
- 11 Select a protection profile, then click **Next**.
 - **Default** — This profile provides maximum performance with optimum protection.
 - **Enhanced** — This profile enables default file filter rules and provides maximum protection. It also provides real-time protection using McAfee Global Threat Intelligence file and messaging reputation.
 - **Use existing** — (Upgrade only) This option uses the existing protection profile.

- 12 Select **Create Desktop shortcuts** if you want the installation wizard to create shortcuts for the application on the desktop, then click **Next**.
- 13 In the **Ready to Install the Program** screen, verify the selected configuration, then click **Install**. The **Installing McAfee Security for Microsoft Exchange** screen appears that displays the features being copied, initialized, and installed.



MSME creates a user named **MSMEODuser** in the active directory. This user is required to perform on-demand scans.

- 14 When the installation is complete, the **Installation Wizard Completed** screen appears. Select the options as required, then click **Finish**.



You might be prompted to provide the domain administrator credentials.

- **Launch Product User Interface** — To launch the MSME standalone user interface after you exit the installation wizard.
- **Show the readme file** — To view the Release Notes of the product (**Readme.html**) for information on any last-minute additions or changes to the product, known issues, or resolved issues.
- **Update Now** — (Recommended) To update MSME with the latest DAT files, engine, and anti-spam updates.
- **Register at McAfee Business Community to stay up to date** — To receive information regarding the product, new releases, updates, and other relevant information.
- **Show Windows Installer logs** — To view the log file of the installation process.



We recommend that you restart your computer after the installation process is complete.

The MSME software is successfully installed on your system.

Install the McAfee Anti-spam add-on manually

If you've not installed McAfee Anti-spam as part of the complete or custom installation of MSME, install the add-on manually.

The MSME package includes an evaluation version of the McAfee Anti-Spam add-on. To upgrade it to licensed, contact McAfee Support.

Task

- 1 As an administrator, log on to the system where Microsoft Exchange Server is installed.
- 2 Browse to the `\AntiSpam` folder in the software package, double-click **ASAddOn_x64_Eval.exe**.
- 3 Select a language from the drop-down list, then click **OK**.
- 4 In the **Welcome** screen, click **Next** to display the **End User License Agreement** screen.
- 5 Accept the terms in the license agreement, then click **Next**.
- 6 In the **Ready to Install the Program** screen, verify the selected configuration, then click **Install**. The **Installing McAfee Anti-Spam add-on for Microsoft Exchange** screen appears that displays the features being copied, initialized, and installed.
- 7 When the installation is complete, the installation wizard **Completed** screen appears. Select **Show Windows Installer logs** to view the log file of the installation process, if necessary, then click **Finish**.

The McAfee Anti-spam add-on is successfully installed on your system.

Perform a silent installation

You can automate the installation using the `Silent.bat` file that allows you to record the selections for the installation process.



To install the product with default settings, double-click the `Silent.bat` available in the download package.



`Silent.bat` internally is called from the MSME setup file. Make sure that the `setup_x64.exe` is available in the same directory because the installation can't succeed with `Silent.bat` alone.

To customize the installation, modify these parameters in the batch file before running it:

Parameter	Value	Description
ADMIN_EMAIL_ID	<admin>@<msme>.com	Specify the administrator's email address for notifications. For example, SET ADMIN_EMAIL_ID=administrator@msme.com MSME sends notifications to this email address, when you enable Send notification option for policies.
AUTO_UPDATE	1 or 0	<p>Enable or disable automatic updates:</p> <ul style="list-style-type: none"> • 1 = enabled • 0 = disabled <p>When enabled, the DAT and engine update happens immediately after the software installation.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> McAfee recommends that you enable the automatic update to make sure that the engine and DAT files are up to date. </div>
INSTALL_DIR	%SystemDrive%\MSME	Specify the installation path. For example, if you specify <code>C:\MSME</code> , a folder MSME is created in the C drive.
NEED_DESKTOP_SHORTCUT	1 or 0	<p>Specify whether to create a desktop shortcut after successful installation:</p> <ul style="list-style-type: none"> • 1 = yes • 0 = no <p>The default value is 1.</p>
DB_PATH_CHANGED	1 or 0	<p>Specify whether to change the Postgres database path:</p> <ul style="list-style-type: none"> • 1 = yes • 0 = no <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> You can modify the database path anytime after the installation. When you change the path, a new database is created to store the detected items. However, the detected items stored in the earlier database are not available in the new database. </div>
DATABASEDIR	<New Postgres DB Location>	Specify the new Postgres database location. For example, <code>C:\TestDB</code> .

Parameter	Value	Description
QUARANTINE MECHANISM	1 or 2	<p>Specify the location for quarantined items:</p> <ul style="list-style-type: none"> • 1 = Local database • 2 = McAfee Quarantine Manager <p>Local database — To quarantine detected items in the local system.</p> <p>McAfee Quarantine Manager server — To quarantine detected items in MQM server, a centralized storage server.</p> <p>If you select McAfee Quarantine Manager, make sure that you also define the MQM IPADDRESS, MQS PORT NUMBER, and MQM COMMUNICATION MECHANISM settings.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  You can modify the settings from the software interface any time after the installation. </div>
MQM IPADDRESS	IPv4 or IPv6 address	Specify the IP address of the MQM server. MSME supports both IPv4 and IPv6 format.
MQM COMMUNICATION MECHANISM	0 or 1 or 2	<p>Specify the communication channel to communicate with MQM server:</p> <ul style="list-style-type: none"> • 0 = RPC • 1 = HTTP • 2 = HTTPs <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  McAfee recommends that you use HTTP/HTTPs communication channel because stateless connections make sure that the software can communicate with MQM server seamlessly. </div>
MQM PORT NUMBER	80 or 443 or 49500	<p>Specify port numbers for communication channels:</p> <ul style="list-style-type: none"> • 80 = HTTP protocol • 443 = HTTPs protocol • 49500 = RPC protocol
AGREE_TO_LICENSE	Yes or No	Agree to the license terms to install the software. For example, SET AGREE_TO_LICENSE = Yes.



The silent installation includes all standard features except the McAfee Anti-Spam add-on. You must install the McAfee Anti-Spam add-on separately. For details, see *Install the McAfee Anti-spam add-on manually*.

Upgrade a standalone deployment

MSME version 8.5 supports upgrading your configuration settings from the previous version 7.6.x, or 8.0.

Before you begin

Place your Microsoft Exchange server in maintenance mode because the Exchange Database and Exchange Transport services restart during the installation process.


If you had installed the previously supported version of McAfee Anti-spam module separately earlier, make sure that you uninstall the McAfee Anti-spam module before upgrading the software. You can install the latest version of the McAfee Anti-spam after the upgrade.

MSME provides enhanced security by not supporting the HTML tags that have XSS vulnerability. McAfee recommends that you remove the HTML tags that have XSS vulnerability from the existing notification template before the upgrade. Otherwise, after the upgrade, if you try to modify the notification templates that contain unsupported tags, you will be prompted to remove the unsupported tags from the template or use the template without modification. For the list of unsupported HTML tags, see McAfee KnowledgeBase article [KB82214](#).

When upgrading to a new version, you need not uninstall the existing version. The installation program updates your installation to the new version.

Task

- 1 As an administrator, log on to the system where Microsoft Exchange Server is installed.
- 2 From the setup folder, double-click **setup_x64.exe** (this is the setup application for a 64-bit operating system).
- 3 In the **Preparing to Install** screen, the installation wizard is prepared and all required installation files are extracted. When the process is complete, the **Welcome** screen appears. Click **Next**.
- 4 The **Exchange Server Role Detection** screen lists the roles selected during the Microsoft Exchange Server installation. Click **Next**.
- 5 In the **Setup Type** screen, the **Custom** option is selected by default. Click **Next**.
- 6 The **Custom Setup** screen lists the features installed in the existing installation. Select the features you want to be updated with McAfee Security for Microsoft Exchange, then click **Next**.
- 7 Accept the terms in the license agreement, then click **Next**.
- 8 The **Additional Configuration Settings** screen displays the settings for quarantine mechanism and quarantine database applied in the existing installation. Change the settings, if necessary, then click **Next**. To migrate policies from an earlier version, select the option **Import existing configuration**, then browse and select the configuration file.
- 9 In the **Setup Protection Profile** screen, select **Default**, **Enhanced**, or **Use Existing**, as necessary, then click **Next**.



If you selected the **Import existing configuration**, all options on this screen are grayed-out. The **Use Existing** option is selected by default.
- 10 Select **Create Desktop shortcuts** if you want the installation wizard to create shortcuts for the application on the desktop, then click **Next**.

- 11 In the **Ready to Install the Program** screen, verify the selected configuration, then click **Install**. The **Installing McAfee Security for Microsoft Exchange** screen appears that displays the features being copied, initialized, and installed.



While upgrading, the software checks the existing DAT version in the system and upgrades only if the DAT version packaged with the software is greater than the DAT version available in the system.

- 12 When the installation is complete, the **Installation Wizard Completed** screen appears with the **Migrate Quarantine Data** option selected by default. Click **Finish**.



If you had configured proxy settings in the previous version, you must configure the proxy settings again after the upgrade. We recommend that you restart your computer after the installation.

The McAfee Security for Microsoft Exchange software is successfully upgraded.

Post-installation

Once you've installed MSME, perform certain additional configuration to set it up for your environment.

Quick setup

Steps to quickly set up MSME and protect your Exchange server environment.

As an administrator, perform these tasks once you install MSME on your Exchange server.

Task

- 1 Update the software by performing a Engine/DAT update. For details, see the *Schedule a software update* section.
- 2 If you have installed MSME on an Edge Transport or Hub Transport server, make sure that MSME agents are loaded in the Exchange Power Shell (Exchange Management Shell), using this command:

```
Get-TransportAgent
```

The status for "Enabled" must be true to agents starting with "McAfee".
- 3 Make sure that you install the McAfee anti-spam add-on component to quarantine spam or phish email messages.
- 4 Update the administrator email address from **Settings & Diagnostics | Notifications | Settings** tab.
- 5 Schedule a status report task. For details, see the *Schedule a new status report* section.
- 6 Schedule a configuration report task. For details, see the *Schedule a new configuration report* section.
- 7 Schedule on-demand scans based on your requirement. For details, see the *On-Demand scan and its views* section.
- 8 Configure the on-access scan settings as per your requirement from **Settings & Diagnostics | On-Access Settings** page. For details, see the *On-Access settings* section.
- 9 Configure **DLP and Compliance** scanner settings and rules based on your company policy. For details, see the *Policy Manager* section for instructions on configuring policies, scanners, and filters.
- 10 For exceptions in a policy, create subpolicies based on your organization's requirement.
- 11 Send test email messages to verify the configuration.

Cluster deployment

You need additional configurations to install MSME in cluster deployments of Microsoft Exchange Server 2007, 2010 and 2013.

Cluster replication methods for Microsoft Exchange Server 2007

Cluster replication can be carried out using two methods: Cluster Continuous Replication (CCR) or Single Copy Cluster (SCC).

Cluster Continuous Replication (CCR)

Install MSME on all nodes of the cluster as standalone instances.



MSME is not a cluster aware application on Microsoft Exchange Server 2007 CCR cluster. However, both the nodes can be managed independently and work as standalone instances.

Single Copy Cluster (SCC)

Install MSME on all nodes of the cluster. In a Microsoft Exchange Server 2007 SCC cluster, MSME can be added only as a Cluster Resource.

Make sure that you:

- Install MSME on the **Active** node first, then on the **Passive** node.
- Create MSME Cluster in the same cluster group, where you have Microsoft Exchange resources configured.

Add the software to a cluster group on Windows 2008

Add MSME as a resource to a cluster group in a Windows 2008 (64-bit) environment.

Task

- 1 Click **Start | Run**, type `cmd`, then click **OK**.



Make sure that you have logged in as the administrator.

- 2 Type these commands to navigate to the cluster folder and run the cluster command. Press enter after each command.

```
cd <windows folder>\cluster
cluster /UNREGADMINEXT:McPPClusResEx.dll
```

- 3 Close the command prompt.



Make sure that the MSME cluster resource is created in the same cluster group where you have Microsoft Exchange resources configured.

- 4 Click **Start | Administrative Tools | Failover Cluster Management**.
- 5 In the **Failover Cluster Management** console, select the cluster group in which you would like to create the cluster resource. In the right pane (**Actions** window), click **Add resource**.
- 6 Select **More resources** from the drop-down, then select **Add McAfee Cluster Framework**.
- 7 In the main console, right-click in the **New McAfee Cluster Framework** window, then select **Properties**.
- 8 In the **New McAfee Cluster Framework Properties** window, click the **Properties** tab.

- 9 Under **Grid**, click the **Value** field and enter the drive that was selected to store the MSME configuration and the database, for example `F:\`, then click **OK**.
- 10 In **Cluster Administrator**, right-click on the newly created resource and select **Bring Online**.

This step starts the MSME service on the active node and the quarantine database is created in the designated drive. Multiple instances of the `Postgress.exe*32` process appears under the **Processes** tab of the Task Manager with `RPCServ.exe*32`, and `SAFeService.exe*32`.

Cluster replication utility for Microsoft Exchange 2010 and 2013

The **Cluster Replication Setup Utility** helps in the replication of the quarantine database, Policy configurations, engine, and DATs.

This utility is available only for an MSME installation that is recognized by a *Data Availability Group* (DAG), in which case the MSME Replication Service is also available. Depending on the configuration settings, this utility replicates quarantined items from one server to the other, and makes them highly accessible.

The primary component in a Data Availability Group is called Active Manager. Microsoft Exchange Server 2010 relies on the Active Manager to manage switchovers and failovers between mailbox servers that are a part of a Data Availability Group. Active Manager runs on all Mailbox servers in a given Data Availability Group and can be installed in two roles:

- Primary Active Manager (PAM)
- Standby Active Manager (SAM)

For details regarding these roles, refer to the relevant Exchange 2010 documentation.

Configure the replication settings

Configure the replication settings for Quarantine database, Policy configurations, Engine, and DATs.

Task

- 1 From the **Start** menu, click **All Programs | McAfee | Security for Microsoft Exchange | Cluster Replication Setup**. A dialog box appears with various options to define for this service.



If the Mailbox role is installed in Microsoft Exchange Server 2010 and 2013, the service **Cluster Replication Setup** is automatically installed in all three types of setup: Typical, Complete, and Custom.

- 2 From **Server name**, retrieve the available servers for replication which are part of Data Availability Group and have MSME installed with Exchange Server in the mailbox role.
 - **Available server(s)** displays a list of servers that can be added for replicating the quarantine database, Policy configurations, Engine, and DATs.
 - **Replication server(s)** displays a list of servers that have been configured as replication servers for the quarantine database, Policy configurations, Engine, and DATs.
- 3 Select the server from **Available server(s)** and click **>>** to add it to the Replication servers list.
- 4 Select **Stop Replication service** to stop the MSME Cluster Replication service.
- 5 Select **Start Replication service for** to manage the MSME Cluster Replication service. Select appropriate options:
 - **Policy Configuration**
 - **Engine/DATs**
 - **Quarantine Database**

- 6 Click **Apply** to save and apply the cluster replication settings.
- 7 When prompted, select the option to restart the MSME service, which is required for the replication to work.

Test your installation

When you have completed the installation of MSME, we recommend that you test it.

It makes sure that the software is installed properly and can detect viruses and spam within email messages.

Tasks

- *Test the anti-virus component on page 32*
Attach an EICAR anti-virus test file to an email message, then send the message through the Microsoft Exchange server where you've installed MSME.
- *Test the anti-spam component on page 32*
Run GTUBE (General Test mail for Unsolicited Bulk Email) to test the McAfee anti-spam software.
- *Test the installation using McAfee Virtual Technician on page 32*
McAfee Virtual Technician automatically checks for common deviations that might have occurred since you installed the product.

Installed components and services

MSME installs various components on your Microsoft Exchange server.

To access an MSME component, click **Start | Programs | McAfee | Security for Microsoft Exchange**, then click the component:

- **McAfee Anti-Spam for McAfee Security for Microsoft Exchange** — Detects spam and phishing content.
- **Access Control** — Allows or denies access to the MSME user interface for specific users or groups.
- **Product Configuration** — Launches MSME standalone version or through a web interface.
- **Sitelist Editor** — Specifies the location where automatic updates (including DATs and scanning engines) are downloaded from.
- **Cluster Replication Setup** — Replicates the quarantine database, policy configurations, and product updates (Microsoft Exchange Server 2010 or 2013 only). This is dependent upon the replication setting across a **Data Availability Group (DAG)**, recognized by an MSME installation.

Services available

- **McAfee Framework Service** — Prerequisite for installing and using ePolicy Orchestrator. For more details on this service, refer the ePolicy Orchestrator product documentation.
- **McAfee Security for Microsoft Exchange** — Protects your Microsoft Exchange Server (versions 2007, 2010, 2013) from viruses, unwanted content, potentially unwanted programs, and banned file types/messages.
- **McAfee Anti-Spam rules updater** — Required to update the anti-spam rules.

Test the anti-virus component

Attach an EICAR anti-virus test file to an email message, then send the message through the Microsoft Exchange server where you've installed MSME.

Several anti-virus vendors throughout the world jointly created the EICAR standard anti-virus test file. It is a standard to verify anti-virus installations.



This file is not a virus. Make sure that you delete the file when you have finished testing your installation to avoid alarming users.

Task

- 1 Open a text editor, copy this code to notepad, then save the file with the name `EICAR.COM`:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

The file size is 68 bytes or 70 bytes.

- 2 Send an email message through the Microsoft Exchange server with the EICAR test file as an attachment.



When MSME examines the email message, it reports finding the EICAR test file. However, it cannot clean or repair the EICAR file because it is a test file.

- 3 MSME replaces the EICAR test file with an alert message.

Test the anti-spam component

Run GTUBE (General Test mail for Unsolicited Bulk Email) to test the McAfee anti-spam software.

The test email message must be sent from an external email account (a different domain).

Task

- 1 Create an email message.
- 2 Copy this code in the body text:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Make sure that you copy this text with no extra spaces or line breaks.

- 3 From an external email address, send this email message to a mailbox address on the server where you have installed MSME with McAfee Anti-Spam add-on component. McAfee Anti-Spam scans the message, recognizes it as a junk email message, and takes necessary actions.



The GTUBE test overrides blacklists and whitelists. For more information on the GTUBE test file, visit <http://spamassassin.apache.org/>.

Test the installation using McAfee Virtual Technician

McAfee Virtual Technician automatically checks for common deviations that might have occurred since you installed the product.

Run McAfee Virtual Technician to test whether MSME is installed correctly.

To download McAfee Virtual Technician, visit: <http://mvt.mcafee.com/mvt/index.asp>.

3

Dashboard

Dashboard organizes and presents information in a way that is easy to read and interpret.

The MSME dashboard provides critical information on how well your server is being protected from spam, phishing, viruses, potentially unwanted programs, malicious URLs, and unwanted content. It also provides information about the detection statistics; additional components installed in the product; version information of components such as engine and DAT files; product license information and recently scanned items.

Contents

- ▶ *Statistical information of detected items*
- ▶ *Product versions and updates*
- ▶ *View recently scanned items*
- ▶ *On-Demand scan and its views*
- ▶ *Status reports*
- ▶ *Configuration reports*
- ▶ *Graphical reports*

Statistical information of detected items

Provides detailed information on the total emails scanned by MSME, how many emails triggered the detection and are quarantined based on the detection category. The dashboard also provides this statistical information in the form of a graph, for easy interpretation, and monitor the detection rates.

The **Statistics** tab is categorized into these sections:

- **Detections**
- **Scanning**
- **Graph**



Clicking **Reset** will clear the statistical information of all counters in the **Detections** section and reset the value to zero. Resetting the statistics will not delete any quarantined items from the **Detected Items**. These counters are dependent on the database path, so if you change the database path under **Settings & Diagnostics | Detected Items | Local Database**, the counters will reset to zero.

To modify the dashboard settings such as the refresh rate; maximum items to appear in the **Recently Scanned Items**; graph scale units; graph and chart settings such as the 3D pie-chart, exploded pie-chart, transparency, go to **Settings & Diagnostics | User Interface Preferences**.

Detections

Displays all statistical information on how many emails scanned by MSME are clean and how many items triggered a detection. Based on the detection category, the respective counter is incremented.

The reported numbers indicate the number of emails and documents that trigger any of the detection methods. For example, if an email contains two virus attachments, the statistics for **Viruses** would be incremented by one and not two. Reporting statistics are based on email messages rather than individual files or detections and is more intuitive in a mail server environment.



If your MSME server is managed by ePolicy Orchestrator and if you restart the service or click the **Reset** button, these statistics vary in McAfee ePO reports due to the historical data stored in McAfee ePO. For more information on McAfee ePO reports, see *Integrating MSME with ePolicy Orchestrator*.

Table 3-1 Icons used – Detections section

Icon	Description
	Provides additional information on the detection category when you place the cursor on the icon.
	Indicates that the statistics of the respective detection category is available in the graph.
	Indicates that the statistics of the respective detection category is unavailable in the graph.



The graphical icons and appear only when the **<Select Detections>** option is selected from the **Graph** drop-down list.

The following table provides you more information on each detection category.

Table 3-2 Detection definitions

Category	Additional information	Description
Clean	<p>If the email flow has more clean emails than the detections, enabling this icon for clean emails might suppress the graph of other categories. In such scenarios, disable the icon next to Clean category.</p>	Legitimate email messages that do not pose a threat to the user and does not trigger any of the MSME scanners.
Spam	This counter is available only if you have installed the McAfee Anti-Spam add-on.	An unsolicited email message often sent in bulk to numerous recipients who have not requested or registered for it.
	Scanned for spam	All emails scanned by MSME for spam.
	Detected as spam	Emails that are identified as spam, but not quarantined due to policy settings.
	Blocked as spam	Emails that are identified as spam and quarantined due to policy settings.

Table 3-2 Detection definitions *(continued)*

Category	Additional information	Description
Phish	This counter is available only if you have installed the McAfee Anti-Spam add-on.	Phish or Phishing is a method used by individuals to obtain personal information by unfair or fraudulent means. This personal information can include your credit card details, passwords, and bank account login details. These emails mimic trusted sources like banks and legitimate companies. Usually these emails would request you to click on a link to verify or update certain personal details. Like spam, phishing emails are also sent out in bulk.
	Phish detected	Emails that are identified as phish, but not quarantined due to policy settings.
	Phish blocked	Emails that are identified as phish and quarantined due to policy settings.
IP Reputation	This counter is available only if you have installed the McAfee Anti-Spam add-on.	A method of detecting threat from email messages based on the sending server's IP address. IP reputation score reflects the likelihood that a network connection poses a threat. IP reputation leverages on McAfee Global Threat Intelligence (GTI) to prevent damage and data theft by blocking the email messages at the gateway based on the source IP address of the last email server. MSME processes the message before it enters the organization by rejecting or dropping the connection based on the IP reputation score.
	IP Encountered	All emails that reach the MSME server.
	IP Dropped	Emails that were quarantined by MSME due to IP reputation feature. In this case, the sender is not notified about the email delivery status.
	IP Rejected	Emails that were quarantined by MSME due to IP reputation feature. In this case, the sender will be notified about the email delivery status.
Viruses		A computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files, so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies, or creates files. Some viruses display symptoms, others damage files and computer systems, but neither is essential in the definition of a virus; a non-damaging virus is still a virus.
	Viruses detected	Virus which is detected in an incoming email and an appropriate action is taken based on the policy settings.
	Viruses cleaned	Virus which is removed from an incoming email and an appropriate action is taken based on the policy settings.
Potentially Unwanted Programs		Potentially Unwanted Programs (PUP) are software programs written by legitimate companies that could alter the security or privacy policies of a computer on which they have been inadvertently installed. These programs could be downloaded along with a legitimate application that you might require.
	PUP detected	PUP which is detected in an incoming email and an appropriate action is taken based on the policy settings.
	PUP blocked	PUP which is removed from an incoming email and an appropriate action is taken based on the policy settings.

Table 3-2 Detection definitions *(continued)*


Category	Additional information	Description
Banned File types and Messages		Certain types of file attachments are prone to viruses. The ability to block attachments by file extension is another layer of security for your mail system. Both internal and external email messages are checked for banned file types or messages.
	Banned file types	Certain types of file attachments are prone to viruses. The ability to block attachments by file extension is another layer of security for your mail system.
	Banned messages	Certain email messages that you wish to ban from going through your mail system. Both internal and external mail are checked for banned content.
DLP and Compliance	 To view available dictionaries, click the Category drop-down list from Policy Manager Shared Resource DLP and Compliance Dictionaries .	<p>Stop the loss of sensitive information via email. MSME provides industry-leading email content analysis to provide the tightest control of sensitive content in any form to aid compliance with many state, national, and international regulations.</p> <p>Prevent data leakage with the most extensive email Data Loss Prevention (DLP) in the industry that does pattern matching to detect data; policy-based message handling that prevents outbound data loss.</p>
Unwanted Content		Unwanted Content is any content that the user would not like to receive through emails. The rules can be defined by certain words or phrases which would trigger a corresponding policy and block the email.
	Packers	A packed executable that decompresses and/or decrypts itself in memory while it is running, so that the file on disk is never similar to the memory image of the file. Packers are specially designed to bypass security software and prevent reverse engineering.
	Encrypted/Corrupted content	Email messages that cannot be categorized as having encrypted or corrupted content.
	Encrypted content	Some email messages can be encrypted, which means that the content of those email messages cannot be scanned. Encrypted content policies specify how encrypted email messages are handled when detected.

Table 3-2 Detection definitions *(continued)*

Category	Additional information	Description
	Signed content	<p>Whenever information is sent electronically, it can be accidentally or willfully altered. To overcome this, some email software uses a digital signature - the electronic form of a handwritten signature.</p> <p>A digital signature is extra information added to a sender's message, that identifies and authenticates the sender and the information in the message. It is encrypted and acts like a unique summary of the data. Typically, a long string of letters and numbers appear at the end of a received email message. The email software then re-examines the information in the sender's message, and creates a digital signature. If that signature is identical to the original, the data has not been altered.</p> <p>If the email message contains a virus, bad content, or is too large, the software might clean or remove some part of the message. The email message is still valid, and can be read, but the original digital signature is 'broken'. The recipient cannot rely on the contents of the email message because the contents might also have been altered in other ways.</p>
	Corrupted content	<p>The content of some email messages can become corrupt, which means that the content of the email message cannot be scanned.</p> <p>Corrupt content policies specify how email messages with corrupt content are handled when detected.</p>
	Denial of service	<p>A means of attack against a computer, server, or network. The attack is either an intentional or an accidental by-product of instruction code that is either launched from a separate network or Internet-connected system, or directly from the host. The attack is designed to disable or shut down the target, and disrupts the system's 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.</p>
	Protected content	<p>The content of some email messages is protected, which means that the content of the email message cannot be scanned.</p> <p>Protected content policies specify how email messages with protected content are handled when detected.</p>

Table 3-2 Detection definitions (continued)

Category	Additional information	Description
	Password protected files	It is possible to password protect a file that is sent by email. Password-protected files cannot be scanned. Password-protected file policies specify how email messages that contain a password-protected file are handled.
	Incomplete MIME messages	Multipurpose Internet Mail Extensions (MIME) is a communications standard that enables the transfer of non-ASCII formats over protocols, like SMTP, that only support 7-bit ASCII characters. MIME defines different ways of encoding the non-ASCII formats so that they can be represented using characters in the 7-bit ASCII character set. If the content in the body of a MIME message is too large to pass through the mail transfer system, the body can be passed as a number of smaller MIME messages. These MIME messages are known as partial or incomplete MIME messages, because each MIME message contains only a fragment of the total message that must be transmitted.

Scanning

Displays information on the total items scanned by MSME and the average time taken to scan all items, since the last reset.

Table 3-3 Option definitions

Option	Definition
Average Scan Time (milliseconds)	Specifies the average time taken by MSME to scan all the email messages that reach the Exchange server. To understand how this is calculated, let's consider this example where: <ul style="list-style-type: none"> • T = Total time taken to scan all emails after the last MSME Service restart. • N = Total number of emails scanned after the last MSME Service restart. then, Average scan time = T/N (in milliseconds)
Total Scanned	Total number of email messages scanned, since the last time the statistic counters were reset.

Graph

Displays the statistics of the email messages scanned by MSME in a graphical format.

Table 3-4 Icons used – Graph section



Icon	Description
	View statistical information of the selected counters as a bar graph. This is useful when you want the statistics of total number of emails scanned and the items that triggered a detection during the selected duration.
	View statistical information of the selected counters as a pie chart. This is useful when you want the percentage of emails scanned and the items that triggered a detection during the selected duration.

Table 3-5 Option definitions

Option	Definition
Graph	<ul style="list-style-type: none"> • Spam Summary — Provides additional information on how many spam email messages were detected and blocked by MSME for the selected time range. • Phish Summary — Provides additional information on how many phishing email messages were detected and blocked by MSME for the selected time range.
Magnify Graph	Specify the magnification percentage of the Detections graph. This helps you view an enlarged graph, which is useful when the default graph in the dashboard is cluttered with more information and becomes unreadable in the current browser window.
Time range	Specify for which time period you would like to review the statistics. The available options are: <ul style="list-style-type: none"> • Last 24 Hours • Last 7 Days • Last 30 Days

Product versions and updates

Provides important information on whether the software is up-to-date with all the latest DATs and drivers. It also provides information about the product license type and if any additional components are installed.

Versions and Updates

The **Versions & Updates** section in the **Dashboard** has these tabs:

- Update Information
- Product Information
- Licenses

Update information

Provides information about anti-virus DAT, anti-virus engine, extra drivers, anti-spam engine version, their status and when they were last updated. MSME uses the McAfee update website to automatically update its anti-virus DAT, engine and rules on a daily-basis.




If MSME is managed by an ePolicy Orchestrator server, create an AutoUpdate task using ePolicy Orchestrator.

Table 3-6 Option definitions – Update Information

Option	Definition
Last Successful Update	Displays the time when the software was updated successfully.
Update Now	Click to immediately update the product with latest engine and drivers. This is helpful in a situation when there is a virus out-break and you cannot wait until the scheduled software update occurs.
Update Frequency	Displays the schedule frequency of how often the software is updated.
Edit Schedule	Click to schedule or edit the product's software update. For more information on how to update the software, see <i>Schedule a software update</i> section.
Show Status	Click to view the status of the update task such as the start time, running time, current status and how much the task has progressed.

Table 3-6 Option definitions – Update Information *(continued)*

Option	Definition
Anti-Virus Engine DAT Version Extra Drivers	Displays the latest anti-virus engine, DAT version and extra drivers information and when it was updated.
Viruses that Extra Drivers Detect	Displays items that were detected by ExtraDAT to remove particular viruses. EXTRA.DAT files contain information that is used by MSME to detect a new virus. When a major virus is discovered and extra detection is required, an EXTRA.DAT file is made available until the normal DAT update is released.
Anti-Spam Engine Rules Version	Displays the anti-spam engine and rules version number and when it was updated.
	 This appears only if the McAfee Anti-Spam add-on component is installed.

Schedule a software update

Keep your software up-to-date with the latest anti-virus DAT, anti-virus engine, extra drivers, and anti-spam engine by scheduling an automatic update.



By default the product update occurs based on the repository settings specified in **SiteList Editor**. To change the repository settings, use **SiteList Editor** from **Start | All Programs | McAfee | Security for Microsoft Exchange** option. However, if your computer is managed by an ePolicy Orchestrator server, the product update will occur based on the settings provided in ePolicy Orchestrator.

For option definitions, click ? in the interface.

For option definitions, click ? in the interface.

Task

- 1 Click **Dashboard | Statistics & Information**.
- 2 From the **Versions & Updates** section, click **Update Information** tab.
- 3 From **Update Frequency**, click **Edit Schedule**.

The **Edit Schedule** page appears.

- 4 From **Choose a time**, select an option depending on the required software update frequency.



As a best practice, schedule a daily update, by selecting **Days** and specifying **1** under **Every day(s)** text box. Perform software updates during non-business hours or when the network traffic is low.

- 5 Click **Save**, then **Apply**.

You have now successfully scheduled a software update.

Product information

Provides information on the product name, version, service packs, hotfixes, and any additional component installed.

Table 3-7 Option definitions

Option	Definition
Product Name	Specifies McAfee Security for Microsoft Exchange as the product name.
Product Version	Specifies the product version in the format: 8.5.<build number>.<package number>

Table 3-7 Option definitions (continued)

Option	Definition
Service Pack	Lists the Service Pack or Patch details (if any)
Hotfixes	Lists the hotfixes installed


Licenses

Provides information on the type of license, expiration date, and days to expire of the installed product and components.



License information of McAfee Anti-Spam add-on component appears if you have it installed or activated.

Table 3-8 Option definitions

Option	Definition
Description	Specifies the installed product name.  McAfee Anti-Spam for McAfee Security for Microsoft Exchange appears, if you have the McAfee Anti-Spam add-on component installed.
Type	Specifies if the installed product is a Licensed or Evaluation version.
Expires	Appears when you have an Evaluation version of the software installed. Specifies the date and time on when the license expires.
Days to Expiry	Appears when you have an Evaluation version of the software installed. Specifies the number of days remaining for product expiry.

View recently scanned items

Provides a quick view of the recently scanned items from the dashboard.

The **Recently Scanned Items** section provides you run-time information on all items scanned by MSME. By default, only 10 items appear in the **Recently Scanned Items** section. However, you can view up to 100 items by modifying the **Maximum recently scanned items** option under **Settings & Diagnostics | User Interface Preferences | Dashboard Settings | Report Settings**.



The items in the **Recently Scanned Items** section will be cleared, if you restart **McAfee Security for Microsoft Exchange** service from the **Services** console.

Table 3-9 Option definitions

Option	Definition
Date/Time	Date and time when the most recent scan was executed.
IP Reputation Score	Score which reflects the likelihood that a network connection poses a threat.
Sender	Email addresses of the senders of the items that were scanned.
Recipients	Email addresses of recipients of scanned items.
Subject	Subject line of scanned emails.
Action Taken	What action was taken on scanned items.
Filename	The name of a quarantined file.
Detection Name	The name of a detection. For example, the name of a virus.
Task	The task associated with a particular detection.

Table 3-9 Option definitions (continued)

Option	Definition
Reasons	A rule or rules that were triggered by a particular email.
Scanned By	The policy setting used to scan items.
Policy Name	The name of the policy that triggered a detection.
Reputation Score	The authenticity level of the source of the email based on up to date information available pertaining to a particular source.
Reason	The reason why the email was quarantined (quarantine queue type).



For detailed information on these fields, see *Available primary search filters* section.




— Indicates that the item is clean.



— Indicates that the item triggered one of the scanners or filters.



Hover the cursor on  to see which scanner or filter was triggered. If the item triggered multiple scanners or filters, only the highest priority detection is shown.

On-Demand scan and its views

An on-demand scanner is a security scanner that you start manually at convenient times or regular intervals. It allows you to set various configurations and scan specific mails or mailboxes.

MSME enables you to create scheduled on-demand scans. You can create multiple schedules, each running automatically at predetermined intervals or times.

You can schedule regular scan operations when the server activities are comparatively low and when they do not interfere with your work.



This feature is available only on an Exchange server that has Mailbox role. You cannot schedule an on-demand scan on an Exchange server that has only Edge Transport or Hub Transport role.

When should you perform an on-demand scan

An on-demand scan is highly recommended if there is an outage in your organization due to malicious activity. This will make sure that the Microsoft Exchange databases are clean and are not infected during the outage.

McAfee recommends that you perform an on-demand scan task during non-business hours. When an on-demand scan task is scheduled during a non-business hour and it continues during peak work hours, you must reconsider the databases being scanned and create with alternate schedules by altering the data being scanned.

You can schedule an on-demand scan during the weekends to make sure that the Exchange Databases are clean and older emails are also scanned by the latest Anti-Virus signatures. Administrators must schedule an on-demand scan keeping in mind the number of Exchange servers, databases, and mail flow. Your goal must be to complete this task before business hours.

Why should you perform an on-demand scan

You might want to perform an on-demand scan for a number of reasons. For example:

- To check a specific file or files that has been uploaded or published.
- To check that the messages within your Microsoft Exchange server are virus-free, possibly following DAT update, so that new viruses can be detected.
- If you have detected and cleaned a virus and want to check that your computer is completely clean.

View on-demand scan tasks

View a list of on-demand scan tasks configured for MSME.

Task

- Click **Dashboard | On-Demand Scans**. The **On-Demand Scans** page appears listing the configured on-demand scan tasks.



By default, a scheduled on-demand scan task named **Default Scan** is created when MSME is installed.

From the **On-Demand Scans** page, you can use these options:

Table 3-10 Option definitions

Option	Definition
Name	Indicates the name of the on-demand scan task.
Status	Indicates the current status of the on-demand scan task on whether the task is Idle , Running , Stopped or Completed .
Last Run	Indicates the date and time, when the on-demand scan was last executed.
Next Run	Indicates the date and time, when the next on-demand scan is scheduled to run.
Action	Lists these options for all the available on-demand scan tasks: <ul style="list-style-type: none"> • Modify • Delete • Run Now • Show Status <p>The Stop option appears only if any on-demand scan task is running.</p>
Modify	Edit the settings of an on-demand scan task.
Delete	Deletes the selected on-demand scan task.
Run Now	Starts the selected on-demand scan task immediately.
Show Status	Displays the current status of an on-demand scan task. The Task Status page appears with these tabs: <ul style="list-style-type: none"> • General — Provides more information on the on-demand scan task such as the total running time of the task, progress of the task, DAT and Engine version used for scanning, scan results, total items scanned, rules broken and folders scanned. • Settings — Provides more information on the database scanned and the policy used. <p> The Show Status option is available only after an on-demand scan task is started.</p>
Stop	Stops an on-demand scan task that is running.

Table 3-10 Option definitions (continued)

Option	Definition
Refresh	Refresh the page with latest on-demand scan information.
New Scan	Schedule a new on-demand scan task.

You have now successfully viewed all available on-demand scan tasks configured for MSME.

Create on-demand scan task

Schedule an on-demand scan task to find or remove viruses and banned content in mailboxes, at convenient time intervals.

Before you begin

Make sure that you do not remove the **MSMEODuser** from active directory, that was created during the product installation. This user is required for performing on-demand scans on mailboxes.

Task

- 1 Click **Dashboard | On-Demand Scans**. The **On-Demand Scans** page appears.
- 2 Click **New Scan**. The **Choose when to scan** page appears.
- 3 From **Choose a time** tab, specify when you want the scan to run. The available options are:
 - **Not scheduled** — Select this if you have not decided on when to perform the on-demand scan or disable the schedule for an existing on-demand scan.
 - **Once** — Specify the date and time to schedule an on-demand scan once.
 - **Hours** — Select this to schedule the task based on hours, if you have to execute the on-demand scan task for more than once in a day. For example, let's consider that the current time is 14:00 hours and you have to create an on-demand scan task that satisfies these conditions:
 - The on-demand scan must start exactly at 14:30 hours
 - The on-demand scan must occur twice a day

To achieve this, specify **12** for hours and **30** for minutes.
 - **Days** — Select this to schedule the task based on how often the scan must occur in a week. For example, if you want the on-demand scan to occur once in three days, specify **3** under **day(s)** and select the time when the task starts.
 - **Weeks** — Select this to schedule the task based on how often the scan must occur in a month. For example, if you want the on-demand scan to occur bi-weekly, specify **2** under **week(s)**, select the days and time when the task starts.
 - **Months** — Select this to schedule the task based on how often the scan must occur in a year. For example, if you want the on-demand scan to occur on every second Saturday of each month, select **second** from **On the** drop-down list, **Saturday** from **of** drop-down list, then select all the months and time when the task starts.



Enable **Stop task after it has run for <n> hour(s) <n> minute(s)**, to stop an on-demand scan task if it exceeds the specified hours.

- 4 Click **Next**. The **Choose what to scan** page appears. The available options are:
 - **Scan all folders** — Select this to scan all the mailboxes in the Exchange server.
 - **Scan selected folders** — Select this to scan only specific mailboxes in the Exchange server.
 - **Scan all except selected folders** — Select this to scan all except specific mailboxes that are added to the **Folders to scan** list.



In Microsoft Exchange 2013, the public folder appears as part of the mailbox and on-demand scanning is always recursive for public folders. In Microsoft Exchange 2007 and 2010, you can select public folder at folder or subfolder level to run recursive on-demand scanning.

- 5 Click **Next**. The **Configure scan settings** page appears.
- 6 From the **Policy to use** drop-down list, select any of the policy option based on your scan requirement.

Policy	Description
Default	The default settings for all scanners and filters except these scanners: <ul style="list-style-type: none"> • DLP and Compliance Scanner • File Filtering
Find Viruses	Anti-virus settings and filters. These policies provide an easy means to check the viral content in databases.
Remove Viruses	Anti-virus settings and filters. These policies provide an easy means to remove the viral content in databases.
Find Non-Compliant Content	Content scan settings. These policies are useful if you want to see the effect of newly created/assigned content scan rules.
Remove Non-Compliant Content	Content scan settings. These policies are useful if you want to see the effect of newly created/assigned content scan rules and remove non-compliant content.
Full Scan	Settings for all scanners and filters. These policies are typically used for scanning at regular intervals.

The settings and actions to take are specified in on-demand policies found under **Policy Manager**.

- 7 Select the **Resumable Scanning** and **Restart from last item** options to run the on-demand scan task in multiple sessions on mailbox database.



Sometimes, you might want to run an on-demand scan task for all mailboxes. Scanning all mailboxes in one session might take longer time and that can affect the system's productivity. Instead of scanning all mailboxes in one session, you can schedule the scan for multiple sessions.

- 8 On Exchange Server 2010 or 2013, you now have the option to perform a granular on-demand scan task. You can narrow down the scan using these fields:
 - Subject
 - From
 - To
 - Message ID
 - Recipients
 - Date range
 - Mail size

- Attachments
- Unread items

Performing a granular on-demand scan saves you time and fetches specific scan results.

- 9 Click **Next**. The **Enter a name for the scan** page appears.
- 10 Specify a meaningful on-demand scan task name, based on the policy you selected in the previous page. For example, if you are creating an on-demand scan task to do a full scan over the weekend, specify the task name as `Weekend Full Scan`.
- 11 Click **Finish**, then **Apply**.

By performing these steps, you have successfully created an on-demand scan task.

Status reports

A status report is a scheduled report sent to an administrator at a specific time. The report contains detection statistics within that specified time frame.

Using **Status Reports**, you can automate the task of querying for statistics periodically. You can schedule a periodic task for collecting the simple statistics like the number of detections on a particular date and send an email to the Exchange administrator or a distribution list.

These reports can help you to find out which Exchange servers are receiving more threats, using which you can come up with mechanisms to reduce the threat landscape.

You can choose a time, recipient email address or distribution list to send the report to, and a subject for the email. Status reports are sent to the recipient in HTML or CSV format.

Based on your configuration, the status report email contains statistical information on the detected items such as viruses, spam, phishing, IP reputation, PUP, banned file types, unwanted content, DLP and compliance, clean emails and total number of emails scanned. For more information on how to schedule a status report, see *Schedule a new status report*.



After installing MSME, status reports require at least 24-hour interval to populate the statistics in the notification email.

View status report tasks

View a list of status report tasks configured for MSME.

Task


- Click **Dashboard | Status Reports**. The **Status Reports** page appears listing the configured status report tasks.

From the **Status Reports** page, you can use these options:

Table 3-11 Option definitions

Option	Definition
Name	Indicates the name of the report task.
Status	Indicates the status of the report task, whether the task is Idle , Running , Stopped , or Completed .
Last Run	Indicates the date and time, when the report task was last executed.
Next Run	Indicates the date and time, when the next report task is scheduled to run.

Table 3-11 Option definitions (continued)

Option	Definition
Action	Lists these options for all the available report tasks: <ul style="list-style-type: none"> • Modify • Delete • Run Now • Show Status The Stop option appears only if any report task is running.
Modify	Click Modify to edit the settings of an on-demand scan task.
Delete	Deletes the selected report task.
Run Now	Starts the selected report task immediately.
Show Status	Displays the status of a report task. The Task Status page has this tab: <ul style="list-style-type: none"> • General — Provides more information on the report task such as the start and end time, task runtime, current action, and task progress. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  The Show Status option is available only after a report task is started. </div>
Refresh	Refresh the page with latest report information.
New Report	Schedule a new status report task.

You have now successfully viewed all available status report tasks configured for MSME.

Schedule a new status report

Schedule a new status report task to send the detection statistics to a specific email address or distribution list, at convenient time intervals.

Task

- 1 Click **Dashboard | Status Reports**. The **Status Reports** page appears.
- 2 Click **New Report**. The **Report** page appears.
- 3 From **When to report** tab, specify when you want the status report task to run. The available options are:
 - **Not scheduled** — Select this if you have not decided on when to perform the status report task or disable the schedule for an existing status report task.
 - **Once** — Specify the date and time to schedule a status report task once.
 - **Hours** — Select this to schedule the task based on hours, if you have to execute the status report task for more than once in a day. For example, let's consider that the current time is 14:00 hours and you have to create a report task that satisfies these conditions:
 - The status report task must start exactly at 14:30 hours
 - The status report task must occur twice a day
To achieve this, specify 12 for hours and 30 for minutes.
 - **Days** — Select this to schedule the task based on how often the status report task must occur in a week. For example, if you want the status report task to occur once in three days, specify 3 under **day(s)** and select the time when the task should start.

- **Weeks** — Select this to schedule the task based on how often the status report task must occur in a month. For example, if you want the status report task to occur bi-weekly, specify **2** under **week(s)**, select the days and time when the task should start.
- **Months** — Select this to schedule the task based on how often the status report task must occur in a year. For example, if you want the status report task to occur on every second Saturday of each month, select **second** from **On the** drop-down list, **Saturday** from **of** drop-down list, then select all the months and time when the task should start.



Enable **Stop task after it has run for** <n> hour(s) <n> minute(s), to stop a status report task if it exceeds the specified hours.

- 4 Click **Next**. The **Report Settings** page appears. The available options are:

Table 3-12 Option definitions

Option	Definition
Recipient Email	Specify the recipient email address or SMTP address of the distribution list. In most cases, this should be the Exchange administrator's email address. By default, the email address from Settings & Diagnostics Notifications Settings General Administrator E-mail is used as the recipient email address.
Subject line for report	Specify a meaningful subject line for the email. For example, if you want a daily status report in HTML format, specify <code>MSME Daily Status Report (HTML)</code> .
Number of Rows	Specify the number of rows (n) to be displayed in the status report email. Each row in the status report displays the total number of detections for a particular day. The report contains the detection count for the last (n) days, excluding the day when the status report is triggered. For example: If you specify 1 , the status report will contain one row displaying detections for yesterday. You can specify a maximum value of 365.
Type of Report	Specify the format of the status report, which is sent to the recipient. The available options are: <ul style="list-style-type: none"> • CSV — Select this if you want the status report sent to the recipient in Comma Separated Value format as a <code>.csv</code> file attachment. • HTML — Select this if you want the status report sent to the recipient in HTML format as a <code>.html</code> file attachment or appear in the email message body.

- 5 Click **Next**. The **Please enter a task name** page appears.
- 6 Specify a meaningful status report task name, based on the schedule and format you selected in the previous pages. For example, if you are creating a weekly status report task that provides detection statistics for weekdays in HTML format, specify the task name as `Weekly Status Report (HTML)`.
- 7 Click **Finish**, then **Apply**.


By performing these steps, you have successfully created a new status report task.

Status report email notifications

Based on your scheduled status report, the recipient receives an email with the statistics on all emails scanned and detected by MSME for the specified duration.

Based on your status report configuration, the status report email contains statistical information of the detected items, total clean emails and total number of emails scanned on that day.

Table 3-13 Option definitions

Option	Definition
From	Displays the email address that you have specified under Settings & Diagnostics Notifications Settings General Sender E-mail .
To	Displays the intended recipient email address that you have specified under Settings & Diagnostics Notifications Settings General Administrator E-mail .
Subject	Displays the subject of the status report email notification that you have specified under Dashboard Status Reports Report Settings Subject line for report .
Scanning Statistics for Server	Displays the Computer name where MSME is installed.
Date	Displays the date in MM/DD/YYYY format.
Detections	Displays detection statistics of Viruses, Spam, Phish, IP Reputation, Potentially Unwanted Program, Banned File Types, Unwanted Content, and DLP and Compliance in the message body. <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;">  The Spam, Phish, and IP Reputation statistics are available only if you have installed the McAfee Anti-Spam add-on. </div>
Clean	Displays the total number of clean emails that were detected by MSME as clean and did not pose a threat. For example, even a status report email sent to the administrator will be counted as a clean email in the statistics.
Total Scanned	Displays the total number of emails scanned by MSME for the day.



Status report emails will be blocked if you set the **IP reputation threshold** value to **Trusted IP (below 0)** or **Neutral IP (equal to or above 0)** from **Settings & Diagnostics | Anti-Spam | McAfee GTI IP reputation**.

Configuration reports

A configuration report is a scheduled report sent to an administrator at a specific time. The report contains the MSME product information, policy settings, and system information.

Using **Configuration Reports**, you can automate the task of viewing the summary of product configurations periodically.

This feature is helpful when there are multiple administrators in your organization and you want to keep a track of the MSME configuration settings. It is also useful when there are multiple MSME installations managed by ePolicy Orchestrator and you want to track the product configuration.

You can choose a time, recipient email address, or distribution list to send the report to and a subject for the email.

Based on your configuration, the configuration report has product and system information such as: server information, product version information, product license status and type, hotfix information, debug logging information, on-access scanner settings, on-access policy settings, and gateway policy settings. For more information on how to schedule a configuration report, see *Schedule a new configuration report*.

View configuration report tasks


View a list of configuration report tasks configured for MSME.

Task

- Click **Dashboard | Configuration Reports**. The **Configuration Reports** page appears listing the configured configuration report tasks.

From the **Configuration Reports** page, you can use these options:

Table 3-14 Option definitions

Option	Definition
Name	Indicates the name of the report task.
Status	Indicates the status of the report task, whether the task is Idle , Running , Stopped , or Completed .
Last Run	Indicates the date and time, when the report task was last executed.
Next Run	Indicates the date and time, when the next report task is scheduled to run.
Action	Lists these options for all the available report tasks: <ul style="list-style-type: none"> • Modify • Delete • Run Now • Show Status <p>The Stop option appears only if any report task is running.</p>
Modify	Click Modify to edit the settings of an on-demand scan task.
Delete	Deletes the selected report task.
Run Now	Starts the selected report task immediately.
Show Status	Displays the status of a report task. The Task Status page has this tab: <ul style="list-style-type: none"> • General — Provides more information on the report task such as the start and end time, task runtime, current action, and task progress. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  The Show Status option is available only after a report task is started. </div>
Refresh	Refresh the page with latest report information.
New Report	Schedule a new configuration report task.

You have now successfully viewed all available configuration report tasks configured for MSME.

Schedule a new configuration report

Schedule a new configuration report task to send the product configuration and system information to a specific email address or distribution list, at convenient time intervals.

Task

- 1 Click **Dashboard | Configuration Reports**. The **Configuration Reports** page appears.
- 2 Click **New Report**. The **Report** page appears.
- 3 From **When to report** tab, specify when you want the configuration report task to run. The available options are:
 - **Not scheduled** — Select this if you have not decided on when to perform the configuration report task or disable the schedule for an existing configuration report task.
 - **Once** — Specify the date and time to schedule a configuration report task once.

- **Hours** — Select this to schedule the task based on hours, if you have to execute the configuration report task for more than once in a day. For example, let's consider that the current time is 14:00 hours and you have to create a report task that satisfies these conditions:
 - The configuration report task must start exactly at 14:30 hours
 - The configuration report task must occur twice a day

To achieve this, specify 12 for hours and 30 for minutes.


- **Days** — Select this to schedule the task based on how often the configuration report task must occur in a week. For example, if you want the configuration report task to occur once in three days, specify 3 under **day(s)** and select the time when the task should start.
- **Weeks** — Select this to schedule the task based on how often the configuration report task must occur in a month. For example, if you want the configuration report task to occur bi-weekly, specify 2 under **week(s)**, select the days and time when the task should start.
- **Months** — Select this to schedule the task based on how often the configuration report task must occur in a year. For example, if you want the configuration report task to occur on every second Saturday of each month, select **second** from **On the** drop-down list, **Saturday** from **of** drop-down list, then select all the months and time when the task should start.



Enable **Stop task after it has run for <n> hour(s) <n> minute(s)**, to stop a configuration report task if it exceeds the specified hours.

4 Click **Next**. The **Report Settings** page appears. The available options are:

Table 3-15 Option definitions

Option	Definition
Recipient Email	Specify the recipient email address or SMTP address of the distribution list. In most cases, this should be the Exchange administrator's email address.  By default, the email address from Settings & Diagnostics Notifications Settings General Administrator E-mail is used as the recipient email address.
Subject line for report	Specify a meaningful subject line for the email. For example, if you want a weekly configuration report, specify <code>MSME Weekly Configuration Report</code> .

5 Click **Next**. The **Please enter a task name** page appears.

6 Specify a meaningful configuration report task name, based on the schedule and format you selected in the previous pages. For example, if you are creating a monthly configuration report task that provides product and system information on the first Monday of each month, specify the task name as `Monthly Configuration Report (First Monday)`.


7 Click **Finish**, then **Apply**.

By performing these steps, you have successfully created a new configuration report task.

Configuration report email notifications

Based on your scheduled configuration report, the recipient receives an email containing MSME product information, policy settings and system information for the specified duration.

Table 3-16 Option definitions

Option	Definition
Server Info	Displays server information such as the computer name, IP address and Exchange version.
Version Info	Displays MSME information such as the product version, DAT version and date, Engine version, Anti-Spam Rules and Engine information (if any).
License Status	Displays product license information such as the MSME and Anti-Spam add-on component license type.
Product Information	Displays additional product information on whether any service pack or hotfix is installed.
Debug Logging	Displays Debug Logging information such as the level, maximum size of the log file and location of the file.
On-Access Settings	Displays the current On-Access Settings configuration specifying which setting is enabled or disabled.
On-Access Policies	Displays the core scanners and filters enabled for the On-Access Master policy .
Gateway Policies	Displays the current status of the Anti-Spam and Anti-Phishing scanner for the Gateway Master policy .
	 This is applicable only if you installed the McAfee Anti-Spam add-on component.

Graphical reports

Generate graphical reports to understand the threat-level during a specific time-frame. Provides an explicit view of detected items in the form of a **Bar Graph** or **Pie Chart**.

These reports along with the status report will help you and your organization to identify servers facing higher threats and help you in coming up with mitigation plans.

Use graphical reports when you want to only view the current threat-level and doesn't have to take any action on the detected items. **Graphical Reports** allow you to query based on certain filters, where you can view **Top 10** reports for various detections.

Graphical Reports are classified into:

- **Simple** — Limited search filters to view Top 10 report of the day or week.
- **Advanced** — More search options to query on different filters, time-range, and chart options.

View graphical report using simple search filters

Generate graphical report on detections using simple search filters for the day or week.

Task

- 1 Click **Dashboard | Graphical Reports**. The **Graphical Reports** page appears.
- 2 Click the **Simple** tab.
- 3 From **Time Span** drop-down list, select **Today** or **This week** to view detections quarantined for the day or for the week.

- 4 From **Filter** drop-down list, select the report that you want to view. The options available are:
 - **Top 10 Viruses** — Lists the top 10 virus names ranked by their detection count.
 - **Top 10 Spam Detections** — Lists the top 10 detected spam emails ranked by the spam message count.
 - **Top 10 Spam Recipients** — Lists the top 10 spam recipients ranked by their total received spam message count.
 - **Top 10 Phish Detections** — Lists the top 10 detected phishing emails ranked by their phishing message count.
 - **Top 10 Blocked IP addresses** — Lists the top 10 IP addresses ranked by the blocked count for bounced emails.
 - **Top 10 Unwanted Programs** — Lists the top 10 potentially unwanted programs detected that might be threats.
 - **Top 10 DLP and Compliance Detections** — Lists the top 10 data loss prevention and compliance regulatory violations ranked by the number of detections that triggered the rule.
 - **Top 10 Infected Files** — Lists the top 10 file names ranked by their detection count.
 - **Top 10 Blocked URLs** — Lists the top 10 URLs detected that might be threats.
 - **Top 10 Detections** — Lists the top 10 detections ranked by their detection count. This graph contains all the categories such as viruses, spam detections, spam recipients, phish detections, blocked IP addresses, unwanted programs, DLP and compliance, malicious URLs, and infected files listed above.
- 5 Click **Search**. The search results are shown in the **View Results** pane.

In **Magnify Graph**, select the zoom percentage to let you enlarge or reduce the view of the graph in the **View Results** pane

Using advanced search filters

Generate graphical report on detections using advanced search filters.

Task

- 1 Click **Dashboard | Graphical Reports**. The **Graphical Reports** page appears.
- 2 Click **Advanced** tab.

- 3 Select at least one filter or up to three filters from the list:

Table 3-17 Primary filters

Filter	Description
Subject	Search using the "subject" of an email.
Recipients	Search using an email address of the recipient.
Reason	Search using the detection trigger or using the reason why the item was quarantined. When you select the Reason filter, secondary filters are enabled for further refining your search. For example, you might want to search for all items that was quarantined due to the Mail Size rule being triggered as the reason.
Ticket Number	To search using the ticket number. A ticket number is a 16-digit alpha-numeric entry which is auto-generated by the software for every detection.
Detection Name	To search by the name of a detected item.
Spam Score	To search based on the spam score. For example, you might want to search for all items that was quarantined with a Spam Score equal to 3.

Spam Score is a number that indicates the amount of potential spam contained within an email message. The engine applies anti-spam rules to each email message it scans. Each rule is associated with a score. To assess the risk that an email message contains spam, these scores are added together to give an overall spam score for that email message. The higher the overall spam score, the higher the risk that the email messages contains spam. The spam score can range between 0 and 100. Incoming messages start with a spam score of zero. Each time a message violates a filter, its spam score increases.



A secondary filter is only available for the **Reason** filter. If you do not want to specify the secondary filter, ensure that the field is blank so that all detections are queried upon.

Table 3-18 Secondary filters

Filter	Description
Anti-Virus	Search for items that was quarantined when a potential virus was found in the message.
Banned Content	Search for items that was quarantined when a banned content was found in the message. For example: inappropriate words.
File Filter	Search for items that was quarantined when a banned file was found in the message.
Anti-Spam	Search for items that was quarantined when spam was found. For example: chain email messages
Encrypted or Corrupted	Search for items that was quarantined when encrypted or corrupt content was found in the email.
Potentially Unwanted Program	Search for items that was quarantined when potentially unwanted program was found in the email.
Phish	Search for items that was quarantined when phishing content was found in the email
Packer	Search for items that was quarantined when packers (small programs, compressed executables files, encrypted code) was found in the email.
Mail Size	Search for items that was quarantined when mail size exceed the maximum limit set.
Encrypted	Search for items that was quarantined when encrypted content was found in the email.

Table 3-18 Secondary filters (continued)

Filter	Description
Signed	Search for items that was quarantined when signed content was found in the email.
Corrupted	Search for items that was quarantined when corrupt content was found in the email.
Denial of Service	Search for items that was quarantined when denial-of-service threat occurred. For example: if you want to retrieve all email messages that were quarantined during the event.
Protected Content	Search for items that was quarantine when protected content was found and the content might not be accessed for scrutiny.
Password Protected	Search for items that was quarantined when password protected content was found and the content might not be accessed for scrutiny.
Blocked MIME	Search for items that was quarantined when blocked MIME (multipurpose Internet Mail Extension) were found in the email.
URL Reputation	Search for items that was quarantined when URL reputation exceeds the defined threshold.



For more information about the search filters, see *Search filters*.

- 4 Select **All Dates** or a **Date Range** from the drop-down lists.

If you select **All Dates**, the query returns search results from quarantine database from day it started quarantining any detected items. If you select **Date Range**, select the **Date**, **Month**, **Year**, **Hour**, and **Minutes** from the **From** and **To** fields to enable your query to search within a date range.

- 5 Select **Bar Graph** or **Pie Chart** as required.
- 6 If you select **Pie Chart**, select a filter from the drop-down list to further refine your search:

Table 3-19 Query on

Filter	Description
Recipients	Search using the recipient email address
Sender	Search using the senders email address
Filename	Search using a quarantined file name.
Detection Name	Search using the name of a detected item.
Subject	Search using the "subject" of an email.
Reason	Search using the detection trigger or using the reason why the item was quarantined.
Rule Name	Search using the name of the rule that triggered the detection.
Policy Name	Search using the policy name that made the detection.

- a In **Maximum Results**, specify the number of search results you want to view. You can view a maximum of 99 search results and this field is available only if you select pie chart.
- 7 Click **Search**. The search results are shown in the **View Results** pane. In **Magnify Graph**, select the zoom percentage to let you enlarge or reduce the view of the graph in the View Results pane The search results are shown in the **View Results** pane.

4

Detected items

View information about all email messages containing potential threats that are detected and quarantined by MSME. You can use various search filters to refine the search and find quarantined items that are of interest to you, view the results and take necessary action on the quarantined items.

From the product's user interface, click **Detected Items** to view quarantined items based on the detection category. The detection categories are:

- Spam
- IP Reputation
- Phish
- Viruses
- Potentially Unwanted Programs
- Unwanted Content
- Banned File types and Messages
- DLP and Compliance
- Mail URL Reputation
- All Items



The **Spam**, **Phish**, and **IP Reputation** options are available only if you have installed the McAfee Anti-Spam add-on.

Contents

- ▶ [Manage quarantined data](#)
- ▶ [Detection types](#)
- ▶ [Available primary search filters](#)
- ▶ [Search filter comparison chart](#)
- ▶ [Additional search options](#)
- ▶ [Search detected items](#)
- ▶ [Actions that you can take on quarantined items](#)

Manage quarantined data

Based on your requirement, decide whether to use the local database or a dedicated quarantine management server known as McAfee Quarantine Manager, to quarantine detected items.

By default, detected items are quarantined locally to a PostgreSQL database installed by MSME.

Configure quarantine location

Based on the **Detected Items** configuration settings, you can choose to quarantine detected items in the local database or use McAfee's quarantine management software, widely known as McAfee Quarantine Manager to quarantine detected items on a separate server.




For managed systems, if you select MQM server to quarantine the detected items, make sure that the configuration is enforced only to the systems you intended. Otherwise, the configuration is applied to all MSME servers in the **System Tree**.

From the product's user interface, click **Settings & Diagnostics | Detected Items** and select:

- **McAfee Quarantine Manager** — To quarantine detected items in the MQM server.
- **Local Database** — To quarantine detected items in the local MSME server, at the specified path.

Local Database Vs. McAfee Quarantine Manager — When to use

This table helps you understand when to use the local database or McAfee Quarantine Manager for quarantine management:

Use Local Database...	Use McAfee Quarantine Manager...
To manage quarantined items of one MSME installation.	To manage quarantined items from multiple MSME installations or any of these MSME products configured in your organization: <ul style="list-style-type: none"> • McAfee Security for Microsoft Exchange • McAfee Email and WebSecurity Appliance • McAfee Security for Lotus Domino (Windows) • McAfee Security for Lotus Domino (Linux) <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  You can download and install McAfee Quarantine Manager for free, if you have purchased any of the products mentioned above. </div>
If you want to use PostgreSQL database to quarantine items.	If you want to use MySQL or Microsoft SQL Server database to quarantine items.




For more information on McAfee Quarantine Manager software and its features, refer to its product documentation.

Detection types

Detected items are email messages identified by MSME as a potential threat, that could be a virus, spam, phishing, non-compliant content, a URL, or banned file types.

The detection types in MSME are:

Detection types	Description
Spam	An unwanted electronic message, most commonly unsolicited bulk email. Typically, spam is sent to multiple recipients who did not ask to receive it. Types include email spam, instant messaging spam, Usenet newsgroup spam, web search-engine spam, spam in blogs, and mobile phone-messaging spam. Spam includes legitimate advertisements, misleading advertisements, and phishing messages designed to trick recipients into giving up personal and financial information. Email messages are not considered spam if a user has signed up to receive them.
IP Reputation	A method of detecting messages based on the sending server's IP address. McAfee collects data from billions of IP addresses and network ports, providing hundreds of trillions of unique views, and calculates a reputation score based on network traffic, including port, destination, protocol, and inbound and outbound connection requests. This score is known as IP Reputation Score and reflects the likelihood that a network connection poses a threat. MSME uses this score to determine action based on a local policy.

Detection types	Description
Phish	A method of fraudulently obtaining personal information, such as passwords, Social Security numbers, and credit card details by sending spoofed emails that look like they are sent from trusted sources, such as banks or legitimate companies. Typically, phishing emails request that recipients click on the link in the email to verify or update contact details or credit card information. Like spam, phishing emails are sent to a large number of email addresses, with the expectation that someone will act on the information in the email and disclose their personal information.
Viruses	<p>A computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files, so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies, or creates files. Some viruses display symptoms, others damage files and computer systems, but neither is essential in the definition of a virus; a non-damaging virus is still a virus.</p> <p> You cannot Download, Release, Forward, or View quarantined items from the Viruses detection category.</p>
Potentially Unwanted Programs	Often legitimate software (non-malware) that may alter the security state or the privacy posture of the system on which they are installed. This software can, but not necessarily, include spyware, adware, keyloggers, password crackers, hacker tools, and dialer applications and could be downloaded in conjunction with a program that the user wants. Security-minded users may want to know about such programs and, in some cases, have them removed.
Unwanted Content	<p>This is any content that triggers a content scanning rule. It might include offensive, abusive, unpleasing words or even a company's confidential information. Unwanted Content can be categorized into:</p> <ul style="list-style-type: none"> • Packers • Encrypted Content • Signed Content • Corrupted Content • Denial of service • Protected Content • Password protected files • Incomplete MIME messages
Banned File types and Messages	Certain types of file attachments are prone to viruses. The ability to block attachments by file extension is another layer of security for your mail system. Both internal and external email messages are checked for banned file types or messages.
DLP and Compliance	<p>Stop the loss of sensitive information via email. MSME provides industry-leading email content analysis to provide the tightest control of sensitive content in any form to aid compliance with many state, national, and international regulations.</p> <p>Prevent data leakage with the most extensive email Data Loss Prevention (DLP) in the industry that does pattern matching to detecting data; policy-based message handling that prevents outbound data loss.</p>
Mail URL Reputation	Prevents delivery of emails with unwanted URLs that might contain unwanted links, phishing links, or malware.



The **Spam**, **Phish**, and **IP Reputation** options are available only if you have installed the McAfee Anti-Spam add-on.

See also

[Search filter comparison chart on page 62](#)

[Additional search options on page 63](#)

Available primary search filters

Search filters enable you to define the search criteria and provide more efficient and effective searches from the quarantine database.

The available primary search filter option varies based on the detected item category you have selected. These search filters appear in the **View Results** section of the detected item category.



Use **Columns** to display in the **View Results** section, to select the search filters that you want to view.

Table 4-1 Detected Items – Primary search filters

Search filter	Definition
Action taken	<p>Search for an item based on the action that was taken on it. The actions taken by MSME are:</p> <ul style="list-style-type: none"> • Clean • Cleaned • Deleted • Deleted Message • Denied Access • Logged • Replaced • Rejected
Anti-Spam Engine	<p>Search for an item based on the anti-spam engine that scans email messages for spam and phishing attacks.</p> <p>To view the current Anti-Spam Engine used, go to Dashboard Versions & Updates Update Information Anti-Spam Engine Rules Version. For example, the Anti-Spam Engine version appears in this format: 9286</p>
Anti-Spam Rule	<p>Search for an item based on the anti-spam rules that are updated every few minutes to catch the latest spam campaigns sent by spammers.</p> <p>To view the current Anti-Spam Rule used, go to Dashboard Versions & Updates Update Information Anti-Spam Engine Rules Version. For example, the rule version appears in this format: core:4373:streams:840082:uri:1245250</p>
Anti-Virus DAT	<p>Search for an item based on the anti-virus DAT version with a distinctive signature.</p> <p>To view the current Anti-Virus DAT used, go to Dashboard Versions & Updates Update Information Anti-Virus Engine DAT Version Extra Drivers. For example, the DAT version appears in this format: 6860.0000</p>
Anti-Virus Engine	<p>Search for an item based on the anti-virus engine that had a sequence of characters unique to a virus/unwanted content.</p> <p>To view the current Anti-Virus Engine used, go to Dashboard Versions & Updates Update Information Anti-Virus Engine DAT Version Extra Drivers. For example, the Anti-Virus Engine version appears in this format: 5400.1158</p>
Banned Phrases	<p>Search by the content of banned phrases that are defined in the DLP and Compliance Rules under Policy Manager Shared Resource DLP and Compliance Dictionaries.</p>
Detection Name	<p>Search for a detected item based on its name.</p>
File Name	<p>Search by the name of the detected file in the quarantined item.</p> <p>To view the File Name used, go to Policy Manager Shared Resource DLP and Compliance Dictionaries File Filtering Rules.</p>
Folder	<p>Search by the folder where quarantined items are stored such as a user's mailbox.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> The folder will not be available if the email is quarantined at the On-Access (Transport) level. </div>

Table 4-1 Detected Items — Primary search filters *(continued)*





Search filter	Definition
IP Reputation Score	<p>Search for an item based on the sender's IP Reputation Score. The items quarantined are based on the IP reputation threshold specified under Settings & Diagnostics Anti-Spam McAfee GTI IP reputation.</p> <p> This filter is available only if you have installed the McAfee Anti-Spam add-on.</p>
Policy Name	Search for an item by a policy name such as a Master policy or sub-policy that detected the item.
Reason	Search for an item based on the reason why it was detected. This could be based on the scanners and filters such as Anti-Virus, Anti-Spam, Anti-Phish, DLP and Compliance , and so on.
Reasons	Search by a rule or rules that were triggered by a particular email. Use this if an item has triggered multiple scanners or filters. For example, if a spam email contains a virus, the Reasons are Anti-Spam and Anti-Virus .
Recipients	Search for an item through the recipient's email address.
Reputation Score	<p>Search by the authenticity level of the source of the email based on up to date information available. The items quarantined are based on the Message reputation threshold specified under Settings & Diagnostics Anti-Spam McAfee GTI message reputation.</p> <p> This filter is available only if you have installed the McAfee Anti-Spam add-on.</p>
Rule Name	Search for an item based on the rule that triggered one or more scanners/filters. The rule that triggered the scanner or filter is based on the Actions set for each policy.
Scanned by	Search for an item by the scanner name that detected the item.
Sender	Search for an item by the sender's email address.
Sender IP	<p>Search for an item by the IP address of the sender's system. The items quarantined are based on the IP reputation threshold specified under Settings & Diagnostics Anti-Spam McAfee GTI IP reputation.</p> <p> This filter is available only if you have installed the McAfee Anti-Spam add-on.</p>
Server	Search for an item based on the computer name.
Spam Score	<p>Search for an item based on the spam score, which is a number that indicates the amount of potential spam contained within an email message. The engine applies anti-spam rules to each email message it scans. Each rule is associated with a score. To assess the risk that an email message contains spam, these scores are added together to give an overall spam score for that email message. The higher the overall spam score, the higher the risk that the email messages contains spam.</p> <p> This filter is available only if you have installed the McAfee Anti-Spam add-on.</p>
State	<p>Search for an item based on its current status. The available items states are:</p> <ul style="list-style-type: none"> • Untrained — Items that are not acted upon such as purged, released, forwarded or deleted. The initial state of all items will be Untrained. • Released — Items that are released from the quarantine database. • In Quarantine Manager Queue — Items that are currently in the queued in the McAfee Quarantine Manager database. • Forwarded — Items that are forwarded to the intended recipients.
Subject	Search for an item based on the subject line of the email message.

Table 4-1 Detected Items – Primary search filters *(continued)*

Search filter	Definition
Task	Search for an item based on the scan task name which can be an On-Access (VSAPI), On-Access (Transport) scan task or On-Demand scan task. The on-access scan task that appears in the View Results section is based on the settings you have enabled under Settings & Diagnostics On-Access Settings . To know whether the item was detected due to an on-demand scan task, go to Dashboard On-Demand Scans .
Ticket Number	Search for an item based on the ticket number, which is a unique alphanumeric identifier assigned to a specific detection and delivered as a notification through email. It helps identify the associated detection.



The primary search filters applicable to **Spam**, **Phish** and, **IP Reputation** detection category are available only if you have installed the McAfee Anti-Spam add-on component.

See also

[Additional search options on page 63](#)

Search filter comparison chart

Provides information on which search filter is available for a selected detected item category.

The available search filters in MSME vary based on the detected item category you have selected. Use this as a reference material, when you are not sure about which search filter is available for a specific detected item category.

A quick look into this comparison chart helps you know the available search filters for a specific detection type.

Table 4-2 Comparison chart – Search filters for detection types

Filter	Spam	IP Reputation	Phish	Viruses	Potentially Unwanted Programs	Unwanted Content	Banned File types and Messages	DLP and Compliance	Mail URL Reputation
Action Taken	✓	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Spam Engine	✓		✓						
Anti-Spam Rule	✓		✓						
Anti-Virus DAT				✓	✓				
Anti-Virus Engine				✓	✓				
Banned Phrases						✓		✓	✓
Detection Name				✓	✓				
Filename				✓	✓	✓	✓	✓	✓
Folder				✓	✓	✓	✓	✓	✓

Table 4-2 Comparison chart – Search filters for detection types *(continued)*

Filter	Spam	IP Reputation	Phish	Viruses	Potentially Unwanted Programs	Unwanted Content	Banned File types and Messages	DLP and Compliance	Mail URL Reputation
IP Reputation Score		✓							
Policy Name	✓		✓	✓	✓	✓	✓	✓	✓
Recipients	✓		✓	✓	✓	✓	✓	✓	✓
Reputation Score	✓		✓						
Rule Name	✓		✓		✓	✓	✓	✓	✓
Scanned By	✓		✓	✓	✓	✓	✓	✓	✓
Sender	✓		✓	✓	✓	✓	✓	✓	✓
Sender IP	✓	✓	✓						
Server	✓		✓	✓	✓	✓	✓	✓	✓
Spam Score	✓		✓						
Subject	✓		✓	✓	✓	✓	✓	✓	✓
Ticket Number	✓		✓	✓	✓	✓	✓	✓	✓



The search filters **Reason**, **Reasons**, **State** and **Task** are not available in this comparison chart, as it is available only for **Detected Items** | **All Items** category.

See also

[Detection types on page 58](#)



Additional search options

Provides information on additional search options to narrow-down the detected items search results.

Table 4-3 Option definitions

Option	Definition
AND	Search items based on the conditions set in the previous and next filter option, where the search results satisfy both the conditions.
OR	Search items based on the conditions set in the previous and next filter option, where the search results satisfy either of the conditions.
Contains	Search for an item that contains the specified text in the primary search filter. For example, if you want to search for quarantined items that were detected in the Outbox folder, select Folder as the primary search filter, select Contains from the drop-down list, then type <code>out</code> in the text box and click Search to view the search results in the View Results section.
Not Contains	Search for an item that excludes the specified text in the search results. For example, if you do not want logged items to appear in your search results, select Action Taken as the primary search filter, select Not Contains from the drop-down list, then type <code>log</code> and click Search to view the search results in the View Results section.

Table 4-3 Option definitions (continued)

Option	Definition
Exact Match	Search for an item that is an exact match of the specified text. For example, if you want to search for quarantined items that were detected by a specific Anti-Virus Engine version number 5400.1158, select Anti-Virus Engine as the primary search filter, select Exact Match from the drop-down list, then type 5400.1158 in the text box and click Search to view the search results in the View Results section.
Match RegExp	Search for an item matching a particular pattern, using regular expressions. For example, if you want to search based on a valid email address anywhere in the detection, select Detection Name as the primary search filter, select Match RegExp from the drop-down list, then type <code>\b[A-Z0-9._%+-]+@[?:[A-Z0-9-]+\.]+[A-Z]{2,4}\b</code> in the text box and click Search to view the search results in the View Results section.
Equal to	Search for an item containing the Spam Score , Reputation Score or IP Reputation Score that equals the specified value.
Less than	Search for an item containing the Spam Score , Reputation Score or IP Reputation Score that is less than the specified value.
Greater than	Search for an item containing the Spam Score , Reputation Score or IP Reputation Score that is more than the specified value.
Case Sensitive	Select if your search criteria is case-sensitive.
All Dates	Select if you want to search for items on all dates.  The search results appear based on the date stored in the quarantined items database.
Date Range	Search for an item within a defined date range according to your requirements. Here you can specify the date, month, year and time against the parameters From and To . You can also use the calendar icon to specify a date range.  The date range is based on the local system time.
Search	Click to view a list of quarantined items matching your search criteria that appear in the View Results section.
Clear Filter	Click to return to default search settings.

See also

[Available primary search filters on page 60](#)

Search detected items




Use search filters to find specific quarantined items that are of interest to you and take corresponding action.

You can use a combination of search filters such as boolean logic operators, regular expressions, case-sensitive text or date range.

Task

- 1 From the product's user interface, click **Detected Items**.
- 2 From the left-pane, click the desired detection category such as **Spam**, **Phish** or **All Items**.
- 3 From the **Search** pane, select the desired search filters from the drop-down lists (if required). The available search options are:

Table 4-4 Search options

Search feature	Description
Primary search filter	<p>Select if you want to refine your search criteria based on a specific filter such as Policy Name, Action Taken, Sender and so on.</p> <p> For more information on all primary search filters, see <i>Available primary search options</i> section.</p>
Boolean logic operator	<p>Select if you want to refine your search by using these logical operators:</p> <ul style="list-style-type: none"> • AND • OR <p> For more information on these filter options, see <i>Additional search options</i> section.</p>
Secondary search filter	<p>Select if you want to refine your search by using these secondary filters:</p> <ul style="list-style-type: none"> • Contains • Not Contains • Exact Match • Match RegExp • Equal to • Less than • Greater than <p> For more information on these filter options, see <i>Additional search options</i> section.</p>
Case Sensitive	Select if your search criteria is case-sensitive.
Date Range	<p>Select if you want to refine your search to all dates or to a specific time frame.</p> <ul style="list-style-type: none"> • All Dates • Date Range

4 Click **Search**.

By performing this task, you have successfully searched for detected items matching your search criteria, that now appear in the **View Results** section.

Actions that you can take on quarantined items


View results of the search based on the parameters you defined and take necessary action on quarantined items.

You can then execute various actions on these quarantined items.



Table 4-5 Types of action

Action	Definition
Release	<p>To release a quarantined item. Select an applicable record from the View Results pane and click Release. The original email message is released from the database for delivery to the intended recipient.</p> <ul style="list-style-type: none"> When an item is downloaded, released or forwarded, it will be scanned for viruses and will appear in the Dashboard Recently Scanned Items section. After a successful release, the item will appear with status as Released under Detected Items All Items category.
Download	<p>To download a quarantined item for research or analysis. Select one applicable record from the View Results pane and click Download.</p> <p>You cannot Download, Forward, View or Release multiple records at a time from Detected Items All Items category. However, you can Release multiple records from a specific category.</p>
Export to CSV File	<p>To export and save information about all quarantined items returned by the search in a .CSV format. If there are thousands of quarantined items in the database, instead of navigating through multiple pages, you can use this option to download these records to a file in CSV format and later generate custom reports in Microsoft Excel.</p> <p>From the View Results pane, click Export to CSV File to Open or Save the search results to the desired folder or location.</p> <p>To specify a limit on how many quarantined items need to appear in the View Results, modify the Maximum query size (records) value from Settings & Diagnostics Detected Items Local Database.</p> <ul style="list-style-type: none"> If you do not find a specific field in the search result of the CSV file, make sure to enable the required field in the Columns to Display option. Use the Import Data option in Microsoft Excel, to open the CSV file in a different locale.
Forward	<p>To forward the quarantined item to the desired recipient. Use semi-colon as a delimiter to forward the quarantined item to multiple recipients. Performing this action will send the quarantined item in a new email as an attachment (.eml format.)</p> <p>To forward the quarantined item to a Distribution List (DL) within your organization, specify the SMTP address of the DL.</p>
View	To view the quarantined item in a separate window.
Add to Block Senders	To add a sender's email address to the list of addresses from which emails should be blocked, which is also known as blacklisting.
Add to Allow Senders	To add a sender's email address to the list of addresses from which emails should be allowed, which is also known as whitelisting.
Columns to display	To select additional column headers to be listed in the View Results pane. This option has a list of all the filters available in the Search pane and some more options.
Select All	To select all quarantined items that appear in that page of the View Results section. For example, if you have 100 quarantined items and set the items to view per page as 10, then only 10 items that appear in the View Results section are selected.
Select None	To deselect all quarantined items that appear in the View Results section.

Table 4-5 Types of action *(continued)*

Action	Definition
Delete	To delete the quarantined items that you selected in that page of the View Results section for the selected category.  Press and hold down the Ctrl key to select multiple items.
Delete All	To delete all quarantined items from the database for the selected category.
Views per page	To specify the maximum number of quarantined items that you want to view per page. The options are: <ul style="list-style-type: none"> • 10 • 20 • 50 • 100

Each item in the **View Results** pane has an image, which indicates:

Icon	Description
	An item that is quarantined and can be downloaded, forwarded, released or viewed.
	An item that is only logged and cannot be downloaded, forwarded, released or viewed.

Detected items

Actions that you can take on quarantined items

5

Policy Manager

Allows you to configure or manage different policies and corresponding actions in the product. Determine how different types of threats are treated when detected.

A policy is typically described as a principle or rule to guide decisions and achieve rational outcomes. Policies are adopted within an organization to help objective decision making.

In MSME, a policy specifies the settings that are used and the actions taken when a detection is triggered in the Exchange environment. You can create multiple policies and define specific settings and actions to particular policies. For example, you can create multiple subpolicies for the **On-Access** menu option and have a different setting and action set for each policy.

To simplify, an MSME policy = Scanner settings + Actions to take.



Use the **Shared Resource** menu option under **Policy Manager**, to modify or create rules for scanner, filter, and alert settings from one common location. Use **Shared Resource** to save time in creating and applying MSME policies.

Steps to create a policy

As an administrator, to create a policy, you must:

- 1 Enable the scanner or filter.
- 2 Edit scanner or filter settings from the policy or **Shared Resource**.
- 3 Specify an action to take when a detection is triggered.
- 4 Specify users for whom this policy applies.
- 5 Apply the settings for the required policy category.

Contents

- ▶ *Policy Manager menu options*
- ▶ *Policy categories to handle threats*
- ▶ *Policy Manager views*
- ▶ *Master policy and subpolicy*
- ▶ *Core scanners and filters*
- ▶ *Scanners and filters comparison chart*
- ▶ *List all scanners and filters for a selected policy*
- ▶ *Adding a scanner or filter*
- ▶ *Create new rule for specific users*
- ▶ *Actions you can take on detections*
- ▶ *Shared Resource*
- ▶ *Manage core scanner settings for a policy*
- ▶ *Manage filter settings for a policy*
- ▶ *Manage miscellaneous settings for a policy*

Policy Manager menu options

View the menu options available under **Policy Manager**.

From the product's user interface, click **Policy Manager**. These menu options appear on the left-pane.

Option	Description
On-Access	Contains policies for email messages every time they are accessed, to determine if the email message contains a virus or other potentially unwanted code.
On-Demand (Default)	Contains policies that are activated at set intervals or on demand, to find a virus or other potentially unwanted code.
On-Demand (Find Viruses)	Contains policies that are activated at set intervals or on demand, to find a virus or other Potentially Unwanted Programs (PUPs) and other possible threats.
On-Demand (Remove Viruses)	Contains policies that are activated at set intervals or on demand, and which remove viruses, Potentially Unwanted Programs (PUPs) and other possible threats.
On-Demand (Find Banned Content)	Contains policies that are activated at set intervals or on demand, to find a banned content that you do not want to appear in email messages.
On-Demand (Remove Banned Content)	Contains policies that are activated at set intervals or on demand, and which remove content that you do not want to appear in email messages. For example, if an email message contains a particular word or phrase, you can set up a policy to automatically replace the content of that email message with an alert message. You can use this type of policy to prevent unwanted information entering or leaving your organization.
On-Demand (Full Scan)	Contains policies that are activated at set intervals to scan for viruses, spam, phishing email messages, banned/unwanted content, and other harmful codes.
Gateway	Contains policies for email messages every time they are accessed, to determine spam, phish, MIME files or HTML files.
Shared Resource	One common location to edit settings for scanners, filters, alerts, DLP and Compliance dictionaries, and time slots.

Policy categories to handle threats

View available policy categories and apply an existing default policy (known as a *Master Policy*) to your entire organization.

MSME helps you mitigate electronic threats with special set of rules and settings called policies, that you can create to suit your Exchange organization needs.

When you install MSME for the first time on your Exchange server, a default **Master policy** is available for these menu options:

- **On-Access**
- **On-Demand (Default)**
- **On-Demand (Find Viruses)**
- **On-Demand (Remove Viruses)**
- **On-Demand (Find Banned Content)**
- **On-Demand (Remove Banned Content)**
- **On-Demand (Full Scan)**
- **Gateway**

You can customize policies under each of these categories to precisely handle specific threats that could affect your Exchange organization.

Policy Manager views

View and sort subpolicies based on inheritance or priority.

The types of **Policy Manager** views are:

- **Inheritance View**
- **Advanced View**

Inheritance view

Displays the priority and status of the Master policy and all subpolicies. MSME acts on an email, based on the settings configured for the subpolicy with highest priority. When the rules of a subpolicy are not satisfied, MSME moves on to the subpolicy with the next priority. Settings configured in the Master policy are applied, when rules in none of the subpolicies are satisfied.

When you select **Inheritance View**, the subpolicies appear based on the inheritance of the policy.

In this view, you can:

- View the policy and its priority
- View the inherited subpolicy and its parent policy
- Enable or disable subpolicies
- Delete subpolicies

Advanced view



Display all policies in ascending order, based on the priority and provides an option to change the priority of a subpolicy.

In this view, you can:

- View the policies sorted on priority
- Modify the priority of a policy



Use these icons to modify the priority of a policy:

-  — Increase the priority of a policy.
-  — Decrease the priority of a policy.

- Enable or disable subpolicies
- Delete subpolicies
- Edit the policy name, description, and parent policy by clicking **Details**

Master policy and subpolicy

A policy setting inside a hierarchical structure is ordinarily passed from parent to children, and from children to grandchildren, and so forth. This concept is termed as inheritance. In MSME, the default parent policy is referred as **Master policy** and child policy is referred as **Subpolicy**.

Master policy

Default parent policy available for all policy categories that define how items are scanned for viruses, how files are filtered, and various other settings. These policies apply to all users within an organization.



You cannot delete the **Master policy**, as it acts as a baseline to create subpolicies.

Subpolicy

Policies which inherit their settings and actions from another policy is known as a subpolicy. You can create more subpolicies with different settings and actions as needed, to apply to specific users.

Subpolicies are required in situations where you need exceptions to the **Master policy** to suit any geographical areas, functions, mailboxes, domains, or departments within your organization. In MSME, the general term for such more policies is known as a policy group.

Action taken on an email is based on the settings configured for the subpolicy with highest priority. When the rules of a subpolicy with highest priority are not satisfied, MSME moves on to the subpolicy with the next priority. Settings configured in the Master policy are applied only when rules in none of the subpolicies are satisfied.

If you select **Inherit settings from parent policy** in the scanner or filter settings page, an inherited policy (subpolicy) uses the same setting as the parent policy. However, if there is a detection, you can take a different action. Any changes to the settings in the parent or **Master policy** is reflected in these subpolicies.

Example: Creating a subpolicy to act on all email messages identified by MSME as a threat to be:

- Quarantined — For all users
- Logged, quarantined, and notify the administrator — For administrators

This simple example provides you more insight on when you might need a subpolicy.

Table 5-1 Example — When do you need a subpolicy

Policy type	Scanner	Protection level	Users	Actions to take
Master policy	Anti-virus	Medium Protection	All users	Quarantine
Subpolicy	Anti-virus	High Protection	Administrators	Log, Quarantine, and Notify administrator



Restoring MSME to default setting removes the existing subpolicies. Make sure to back up the policies and settings using **Export** from **Settings & Diagnostics | Import and Export Configuration | Configuration** tab, before restoring MSME to factory settings.

Create subpolicies

Create other policies based on the **Master policy** or a parent policy to suit specific needs of any part of your organization. Create subpolicies for any exceptional situations that are not covered by the **Master policy**.

This is useful when you do not want to apply rules from the **Master policy** for certain users or groups in your organization. You can create exceptions and allow MSME to perform specific scan.

Some example's on when to create a subpolicy:

- Allow through inbound emails to Executive level users in your organization after scanning, but quarantine for other users.
- Allow certain file formats for specific user groups. For example, if you want to block .wav files for all users, except a specific department in your organization.

Task

1 From **Policy Manager**, select a menu item for which you want to create a subpolicy.

2 Click **Create Subpolicy**.

The **Create a Subpolicy** page appears.

3 Under **Initial configuration | Identification | Subpolicy name**, specify a name that identifies the policy and what it does.

4 Type a **Description** for the policy (optional).

5 Select the **Parent policy** for the subpolicy from where to inherit the settings.

6 Click **Next**.

7 Under **Trigger Rules | Rules**, click **New Rule**.

8 From **Specify a policy rule**, you can select:

- **<select a rule template>** — To specify a policy rule based on the sender or recipient. You can create new rules, based on these options:
 - **The SMTP address of the sender is email address**
 - **The SMTP address of the sender is not email address**
 - **The SMTP address of any recipients is email address**
 - **The SMTP address of any recipients is not email address**
 - **The sender is in Active Directory Group**
 - **The sender is not in Active Directory Group**
 - **Any of the recipients is in Active Directory Group**
 - **Any of the recipients is not in Active Directory Group**



Make sure that you do not create rules with conflicting email addresses or user names. Regular expression (regex) is not supported for specifying users, only wildcard is supported.

- **Copy rules from another policy** — To copy the rules from another policy.

9 Click **Add**.

10 Specify the conditions when the policy should trigger for the user. You can select:

- **Any of the rules apply**
- **All rules apply**
- **None of the rules apply**

11 Click **Next**.

12 From **Scanner and Filters**, you can select:

- **Inherit all settings from the parent policy** — To inherit all properties of the parent policy.
- **Initialize selected settings with values copied from another policy** — To select specific scanners and filters from the available policies.

13 Click **Finish**.

Core scanners and filters

Determine the types of scanners and filters that can be applied when creating policies.

Core scanners

View and configure settings for these scanners from **Policy Manager** | [Shared Resource](#).

Scanner	Definition
Anti-Virus Scanner	Configure settings to detect threats such as viruses, trojans, worms, packers, spyware, adware, and more.
DLP and Compliance Scanner	Create or configure DLP and Compliance Rules to meet your Exchange organization's confidential and compliance policies with the addition of 60 new DLP and Compliance Dictionaries .
File Filtering	Create new file filtering rules to meet the Exchange organization needs. Configure these settings based on file name, file category, or file size.
Mail URL Reputation	Configure settings to detect URLs that contain unwanted links, phishing links, and malware.
Anti-Spam	Configure settings to detect email messages that are categorized as spam, based on spam score, size, rules, and mailing lists.
Anti-Phishing	Configure report settings for email messages that are categorized as phish.



The **Anti-Spam** and **Anti-Phishing** options are available only if you have installed the McAfee Anti-Spam add-on.

Filters

Enable or disable these filters and specify actions to take when there is a detection, based on your Exchange organization needs.



You can enable or disable some filters, but cannot configure the customized settings. Those filters do not appear under [Shared Resource](#) | [Scanners & Alerts](#) | [Scanners](#) | [Category](#) drop-down list.

Filter	Definition
Corrupt Content	Configure settings to act on email messages that are detected as corrupt content.
Protected Content	Configure settings to act on email messages that are detected as protected content.
Encrypted Content	Configure settings to act on email messages that are detected as encrypted content.
Signed Content	Configure settings to act on email messages that are detected as signed content.

Filter	Definition
Password-Protected Files	Configure settings to act on email messages that contain password protected files. You can override the file filtering policy to allow through emails that contain password-protected files attachments as required. For more information, see <i>Configure password-protected file settings</i> .
Mail Size Filtering	Create or configure settings to act on email messages that exceed the mail size filtering options. Configure settings to quarantine email messages based on the overall mail size, attachment size, and number of attachments.
Scanner Control	Create or configure core scanner settings to act on email messages based on the nesting level, expanded file size, and scanning time.
MIME Mail Settings	Create or configure settings to detect threats that are categorized as MIME message.
HTML Files	Create or configure settings to act on email messages containing HTML elements such as comments, URLs, metadata, and scripts.

Miscellaneous

Configure miscellaneous settings such as alerts and disclaimers that are sent to end users, if there is a detection.

Miscellaneous	Definition
Alert Settings	Create or configure settings for an email alert if there is a detection. Configure settings such as the alert email format (HTML or text), encoding, file name, header, and footer.
Disclaimer Text	Create or configure the disclaimer text that has to appear in the email sent to end user, if there is a detection.

Scanners and filters comparison chart

Provides information on which search scanner or filter is available for each policy category by default.

The available scanner or filter in MSME varies based on the policy category you have selected.

Use this as a reference material, when you are not sure about which scanner or filter is available for a specific policy category. A quick look into this comparison chart helps you know the available scanners and filters for each policy category, where the acronyms are:

- OA — On-Access
- OD (D) — On-Demand (Default)
- OD (FV) — On-Demand (Find Viruses)
- OD (RV) — On-Demand (Remove Viruses)
- OD (FC) — On-Demand (Find Non-Compliant Content)
- OD (RC) — On-Demand (Remove Non-Compliant Content)
- OD (FS) — On-Demand (Full Scan)
- GW — Gateway

Core scanners

Core Scanners	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
Anti-Virus Scanner	✓	✓	✓	✓			✓	
DLP and Compliance Scanner	✓	✓			✓	✓	✓	
File Filtering	✓	✓					✓	
Mail URL Reputation	✓	✓					✓	
Anti-Spam								✓
Anti-Phishing								✓



Even though **DLP and Compliance Scanner** is available for the **On-Access** and **On-Demand (Default)** policy category, it is not active or enabled by default. You must create the required rules, then specify an action to take when a rule is triggered and enable the scanner.

Filters

Filters	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
Corrupt Content	✓	✓					✓	
Protected Content	✓	✓			✓	✓	✓	
Encrypted Content	✓	✓			✓	✓	✓	
Signed Content	✓	✓			✓	✓	✓	
Password-Protected Files	✓	✓			✓	✓	✓	
Mail Size Filtering	✓							✓
Scanner Control	✓	✓	✓	✓	✓	✓	✓	✓

Filters	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
MIME Mail Settings	✓	✓			✓		✓	✓
HTML Files	✓	✓			✓		✓	✓

Alert and disclaimer settings

Miscellaneous settings	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
Alert Settings	✓	✓		✓	✓	✓	✓	✓
Disclaimer Text	✓							

List all scanners and filters for a selected policy

View status of the available scanners and filters for the selected policy category. The type of settings that is available depends on which policy is selected.

Task

- 1 From the product's user interface, click **Policy Manager** and policy category menu item.

The policy page for the selected menu item appears.

- 2 Click **Master policy** or the wanted subpolicy.

The corresponding policies page appears.

- 3 In the policies page, you can use these tabs:

- **List All Scanners** — To view which scanner or filter is enabled for the policy.
- **View Settings** — To view settings of the scanner or filter and the actions specified.
- **Specify Users** — To specify policy rules that apply to specific users.



You can specify users only to subpolicies.

- 4 From the **List All Scanners** tab, you can use:

Table 5-2 Policy configuration

Option	Definition
Policy	To select the policy, you want to configure.
Add Scanner/Filter	To configure the policy so that it applies only at specific times. For example, you can create new anti-virus setting with different rules, which is applicable only on weekends.

Table 5-2 Policy configuration (continued)

Option	Definition
Core Scanners	To configure the policy for each of these scanners: <ul style="list-style-type: none"> • Anti-Virus Scanner • DLP and Compliance Scanner • File Filtering • Mail URL Reputation • Anti-Spam • Anti-Phishing
Filters	To configure the policy for each of these filters: <ul style="list-style-type: none"> • Corrupt Content • Protected Content • Encrypted Content • Signed Content • Password Protected Files • Mail Size Filtering • Scanner Control • MIME Mail Settings • HTML Files
Miscellaneous settings	To configure the alert settings and disclaimer messages for policies. Miscellaneous options include: <ul style="list-style-type: none"> • Alert Settings • Disclaimer Text

Adding a scanner or filter

Add a scanner or filter to create settings for exceptional scenarios in your Exchange organization. Adding a scanner or filter is useful, when you want an additional scanner or filter:

- With different options and rules
- Enabled only during a specific time slot

Task

- 1 From **Policy Manager**, select a policy category.
- 2 Click **Master Policy** or any subpolicy.
- 3 From the **List All Scanners** tab, click **Add Scanner/Filter**.



The **Add Scanner/Filter** option is available only for **On-Access** and **Gateway** policy category.

- 4 From **Specify the category** drop-down list, select the required scanner or filter.
- 5 From **When to use this instance** section, select an existing time slot or create a new one.
- 6 Click **Save**.
- 7 Click **Apply**.



Edit the options and rules to suit your organization needs.

Create new rule for specific users

Build new rules and specify conditions to be applied for a particular user.

You can create rules for specific users or groups to have an exception in the policy.

Task

- 1 From **Policy Manager**, select a policy category.
- 2 Click **Master policy** or a wanted subpolicy.
- 3 Click the **Specify Users** tab.
- 4 Click **New Rule**.
- 5 From **Specify a policy rule**, you can select:
 - **<select a rule template>** — To specify a policy rule based on the sender or recipient. You can create new rules, based on these options:
 - **The SMTP address of the sender is email address**
 - **The SMTP address of the sender is not email address**
 - **The SMTP address of any recipients is email address**
 - **The SMTP address of any recipients is not email address**
 - **The sender is in Active Directory Group**
 - **The sender is not in Active Directory Group**
 - **Any of the recipients is in Active Directory Group**
 - **Any of the recipients is not in Active Directory Group**
 - **Copy rules from another policy** — To copy the rules from another policy.
- 6 Click **Add**.
- 7 Specify the conditions when the policy should trigger for the user. You can select:
 - **Any of the rules apply**
 - **All rules apply**
 - **None of the rules apply**
- 8 Click **Apply** to save the rule to the specific user.



Make sure that you do not create rules with conflicting email addresses or user names. Regular expression (regex) is not supported for specifying users, only wildcard is supported.

Actions you can take on detections

For each scanner and filter settings in a policy, you can specify a primary and secondary action to take on a detection. You can specify what happens to an email message or its attachment, when it triggers a detection.

When a policy rule is triggered based on the scanner or filter settings, MSME acts on the detection based on the primary and secondary action configured.

When configuring actions, at least one primary action must be selected. You can also select a number of secondary actions. For example, if the primary action is deleting the email that triggers a detection, the secondary action might be logging the detection and notifying the administrator.

The available primary actions depend on the type of policy category and scanner or filter settings you configure.



Click **Reset**, to restore the actions to default settings for the policy category and scanner.

Table 5-3 Primary actions

Action	Definition
Attempt to clean any detected virus or trojan	To clean the email containing a virus or trojan detected by the Anti-Virus Scanner .
Replace item with an alert	To replace the email that triggered the detection with an alert.
Delete embedded item	To delete the attachment that triggered the detection in an email.
Delete message	To delete the email that triggered the detection.
Allow through	To allow the email to continue to the next scanning phase or reach the end user.
Score-based action	To take an action based on the spam score. This is available only for the Anti-Spam scanner, where you must select If the spam score is High, Medium or Low .
Route to System Junk Folder	To route the email detected by the Anti-Spam scanner to the email address specified under Settings & Diagnostics Anti-Spam Gateway Spam Filter System Junk Folder Address .
Route to User Junk Folder	To route the email detected by the Anti-Spam scanner to the recipient's Junk E-mail folder.
Reject the Message	To reject the email and send a notification to the user.
Replace the attachment with an alert	To replace the attachment in an email message with an alert, if the Mail Size Filtering scanner is triggered when the attachment size exceeds.
Replace all attachments with a single alert	To replace the email message containing multiple attachments with a single alert, if the Mail Size Filtering scanner is triggered when the attachment count exceeds.
Do not allow changes to break the signature	To stop MSME from breaking the signature, when an email message containing Signed Content is detected.
Allow changes to break the signature	To allow MSME to break the signature, when an email message containing Signed Content is detected.

Table 5-4 Secondary actions

Action	Definition
Log	To record the detection in a log.
Quarantine	<p>To store a copy of the email that triggered the detection, in the quarantine database. To view all quarantined items, go to Detected Items All Items or the specific detection category.</p> <p>Select Forward Quarantined email to send the email to a specific reviewer or distribution list, based on the detection category. To configure notifications based on the detection category, go to Settings & Diagnostics Notifications Settings Advanced.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> The Forward Quarantined email option is not applicable for Anti-Virus Scanner or Gateway policies. </div>
Notify administrator	To send a copy of the email to the administrator specified under Administrator E-mail from Settings & Diagnostics Notifications Settings General .

Table 5-4 Secondary actions (continued)

Action	Definition
Notify internal sender	To send an alert message to the internal sender, if the original email originates within the Exchange server's Authoritative Domain.
Notify external sender	To send an alert message to the sender, if the original email message does not originate within the Exchange server's Authoritative Domain.
Notify internal recipient	To send an alert message to the recipient, if the recipient is within the Exchange server's Authoritative Domain.
Notify external recipient	To send an alert message to the recipient, if the recipient is not within the Exchange server's Authoritative Domain.

Shared Resource

One common location to edit settings for scanners, filters, alerts, DLP and Compliance dictionaries, and time slots. When setting up policies, you might want the same resource (scanner and filter settings) applied to more than one policy. In such scenarios, use **Shared Resource**.

For example, if you want to use a different disclaimer for internal and external recipients, create different disclaimers for recipients and apply in the required subpolicy.

From the product 's user interface, click **Policy Manager | Shared Resource**. You can use these tabs:

- **Scanners & Alerts** — To edit or create new scanner and filter settings.
- **DLP and Compliance Dictionaries** — To edit or create new **DLP and Compliance Rules** and **File Filtering Rules**.
- **Time Slots** — To edit or create new time slots such as weekdays or weekends.



Any changes made to these settings are applied automatically to all policies using these configurations.

Configure scanner settings

Create or modify scanner settings to suit your Exchange organization's requirement.

Task

- 1 From the product's user interface, click **Policy Manager | Shared Resource**.

The **Shared Resources** page appears.

- 2 Click **Scanners & Alerts** tab.
- 3 From the **Category** drop-down list under **Scanners** section, select the scanner you want to configure. The scanner type appears with the settings name, policies used by, and action to configure. You can use:

Table 5-5 Option definitions

Option	Definition
Category	To select the required scanner that you want to configure.
Create New	To create new settings for a scanner based on your requirement. Required in a situation where you need exceptions for certain scanner settings and apply it in a policy.

Table 5-5 Option definitions (continued)

Option	Definition
Edit	To edit settings for the selected scanner.
Delete	To delete the scanner settings.
	<div style="border: 1px solid gray; padding: 10px; background-color: #f0f0f0;"> <p>You cannot delete a scanner, if</p> <ul style="list-style-type: none"> • It is a default scanner. • If it is used by any policy. To know, how many policies use this scanner setting, see the Used By column. </div>

- Once you configure the scanner settings, click **Save**, then **Apply**.

You have now successfully configured the settings for a scanner, based on your Exchange organization's requirement.

Configure alert settings

Create or modify alert settings for the selected scanner to suit your Exchange organization's requirement.

Task

- From the product's user interface, click **Policy Manager | Shared Resource**.

The **Shared Resources** page appears.

- Click **Scanners & Alerts** tab.
- From the **Category** drop-down list under **Alerts** section, select the alert you want to configure for a scanner. The scanner type appears with the settings name, policies used by, and action to configure. You can use:

Table 5-6 Option definitions

Option	Definition
Category	To select the required scanner that you want to configure.
Create New	To create new settings for a scanner based on your requirement. Required in a situation where you need exceptions for certain scanner settings and apply it in a policy.
View	To view the default alert settings for a scanner.
Edit	To edit settings for the selected scanner. For more information on the variables you can use in the alerts, refer to the <i>Notification fields that you can use</i> section.
Delete	To delete the scanner settings.
	<div style="border: 1px solid gray; padding: 10px; background-color: #f0f0f0;"> <p>You cannot delete an alert, if</p> <ul style="list-style-type: none"> • It is a default scanner alert. • If it is used by any policy. To know, how many policies use this alert setting, see the Used By column. </div>

- Once you configure the scanner settings, click **Save**, then **Apply**.

You have now successfully configured the settings for an alert, based on your Exchange organization's requirement.

Create an alert

Create an alert message for actions taken by a scanner or filter.

Task

- 1 From the product's user interface, click **Policy Manager | Shared Resource**.

The **Shared Resources** page appears.

- 2 Click **Scanners & Alerts** tab.

- 3 From the **Category** drop-down list under **Alerts** section, select the alert you want to configure for a scanner.

- 4 Click **Create New**.

The **Alert Editor** page appears.

- 5 Type a meaningful **Alert name**.

- 6 Select the required **Style**, **Font**, **Size**, and **Tokens** from the respective drop-down lists.



These options are available only if you select **HTML content (WYSIWYG)** from the **Show** drop-down menu.

7 Use any of these tools to customize your alert:



Table 5-7 Toolbar options

Options	Description
Bold	To make the selected text bold.
Italic	To make the selected text italic.
Underline	To underline the selected text.
Align Left	To left align the selected paragraph.
Center	To center the selected paragraph.
Align Right	To right align the selected paragraph.
Justify	To adjust the selected paragraph so that the lines within the paragraph fill a given width, with straight left and right edges.
Ordered List	To make the selected text into a numbered list.
Unordered List	To make the selected text into a bulleted list.
Outdent	To move the selected text a set distance to the right.
Indent	To move the selected text a set distance to the left.
Text Color	To change the color of the selected text.
Background Color	To change the background color of the selected text.
Horizontal Rule	To insert a horizontal line.
Insert Link	To insert a hyperlink where the cursor is currently positioned. In URL , type the URL . In Text , type the name of the hyperlink as you want it to appear in the alert message. If you want the link to open a new window, select Open link in new window , then click Insert Link .
Insert Image	To insert an image where the cursor is currently positioned. In Image URL , type the location of the image. In Alternative text , type the text you want to use in place of the image when images are suppressed or the alert message is displayed in a text-only browser. If you want to give the image a title, type the title name in Use this text as the image title . Click Insert Image .
Insert Table	To insert a table at the current cursor position. Type the values in Rows , Columns , Table width , Border thickness , Cell padding , and Cell spacing to configure the table, then click Insert Table .

- 8 From the **Show** drop-down menu, specify how the alert message should be displayed within the user interface. You can select:
 - **HTML content (WYSIWYG)** — To hide the underlying HTML code and display only the content of the alert message.
 - **HTML content (source)** — To display the alert message with the HTML code as it appears before compilation.
 - **Plain-text content** — To display the content as plain text.

You can use the following notification fields to include them in your alert message. For example, in your alert message, if you want the name of the detected item and the action taken when it was detected, use **%vrs%** and **%act%** on the **Alert Editor** page. For more information on the notification field options, see the *Notification fields that you can use* section.



McAfee recommends that you save the log files in plain text format so that the content can be viewed by any email client.

- 9 Click **Save** to return to the policy page.



Click **Reset** to undo all changes you have made since you last saved the alert message.

Configure DLP and compliance rules

Create or modify DLP and Compliance rules and dictionaries, to suit your Exchange organization's requirement.

Task

- 1 From the product's user interface, click **Policy Manager | Shared Resource**.

The **Shared Resources** page appears.



- 2 Click **DLP and Compliance Dictionaries** tab.
- 3 From the **Select a Language** drop-down list under **DLP and Compliance Rules** section, select the language.



You can also view and edit all supported locale dictionaries. (The supported locales are Chinese Simplified, French, German, Japanese, and Spanish.)

- 4 From the **Category** drop-down list under **DLP and Compliance Rules** section, select the category you want to view or configure. The rules group appears with the name, policies used by, and action to configure. You can use:

Table 5-8 Option definitions

Option	Definition
Category	<p>To select the required scanner that you want to configure. This release has 60 more DLP and Compliance dictionaries ensuring that email content is in accordance with your organization's confidentiality and compliance policies.</p> <p>Pre-defined Compliance Dictionaries include:</p> <ul style="list-style-type: none"> • Addition of 60 new DLP and Compliance dictionaries • Support for industry specific compliance dictionaries - HIPAA, PCI, Source Code (Java, C++ etc.) <p>These dictionaries are categorized as:</p> <ul style="list-style-type: none"> • Score based — A rule is triggered when email exceeds the threshold score and maximum term count, resulting in reduced false positives. • Non-score based — A rule is triggered when a word or phrase is found in the email message.
New Category	<p>To create a new DLP and Compliance Rules dictionary.</p> <p> Any new category or condition that you create is non-score based.</p>
Create New	<p>To create new rules group for the selected category, based on your requirement. Required in a situation where you need specific rules to trigger a detection and apply it in a policy.</p>
Edit	<p>To edit settings for the selected DLP and Compliance rule.</p>
Delete	<p>To delete the DLP and Compliance rule.</p> <p> You cannot delete a DLP and Compliance rule, if</p> <ul style="list-style-type: none"> • It is enabled. Deselect the rule, Apply the settings, then click Delete. • If it is used by any policy. To know, how many policies use this scanner setting, see the Used By column.



For example, select **Credit Card Number** or any dictionary that suits your needs, from the **Category** drop-down list and see the enhanced **Rules Group** option available.

- To create a new rules group, click **Create New** for **DLP and Compliance Rules** for a selected category.
The **New DLP and Compliance Scanner Rule** page appears for the selected category.
- Type the **Rule Name** and **Description** for the rule.
- Select **Add this rule to this category's rules group** to add the new rule to the rules group for the selected category.
- Under **Word or Phrase**, specify the words or phrases to look for, in **The rule will trigger when the following word or phrase is found**. Then select one of the following options:
 - **Regular Expression** — If enabled, the rule is triggered for specified text that is a regular expression (regex). Regex is a precise and concise method for matching strings of text, such as words, characters, or patterns of characters.

For example, the sequence of characters "tree" appearing consecutively in any context, such as trees, street, or backstreet.



- Regex is disabled for some phrases.
- See <http://www.regular-expressions.info/reference.html> or <http://www.zytrax.com/tech/web/regex.htm> for more details.

- **Use Wildcard** — If enabled, the rule is triggered for the specified word or phrase that contain wildcard characters. (Wildcard characters are often used in place of one or more characters when you do not know what the real character is or you do not want to type the entire name).
- **Starts with** — If enabled, the rule is triggered for specified text that forms the beginning of the word or phrase.
- **Ends with** — If enabled, the rule is triggered for specified text that forms the last part of the word or phrase.
- **Case Sensitive** — If enabled, the rule is triggered if the case of the specified text matches the word or phrase.



To detect a word or phrase with exact match, select both **Starts with** and **Ends with** option.

- 9 Select **Specify additional contextual words or phrases**, which is a secondary action when the primary word or phrase is detected. Specify any additional word or phrase that can accompany the primary word or phrase that triggers a detection.
- 10 Select from **Trigger if ALL of the phrases are present**, **Trigger if ANY of the phrases are present** or **Trigger if NONE of the phrases are present** from the drop-down menu.
- 11 Select **within a block of** to specify the number of **Characters** from a block to be scanned.
- 12 Click **Add Contextual word** to type additional words or phrases.
- 13 Specify the word or phrase in **Specify words or phrases**, select one of the conditions (same options as in Step 7), then click **Add**.
- 14 Under **File Format**, select **Everything** to enable all file categories and its subcategories. You can select multiple categories and file types within the selected categories to be matched. Selecting **All** in the subcategory selector overrides any other selections that may have already been made.
- 15 If you have not selected **Everything**, then click **Clear selections** to deselect any of the selected file type options.
- 16 Click **Save** to return to **Shared Resources** page.
- 17 Click **Apply** to save the settings.

You have now successfully configured the DLP and Compliance rules and dictionaries, to suit your Exchange organization's requirement.

Configure file filtering rules

Create new rules to detect files based on their name, type, or size.

Before you begin

The file filtering rule triggers only when you select one condition. Make sure that you create an individual rule for each of these categories:

- File name
- File category
- File size



This task provides information on configuring all three categories. Based on your Exchange organization's requirement, select only one category for a file filtering rule and create separate rules for each category. If a rule contains multiple criteria such as **File name filtering**, **File category filtering**, and **File size filtering**, all criteria must be satisfied to trigger the rule.

Task

- 1 From the product's user interface, click **Policy Manager | Shared Resource**.
- 2 Click **DLP and Compliance Dictionaries** tab.
- 3 From **File Filtering Rules**, click **Create New**.
- 4 Type a unique **Rule name**. Give the rule a meaningful name, so that you can easily identify it and what it does. For example, **FilesOver5MB** or **Block MPP files**.
- 5 In the **File Filtering Rule** page, you can use:

Table 5-9 Option definitions – filename filtering

Option	Definition
Enable file name filtering	To enable file filtering according to the file names.
Take action when the file name matches	Specify the name of the files that triggers this rule. You can use wildcard characters (* or ?) to match multiple file names. For example, if you want to filter any Microsoft PowerPoint files, type *.ppt.
Add	To add the file name specified under Take action when the file name matches , to the file name filtering list.
Edit	To edit or modify an existing file filtering rule.
Delete	To remove the file name from the filter list.


 You cannot delete a file filtering rule, if it is used by any policy. The **Used By** column must display **0 policies** for the rule that you want to delete. You must first remove the file filtering rule from the policy, then click **Delete**.

Table 5-10 Option definitions – File category filtering


Option	Definition
Enable file category filtering	To enable file filtering according to their file type.
Take action when the file category is	Specify the type of files that affects this rule.
	 File types are divided into categories and subcategories.
File categories	Select a file type category. An asterisk symbol (*) appears next to the file type, to indicate that the selected file type will be filtered.

Table 5-10 Option definitions – File category filtering (continued)

Option	Definition
Subcategories	Select the subcategory you want to filter. To select more than one subcategory, use Ctrl+Click or Shift+Click . To select all of the subcategories, click All . Click Clear selections to undo the last selection.
Extend this rule to unrecognized file categories	To apply this rule to any other file categories and subcategories that are not mentioned in the categories and subcategories list.



To allow through the password-protected .zip files that contains restricted files, make sure that the **Password protected bypass** rule appears as a first rule in the list.

Table 5-11 Option definitions – File size filtering

Option	Definition
Enable file size filtering	To filter files according to their file size.
Take action when the file size is	Specify a value in the adjacent text box and drop-down list, then select: <ul style="list-style-type: none"> • Greater than — To specify that the action should only be applied if the file is larger than the size specified. • Less than — To specify that the action should only be applied if the file is smaller than the size specified.

6 Click **Save** to return to the **Shared Resources** page.

7 Click **Apply** to create the file filtering rule.

You have now successfully created a file filtering rule, to suit your Exchange organization's requirement.

Configure time slots

Set up different time slots or configure existing time slots that can be applied to policies, based on your Exchange organization's requirement.

Time Slots enable you to specify the time during which certain rules must be triggered. For example, you might want to restrict large file upload or download during office hours.

There might be situations where you require more time slots, based on different users, their geographical locations, or working hours. You can create more time slots based on business hours, non-business hours, weekly maintenance, and so on.

By default, MSME has these time slots:

- **All the time**
- **Weekdays**
- **Weekends**



You cannot delete or edit the default time slot **All the time**, as the **Master policy** uses it.

Task

1 From the product's user interface, click **Policy Manager | Shared Resource**.

The **Shared Resources** page appears.

- 2 Click **Time Slots** tab.
- 3 Click **Create New**.
The **Time Slot** page appears.
- 4 Type a unique **Time slot name** such as `Business hours` or `System Maintenance (Weekly)`.
- 5 Under **Select day and time**, select the required days.
- 6 Select **All day** or **Selected hours**.
- 7 Specify the **Start** and **End** time from the drop-down list, if you choose **Selected hours**.
- 8 Click **Save** to return to the **Shared Resources** page.
- 9 Click **Apply** to save the settings.

You have now successfully configured or created a time slot, to suit your Exchange organization's requirement.

Manage core scanner settings for a policy

Create or edit scanner options, then specify an appropriate action to take on the detected item when a policy is triggered.

The available core scanners are:

- **Anti-Virus Scanner**
- **Anti-Spam**
- **DLP and Compliance Scanner**
- **Anti-Phishing**
- **File Filtering**

Tasks

- [Configure anti-virus scanner settings on page 91](#)
Configure **Anti-Virus Scanner** settings in a policy to identify, thwart, eliminate computer viruses and other malware.
- [Configure DLP and compliance scanner settings on page 93](#)
Configure **DLP and Compliance Scanner** settings in a policy to identify noncompliant textual data in an email or attachment and take necessary actions.
- [Configure file filtering settings on page 95](#)
Configure settings in a policy to detect files based on their name, type, or size and take necessary actions.
- [Configure mail URL reputation settings on page 96](#)
Configure the **Mail URL reputation** settings to detect malicious URLs in the email body.
- [Configure anti-spam settings on page 99](#)
Configure settings in a policy to detect spam email messages and take necessary actions.
- [Configure anti-phishing settings on page 102](#)
Configure settings in a policy to block phishing messages using the anti-spam rules and engine, and take necessary actions.

Configure anti-virus scanner settings

Configure **Anti-Virus Scanner** settings in a policy to identify, thwart, eliminate computer viruses and other malware.

Task

- 1 From **Policy Manager**, select a submenu item that has the anti-virus scanner.
The policy page for the submenu item appears.
- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **Anti-Virus Scanner**.
- 4 In **Activation**, select **Enable** to activate the anti-virus scanner settings for the selected submenu item.



- If you are configuring settings for a subpolicy, select **Use configuration from parent policy** to inherit settings from the parent policy.
- If you add a new scanner to the policy, you can specify a time slot when to enable the scanner, using **What time would you like this to apply** drop-down list.

- 5 From the **Options** section, you can use:

Table 5-12 Option definitions

Option	Definition
High Protection	To scan all files, archive files, unknown viruses, unknown macro viruses, mass mailers, potentially unwanted programs, and scan all files for macros.
Medium Protection	To scan all files, archive files, unknown viruses, unknown macro viruses, mass mailers, and potentially unwanted programs.
Low Protection	To scan only default file types, archive files, mass mailers, and potentially unwanted programs.
<create new set of options>	To create your customized anti-virus scanner settings.
Edit	To edit the existing level of protection.

- 6 If you select to edit or modify the scanner settings, in **Instance name**, type a unique name for the anti-virus scanner setting instance. This field is mandatory.
- 7 In **Basic Options** tab under **Specify which files to scan**, select one of these options:
 - **Scan all files** — To specify that all files to scan regardless of their type.
 - **Default file types** — To specify that only the default file types to scan.
 - **Defined file types** — To specify which file types to scan.
- 8 Select more scanner options available in **Scanner options**. You can select:
 - **Scan archive files (ZIP, ARJ, RAR...)**
 - **Find unknown file viruses**
 - **Find unknown macro viruses**
 - **Enable McAfee Global Threat Intelligence file reputation** — This enables the threat intelligence gathered by McAfee Labs that would prevent damage and data theft before a signature update is available. Select the Sensitivity level from the options available.
 - **Scan all files for macros**

- **Find all macros and treat as infected**
 - **Remove all macros from document files**
- 9 On the **Advanced** tab under **Custom malware categories**, specify the items to be treated as malware. There are two ways to select malware types:
- Select the malware types from the list of checkboxes.
 - Select **Specific detection names**, type a malware category, then click **Add**.




When typing a malware category name, you can use wildcards for pattern matching.

- 10 Select the **Do not perform custom malware check if the object has already been cleaned** option, if the cleaned items must not be subjected to the custom malware check.
- 11 In **Clean options**, specify what happens to files that are reduced to zero bytes after being cleaned. Select any one of these options:
- **Keep zero byte file** — To keep files that have been cleaned and is of zero bytes.
 - **Remove zero byte file** — To remove any file that has zero bytes after being cleaned.
 - **Treat as a failure to clean** — To treat zero-byte files as if they cannot be cleaned, and apply the failure to clean action.
- 12 In **Packers** tab, select:
- **Enable detection** — To enable or disable the detection of packers.
 - **Exclude specified names** — To specify which packers can be excluded from being scanned.
 - **Include only specified names** — To specify which packers you want the software to detect.
 - **Add** — To add packer names to a list. You can use wildcards to match names.
 - **Delete** — To remove packer names you have added. This link is activated if you click **Add**.
- 13 In **PUPs** tab, select:
- **Enable detection** — To enable or disable the detection of potentially unwanted programs. Click the disclaimer link and read the disclaimer before configuring potentially unwanted programs detection.
 - **Select the program types to detect** — To specify whether each type of potentially unwanted programs in the list to be detected or ignored.
 - **Exclude specified names** — To specify which potentially unwanted programs can be excluded from being scanned. For example, if you have enabled spyware detection, you can create a list of spyware programs that you want the software to ignore.
 - **Include only specified names** — To specify which potentially unwanted programs you want the software to detect. For example, if you enable spyware detection and specify that only named spyware programs should be detected, all other spyware programs are ignored.
 - **Add** — To add potentially unwanted programs names to a list. You can use wildcards to match names.
 - **Delete** — To delete potentially unwanted programs names that you have added. This link is activated if you click **Add**.



The [McAfee Threat Intelligence](#) website contains a list of recent malware names. Use **Search the Threat Library** to view information about specific malware.

- 14 Click **Save** to return to the policy page.

- 15 In **Actions to take**, click **Edit**. In these following tabs, specify the anti-virus scanner actions that must be taken if a virus (or virus-like behavior) is detected:
- **Cleaning** — Select **Attempt to clean any detected virus or trojan** to activate various actions. Select the actions to be taken from:
 - **Log**
 - **Quarantine**
 - **Notify administrator**
 - **Notify internal sender**
 - **Notify external sender**
 - **Notify internal recipient**
 - **Notify external recipient**
 - **Default Actions** — From **Take the following action** drop-down list, select an action.
 - **Replace item with an alert**
 - **Delete embedded item**
 - **Delete message**
 - **Allow through**
-  For more information on the primary and secondary actions, see the *Actions you can take on detections* section.
- 16 Select the corresponding alert document or click **Create** to make a new alert document. From **And also**, select more actions to be taken for these tabs:
- **Custom Malware**
 - **Packers**
 - **PUPs**
- 17 Click **Save** to apply the settings and return to the policy settings page.
- 18 Click **Apply** to configure these settings to a policy.

Configure DLP and compliance scanner settings

Configure **DLP and Compliance Scanner** settings in a policy to identify noncompliant textual data in an email or attachment and take necessary actions.

Task

- 1 From **Policy Manager**, select a submenu item that has the **DLP and Compliance** scanner.
The policy page for the submenu item appears.
- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **DLP and Compliance Scanner**.

- 4 In **Activation**, select **Enable** to activate the DLP and compliance scanner settings for the selected submenu item.



- By default, all scanner setting options are disabled for **DLP and Compliance Scanner**.
- If you are configuring settings for a subpolicy, select **Use configuration from parent policy** to inherit settings from the parent policy.
- If you add a new scanner to the policy, you can specify a time slot when to enable the scanner, using **What time would you like this to apply** drop-down list.

- 5 In **Options**, you can use:

- **Include document and database formats** — To scan documents and database formats, for noncompliant content.
- **Scan the text of all attachments** — To scan the text of all attachments.
- **Create** — To create an alert message when the content of an email message is replaced due to a rule being triggered. See *Create an alert* for more instructions.
- **View/Hide** — To display or hide the preview of the alert message. If the preview is hidden, clicking this link displays it. If the preview is displayed, clicking this link hides it.

- 6 In **DLP and Compliance rules and associated actions**, click **Add rule**.

The **DLP and Compliance Rules** page appears.

- 7 In **Specify actions for rule**, select the language from the **Select a Language** drop-down menu.

You can also view and edit all supported locale dictionaries. (The supported locales are Chinese Simplified, French, German, Japanese, and Spanish.)

For example, when MSME is installed in the German locale, you can still view and edit other supported locale dictionaries. Any new category that you create is available for all supported locales.

- 8 In **Specify actions for rule**, select a rule group from the **Select rule group** drop-down menu that triggers an action, if one or more of its rules are broken. Each phrase can have a **Score** set for a category, under **DLP and Compliance Scanner Phrase**.

For some rule groups, you might need to specify these options:

- **Threshold score** — To specify the maximum threshold score upon which the scanner triggers.
- **Max Term Count** — To specify the maximum number of times this rule group can be triggered. Exceeding this count triggers the scanner to take the specified action.

The equation for current **Threshold score** = **Score** x Term Count (instance). A rule is triggered when the value equals or exceeds the **Threshold score**.

To understand how **Threshold score** and **Max Term Count** helps in triggering a rule, let us consider an example on Pascal Language dictionary. Consider that you have set the **Score** for the **DLP and Compliance Scanner Phrase** "PAnsiChar" to 5.

Under **Select rule group**, if you have selected **Pascal Language** dictionary, and set the value for:

- **Threshold score** = 15
- **Max Term Count** = 4

If "PAnsiChar" is found twice in the code, the current threshold score becomes 10, and the rule is not triggered.

If "PAnsiChar" is found five times in the code, the current threshold score will still be calculated as **Score** x **Max Term Count** which is $5 * 4 = 20$. This value is greater than the defined threshold score. So, the rule is triggered.

Consider that you have modified the **Score** for "PAnsiChar" to 8. If the phrase "PAnsiChar" is found thrice in the code, the current threshold score becomes 24. Now the rule will be triggered as it exceeded the specified **Threshold score**.

If there are multiple rules, the **Threshold score** is the combined value of all the rules for a dictionary.



A rule will be triggered only when the value equals or exceeds the **Threshold score** and is not triggered even if the instance of phrase exceeds the **Max Term Count** value in an email.

- 9 From **If detected, take the following action:**, select the DLP and compliance scanner actions that must be taken if some content in an email message is detected as noncompliant.
- 10 From **And also**, select one or more actions.
- 11 Click **Save** to apply the settings and return to the policy settings page.
- 12 Click **Apply** to configure these settings to a policy.

Configure file filtering settings

Configure settings in a policy to detect files based on their name, type, or size and take necessary actions.

Task

- 1 From **Policy Manager**, select a submenu item that has the **File Filtering** scanner.
The policy page for the submenu item appears.
- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **File Filtering**.
- 4 In **Activation**, select **Enable** to activate the file filtering scanner settings for the selected submenu item.



- If you are configuring settings for a subpolicy, select **Use configuration from parent policy** to inherit settings from the parent policy.
- If you add a scanner to the policy, you can specify a time slot when to enable the scanner, using **What time would you like this to apply** drop-down list.

- 5 In **Alert Selection**, click:
 - **Create** — To create an alert message when the attachment of an email message is replaced due to a rule being triggered. See *Create an alert* for more instructions.
 - **View/Hide** — To display or hide the preview of the alert message. If the preview is hidden, clicking this link displays it. If the preview is displayed, clicking this link hides it.

- 6 In **File filtering rules and associated actions**, from the **Available rules** drop-down menu, select an available rule. If you want to create new file filtering rules, select **<Create new rule...>**. See *Configure file filtering rules* for more instructions on how to create new file filtering rules.

File filtering settings can block restricted files such as .exe files that come as an email attachment. If the .exe file is sent as a password-protected .zip file, although the **Password-Protected Files** setting is configured to allow the file, the file filtering rule can block the file.

Sometimes you might need to allow the legitimate restricted files that come as a password-protected .zip file. To allow the password-protected .zip file that contains restricted files such as .exe files, you must add the **Password protect bypass rule** from the **Available rules** drop-down list.



Make sure that this rule is the first rule in the list. If the rule is already listed at a different level, delete the rule, then select the rule from the **Available rules** drop-down list.



Make sure that you create separate file filtering rules for each category such as file name, type, and size.

- 7 Click **Change** to specify actions that must be taken when a file/attachment in an email message triggers the scanner.
- 8 Click **Delete**, to remove an existing rule from the policy.
- 9 Click **Apply** to configure these settings to a policy.

Configure mail URL reputation settings

Configure the **Mail URL reputation** settings to detect malicious URLs in the email body.

When enabled, MSME scans each URL in the email body, gets the reputation score, compares the score with the defined threshold, and takes appropriate action.

The software processes the message before it enters the organization by removing the URLs from the email body. If an email contains multiple URLs, and one URL among them exceeds the defined threshold, action is taken on the email according to the configuration.

Enabling this feature protects your system from threats such as denial-of-service (DoS) attack, phishing links, URLs that contain malware, or unwanted URLs.

The Mail URL reputation feature is available for these policies:

- **On-Access**
- **On-Demand default**, and
- **On-Demand (Full Scan)**

Depending on the configuration option that you selected during the software installation, the mail URL reputation is enabled or disabled by default for policies:

- For the **Default configuration** — Disabled for all policies.
- For the **Enhanced configuration** — Enabled only for on-access scanning policies.

When you enable the **Mail URL Reputation** for first time, the software downloads the local cache of URLs from the McAfee GTI server.

For each URL, the software checks with the local database for reputation score and takes appropriate action according to the configuration. If the reputation score is not available in the local database, the software gets the score from the McAfee GTI server. The software checks with the McAfee GTI server and updates the local database at regular intervals. If the local database is not updated for 30 days,

the software downloads the entire database during the next update. Otherwise, the update is incremental. By default, the local database is updated once everyday. You can't modify the storage location of the database.



You can't update the local database using ePolicy Orchestrator because the server needs direct Internet connections. However, if you use the proxy server to download anti-spam rules, the same configuration can be used to download the URL database.

Task

- 1 From **Policy Manager**, select a submenu item that has the **Mail URL Reputation** scanner.



The **Mail URL Reputation** protection is available only for **On-Access**, **On-Demand (Default)**, and **On-Demand (Full Scan)** policies.

- 2 Click **Master policy** or any **Sub-policy** that you want to configure, click **List All Scanners** tab, then click **Mail URL Reputation**.
- 3 From **Activation**, select **Enable**.
 - If you are configuring settings for a subpolicy, select **Use configuration from parent policy** to inherit settings from the parent policy.
 - If you add a scanner to the policy, you can specify when to enable the scanner, using **What time would you like this to apply** drop-down list.
- 4 From the **Options** drop-down list, you can select:
 - **Default Mail URL Settings** — To apply the default threshold values.
 - **Create new set of options** — To define the thresholds value as required.



If you edit the existing settings, make sure that you provide a unique **Instance name** for the scanner settings.

- 5 To define the scanner settings, select **Create new set of options**.
- 6 On the **Mail URL Reputation** page, define these values, then click **Save**.
 - **Instance name**
 - **Higher URL reputation threshold**
 - **Lower URL reputation threshold**
 - **Maximum number of URLs per email**



The **Higher URL reputation threshold** value must always be greater than the **Lower URL reputation threshold** value.



If a URL appears multiple times, the URL counted is 1 and not the number of occurrence. For example, if the email contains 50 URLs and one URL appears 20 times, the sum of URL is 31 and not 50.

- 7 From the **Actions to take** section, click **Edit** to define the actions.



You can also apply the default settings.

8 On the **Mail URL Reputation Actions** page, define these settings for **When Mail URL reputation score is above the higher threshold**, **When Mail URL reputation score is above the lower threshold**, and **When Mail URL lookup count exceeds the limit**.

a From the **Take the following action** drop-down list, select:

- **Replace item with an alert.**
- **Delete message.**
- **Allow through.**

When you select **Replace item with an alert**, select the alert format:

- **Default Mail URL Reputation Alert** — To use the default alert message.
- **Create** — To define the alert message as you required. Type a unique name for the **Alert name**, define the alert message, define the text format from the **Show** drop-down list, then click **Save**.



McAfee recommends that you save the alerts in plain text format, so that the text content can be viewed by all email client.

b From the **And also** section, define these options:

- **Log**
- **Quarantine**
- **Forward Quarantined email**
- **Notify administrator**
- **Notify internal sender**
- **Notify external sender**
- **Notify internal recipient**
- **Notify external recipient**



For definitions of each of these options, see *Actions you can take on detections*.

9 Click **Save** to apply the settings and return to the policy settings page.

10 Click **Apply** to implement these settings to a policy.



You can view the detected URLs from the **Detected Items | Mail URL Reputation** page. Under **View Results** section, you can view the list of detected URLs. Click the **Blocked URLs** under the **Banned Phrases** column for detailed view.

Higher and Lower URL reputation threshold examples

Set the **Higher URL reputation threshold** value to 80 and the **Lower URL reputation threshold** value to 50. If the reputation score of the URL is:

GTI reputation score is	Action
Greater than 80	Action is taken according to the Mail URL reputation settings.
Lesser than 50	MSME allows the email with the URL.
Between 50 and 80	MSME suspects that the URL could be malicious and takes action according to the settings.



The **Highly Suspect** threshold value detects the most dangerous malicious URLs. As you decrease the threshold value, the chances to get false positive are high. False positive – A URL might be legitimate, but the database considers it as a potential malicious URL.

Configure anti-spam settings

Configure settings in a policy to detect spam email messages and take necessary actions.

Task

- 1 From **Policy Manager**, select the submenu item **Gateway** that has the **Anti-Spam** scanner.

The policy page for the submenu item appears.

- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.

- 3 Click **Anti-Spam**.

- 4 In **Activation**, select **Enable** to activate the anti-spam scanner settings for the selected submenu item.



- If you are configuring settings for a subpolicy, select **Use configuration from parent policy** to inherit settings from the parent policy.
- If you add a new scanner to the policy, you can specify a time slot when to enable the scanner, using **What time would you like this to apply** drop-down list.

- 5 In the **Options** drop-down list, select an existing scanner setting or **<create new set of options>**.

The **Anti-Spam Settings** page appears.

- 6 In **Instance name**, type a unique name for the anti-spam scanner setting instance. This field is mandatory.

- 7 In **Options** tab, under **Scoring**, type the values for:

- **High score threshold** — If the overall spam score is 15 or more.
- **Medium score threshold** — If the overall spam score is from 10 to 15.
- **Low score threshold** — If the overall spam score is from 5 to 10.



To use the default values of spam scores, select the **Use default** option. These default settings have been carefully optimized to maintain the balance between a high spam detection rate and a low false positive rate. In the unlikely event that you need to change these settings, a technical notice is available from Technical Support.

- 8 In **Reporting**, under the **Spam reporting threshold is** drop-down list, select **High**, **Medium**, **Low**, or **Custom** to specify the point at which an email message should be marked as spam.

- 9 In **Custom score**, type a specific spam score at which email messages should be marked as spam. This field is enabled only if you select **Custom** from **Spam reporting threshold is** drop-down list.

- 10 Select or deselect **Add prefix to subject of spam messages** as required.

- 11 From the **Add a spam score indicator** drop-down list, select:

- **Never** - To have the Internet header of an email message without the spam score indicator.
- **To spam messages only** — To add a spam score indicator to the Internet header of spam email messages only.

- **To non-spam messages only** — To add a spam score indicator to the Internet header of non-spam email messages only.
- **To all messages** — To add a spam score indicator to the Internet header of all email messages.



Spam score indicator is a symbol used in the spam report that is added to the email message's Internet headers to indicate the amount of potential spam contained in an email.

12 From the **Attach a spam report** drop-down list, select:

- **Never** - To display an email message without the spam score indicator.
- **To spam messages only** — To add a spam report to spam email messages only.
- **To non-spam messages only** — To add a spam report to non-spam email messages only.
- **To all messages** — To add a spam report to all email messages.

13 Select or deselect **Verbose reporting** to specify whether verbose reporting is required or not. Verbose reporting includes the names and descriptions of the anti-spam rules that have been triggered.



Selecting **Never** for **Attach a spam report** disables **Verbose reporting**.

14 On the **Advanced** tab, use:

- **Maximum message size to scan (KB)** — To specify the maximum size of an email message (in kilobytes) that can be scanned. You can type a size up to 999,999,999 kilobytes, although typical spam email messages are small. Default value is 250 KB.
- **Maximum width of spam headers (Bytes)** — To specify the maximum size (in bytes) that the spam email message header can be. The minimum header width that you can specify is 40 characters and the maximum is 999 characters. Default value is 76.



Spammers often add extra information to headers for their own purposes.

- **Maximum number of reported rules** — To specify the maximum number of anti-spam rules that can be included in a spam report. The minimum number of rules you can specify is 1 and the maximum is 999. Default value is 180.
- **Header name** — To specify a different name for the email header. You can use this email header and its header value (below) when tracking email messages and applying rules to those messages. These fields are optional, and accept up to 40 characters.
- **Header value** — To specify a different value for the email header.
- **Add header** — To specify that the header should be added to none of the email messages, all email messages, only spam email messages or only to non-spam email messages.
- Select or deselect the **Use alternative header names when a mail is not spam** option as required.

15 In **Mail Lists** tab, under **Blacklisted senders**, **Whitelisted senders**, **Blacklisted recipients** and **Whitelisted recipients**, type the email addresses of the blacklisted and whitelisted senders and recipients.

Email messages sent to or from an email address on a blacklist are treated as spam, even if they do not contain spam-like characteristics. Email messages sent to or from email addresses on a whitelist are not treated as spam, even if they contain spam-like characteristics.



Click **Add** to add email addresses to a list and the checkbox beside each address to specify whether it is enabled or not. Click **Delete All** to remove an email address from the list. You cannot add the same email address more than once. You can use wildcard characters to match multiple addresses.

- 16 In **Rules** tab, enter the rule name and select **Enable rule** to activate it. Click **Add** to display a list of available rules.



Click **Reset** to return to the default anti-spam settings.

- 17 In the list, against each rule, click **Edit** to modify the rule.
- 18 Click **Delete** to remove the rule.
- 19 Click **Save** to return to the policy page.
- 20 In **Actions to take if spam is detected**, click **Edit**. In the following tabs, specify the anti-spam scanner actions that must be taken if a spam is detected:
 - **High Score**
 - **Medium Score**
 - **Low Score**
- 21 Click **Save** to apply the settings and return to the policy settings page.
- 22 Click **Apply** to configure these settings to a policy.

Tasks

- [Import or export blacklists and whitelists on page 101](#)
Import or export blacklists and whitelists for backup or use on any other Exchange server.

Import or export blacklists and whitelists

Import or export blacklists and whitelists for backup or use on any other Exchange server.

Task

- 1 From **Policy Manager**, select the submenu item **Gateway** that has the anti-spam scanner.
The policy page for the submenu item appears.
- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **Anti-Spam**.
- 4 From **Options**, click the link **Block list and allow list**.
The **Anti-Spam Settings** page appears.
- 5 Click the **Mail Lists** tab.
- 6 Select the required list from:
 - **Blacklisted senders**
 - **Whitelisted senders**
 - **Blacklisted recipients**
 - **Whitelisted recipients**
- 7 To import a list, click **Import**. In the pop-up window, click **Browse** to navigate to the required `.cfg` file, then click **OK**.

8 To export a list, click the link **Export**.



Click **Delete** to remove a list from the database.

9 Click **Save** to apply the settings and return to the policy settings page.

Configure anti-phishing settings

Configure settings in a policy to block phishing messages using the anti-spam rules and engine, and take necessary actions.

Task

1 From **Policy Manager**, select the submenu item **Gateway** that has the **Anti-Phishing** scanner.

The policy page for the submenu item appears.

2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.

3 Click **Anti-Phishing**.

4 In **Activation**, select **Enable** to activate the anti-phishing scanner settings for the selected submenu item.



- If you are configuring settings for a subpolicy, select **Use configuration from parent policy** to inherit settings from the parent policy.
- If you add a new scanner to the policy, you can specify a time slot when to enable the scanner, using **What time would you like this to apply** drop-down list.

5 In the **Options** drop-down list, select an existing scanner setting or **<create new set of options>**.

The **Anti-Phishing Settings** page appears.

6 In **Instance name**, type a unique name for the anti-phishing scanner setting instance. This field is mandatory.

7 In **Reporting Options**, select or deselect these options as required:

- **Add prefix to subject of phishing messages** — To specify that you want to add text to the start of the subject line of any email message that probably contains phishing information.
- **Add a phish indicator header to messages** — To specify whether a phish indicator is added to the Internet header of any email message that probably contains phishing information.
- **Attach a phish report** — To specify whether a phish report should be generated and added to the email message detected as phish.
- **Verbose reporting** — To specify whether the names and a detailed description of the anti-phish rules that triggered, is included in the email message. This option is available only if you select the **Attach a phish report** option.

8 Click **Save** to return to the policy page.

9 In **Actions to take**, click **Edit** and specify the antiphish scanner actions that must be taken if a phish is detected.

10 Click **Save** to apply the settings and return to the policy settings page.

11 Click **Apply** to configure these settings to a policy.

Manage filter settings for a policy

Enable or disable filter options, then specify an appropriate action to take on the detected item when a policy is triggered.

The available filters are:

- **Corrupt Content**
- **Protected Content**
- **Encrypted Content**
- **Signed Content**
- **Password-Protected Files**
- **Mail Size Filtering**
- **Scanner Control**
- **MIME Mail Settings**
- **HTML Files**

Tasks

- [Configure corrupt content settings on page 103](#)
Configure settings in a policy to identify emails with corrupt content and take necessary actions.
- [Configure protected content settings on page 104](#)
Configure settings in a policy to identify emails with protected content and take necessary actions.
- [Configure encrypted content settings on page 104](#)
Configure settings in a policy to identify emails with encrypted content and take necessary actions.
- [Configure signed content settings on page 105](#)
Configure settings in a policy to identify emails with signed content and take necessary actions.
- [Configure password-protected file settings on page 105](#)
Configure settings in a policy to identify emails with password-protected archives and take necessary actions.
- [Configure mail size filtering settings on page 106](#)
Mail size filtering settings in a policy detect emails based on their size, number of attachments, and attachment size.
- [Configure scanner control settings on page 107](#)
Configure settings in a policy that defines the nesting level, expanded file size, and maximum scan time that is allowed, when an email is scanned.
- [Configure MIME mail settings on page 108](#)
Configure settings in a policy to identify encoded MIME messages and take necessary actions.
- [Configure HTML file settings on page 110](#)
Configure settings in a policy to scan for elements or remove executables such as ActiveX, Java applets, VBScripts in HTML components in an email.

Configure corrupt content settings

Configure settings in a policy to identify emails with corrupt content and take necessary actions.

The content of some email messages can become corrupt and cannot be scanned. Corrupt content policies specify how email messages with corrupt content are handled when detected.

Task

- 1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **Corrupt Content**.



If you add a new filter to the policy, you can specify a time slot when to enable the filter, using **What time would you like this to apply** drop-down list.

- 4 In **Actions**, click **Edit** to specify the filter actions that must be taken when corrupt content is detected.
- 5 Click **Save** to return to the policy page.
- 6 Click **Apply** to configure these settings to a policy.

Configure protected content settings

Configure settings in a policy to identify emails with protected content and take necessary actions. Protected content policies specify how email messages with protected content are handled when detected.

Task

- 1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **Protected Content**.



If you add a new filter to the policy, you can specify a time slot when to enable the filter, using **What time would you like this to apply** drop-down list.

- 4 In **Actions**, click **Edit** to specify the filter actions that must be taken when protected content is detected.
- 5 Click **Save** to return to the policy page.
- 6 Click **Apply** to configure these settings to a policy.

Configure encrypted content settings

Configure settings in a policy to identify emails with encrypted content and take necessary actions. Email messages can be encrypted to prevent access by unauthorized parties. Encrypted content uses a *key* and encryption mathematical algorithms to decrypt it. Encrypted content policies specify how encrypted email messages are handled when detected.

Task

- 1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **Encrypted Content**.



If you add a new filter to the policy, you can specify a time slot when to enable the filter, using **What time would you like this to apply** drop-down list.

- 4 In **Actions**, click **Edit** to specify the filter actions that must be taken when encrypted content is detected.

- 5 Click **Save** to return to the policy page.



Encrypted content settings are applicable to encrypted attachments in internal emails and to encrypted internet email messages.

- 6 Click **Apply** to configure these settings to a policy.

Configure signed content settings

Configure settings in a policy to identify emails with signed content and take necessary actions.

Whenever information is sent electronically, it can be accidentally or willfully altered. To overcome this issue, some email software use a digital signature — the electronic form of a handwritten signature.

A digital signature is extra information added to a sender's message that identifies and authenticates the sender and the information in the message. It is encrypted and acts like a unique summary of the data. Typically, a long string of letters and numbers appears at the end of a received email message. The email software then re-examines the information in the sender's message, and creates a digital signature. If that signature is identical to the original, the data has not been altered.

If the email message contains a virus, bad content, or is too large, the software might clean or remove some part of the message. The email message is still valid and can be read, but the original digital signature is 'broken'. The recipient cannot rely on the contents of the email message because the contents might also have been altered in other ways. Signed content policies specify how email messages with digital signatures are handled.

Task

- 1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **Signed Content**.



If you add a new filter to the policy, you can specify a time slot when to enable the filter, using **What time would you like this to apply** drop-down list.

- 4 In **Actions**, click **Edit** to specify the filter actions that must be taken when signed content is detected.
- 5 Click **Save** to return to the policy page.



Signed content settings are applicable to signed emails and attachments.

- 6 Click **Apply** to configure these settings to a policy.

Configure password-protected file settings

Configure settings in a policy to identify emails with password-protected archives and take necessary actions.

Password-protected files cannot be accessed without a password and cannot be scanned for malware. Password-protected files' policies specify how email messages that contain a password-protected file are handled.

Task

- 1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **Password-Protected Files**.



If you add a new filter to the policy, you can specify a time slot when to enable the filter, using **What time would you like this to apply** drop-down list.

- 4 In **Actions**, click **Edit** to specify the filter actions that must be taken when an email message containing password-protected file is detected.



If you set the action as **Allow through**, make sure that the **Password protected bypass rule** under **File filtering rules and associated actions** in **File filtering** scanner settings is the first rule in the list. If the rule is already listed at a different level, delete the rule, then select the rule from the **Available rules** drop-down list.

- 5 Click **Save** to return to the policy page.
- 6 Click **Apply** to configure these settings to a policy.

Configure mail size filtering settings

Mail size filtering settings in a policy detect emails based on their size, number of attachments, and attachment size.

Before you begin

Make sure that on the **On-Access Settings** page, the **Scan Inbound Mails** and **Scan Outbound Mails** options are selected.

You can configure mail size filtering settings for **Gateway** policy and **On-Access** policy separately. Configure the **Gateway** settings for inbound emails and **On-Access** settings for outbound emails. For example:

- To block all inbound emails that contain more than five attachments, configure the **Mail Size Filtering** settings from the **Gateway** policy.
- To block all outbound emails that contain more than three attachments, configure the **Mail Size Filtering** settings from **On-Access** policy.



Mail size filtering for on-access scanning is not applicable for mailbox server role.

Task

- 1 From **Policy Manager**, select a submenu item that has the anti-virus scanner.
The policy page for the submenu item appears.
- 2 Select the policy as required from **On-Access** or **Gateway** policy:
- 3 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 4 Click **Mail Size Filtering**.
- 5 In **Activation**, select **Enable** to activate the email size filter settings for the selected submenu item.



If you add a new filter to the policy, you can specify a time slot when to enable the filter, using **What time would you like this to apply** drop-down list.

- 6 In **Options**, you can use:
 - **Default Settings** — To view a summary of the mail size option set that is used by default.
 - **Default Gateway Settings** — To view a summary of the default mail size option used by gateway policy.

- **<create new set of options>** — To configure mail size filtering options. The options are:
 - **Instance name** — Type a unique name for the mail size filter setting instance. This field is mandatory.
 - **Maximum overall mail size (KB)** — Specify the maximum size (in kilobytes) that an email message can be. You can specify a value from 2 KB to 2 GB, where the default value is 20,000 KB.
 - **Maximum attachment size (KB)** — Specify the maximum size (in kilobytes) that the attachments of an email message can be. You can specify a value from 1 KB to 2 GB, where the default value is 4096 KB.
 - **Maximum number of attachments** — Specify the maximum number of attachments an email message can have. You can specify up to 999, where the default value is 25.
 - **Edit** — To edit the selected option set.
- 7 In **Actions**, click **Edit**. Specify the mail size filter actions to take, if the value exceeds the specified settings for these options:
- **Message Size**
 - **Attachment Size**
 - **Attachment Count**
- 8 Click **Save** to return to the policy page.



Internal emails are not detected by mail size filtering rules.

Configure scanner control settings

Configure settings in a policy that defines the nesting level, expanded file size, and maximum scan time that is allowed, when an email is scanned.

Task

- 1 From **Policy Manager**, select a submenu item that has the scanner.
The policy page for the submenu item appears.
- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **Scanner Control**.



If you add a new filter to the policy, you can specify a time slot when to enable the filter, using **What time would you like this to apply** drop-down list.

- 4 In **Options**, click **<create new set of options>**.
- 5 In **Instance name**, type a unique name for the scanner control filter setting instance. This field is mandatory.
- 6 In **Maximum nesting level**, specify the level to which the scanner should scan, when an attachment contains compressed files, and other compressed files within. You can specify a value from 2–100, where the default value is 10.
- 7 In **Maximum expanded file size (MB)**, specify the maximum size allowed for a file when it is expanded for scanning. You can specify a value from 1–2047, where the default value is 10.
- 8 In **Maximum scan time (minutes)**, specify the maximum time allowed to scan any file. You can specify a value from 1–999, where the default value is 1.

- 9 Click **Save** to return to the policy page.
- 10 In **Alert selection**, you can select which alert to use when a scanner control option is triggered. You can use:
 - **Create** — To create a new alert message for this policy.
 - **View/Hide** — To display or hide the alert text. If the text is hidden, clicking this link displays it. If the text is displayed, clicking this link hides it.
- 11 In **Actions**, click **Edit** to specify the actions to take, if the value exceeds the specified settings for these options:
 - **Maximum nesting level**
 - **Maximum expanded file size (MB)**
 - **Maximum scanning time (minutes)**
- 12 Click **Save** to return to the policy page.
- 13 Click **Apply** to configure these settings to a policy.

Configure MIME mail settings

Configure settings in a policy to identify encoded MIME messages and take necessary actions.

Multipurpose Internet Mail Extensions (MIME) is a communications standard that enables the transfer of non-ASCII formats over protocols (such as SMTP) that supports only 7-bit ASCII characters.

MIME defines different ways of encoding the non-ASCII formats so that they can be represented using characters in the 7-bit ASCII character set.

Task

- 1 From **Policy Manager**, select a submenu item that has the filter.

The policy page for the submenu item appears.

- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **MIME Mail Settings**.



If you add a new filter to the policy, you can specify a time slot when to enable the filter, using **What time would you like this to apply** drop-down list.


- 4 In **Options**, select **<create new set of options>**.

The **Mail Settings** page appears.

- 5 In **Instance name**, type a unique name for the MIME email filter setting instance. This field is mandatory.


- 6 In **Options** tab, type a **Prefix to message subject**.
 - a In **Preferred re-encoding of attachments in a MIME message**, select a re-encoding method that is used when re-encoding attachments in MIME messages from the options available.
 - b In **Preferred re-encoding of modified subject headers**, select a re-encoding method that is used when re-encoding the subject headers in the MIME messages from the options available.
 - c In **If re-encoding a subject header fails**, select one of these options:
 - **Treat as an error** — If the MIME message is bounced.
 - **Fallback to UTF-8** — If the MIME message is encoded into UTF-8.

- 7 In **Advanced** tab, select one of these encoding methods to use while encoding the text part of an email message:
 - **Quoted-Printable**, which is best suited for messages that mainly contain ASCII characters, but also contains some byte values outside that range.
 - **Base64**, which has a fixed overhead and is best suited for non-text data, and for messages that do not have a lot of ASCII text.
 - **8-Bit**, which is best suited for use with SMTP servers that support the 8BIT MIME transport SMTP extension.


 You can perform *step 6b* only if you select **Re-encode using the original encoding scheme** or **Re-encode using the following character set** from **Preferred re-encoding of modified subject headers**.

 - a Select or deselect **Do not encode if text is 7-bit** as required.
 - b In **Default decode character set**, select a character set that should be used for decoding when one is not specified by the MIME headers.
 - c In **Maximum number of MIME parts**, specify the maximum number of MIME parts that can be contained in a MIME message. Default value is 10000 MIME parts.
 - d In **Header corruption in a MIME message**, select the required option.
 - e In **NULL characters in the headers of a MIME message**, select the required option.
 - f In **Quoted-printable characters encoding in a MIME message**, select the required option.

- 8 In **MIME Types** tab, specify which MIME types should be treated as text attachments and which, as binary attachments.

 Click **Add** to add the MIME types to the list or **Delete** to delete a MIME type from a list. Duplicate entries are not allowed.

- 9 In **Character Sets** tab, select **Character set** and **Alternatives**, deselect the **Fixed** checkbox, and click **Add** to specify an alternative character set mapping to the one specified in the MIME message.

 Click **Edit** to edit character mappings, **Delete** to delete character mappings and click **Save** to apply any changes you have made to the character mappings.
The **Save** option is available only when you click **Edit**.

- 10 Click **Save**.

- 11 In **Alert selection**, you can select which alert to use when a MIME type is blocked. You can use:
 - **Create** — To create a new alert message for this policy.
 - **View/Hide** — To display or hide the alert text. If the text is hidden, clicking this link displays it. If the text is displayed, clicking this link hides it.
- 12 In **Incomplete message actions**, click **Edit** to specify the filter actions that must be taken when a partial MIME or external MIME type is encountered.
- 13 Click **Save** to return to the policy page.
- 14 Click **Apply** to configure these settings to a policy.

Configure HTML file settings

Configure settings in a policy to scan for elements or remove executables such as ActiveX, Java applets, VBScripts in HTML components in an email.

If any of this content is found in HTML, it is removed. This filter works only if Content Scanner is enabled.

Task

- 1 From **Policy Manager**, select a submenu item that has the filter.
The policy page for the submenu item appears.
- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **HTML Files**.
- 4 In **Options**, click **<create new set of options>**.
The **HTML Files** page appears.
- 5 In **Instance name**, type a unique name for the filter setting instance. This field is mandatory.
- 6 In **Scan the following elements**, select any of these option(s):

- **Comments** — To scan for comment elements in the HTML message. For example:

```
<!-- comment text --!>
```

- **Metadata** — To scan for metadata elements in the HTML message. For example:

```
< META EQUI="Expires" Content="Tue, 04 January 2013 21:29:02">
```

- **Links URLs ("**<a href=...**")** — To scan for URL elements in the HTML message. For example:

```
<a HREF="McAfee.htm">
```

- **Source URLs ("**<img src=...**")** — To scan for source URL elements in the HTML message. For example:

```
<IMG SRC="..\..\images\icons\mcafee_logo_rotating75.gif">
```

- **JavaScript/VBScript** — To scan for JavaScript or Visual Basic script in the HTML message. For example:

```
<script language="javascript" scr="mfe/mfe.js">
```

7 In **Remove the following executable elements**, select any of these option(s):

- **JavaScript / VBScript** — To remove JavaScript or Visual Basic script elements from the HTML message. For example:

```
<script language="javascript" src="mfe/mfe.js">
```

- **Java applets** — To remove Java applet elements from the HTML message. For example:

```
<APPLET code="XYZApp.class" codebase="HTML . . . . ."></APPLET>
```

- **ActiveX controls** — To remove ActiveX control elements from the HTML message. For example:

```
<OBJECT ID="clock" data="http://www.mcafee.com/vscan.png" type="image/png"> VirusScan  
Image </OBJECT>
```

- **Macromedia Flash** — To remove Macromedia Flash elements from the HTML message. This option gets enabled if you have selected ActiveX controls. For example:

```
<EMBED SCR="somefilename.swf" width="500" height="200">
```

8 Click **Save** to return to the policy page.

9 Click **Apply** to configure these settings to a policy.

Manage miscellaneous settings for a policy

Create or edit miscellaneous settings such as alerts and disclaimers, that are applied when a policy is triggered.

The available options are:

- **Alert Settings**
- **Disclaimer Text**

Tasks

- [Configuring alert message settings on page 111](#)
Configure settings in a policy to notify the end user with an alert message, when a detection occurs.
- [Configuring disclaimer text settings on page 112](#)
Configure disclaimer text settings in a policy which is a piece of text, typically a legal statement that is added to all outbound email messages.

Configuring alert message settings

Configure settings in a policy to notify the end user with an alert message, when a detection occurs.

Task

- 1 From **Policy Manager**, select a submenu item that has the scanner.
The policy page for the submenu item appears.
- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **Alert Settings**.

4 Select **Enable** to activate the alert message settings for the selected submenu item.



- If you are configuring settings for a subpolicy, select **Use configuration from parent policy** to inherit settings from the parent policy.
- If you add a new alert message setting to the policy, you can specify a time slot when to enable, using **What time would you like this to apply** drop-down list.

5 In **Options**, select the default alert settings available or select **<create new set of options>** to define your alert settings.



For step-by-step instructions on how to create a new alert, see the *Create a new alert* section.

6 Click **Edit** to modify an existing alert.

The **Alert Settings** page appears.

7 Select **HTML** or **Plain text** as the **Alert format**.

8 From the **Character encoding** drop-down menu, select a required character set.

9 In **Alert filename**, specify the file name for this alert, including the appropriate HTML (.htm) or plain text (.txt) file extension.

10 Select or deselect **Enable alert headers** to enable the use of an alert header.

11 In the **Alert header** text entry box, type the header for the alert.

12 From **Show**, select **HTML content (WYSIWYG)** or **HTML content (source)** depending on whether the HTML text should be shown as compiled code or source code in the **Alert header**.



The **Show** option is only available if you have selected **HTML** as the alert message format.

13 Select **Enable alert footers** to enable the use of an alert footer as needed.

14 In the **Alert footer** text entry box, type the footer for the alert.

15 From **Show**, select **HTML content (WYSIWYG)** or **HTML content (source)** depending on whether the HTML text should be shown as compiled code or source code in the **Alert footer**.



The **Show** option is only available if you have selected **HTML** as the alert message format.

16 Click **Save** to return to the policy page.

17 Click **Apply** to configure these settings to a policy.

Configuring disclaimer text settings

Configure disclaimer text settings in a policy which is a piece of text, typically a legal statement that is added to all outbound email messages.

When assigned to a policy, all emails leaving the exchange organization through the MSME server will have the disclaimer text applied, based on the settings configured.



Disclaimer text settings are applicable only on Microsoft Exchange Transport servers.

Task

- 1 From **Policy Manager**, select a submenu item that has the scanner.

The policy page for the submenu item appears.

- 2 Click **Master policy** or any subpolicy you want to configure, then click **List All Scanners** tab.
- 3 Click **Disclaimer Text**.
- 4 Select **Enable** to activate the disclaimer text settings for the selected submenu item.



- If you are configuring settings for a subpolicy, select **Use configuration from parent policy** to inherit settings from the parent policy.
- If you add a new disclaimer text setting to the policy, you can specify a time slot when to enable, using **What time would you like this to apply** drop-down list.

- 5 In **Options**, select **<create new set of options>**. The **Disclaimer Text** page appears.
- 6 In **Instance name**, type a unique name for the disclaimer text setting instance. This field is mandatory.
- 7 From **Disclaimer format**, you can select:
 - **HTML** — To specify whether you want the disclaimer to appear in HTML format in the notification email.
 - **Plain text** — To specify whether you want the disclaimer to appear in plain text format in the notification email.
- 8 In **Edit Disclaimer content**, type the disclaimer text message.
- 9 From **Show**, select **HTML content (WYSIWYG)** or **HTML content (source)** depending on whether the HTML text should be shown as compiled code or source code in the **Alert footer**.



The **Show** option is only available if you have selected **HTML** as the disclaimer text format.

- 10 From the **Insert disclaimer** drop-down list, select **Before any message text**, **After any message text** or **As an attachment** depending on where and how the disclaimer text should be inserted in the email message.
- 11 Click **Save** to return to the policy page.



Disclaimers are applicable only to outbound email messages.

- 12 Click **Apply** to configure these settings to a policy.

6

Settings and diagnostics

Settings & Diagnostics has menus for MSME feature enablement and disablement, feature configuration, feature administration and logs. Configure these settings based on your organization's security policies.

To modify or view MSME product settings, from the product's user interface, click **Settings & Diagnostics**. This table briefly explains when to configure these settings:

Table 6-1 Settings & Diagnostics


Use...	To...
On-Access Settings  The On-Access Settings are available only on Microsoft Exchange 2007/2010 server. As Microsoft VSAPI support is removed from Microsoft Exchange 2013, the On-Access VSAPI and Background scan settings feature is disabled on Exchange 2013 server.	Define what to do with an email should a scan fail. The options are: <ul style="list-style-type: none">• Allow Through• Remove It also has submenus for enabling or disabling settings for: <ul style="list-style-type: none">• Microsoft Virus Scanning API (VSAPI)• Background Scan Settings• Transport Scan Settings
On-Demand Settings	Modify the password credential for the MSMEODUser and to synchronize the password update with the Active Directory and other exchange servers.
Mailbox Exclusion Settings	Define which mailboxes, folders, or subfolders to exclude from On-Access VSAPI scanning.
Notifications	<ul style="list-style-type: none">• Define an administrator email account to receive notifications or send notification emails to specific reviewers or DLs, when an email is detected.• Create customized notification emails that go out to users when an email is quarantined.• Define product health alerts that are emailed to the administrator on a daily basis or immediately when specific events occur, such as issues with the Postgres database or loading a service fails.
Anti-Spam	<ul style="list-style-type: none">• Define settings for junk email folder in which to forward a spam on an Edge Transport (Gateway) server.• Enable or disable McAfee GTI message reputation feature.• Enable or disable McAfee GTI IP reputation feature.

Table 6-1 Settings & Diagnostics (continued)

Use...	To...
Detected Items	Configure and manage quarantine repositories, using either: <ul style="list-style-type: none"> • McAfee Quarantine Manager — To configure communication settings between MSME and MQM server (if any). • Local Database — To manage and administer the local quarantine database activities such as purge and optimization.
User Interface Preferences	Define settings in the Dashboard such as the refresh rate, report settings, unit scale of graphics, reporting interval, graph and chart settings.
Diagnostics	Define settings for debug event and product logs, including information on how large the logs are and where they are stored. Diagnostics settings include: <ul style="list-style-type: none"> • Debug Logging • Event Logging • Product Log • Error Reporting Service
Product Log	View the Product Log and filter the output by date, type or description.
DAT Settings	Keep older DATs instead of over-writing with each update and define how many detection definition files to maintain.
Import and Export Configuration	Set up your current MSME server with the same configurations as one already built, restore default or enhanced settings, or create SiteLists to point to DAT download sites.
Proxy Settings	Configure or modify proxy settings for the McAfee Anti-Spam Rules Updater Service .

If you modify any of these settings, make sure you click **Apply** to save the changes. The background color behind **Apply**, changes to:



- Yellow — If you have changed the existing setting or the change is still not applied.
- Green — If you have not changed the existing setting or the change is applied.

Contents

- ▶ *On-Access settings*
- ▶ *On-Demand settings*
- ▶ *Configure mailbox exclusion settings*
- ▶ *Notification settings*
- ▶ *Anti-spam settings*
- ▶ *Detected items settings*
- ▶ *User interface preferences settings*
- ▶ *Diagnostics settings*
- ▶ *View product logs*
- ▶ *Configure DAT settings*
- ▶ *Import and export configuration settings*
- ▶ *Configure anti-spam proxy settings*

On-Access settings

On-access scanning is triggered at the Gateway or every time email messages are accessed, to determine if an item is detected by the on-access policy. On-access scanning is also known as real-time scanning.

Each scan has its own benefit based on the Exchange server role where MSME is installed. This table helps you understand the types of scan, its function, and when each scan is applicable:

Exchange Server role	Applicable policies	Scan type	Description
Edge Transport or Hub Transport	<ul style="list-style-type: none"> On-Access Gateway 	On-Access Transport scan	Scans for threats before it reaches the Mailbox server. By enabling this, MSME can detect threats at the perimeter of your organization and thus reduce the load on the Mailbox server.
Mailbox	<ul style="list-style-type: none"> On-Access 	On-Access VSAPI scan	Scans for threats when an email is accessed by the user with an email client such as Outlook.
		Proactive scan	Scans for threats before an email is written to the Microsoft Exchange Information Store.
		Outbox scan	Scans for threats in an email that is in the Outbox folder.
		Background scan	A low-priority scan which scans for threats on all Exchange databases in the background.

From the **General** section, define an action to take when a scan failure occurs.

A scan failure can occur for any of these reasons:

- **On Generic failure** — Scanner is not able to scan a particular file.
- **On Product failure** — Scanning fails due to incorrect DAT or engine, or incorrect spam rules.


Some of the reasons might be due to technical issues such as:

- Scan timeout
- Scan Engine failed to load
- DAT issues
- Incorrectly formatted emails

For example, if there is a DAT mismatch in the registry and actual location (`\bin\DATs`), a scan failure will occur.

If there is a scan failure, an action will be triggered based on the settings specified under **Settings & Diagnostics | On-Access Settings | General**.

Table 6-2 Option definitions

Option	Definition
On Generic Scan Failure	<ul style="list-style-type: none"> • Allow Through — Allows the email message to the intended recipient, when a scan failure occurs. • Remove — Removes the email message, when a scan failure occurs.
On Product Scan Failure	<ul style="list-style-type: none"> • Allow Through — Allows the email message to the intended recipient, when a scan failure occurs. • Remove — Removes the email message, when a scan failure occurs.
 McAfee recommends that you always set this option to Allow Through to avoid legitimate emails being quarantined should a scan failure occur. By default, this option is set to Allow Through , so that emails are not lost during a scan failure.	

The other categories in the **On-Access Settings** page are:

- **Microsoft Virus Scanning API (VSAPI)**
- **Background Scan Settings**
- **Transport Scan Settings**



For more information on the types of scan, see McAfee KnowledgeBase article [KB51129](#).

Microsoft Virus Scanning API (VSAPI) settings

Microsoft VSAPI allows MSME to scan emails when they are accessed by the end-user using any email client.

In Microsoft Exchange, emails are stored in a database called Exchange Information Store. When a new mail is received, the Exchange server notifies the outlook client about a change. This is when On-access scan is triggered.



This feature is available only on Microsoft Exchange 2007/2010 Server with Mailbox role.

Table 6-3 Option definitions

Option	Definition
Enable	Select to scan email messages only when they are accessed by the end-user using an email client such as Outlook. This feature scans emails that are already available in the Microsoft Exchange Information Store or if there is a mismatch in the AV stamp.
Proactive scanning	Select to scan email messages before it is being written to the Microsoft Exchange Information Store. Enable this feature in these situations: <ul style="list-style-type: none"> • Where MSME is not configured on the HUB Transport server and if an infected email reaches the Mailbox server, it will be detected before it is being written to the Exchange Information Store. • Usually content posted to a public folder database is usually not routed through a HUB Transport server. In order to ensure that the content is scanned before it gets to the store, it is recommended that you enable proactive scanning for public folder databases.

Table 6-3 Option definitions (continued)

Option	Definition
Outbox Scanning	Select to scan email messages in the Outbox folder. MSME scans the email in the Outbox itself, even before the email reaches the HUB Transport server, thus reducing the load on the HUB server.
Lower Age Limit (seconds)	Specify a value, where emails received within the specified duration are only scanned. Emails received before the specified time will not be scanned. By default, the value is set to 86400 seconds, which is equal to one day.
Scan Timeout (seconds)	Maximum time allowed to scan an email. If scanning an email exceeds the specified value, the action specified under Settings & Diagnostics On-Access Settings General On Scan Failure will occur. By default, the value is set to 180 seconds.
Number of Scan Threads	Specify the number of pool threads used to process items in the On-access and Proactive scan queue. The default value is $2 * \langle \# \text{ of processors} \rangle + 1$. McAfee recommends that you select the Default checkbox for better performance.

Background scan settings

Methodically scan the desired messages stored in a database. For each database, a thread running at below normal priority enumerates all the folders in the database and then requests MSME to scan the content as appropriate.


Table 6-4 Option definitions

Option	Definition
Enable	Select to scan the entire database in the background, after a virus outbreak. By default this option is disabled.
Schedule	Schedule when to enable or disable background scanning. <ul style="list-style-type: none"> Click Enable At to specify when to start background scanning. Click Disable At to specify when to stop background scanning. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <ul style="list-style-type: none"> Schedule this during non-peak hours of the day or during weekends. If you have not created a schedule, background scan starts whenever a DAT update occurs. </div>
Only Messages With Attachment	Select to scan only email messages with attachments. This feature is useful if you are concerned about a specific virus that spreads through attachments. As the email messages having attachments are more vulnerable and have malicious content, any viruses or executables will be replaced in this task. Enabling this feature saves time, as MSME scans only emails with attachments.
Only Un-Scanned Items	Select to scan email messages that are unscanned. Enable this in scenarios where you had Microsoft VSAPI disabled on the Mailbox server for sometime and want to scan the unscanned items.
Force Scan All	Select to scan items irrespective of whether the item has an AV scan stamp or not.
Update Scan Stamp	Select to update email messages with the latest AV stamp.
From Date	To perform background scanning only on emails received from the date specified.
To Date	To perform background scanning only on emails received until the date specified. Select Till Date to scan emails until the current system date.

Transport scan settings

Transport scanning allows you to scan SMTP traffic before it enters the Exchange information store. SMTP Transport scanning can perform scanning of routed email messages that are not destined for the local server and can stop delivery of messages.

Table 6-5 Option definitions

Option	Definition
Enable	Select to enable scanning at the Exchange Transport level. By default, this option is enabled.  This option will work only on Microsoft Exchange servers with Edge Transport, Hub Transport or Mailbox + Hub role.
Transport Scan Stamp	Select to apply DAT signatures to the email header, so that the emails are not scanned again at the Mailbox role. Recommended settings: If you have enabled Transport scan, make sure to enable this option as well.
Direction Based Scanning	Configure on-access scan settings based on the email flow.
Scan Inbound Mails	Select to scan any email message that comes into the Exchange server or Exchange organization.
Scan Outbound Mails	Select to scan any email message that leaves your Exchange server or Exchange organization. Email messages are designated as outbound, if at least one recipient has an external email address.
Scan Internal Mails	Select to scan email messages that are being routed from one location inside your domain to another location inside your domain. Anything within the Exchange server's Authoritative Domain is considered as an internal domain. Email messages are designated as internal if they originate from inside your domain and all the recipients are located inside your domain.


On-Demand settings


Access the **On-Demand Settings** page to modify the **MSMEODUser** password credentials.

McAfee Security for Microsoft Exchange creates a user **MSMEODUser** in the Active Directory during the product installation on the mailbox server. This user is required to perform on-demand scanning on mailboxes.

To comply with your organization security policy, you might require to update the **MSMEODUser** password at regular intervals.

From the interface, navigate to **Settings & Diagnostics | On-Demand Settings**.


Option	Definition
User Name	MSMEODUser — The user that performs on-demand scanning.  This is a read-only field.
Type password	Type the password.


Option	Definition
Confirm password	Confirm the password.
Reset this password in LDAP also	<p>Select this option to synchronize the password update with the Active Directory and other exchange servers.</p> <p> Check this option only when you initiate the password reset from the On-Demand settings page.</p>

You can update the **MSMEODUser** password in two ways:

- Reset the password in the Active Directory, then update the password in the **On-Demand Settings** page.
- Reset the password from the **On-Demand Settings** page.

Reset the password using Active Directory	Reset the password using On-Demand Settings page
<ol style="list-style-type: none"> 1 Update the password in the Active Directory. 2 Go to any of the mailbox role system within the same Active Directory. 3 Launch the McAfee Security for Microsoft Exchange interface. 4 From Settings & Diagnostics, navigate to the On-Demand settings page, then update the password. 5 Deselect the Reset the password in LDAP also option. 6 Click Apply. 	<ol style="list-style-type: none"> 1 Launch the McAfee Security for Microsoft Exchange interface. 2 From Settings & Diagnostics, navigate to the On-Demand settings page, then update the password. 3 Check the Reset the password in LDAP also option to make sure that the password update is synchronized with the Active Directory. 4 Click Apply.

 For managed systems, you can update the **MSMEODUser** password from ePolicy Orchestrator.

 It might take up to a minute to apply this setting in all exchange servers within the domain. Please run an on-demand scan after updating the password for verification.


For more information about the **MSMEODUser**, see McAfee KnowledgeBase article [KB82332](#).

Configure mailbox exclusion settings

Configure mailboxes or folders that are to be excluded from a VSAPI scan.


Configure mailbox exclusion settings during specific scenarios where:


- Company officials who do not want their emails scanned.
- Company policy that identifies non-scan folders.
- Folders that are to be excluded from scanning.

 McAfee does not recommend excluding mailboxes and cannot be held liable, if you have any mailboxes that are infected due to the exclusion settings.


Task


- 1 Click **Settings & Diagnostics | Mailbox Exclusion Settings**. The **Mailbox Exclusion Settings** page appears.
- 2 To exclude the mailbox or subfolder:

To exclude a mailbox	To exclude a folder in the mailbox
<p>1 From the Available mailboxes pane, select a mailbox, then click >>.</p> <p>The selected mailbox is moved to the Mailboxes to exclude pane. Repeat this step for all mailboxes that are to be excluded from a VSAPI scan.</p> <p>To remove a mailbox from the exclusion list, select a mailbox in the Mailboxes to exclude pane and click << to move the mailbox to the list of Available mailboxes.</p> <div data-bbox="349 688 976 793" style="background-color: #f0f0f0; padding: 5px;">  When a mailbox is added to the Mailboxes to exclude pane, all folders in the mailbox are excluded from scanning. </div>	<p>1 From the Available mailboxes pane, select a mailbox.</p> <p>2 In the Folders within the mailbox to be excluded box, type the folder name to be excluded, then click >>.</p> <p>The selected mailbox folder is moved to the Mailboxes to exclude pane.</p> <p>You can also use wildcard to exclude multiple folders from VSAPI scanning. For more information, see Using wildcard to exclude mailbox folders.</p>

 If you are configuring mailbox exclusions from ePolicy Orchestrator, you need to provide the complete path manually.

- 3 Click **Apply** to save the settings.


 This exclusion overrides the **Outbox Scanning** in the **Microsoft Virus Scanning API (VSAPI)** settings in the **On-Access settings** page that you configured already. For example, if you exclude the outbox scanning for a user, mailbox exclusion setting overrides the global outbox scanning.

 For more information on mailbox exclusion examples, see [Examples of using wildcards for mailbox exclusions](#).

Examples of using wildcards for mailbox exclusions

You can use a comma separator or the wildcard * to exclude folders from VSAPI scanning at mailbox level and at database level.

Table 6-6 Examples

Level...	To exclude...	Configure...
Database level	The Draft folders of all mailboxes in the database.	<ol style="list-style-type: none"> 1 From the product interface, click Settings & Diagnostics Mailbox Exclusion Settings. 2 From the Available mailboxes pane, select the database. 3 In the Folders within the mailbox to be excluded box, type Draft, click >>, then click Apply. The selected mailbox folder is listed in the Mailboxes to exclude pane. <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  You can't select a database for exclusion without specifying folders to exclude. </div>
	All folders in all mailboxes that start with the name person in the database.	<ol style="list-style-type: none"> 1 From the product interface, click Settings & Diagnostics Mailbox Exclusion Settings. 2 From the Available mailboxes pane, select the database. 3 In the Folders within the mailbox to be excluded box, type person*, click >>, then click Apply. The selected mailbox folder is listed in the Mailboxes to exclude pane.
Mailbox level	Multiple folders under a mailbox using a comma separator. For example, you can exclude folders Data1 , Project1 , and Report1 located under Inbox .	<ol style="list-style-type: none"> 1 From the product interface, click Settings & Diagnostics Mailbox Exclusion Settings. 2 From the Available mailboxes pane, select a mailbox. 3 In the Folders within the mailbox to be excluded box, type Inbox \Data1, Inbox \Project1, Inbox \Report1, click >>, then click Apply.
	Folders and their subfolders. <ul style="list-style-type: none"> • You can exclude emails in subfolders but scans emails in a folder. • You can exclude emails and subfolders of a folder. 	<ol style="list-style-type: none"> 1 From the product interface, click Settings & Diagnostics Mailbox Exclusion Settings. 2 From the Available mailboxes pane, select a mailbox. <ul style="list-style-type: none"> • Inbox \Personal* — To exclude emails and subfolders in the Personal folder from VSAPI scanning. • Inbox \Personal * — To exclude all subfolders under the Personal folder from VSAPI scanning. The emails in the Personal folder are not excluded from VSAPI scanning.

Notification settings

Allows you to configure the content and SMTP address for the administrator to send email notifications, when an email is quarantined.

From the product's user interface, click **Settings & Diagnostics | Notifications** to configure notification settings.

In the **Notifications** page, you can use:

- **Settings** — To define an email account to receive notifications, when an email is quarantined. Additionally, you can send notification emails to specific reviewers or DLs, when an email is quarantined due to a specific scanner or filter.
- **Template** — To create customized notification email that goes out to specific users, when an email is quarantined.
- **Product Health Alerts** — To define product health alerts that are emailed to the administrator on a daily-basis or immediately when specific events occur, such as issues with the Postgres database or loading a service fails.



Make sure that email addresses are updated as required for systems or group systems in the **Notification** page to receive notifications for managed and standalone systems.



To send email notifications to a distribution list (DL), specify the SMTP address of the DL.



When configuring the product, such as notification or policy name, make sure that you do not use characters that can cause Cross Site Scripting (XSS) vulnerability. For the list of characters that you must avoid, see McAfee KnowledgeBase article [KB82214](#).

Configure notification settings

Configure an email account to receive notifications, when an email is quarantined. Also send notification emails to specific reviewers or DLs, when an email is detected.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Notifications**.
- 2 In the **Notifications | Settings** tab, you can use:

Table 6-7 Option definitions

Option	Definition
General	To define simple email notification settings.
Administrator E-mail	To notify the Microsoft Exchange administrator in case of an event such as quarantine action or alert. <ul style="list-style-type: none"> • To send email notifications to multiple users, use semi-colon (;) as the delimiter. • To send email notifications to a distribution list (DL), specify the SMTP address of the DL.
Sender E-mail	To specify the sender's email address in the From field of the notification email. <p>McAfee recommends that you do not modify the Sender E-mail address because the software creates and uses this address for multiple purposes. If you change this email address and do not enable Anonymous receive connector in Microsoft Exchange, you don't receive product notifications.</p>
Enable Task results notification	To send emails with on-demand scan and update tasks results. The email is in HTML format and has the same data and format as Task Result window in the user interface. This feature can be enabled/disabled through this option. By default, this feature is disabled.

Table 6-7 Option definitions (continued)

Option	Definition
Advanced	To define advanced notification settings such as specifying individual email addresses and subject line for each scanner or filter.
Mail Body	To define a generic email message body for all notifications.

- Click **Apply** to save the settings.



MSME provides enhanced security by not supporting the HTML tags that have XSS vulnerability. McAfee recommends that you remove the HTML tags that have XSS vulnerability from the existing notification template before the upgrade. Otherwise, after the upgrade, if you try to modify the notification templates that contain unsupported tags, you will be prompted to remove the unsupported tags from the template or use the template without modification. For the list of unsupported HTML tags, see McAfee KnowledgeBase article [KB82214](#).

Edit notification template

View or edit the message body of the notification email sent to end-user.

Task

- From the product's user interface, click **Settings & Diagnostics | Notifications**.
- In the **Notifications | Template** tab, you can use:

Table 6-8 Option definitions

Option	Definition
Template	To view the notification template for a specific end-user. The available options are: <ul style="list-style-type: none"> • Internal Sender • Internal Recipient • External Sender • External Recipient You can define specific notification text for each of these user types.
Subject	To specify the subject line for the notification email. By default the notification subject is McAfee Security for Microsoft Exchange Alert .
Notification Text	To preview of the notification email's message body, based on the selected Template . The notification text contains information about the quarantined item, such as the date and time, subject, action taken and so on.
Edit	To modify the notification text using HTML in plain text format. After editing the notification based on your company's requirement, click Save to apply the changes.

- Click **Apply** to save the settings.

You have now successfully viewed or modified the notification template. For more information on the available notification fields, refer to the *Notification fields that you can use* section.

Notification fields that you can use

Use these fields to include them in your notifications. For example, if you want the name of the detected item and the action taken when it was detected, use **%vrs%** and **%act%** in the **Settings & Diagnostics | Notifications | Template** page.

Table 6-9 Notification fields you can use

Notification field options	Description
%dts%	Date and time
%sdr%	Sender
%ftr%	Filter
%fln%	File name
%rul%	Rule name
%act%	Action taken
%fdr%	Folder
%vrs%	Detection name
%trs%	State (Train state)
%tik%	Ticket number
%idy%	Scanned by
%psn%	Policy name
%svr%	Server
%avd%	Anti-virus DAT
%ave%	Anti-virus engine
%rpt%	Recipient
%rsn%	Reason
%sbj%	Subject
%ssc%	Spam score
%ase%	Anti-spam engine
%asr%	Anti-spam rules

Enable product health alerts

Send notifications immediately or on a daily-basis to the Microsoft Exchange administrator, when a product specific task fails.


Task

- 1 From the product's user interface, click **Settings & Diagnostics | Notifications**.
- 2 In the **Notifications | Product Health Alerts** tab, you can use:

Table 6-10 Option definitions

Option	Definition
Enable	To enable sending product health alert notifications to the administrator, when a product specific task fails.
Alert ePolicy Orchestrator	To alert the McAfee ePolicy Orchestrator server that manages this MSME server, when a product specific task fails.

Table 6-10 Option definitions (continued)

Option	Definition
Alert Administrator	To send the product health alerts to the email address specified under Settings & Diagnostics Notifications Settings Administrator E-mail .
Notify when	<p>To notify the administrator when any of the selected product specific task fails. You can select these options to send product health alerts to the administrator:</p> <p> These options may vary based on your Exchange server role.</p> <ul style="list-style-type: none"> • Downloading DATs/Anti-Virus Engine fails • Downloading Anti-Spam Rules fails • Loading Anti-Virus Engine fails • Loading TransportScan module fails • Loading VSAPI module fails • RPCServ process quits unexpectedly • DLLHost process quits unexpectedly • Postgres process fails • Postgres failed to quarantine or log detections • Postgres database initialization fails • Postgres failed to store a record • On-Demand scan fails • Database diskspace goes below the threshold • Product service fails to start • McAfee Global Threat Intelligence file reputation scanning fails
Immediate	To send a notification to the administrator immediately after the task fails.
Daily	To send a notification to the administrator on a daily-basis at a specific time when the task fails.

3 Click **Apply** to save the settings.

You have now successfully enabled the **Product Health Alerts** feature.


Anti-spam settings

Define settings for junk email folder in which to forward a spam detected on an Edge Transport or Hub Transport server. Also enable or disable settings for the McAfee GTI message reputation and McAfee GTI IP reputation feature.

Table 6-11 Option definitions

Option	Definition
System Junk Folder Address	Specify the email address to which all emails categorized as spam are sent.
McAfee GTI message reputation	<p>McAfee Global Threat Intelligence message reputation is McAfee’s comprehensive, real time, cloud-based message and sender reputation service that enables MSME to protect your Exchange server against both known and emerging message-based threats such as spam.</p> <p>MSME receives millions of email queries daily, takes a fingerprint of the message content (versus the content itself, for privacy reasons) and analyzes it along many dimensions. Message reputation combines with factors such as spam-sending patterns and IP behavior to determine the likelihood that the message in question is malicious.</p> <p>The score is based not only on the collective intelligence from sensors querying the McAfee cloud and the analysis performed by McAfee Labs researchers and automated tools, but also on the correlation of cross-vector intelligence from file, web, and network threat data. MSME uses this score to determine an action based on the Policy Manager Gateway policy.</p>
Enable	To block email messages at the gateway, based on the email's message reputation score.
Perform message reputation after Anti-Spam	To perform McAfee GTI message reputation after performing a scan based on the local MSME policy.
Message reputation threshold	Specify a threshold value to block email messages based on the message reputation score. By default, the value is set to 80.
Action to take	<p>Select:</p> <ul style="list-style-type: none"> • Drop and Quarantine — To drop the email and quarantine it in the database. When an email is dropped due to this setting, the sender will not be notified on the email delivery status. • Pass score to Anti-Spam Engine — To send the message reputation score detected by McAfee GTI to the Anti-Spam engine. This option is available only when you enable the Perform message reputation after Anti-Spam option.
McAfee GTI IP reputation	IP reputation acts as the first level of protection for your Exchange environment, by safeguarding your Exchange server from unsafe email sources. It enables you to leverage the threat intelligence gathered by McAfee Global Threat Intelligence to prevent damage and data theft by blocking the email messages at the gateway, based on the source IP address.
Enable	To block email messages at the gateway, based on the source IP address.

Table 6-11 Option definitions (continued)

Option	Definition
IP reputation threshold	<p>Specify a threshold value to block email messages based on the IP reputation score.</p> <p> The action will be applied to all IP addresses having a reputation score greater than the selected threshold. All other email messages will be allowed through.</p> <p>You can whitelist the legitimate IP addresses that are blocked by the IP reputation threshold settings in the Anti-Spam Settings page by modifying the registry values. After whitelisting the IP address, emails from the whitelisted IP address are allowed through, regardless of its reputation score.</p> <p>Important: IP address whitelisting overrides only the IP reputation threshold settings. MSME further scans the email for corrupt or encrypted content, file filter, content scanning, URL reputation, and anti-malware. If there is a detection, action is taken according to the product configuration.</p> <p>Before whitelisting the IP address, McAfee recommends that you verify the reputation score of the IP address from www.trustedsource.org for its legitimacy.</p> <p>McAfee cannot be held liable, if you have any mailboxes that are infected by the whitelisted IP address.</p> <p>For more information about configuring IP whitelisting for IP Agent using the registry, see McAfee KnowledgeBase article KB82216.</p>
Action to take	<p>Select either of these options to take an action on an email message, based on the reputation score of the source IP address:</p> <ul style="list-style-type: none"> • Drop connection and Log — To drop the email from the detected source IP address and log the action taken on the item. • Reject connection and Log — To reject the email from the source IP, by notifying the sender and log the action taken on the item.

Detected items settings

Specify repository settings to store the quarantined items detected by MSME.

Configure and manage quarantine repositories using:

- **McAfee Quarantine Manager** — To quarantine detected items on the MQM server.
- **Local Database** — To quarantine detected items in the local MSME server.

Quarantine using McAfee Quarantine Manager

Specify repository settings to quarantine items detected by MSME on a McAfee Quarantine Manager server.

McAfee products such as McAfee Security for Microsoft Exchange and McAfee Email Gateway use a pre-assigned port number to send the detection information to McAfee Quarantine Manager. McAfee Quarantine Manager in turn uses the same port number by default, to release or send configuration information of the detected email messages to the McAfee product.



The communication port mentioned in the McAfee Security for Microsoft Exchange and McAfee Quarantine Manager user interface should be the same.

You can use McAfee Quarantine Manager to consolidate the quarantine and anti-spam management functionality. It gives you a central point from which you can analyze and act upon emails and files that have been quarantined.



This guide does not provide detailed information about installing or using the McAfee Quarantine Manager software. See the McAfee Quarantine Manager product documentation for more information.

Task

- 1 Install McAfee Security for Microsoft Exchange software on <server 1>.
- 2 Install the supported McAfee Quarantine Manager software on <server 2>.
- 3 Launch the MSME user interface from <server 1>.
- 4 From the product's user interface, click **Settings & Diagnostics | Detected Items**.

The **Detected Items** page appears.

- 5 From the **McAfee Quarantine Manager** section, select **Enable**.
- 6 In **Communication mode**, select the mode.
 - **RPC** — Remote Procedure Call (RPC) is a communication mechanism that requires uninterrupted connection to communicate with McAfee Quarantine Manager server. If there is a communication failure with McAfee Quarantine Manager server, the processes such as quarantine and release are interrupted.
 - **HTTP** — A stateless communication mechanism to communicate with McAfee Quarantine Manager server. If there is a communication failure with McAfee Quarantine Manager server, the items are stored in the local database until the connection is restored. MSME tries to send the quarantined items to MQM for three times. If all three attempts fail, a product log entry is created and the item is stored in the local database.
 - **HTTPs** — A secured HTTP communication mechanism where the data is transferred in encrypted format.



McAfee recommends that you use HTTP/HTTPs communication channel because stateless connections make sure that the software can communicate with McAfee Quarantine Manager seamlessly.

- 7 In **IP address**, specify the IP address of the MQM server.
- 8 In **Port** and **Callback Port**, specify the default values.

Communication mode	Port value	Callback port	BW List Update Interval (hours)
RPC	49500	49500	–
HTTP	80	–	4
HTTPs	443	–	4



Modify this value only if you have configured a different port value on the McAfee Quarantine Manager server.

- 9 Click **Apply** to save the settings.

You have now successfully configured your MSME server to start quarantining detected items on the MQM server.

Quarantine using the local database

Specify repository settings to quarantine items detected by MSME to a PostgreSQL database on the local MSME server.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Detected Items**.

The **Detected Items** page appears.

- 2 From the **Local Database** section, you can use:

Table 6-12 Option definitions




Option	Definition
Specify location of database	To enable the Database location for storing the quarantined items detected by MSME.
Database location	<p>To specify the database location path where items detected by MSME can be stored. You can select:</p> <ul style="list-style-type: none"> • <Install Folder> — To create the database sub-folders under the MSME installation directory. • <System Drive> — To create the database sub-folders under the <code>C:\Windows\system32</code> directory. • <Program Files> — To create the database sub-folders under the Windows <code>C:\Program Files (x86)</code> directory. • <Windows Folder> — To create the database sub-folders under the <code>C:\Windows</code> directory. • <Data Folder> — To create the database sub-folders under the <code>C:\ProgramData\</code> directory. • <Full Path> — To store the MSME database in the complete path specified. <p> Specify the sub-folder path in the field next to the drop-down list. The default sub-folder path specified is: <code>McAfee\MSME\Data\</code></p>
Maximum item size (MB)	To specify the maximum size of a quarantined item that can be stored in the database. You can specify a value from 1 to 999, where the default value is 100.
Maximum query size (records)	To specify the maximum number of records or quarantined items you can query from the Detected Items page. You can specify a value from 1 to 20000, where the default value is 1000.
Maximum item age (days)	To specify the maximum number of days an item will be stored in the local quarantine database, before being marked for deletion. You can specify a value from 1 to 365, where the default value is 30.
Disk size check interval (Minute)	To specify how often MSME should check for the available disk space. You can specify a value from 6 to 2880, where the default value is 6.
Disk space threshold (MB)	<p>To specify the threshold value at which a low disk space warning notification should be sent to the administrator. You can specify a value from 1 to 512000, where the default value is 2048.</p> <p> Make sure that Database disk space goes below the threshold under Settings & Diagnostics Notifications Product Health Alerts Notify when is enabled.</p>
Purge of old items frequency	To specify how frequently old items that are marked for deletion are deleted from the MSME database. The default value is set to Monthly .

Table 6-12 Option definitions (continued)

Option	Definition
Optimization frequency	To recover the disk space taken up by deleted database records. Based on the value set under Maximum item age (days) , old records will be deleted if you have scheduled a purge task. After deleting these old records, MSME will still use the disk space specified under Disk space threshold (MB) field, even if the quarantine database has not reached the size limit. To optimize and shrink the database, schedule an optimization task. The default value is set to Monthly .  Always schedule an optimization task a few hours after you perform the purge task.
Edit Schedule	To modify the schedule of the purge or optimization task. Click Save after modifying the schedule.

- 3 Click **Apply** to save the settings.

You have now successfully configured your MSME server to start quarantining detected items on to the local database.

User interface preferences settings

Define settings in the **Dashboard** such as the refresh rate, report settings, unit scale of graphics, reporting interval, graph and chart settings.

Configure dashboard settings

Configure settings in the **Dashboard** such as the statistics, unit scale of graph, items to view in the **Recently Scanned Items**, and status reporting interval.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | User Interface Preferences**.

The **User Interface Preferences** page appears.

- 2 Click **Dashboard Settings** tab. You can use:

Table 6-13 Option definitions

Option	Definition
Automatic refresh	To specify whether the information shown on the Dashboard Statistics counter should be refreshed automatically.
Refresh rate (seconds)	To specify the duration (in seconds) at which the information on the dashboard should be refreshed. You can specify a value from 30 to 3600, where the default value is 60.
Maximum recently scanned items	To specify the maximum number of items to appear in the Dashboard Reports Recently Scanned Items section. You can specify a value from 10 to 100, where the default value is 10.
Graph scale (units)	To specify the measurement units for the scale of the bar graph that is generated on the Dashboard Graph section. You can specify a value from 100 to 500, where the default value is 100.
Number of hours to report for	To specify the report generation interval (in hours) to generate reports such as status and configuration reports. You can specify a value from 1 to 24, where the default value is 7.

- 3 Click **Apply** to save the settings.

Configure graph and chart settings

Configure settings in the **Dashboard** | **Graph** section to enhance the graph and chart settings.

Task

- 1 Click **Settings & Diagnostics** | **User Interface Preferences**.
- 2 Click **Graph and Chart Settings** tab. You can use:

Table 6-14 Option definitions

Option	Definition
3D	To specify whether you want the dashboard graph to be displayed as a three-dimensional (3D) graph.
Draw transparent	To specify whether the bars in a three-dimensional bar graph should appear solid or transparent. A solid bar hides part of any bar behind it. A transparent bar allows you to look through it and see other transparent bars behind it.
Anti-alias	To specify whether you want to use anti-aliasing techniques when displaying pie charts. When anti-aliasing is used, pie charts have smoother curves. If anti-aliasing is not used, pie chart curves appear jagged.
Explode pie	To specify whether the segments should remain within the circle of the pie chart or be shown with exploded segments.
Pie angle (degrees)	To specify the angle to use when displaying pie charts. You can specify a value from 1 to 360, where the default value is 45.

- 3 Click **Apply** to save the settings.

Diagnostics settings

Determine the causes of symptoms, mitigation for problems and solutions to issues faced while using MSME.

In the **Settings & Diagnostics** | **Diagnostics** page, you can use:

- **Debug Logging** — To configure debug logging settings such as specifying the debug log level, maximum file size limit of the log file, and the file location.
- **Event Logging** — To configure settings to capture product or event related logs based on information, warnings or errors.
- **Product Log** — To configure settings for the MSME product log file (`productlog.bin`). Changes made to this setting will be reflected on the **Settings & Diagnostics** | **Product Log** page.
- **Error Reporting Service** — To configure settings to determine whether to catch exceptions such as system crashes and report to the user.

Configure debug log settings

Configure settings to specify the debug log level, maximum file size limit of the log file, and the log file location. Use these settings when you want to troubleshoot an issue with the product and provide the logs to McAfee Technical Support for further analysis.



Configure **Debug Log** settings for troubleshooting purposes and only for a limited duration. Once you capture sufficient logs for troubleshooting, set the value for **Level** to **None**. Using debug logging indiscriminately could fill up the hard disk space and affect the overall performance of the server. Enable it for a limited duration as advised by an authorized personnel (McAfee Technical Support Engineer).

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Diagnostics**.

The **Diagnostics** page appears.

- 2 In the **Debug Logging** tab, you can use:

Table 6-15 Option definitions




Option	Definition
Level	<p>To enable or disable debug logging and specify the level of information that should be captured in the debug log file. You can select:</p> <ul style="list-style-type: none"> • None — To disable debug logging. • Low — To log critical events such as errors, exceptions, and return values of functions in the debug log file. Select this if you want to keep a low size for the debug log file. • Medium — To log events mentioned in the Low state and additional information that could be of help to the technical support team. • High — To log all critical errors, warnings and debug messages in the debug log file. It contains information about all activities performed by the product. This is the most detailed level of logging supported by the product.
Enable size limit	If you want to specify a maximum file size limit for each debug log file.
Specify maximum file size	<p>To specify how large the debug log files can be. You can specify a value from 1 KB to 2000 MB.</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p> If the debug log files exceed the specified file size, older events will be rewritten due to circular logging, where new log entries are added to the file by deleting the oldest log entries.</p> </div>

Table 6-15 Option definitions (continued)

Option	Definition
Enable debug logging	<p>If you want to modify the default debug file logging location.</p> <p> If this option is disabled, the debug log files will be stored under <Install Folder> \bin\debuglogs default directory.</p>
Specify file location	<p>To specify the debug log file location path where events triggered by MSME can be stored. You can select:</p> <ul style="list-style-type: none"> • <Install Folder> — To create the debug log files under the MSME installation directory. • <System Drive> — To create the debug log files under the C:\Windows\system32 directory. • <Program Files> — To create the debug log files under the Windows C:\Program Files (x86) directory. • <Windows Folder> — To create the debug log files under the C:\Windows directory. • <Data Folder> — To create the debug log files under the C:\ProgramData\ directory. • <Full Path> — To store the debug log files in the complete path specified in the adjacent textbox. <p> To store the debug log files to a custom location or sub-folder, specify the sub-folder name or path in the field next to the drop-down list.</p>



Make sure that the folder that collects the debug logs is provided "Write" permissions for the NETWORK SERVICE account.

3 Click **Apply** to save the settings.



For more information on generating Exchange Web Services (EWS) wrapper log for the on-demand scan task, see McAfee KnowledgeBase article [KB82215](#).

You have now successfully configured the debug log settings, that you can use for troubleshooting.

Configure event logging settings

Configure settings to log the types of MSME events in the **Product Log** and Windows Event Viewer.

An event is a possible action that you perform, which is monitored by MSME. **Event Logging** provides information useful for diagnostics and auditing. The different classes of events are:

- Error
- Information
- Warning

This allows system administrators to more easily obtain information on problems that occur.

Task

1 From the product's user interface, click **Settings & Diagnostics | Diagnostics**.

The **Diagnostics** page appears.

2 Click **Event Logging** tab. You can use:

Table 6-16 Option definitions

Option	Definition
Product Log	To log MSME events in the Product Log . These events can be viewed from Settings & Diagnostics Product Log View Results section.
Event Log	To log MSME events under Windows Event Viewer. To find MSME related events in the Windows Event Viewer: <ol style="list-style-type: none"> 1 Go to Event Viewer (Local) Windows Logs Application. 2 In the Application pane, product related events appear as MSME under the Source column.
Write information events	To log events that are categorized as Information .
Write warning events	To log events that are categorized as Warning .
Write error events	To log events that are categorized as Error .

- 3 Click **Apply** to save the settings.

Configure product log settings

Configure settings for the **Settings & Diagnostics | Product Log** page, by specifying the required parameters to generate product logs.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Diagnostics**.

The **Diagnostics** page appears.

- 2 Click the **Product Log** tab. You can use:

Table 6-17 Option definitions




Option	Definition
Location	If you want to configure a location to store the product log. Select Enable to specify a custom location.
Specify database location	To specify the product log file location path where product log events can be stored. You can select: <ul style="list-style-type: none"> • <Install Folder> — To create the product log file under the MSME installation directory. • <System Drive> — To create the product log file under the <code>C:\Windows\system32</code> directory. • <Program Files> — To create the product log file under the Windows <code>C:\Program Files (x86)</code> directory. • <Windows Folder> — To create the product log file under the <code>C:\Windows</code> directory. • <Data Folder> — To create the product log file under the <code>C:\ProgramData\</code> directory. • <Full Path> — To store the product log file in the complete path specified in the adjacent textbox. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  To store the product log file to a custom location or sub-folder, specify the sub-folder name or path in the field next to the drop-down list. </div>

Table 6-17 Option definitions (continued)

Option	Definition
Filename	If you want to specify a different file name to store the product log. Select Enable to specify a custom file name.
Specify database filename	To specify a custom file name for the product log. The default file name is <code>productlog.bin</code> under <code><Install Folder>\Data\</code> directory.  If you modify the default product log file name or path, the log entries in the Settings & Diagnostics Product Log page will be reset and older log entries will not appear.
Size Limit	If you want to specify a different size limit for the product log file. Select Enable database size limit to specify a custom file size.
Specify maximum database size	To specify how large the product log file can be. You can specify a value from 1 KB to 2000 MB.  If the product log file exceeds the specified file size, older log events will be rewritten due to circular logging, where new log entries are added to the file by deleting the oldest log entries.
Limit age of entries	If you want the product log entries to be deleted after a set period of time.
Specify maximum age of entry	To specify how many days an entry should remain in the product log file before it is deleted. You can specify a value from 1 to 365.
Query Timeout	If you want to limit the amount of time allowed for answering a product log query. Select Enable to specify the duration.
Specify query timeout (seconds)	To specify the maximum number of seconds allowed, when answering a product log query. You can specify a value from 1 to 3600.

- 3 Click **Apply** to save the settings.

You have now successfully configured settings for the **Product Log** page.

Configure error reporting service settings

Configure settings to report product related errors or exceptions to McAfee.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Diagnostics**.

The **Diagnostics** page appears.

- 2 Click the **Error Reporting Service** tab. You can use:

Table 6-18 Option definitions

Option	Definition
Enable	To enable or disable the error reporting service.
Catch exceptions	To capture information about exceptional events, such as system crashes.
Report exceptions to user	To specify whether exceptions should be reported to the administrator.

- 3 Click **Apply** to save the settings.

View product logs

View the product's health using log entries about events, information, warnings, and errors. For example, you can view information on when a task initiated or ended, product service errors and so on.

You can use the available search filters to find log entries that are of interest to you.




To modify settings related to the product log query page, go to **Settings & Diagnostics | Diagnostics | Product Log**.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Product Log**. The **Product Log** page appears.
- 2 From the **Product Log** section, you can use:

Table 6-19 Option definitions

Option	Definition
ID	To specify the number which identifies a specific product log entry. For example, if you want to view product logs only with ID's greater than 2000, specify: <code>200*</code>
Level	To select Information , Warning or Error from the drop-down list, depending on the type of log you want to view.
Description	To specify a relevant description. For example, if you want to view logs based on service start or stop, type: <code>*service*</code>
All Dates	To include events from all dates which is based on the entry in the product log file.
Date Range	To search for an event within a defined date range according to your requirements. Here you can specify the date, month, year and time against the parameters From and To . You can also use the calendar icon to specify a date range.
Clear Filter	To return to the default search settings.
Export to CSV File	To export and save information about all events returned by the search in a <code>.CSV</code> format. If there are thousands of events in the log, instead of navigating through multiple pages, you can use this option to download these events to a file in CSV format and later generate custom reports in Microsoft Excel.



- If you do not find a specific field in the search result of the CSV file, make sure to enable the required field in the **Columns to Display** option.
- Use the **Import Data** option in Microsoft Excel, to open the CSV file in a different locale.

- 3 Click **Search**.



The maximum number of records that can be stored in the product log is based on the log file size.

A list of events matching your search criteria are displayed in the **View Results** section.

Configure DAT settings

Specify the number of old DATs that can be maintained in your system.

DAT files are the detection definition files, also referred to as signature files, that identify the code anti-virus and/or anti-spyware software detects to repair viruses, trojan horses and Potentially Unwanted Programs (PUPs). For glossary information on .DAT files, go to: <http://www.mcafee.com/us/mcafee-labs/resources/threat-glossary.aspx#dat>

Task

- 1 From the product's user interface, click **Settings & Diagnostics | DAT Settings**.

The **DAT Settings** page appears.

- 2 Use **Maximum number of old DATs** to specify the maximum number of DAT generations that shall be preserved in the system during regular updates. MSME retains the latest DATs with old DATs under `<Install Folder>\bin\DATs` directory. Whenever a new DAT update occurs, MSME verifies the number of available DATs. If the available DATs count exceeds the DAT retention value, the oldest DAT will be deleted. You can specify a value from 3 to 10, where the default value is 10.
- 3 Click **Apply** to save the settings.

Import and export configuration settings


Configure settings to export existing MSME configuration (settings and policies) for import and use on another MSME server. Also import sitelists to specify the location from where automatic updates are downloaded.

From the product's user interface, click **Settings & Diagnostics | Import and Export Configuration**. In the **Import and Export Configurations** page, you can use these tabs:

- **Configuration** — To export, import or restore product settings.

Table 6-20 Configuration tab — Option definitions

Option	Definition
Export	To copy the MSME configuration (settings and policies) of this server and save it to a location from where it can be imported by other MSME servers. The default MSME configuration file is <code>McAfeeConfigXML.cfg</code> .
Restore Default	To reset the MSME settings for your product to maximum performance.
Restore Enhanced	To reset the MSME settings for your product to maximum protection.
Browse	To locate the configuration file (<code>McAfeeConfigXML.cfg</code>) that you want to import.
Import	<p>To apply the settings of another MSME server to this server. For example, to install MSME 8.5 on 5 systems:</p> <ol style="list-style-type: none"> 1 Install MSME on system 1. 2 Configure the settings as required. 3 Export the configuration to cfg file. <p>For more information on importing the configuration, see step 10 in <i>Install the software using wizard</i>.</p>

 You must import settings across the same product version. For example, you must not import settings from an MSME 7.6 or 8.0 server to MSME 8.5 server.

- **SiteList** — To import sitelists that specify the location from where automatic updates are downloaded.

Table 6-21 SiteList tab — Option definitions

Option	Definition
Browse	To locate the sitelist file (<code>SiteList.xml</code>) that you want to use.
Import	To apply the sitelist configuration settings specified in the file, to download DAT updates.

Export your existing MSME configuration

Export the configuration of a MSME server and save it to a location, where it can be imported by other MSME servers.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Import and Export Configuration**.
The **Import and Export Configurations** page appears.
- 2 Click the **Configuration** tab.
- 3 Click **Export**.
- 4 Specify a location where to save the configuration file. The default name of the configuration file is `McAfeeConfigXML.cfg`.
- 5 Click **Save**.

You have now successfully exported your existing MSME settings and policies to a configuration file, that can be imported by other MSME servers.

Import configuration from another MSME server

Apply MSME configuration settings from another server to this MSME server.

You can import the configuration in two ways:

- Import the configuration while installing the software.
- Import the configuration file after installing the software using the **Import and Export Configuration** option from the **Settings & Diagnostics** page.



- You must import settings across the same product version. For example, you must not import MSME server settings from an MSME 7.6 server to MSME 8.0 server.
- It is advisable that you import settings from MSME server's having the same Exchange roles.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Import and Export Configuration**.
The **Import and Export Configurations** page appears.
- 2 Click the **Configuration** tab.
- 3 From the **Import Configuration** section, click **Browse** to locate the configuration file. The default name of the configuration file is `McAfeeConfigXML.cfg`.

- 4 Click **Import**.

A dialog box appears with the message **The operation completed successfully**.

- 5 Click **OK**.

You have now successfully imported configuration settings from another MSME server to this server.

Import a sitelist

Import sitemlists that specify the location from where automatic updates are downloaded.

A sitelist specifies from where automatic updates are downloaded. By default, MSME uses **SiteList Editor** that points to a McAfee URL for automatic updates.

If your MSME server is managed by McAfee ePO, the sitelist from ePolicy Orchestrator is used to perform automatic updates. If you are not using ePolicy Orchestrator to manage your MSME server, create a sitelist that points your MSME server to a local repository.

Alternative sitemlists can be created using the McAfee AutoUpdate Architect software or McAfee ePO.

Task

- 1 Click **Settings & Diagnostics | Import and Export Configuration**. The **Import and Export Configurations** page appears.
- 2 Click the **SiteList** tab.
- 3 From the **Import SiteList** section, click **Browse** to locate the sitelist file `SiteList.xml`. This file contains information about the repository settings such as repository name, server URL, and so on.



You can find the `SiteList.xml` file under `C:\ProgramData\McAfee\Common Framework\` directory. The **SiteList Editor** application under **Start | All Programs | McAfee | Security for Microsoft Exchange** uses this file to display the repository settings in the application.

- 4 Click **Import**.

A dialog box appears with the message **The operation completed successfully**.

- 5 Click **OK**.

You have now successfully imported the sitelist that points to a new repository location, to download product updates.

Configure anti-spam proxy settings

Configure these settings if your organization uses a proxy server to connect to the Internet, so that MSME can download the Anti-Spam Rules.

The software can also use this proxy to get the IP reputation, message reputation, and download the local URL database from the GTI server.



This feature is applicable only if you have installed the McAfee Anti-Spam add-on component.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Proxy Settings**.

The **Proxy Settings** page appears.

- 2 Select **Use Proxy**. In the **Proxy Server Details** section, you can use:

Table 6-22 Option definitions

Option	Definition
IP Address	To specify the IP address of the proxy server.
Port	To specify the port used for communications to access the Internet.
Authentication Details	To specify the authentication type. You can use: <ul style="list-style-type: none">• Anonymous — To access the proxy computer without specifying any authentication details.• NTLM — To access the proxy computer using NT LAN Manager credentials.• Basic authentication — To provide a system User Name and Password to access the proxy computer. Retype the password in Confirm Password.

- 3 Click **Apply** to save the settings.

7

Program maintenance

Perform product maintenance tasks such as modify installation, repair, uninstall, restore default settings, purge and optimize the database.

Contents

- ▶ *Modify the installation*
- ▶ *Repair the installation*
- ▶ *Restore default settings*
- ▶ *Purge and optimize*
- ▶ *Uninstall the software*

Modify the installation

Change MSME program features as required and change the way program features are installed on your computer or if you have modified the Exchange server role.



You can also modify the MSME installation from **Control Panel | Programs and Features | Uninstall a program** console by clicking **Uninstall/Change**.

Task

- 1 In the folder containing the installation files, double-click `setup_x64.exe`.
- 2 Click **Next** in the Welcome screen.
The **Program Maintenance** screen appears.
- 3 Select **Modify**, then click **Next**.
- 4 Select the program features you want to modify and click **Next**.
- 5 Select **I accept the terms in the license agreement**, then click **Next**.
- 6 Click **Install** to complete the installation with the modified program features.
- 7 Click **Finish** when the installation completes.

Repair the installation

Resolve installation errors in the program by fixing corrupt or missing files, shortcuts and registry entries.



You can also repair the MSME installation from **Control Panel | Programs and Features | Uninstall a program** console by clicking **Uninstall/Change**. Repairing an installation will revert to the default configuration settings.

Task

- 1 In the folder containing the installation files, double-click `setup_x64.exe`.
- 2 Click **Next**. The **Program Maintenance** screen appears.
- 3 From the **Program Maintenance** screen, select **Repair**, then click **Next**. The **Ready to Repair the program** screen appears.
- 4 Click **Install** to complete the repair. The **InstallShield Wizard Completed** dialog box appears.
- 5 Click **Finish** to exit.

Restore default settings

Restore the product to its default configuration and achieve maximum performance.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Import and Export Configuration**. The **Import and Export Configurations** page appears.
- 2 From the **Configuration** tab, click **Restore Default**.



Restoring the default settings removes all policy settings and subpolicies configured. It is recommended that you take a backup of existing settings, to restore the settings later.

A dialog box appears asking you to confirm the settings.

- 3 Click **OK**.

A dialog box appears confirming that the default configuration settings are applied.

- 4 Click **OK**.

You have now successfully restored your MSME server to default configuration settings for maximum performance.

Purge and optimize

Remove old items marked for deletion from the database and use optimization task to recover disk space being taken up by deleted database records.

Task

- 1 From the product's user interface, click **Settings & Diagnostics | Detected Items**.
The **Detected Items** page appears.

2 From the **Local Database** section, you can use:

- **Purge of old items frequency** — To specify how frequently old items that are marked for deletion are deleted from the MSME database. The default value is set to **Monthly**.
- **Optimization frequency** — To recover the disk space taken up by deleted database records. Based on the value set under **Maximum item age (days)**, old records will be deleted if you have scheduled a purge task. After deleting these old records, MSME will still use the disk space specified under **Disk space threshold (MB)** field, even if the quarantine database has not reached the size limit. To optimize and shrink the database, schedule an optimization task. The default value is set to **Monthly**.



Always schedule an optimization task a few hours after you perform the purge task.

3 Click **Edit Schedule** to modify the schedule.



These tasks should be performed on a regular basis to maintain adequate free space in the database.

Uninstall the software

Remove or uninstall MSME from the Exchange server.



You can also remove MSME from the **Control Panel | Programs and Features | Uninstall a program** console. In this method, the quarantine database is retained by default.

Task

1 In the folder containing the installation files, double-click `setup_x64.exe`.

The **Welcome** screen appears.

2 Click **Next**.

The **Program Maintenance** screen appears.

3 Select **Remove**, then click **Next**.

The **Preserve Settings** screen appears.

4 Select **Preserve quarantine database** to retain the quarantine database, then click **Next**.

The **Remove the program** screen appears.

5 Click **Remove** to uninstall MSME from your Exchange server.

The **InstallShield Wizard Completed** screen appears.

6 Click **Finish** to exit.

8

Integrating MSME with ePolicy Orchestrator

Integrate and manage MSME using ePolicy Orchestrator management software.

ePolicy Orchestrator 4.6.x, 5.0.x, and 5.1.x provides a scalable platform for centralized policy management and enforcement on your McAfee security products and systems on which they reside. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

For instructions about setting up and using ePolicy Orchestrator, see the product guide for your version of the product.

Contents

- ▶ *Prerequisites*
- ▶ *Check in the MSME package*
- ▶ *Install the MSME extension*
- ▶ *Migrate policies from older versions*
- ▶ *Deploy the MSME software to clients*
- ▶ *Set up the McAfee Anti-spam software*
- ▶ *Manage policies*
- ▶ *Create and schedule tasks*
- ▶ *Queries and reports*
- ▶ *Filter events*
- ▶ *Configure automatic responses*
- ▶ *Remove the software*

Prerequisites

Set up your environment before you integrate MSME with ePolicy Orchestrator.

- Make sure that the system requirements are met.
- If a supported McAfee Agent is not installed on the client systems, install or upgrade your McAfee Agent to the version 4.6. McAfee Agent is a component of ePolicy Orchestrator that must be installed on each computer on the network and client computer. The agent collects and sends information between the ePolicy Orchestrator server, repositories, and manages MSME installations across the network. See the McAfee Agent documentation for installation and deployment instructions.

Check in the MSME package

Check in the MSME deployment package to the ePolicy Orchestrator server.

Task

- 1 Log on to ePolicy Orchestrator server as administrator.
- 2 Click **Menu | Software | Master Repository**.
- 3 On the **Packages in Master Repository** page, complete these steps according to your version of ePolicy Orchestrator.

Version 4.6 and 5.0	Version 5.1
Click Action Check In Package	Click Check In Package

- 4 In the **Package** step, select **Product or Update (.zip)**, click **Browse** and browse to the .zip file containing the MSME package (MSME_Deployment_x64_xxxx.zip), then click **Next**.
- 5 In the **Package Options** step, select **Current** as the branch, then click **Save**.

Install the MSME extension

Install the MSME extension on the ePolicy Orchestrator server.



When you already have a previous version of the software extension, this task adds the MSME 8.5 extension to the list. You can retain the previous extensions or remove them, as required.

Task

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Software | Extensions**, then click **Install Extension**.
- 3 Click **Browse** and browse to the .zip file containing the MSME extension (\MSMEv85_x64\epo\epo_Extension_EN\MSME____8500_0409.zip for English), then click **OK**.

When you upgrade the software, the older versions of MSME 7.6.x or 8.0 are not upgraded automatically.

Migrate policies from older versions

When you upgrade the software, migrate existing policies from older versions to MSME version 8.5.0.



Ignore this task when you're performing a fresh installation.

Task

- 1 Browse to the folder containing the MSME_ePOUpgrade.zip (\MSMEv85_x64\epo), then extract it.



Make sure that all files in the .zip are extracted to the same folder.

- 2 Go to the command prompt, navigate to the folder where the .zip file is extracted, and run the MSMEePOUpgrade.exe command.

- 3 Type the ePolicy Orchestrator database password, then press **Enter**.
- 4 Type the ePolicy Orchestrator SQL named instance if created during the server installation, otherwise leave it blank. Then press **Enter**.

The policy upgrade process starts. Wait for it to complete.

On successful completion, a confirmation message appears. See `EP0DebugTrace.txt` in the current directory for log details. Press **Enter** to exit.



For more information on the policy upgrade tool, see McAfee KnowledgeBase article [KB76921 — Using the MSME ePO Upgrade tool](#).

- Verify that the policies are upgraded: In the ePolicy Orchestrator console, navigate to **Policy Catalog**, select the product as **McAfee Security for Microsoft Exchange 8.5.0**, then look for upgraded policies suffixed with **(Upgraded)**. For example, **My Default (Upgraded)**.
- Assign the custom policies to the required systems, otherwise the McAfee default policies are enforced.

See also

[Manage policies on page 151](#)

Deploy the MSME software to clients

Deploy MSME to Microsoft Exchange systems.

Before you begin

Migrate existing policies from older versions to MSME 8.5.

If you had installed the previously supported version of McAfee Anti-spam module separately earlier, make sure that you uninstall the McAfee Anti-spam module before upgrading the software. You can install the latest version of the McAfee Anti-spam after the upgrade.

MSME provides enhanced security by not supporting the HTML tags that have XSS vulnerability. McAfee recommends that you remove the HTML tags that have XSS vulnerability from the existing notification template before the upgrade. Otherwise, after the upgrade, if you try to modify the notification templates that contain unsupported tags, you will be prompted to remove the unsupported tags from the template or use the template without modification. For the list of unsupported HTML tags, see McAfee KnowledgeBase article [KB82214](#).



When you already have a previous version of the software, this task upgrades the software on all managed Microsoft Exchange systems that you select.

Task

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree**, then select the required group or systems.



When upgrading the software, make sure that you select all required systems.

- 3 Click the **Assigned Client Tasks** tab, then click **Actions | New Client Task Assignment**. The **Client Task Assignment Builder** page appears.

- 4 Define these options, then click **Create New Task**.
 - a For **Product**, select **McAfee Agent**
 - b **Task Type**, select **Product Deployment**.
- 5 On the **Client Task Catalog** page, define these options:
 - a For **Task Name**, type a name for the task.
 - b Select **Windows** as a target platform.
 - c In **Products and components**, select **McAfee Security for Microsoft Exchange (x64) - xxxxxxxx 8.5.0.xxxx**, select **Install** as action, select the language, then click **Save**. The task is listed in the **Task Name**.
- 6 Select the task, then click **Next**.
- 7 Schedule the task to run immediately, then click **Next** to view a summary of the task.
- 8 Review the summary of the task, then click **Save**.
- 9 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
- 10 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

On successful execution of this task, the MSME client software is deployed to the selected systems. For more information on deploying the software, see McAfee KnowledgeBase article [KB82484](#).

Set up the McAfee Anti-spam software

To use the anti-spam feature with your ePolicy Orchestrator managed MSME software, check in the McAfee Anti-spam deployment package to ePolicy Orchestrator, then deploy it to the client systems. The MSME package includes an evaluation version of the McAfee Anti-Spam add-on. To upgrade it to licensed, contact McAfee Support.

Tasks

- [Check in the McAfee Anti-spam package on page 150](#)
Check in the McAfee Anti-spam add-on deployment package to the ePolicy Orchestrator server.
- [Deploy the McAfee Anti-spam add-on on page 151](#)
Deploy the McAfee Anti-spam add-on to Microsoft Exchange systems.

Check in the McAfee Anti-spam package

Check in the McAfee Anti-spam add-on deployment package to the ePolicy Orchestrator server.

Task

- 1 Log on to ePolicy Orchestrator server as administrator.
- 2 Click **Menu | Software | Master Repository**.
- 3 On the **Packages in Master Repository** page, complete these steps according to your version of ePolicy Orchestrator.

Version 4.6 and 5.0	Version 5.1
Click Action Check In Package	Click Check In Package

- 4 In the **Package**, select **Product or Update (.zip)**, click **Browse** and browse to the .zip file containing the MSME package (MSME_AS_Deployment_x64_Eval.zip), then click **Next**.
- 5 In the **Package Options** step, select **Current** as the branch, then click **Save**.

Deploy the McAfee Anti-spam add-on

Deploy the McAfee Anti-spam add-on to Microsoft Exchange systems.

Task

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree**, then select the required group or systems.
- 3 Click the **Assigned Client Tasks** tab, then click **Actions | New Client Task Assignment**. The **Client Task Assignment Builder** page appears.
- 4 Define these options, then click **Create New Task**.
 - a For **Product**, select **McAfee Agent**
 - b For **Task Type**, select **Product Deployment**.
- 5 On the **Client Task Catalog** page, define these options:
 - a For **Task Name**, type a name for the task.
 - b Select **Windows** as a target platform.
 - c For **Products and components**, select **McAfee Anti-Spam for McAfee Security for Microsoft Exchange (x64) - xxxxxxxx 8.5.0.xxxx**, select **Install** as action, select the language, then click **Save**. The task is listed in the **Task Name**.
- 6 Select the task, then click **Next**.
- 7 Schedule the task to run immediately, then click **Next** to view a summary of the task.
- 8 Review the summary of the task, then click **Save**.
- 9 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
- 10 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

Manage policies

MSME policies provide options to configure MSME feature enablement and disablement, feature configuration, feature administration, and logs.

These policy settings are nearly identical to those you can access from the **Settings & Diagnostic** tab in the MSME interface.

You can find these policies on the **Policy Catalog** page under the **McAfee Security for Microsoft Exchange 8.5.0** product.

- **Anti-Spam Settings**
- **Mail Notifications**
- **DAT Settings**
- **On Access Settings**

- Detected Items
- Diagnostics
- Proxy Settings
- Scanner Settings

Modify these policies with your preferences, then assign them to groups of managed Microsoft Exchange systems or to a single system (requires McAfee Agent on the systems). For generic information about policies, see the product guide for your version of the ePolicy Orchestrator software.

Tasks

- [Create or modify policies on page 152](#)
Create or modify MSME policies from the **Policy Catalog**.
- [Assign policies on page 152](#)
When you've created or modified MSME policies with the required settings, assign each of them to the required Microsoft Exchange systems that are managed by ePolicy Orchestrator.

See also

[Settings and diagnostics on page 5](#)

Create or modify policies

Create or modify MSME policies from the **Policy Catalog**.

Alternatively, you can create or modify these policies from the **System Tree**, while assigning policies to selected systems. See the product guide for your version of the ePolicy Orchestrator software for more information.

Task

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 From the **Policy Catalog**, select **McAfee Security for Microsoft Exchange 8.5.0** as the product, then select the required policy as the category.
- 3 Perform this step as required:

To create a policy	To modify a policy
Click New Policy , type a name for the policy, then click OK .	
	Click the policy that you want to modify.

- 4 Modify the policy settings as required, then click **Save**.

The policy settings are updated and the new policy (when created) appears in the **Policy Catalog**.

Assign policies

When you've created or modified MSME policies with the required settings, assign each of them to the required Microsoft Exchange systems that are managed by ePolicy Orchestrator.

Task

For option definitions, click ? in the interface.

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Navigate to the **System Tree**, select a required group or systems, then click the **Assigned Policies** tab.
- 3 Select **McAfee Security for Microsoft Exchange 8.5.0** from the products list, locate the required policy, then click **Edit Assignment** next to the policy.

- (Optional) Select a policy, then click **Edit Policy** to modify the policy settings. Click **New Policy** to create a new policy based on the selected category.



Alternatively, you can also modify or create a policy from the **Policy Catalog**.

- Select the policy to assign, select appropriate inheritance options, then click **Save**.

The policy enforcement occurs in the next agent-server communication. Click **Wake Up Agents** to enforce policies immediately.

Create and schedule tasks

Create MSME client tasks on your Microsoft Exchange systems to schedule automated actions.

Tasks

- [Schedule automatic updates on page 153](#)
Schedule automatic updates to keep your software up-to-date with the latest anti-virus definitions (DATs), anti-virus scanning engine, and spam engine.
- [Schedule an on-demand scan on page 154](#)
Schedule an on-demand scan to scan your Microsoft Exchange servers to find a threat, vulnerability, or other potentially unwanted code.
- [Schedule to send status report on page 155](#)
Schedule to send the status report to an administrator at a specific time.
- [Schedule to send configuration report on page 156](#)
Schedule to send the configuration report to an administrator at a specific time.
- [Schedule a task to purge the old DAT files on page 156](#)
Schedule a task to purge the old DAT files from the managed systems.

Schedule automatic updates

Schedule automatic updates to keep your software up-to-date with the latest anti-virus definitions (DATs), anti-virus scanning engine, and spam engine.



McAfee recommends that you run the MSME automatic update task explicitly.

Task

- Log on to the ePolicy Orchestrator server as an administrator.
- Click **Menu | Systems | System Tree**, then select the required group or systems.
- Click the **Assigned Client Tasks** tab, then click **Actions | New Client Task Assignment**. The **Client Task Assignment Builder** screen appears.
- Define these options, then click **Create New Task**.
 - For **Product**, select **McAfee Security for Microsoft Exchange 8.5.0**.
 - For **Task Type**, select **AutoUpdate Task**.
- Type a name for the task, and any notes, then click **Save**. The task is listed in the **Task Name**
- Select the task and click **Next**.
- Schedule the task as required, then click **Next** to view a summary of the task.
- Review the summary of the task, then click **Save**.

- 9 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
- 10 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

See also

Product versions and updates on page 39

Schedule an on-demand scan

Schedule an on-demand scan to scan your Microsoft Exchange servers to find a threat, vulnerability, or other potentially unwanted code.

Before you begin

Make sure that you do not remove the **MSMEODuser** from active directory, that was created during the product installation. This user is required for performing on-demand scans on mailboxes.

Task

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree**, then select the required group or systems.
- 3 Click the **Assigned Client Tasks** tab, then click **Actions | New Client Task Assignment**. The **Client Task Assignment Builder** page appears.
- 4 Define these options, then click **Create New Task**.
 - a For **Product**, select **McAfee Security for Microsoft Exchange 8.5.0**
 - b For **Task Type**, select **On Demand Scan Task**.
- 5 Type a name for the task, and any notes, then click **Save**. The task is listed in the **Task Name**.
- 6 On the **Create New Task** page, define these options, then click **Save**:
 - **Task Name**
 - **Description**
 - **Resumable Scanning**
 - **Select Policy**
 - **Advanced Filters**



Check the **Resumable Scanning** option to schedule the on-demand scan task for large volume items.

- 7 Select the task, then click **Next**.
- 8 Schedule the task as required, then click **Next** to view a summary of the task.
- 9 Review the summary of the task, then click **Save**.
- 10 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
- 11 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.



During the scan, the complete store database is scanned.

On-demand scanning events are reported to ePolicy Orchestrator with the details start time, stop time, completed time, and infection status.

See also

[On-Demand scan and its views on page 42](#)

[Create on-demand scan task on page 44](#)

Schedule to send status report

Schedule to send the status report to an administrator at a specific time.

You can configure these settings in the status report task wizard.

- When to send the status report
- A time limit for the reporting task
- Recipients of the status report
- A name for the report task to help identify it

Task

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree**, then select the required group or systems.
- 3 Click the **Assigned Client Tasks** tab, then click **Actions | New Client Task Assignment**. The **Client Task Assignment Builder** page appears.
- 4 Define these options, then click **Create New Task**.
 - a For **Product**, select **McAfee Security for Microsoft Exchange 8.5.0**
 - b For **Task Type**, select **Status Report Task**.
- 5 Type a name for the task, and any notes, then click **Save**. The task is listed in the **Task Name**.
- 6 On the **Create Task Catalog** page, define these options, then click **Save**:

• Task Name	• Subject line for report
• Description	• Number of Rows
• Recipient E-mail	• Type of Report
- 7 Select the task and click **Next**.
- 8 Schedule the task as required, then click **Next** to view a summary of the task.
- 9 Review the summary of the task, then click **Save**.
- 10 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
- 11 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

See also

[Status reports on page 46](#)

Schedule to send configuration report

Schedule to send the configuration report to an administrator at a specific time.

Task

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree**, then select the required group or systems.
- 3 Click the **Assigned Client Tasks** tab, then click **Actions | New Client Task Assignment**. The **Client Task Assignment Builder** page appears.
- 4 Define these options, then click **Create New Task**.
 - a For **Product**, select **McAfee Security for Microsoft Exchange 8.5.0**.
 - b For **Task Type**, select **Configuration Report Task**.
- 5 Type a name for the task, and any notes, then click **Save**. The task is listed in the **Task Name**.
- 6 On the **Create New Task** page, define these options, then click **Save**:
 - **Task Name**
 - **Description**
 - **Recipient E-mail**
 - **Subject line for report**
- 7 Select the task, then click **Next**.
- 8 Schedule the task as required, then click **Next** to view a summary of the task.
- 9 Review the summary of the task, then click **Save**.
- 10 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
- 11 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.



During the scan, the complete store database is scanned.

See also

[Configuration reports on page 49](#)

Schedule a task to purge the old DAT files

Schedule a task to purge the old DAT files from the managed systems.

Task

For option definitions, click ? in the interface.

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | System Tree**, then select the required group or systems.
- 3 Click the **Assigned Client Tasks** tab, then click **Actions | New Client Task Assignment**. The **Client Task Assignment Builder** screen appears.

- 4 Define these options, then click **Create New Task**:
 - a For **Product**, select **McAfee Security for Microsoft Exchange 8.5.0**
 - b For **Task Type**, select **PurgeOldDats Task**.
- 5 Type a name for the task, and any notes, then click **Save**. The task is listed in the **Task Name**
- 6 Select the task and click **Next**.
- 7 Schedule the task as required, then click **Next** to view a summary of the task.
- 8 Review the summary of the task, then click **Save**.
- 9 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
- 10 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.



For the number of DAT files, the policy uses the managed system's MSME configuration defined in **DAT Settings**.

Queries and reports

Run the predefined MSME queries to generate your reports, or modify them to generate custom reports.

Predefined queries

These predefined queries are added to the **McAfee Security for Microsoft Exchange Reports** group in ePolicy Orchestrator

Query	Retrieves information on...
MSME 85 : DLP and Compliance History	Historical data for the DLP and Compliance threat category of all managed MSME servers.
MSME 85 : File Attachments Blocked History	Historical data of managed MSME servers with file attachments blocked in email messages.
MSME 85 : File Attachments Blocked Today	The file attachments blocked in email messages as on current date.
MSME 85 : Number of Messages and Average Processing Time Today	The number of email messages scanned on each managed MSME server as on current date and their average scan time.
MSME 85 : Percentage of PUPs Detected Today	The percentage of potentially unwanted programs infected email messages detected on each server as on current date.
MSME 85 : Percentage of Spam Detected Today	The percentage of spam infected email messages detected on each server as on current date.
MSME 85 : Percentage of Virus Detected Today	The percentage of virus infected email messages detected on each server as on current date.
MSME 85 : PUPs Deleted Today	The potentially unwanted programs infected email messages deleted as on current date.
MSME 85 : PUPs Detection History	All potentially unwanted programs infected email messages detected.
MSME 85 : PUPs Detection Today	The potentially unwanted programs infected email messages detected as on current date.
MSME 85 : Spam detected in the last one week	The number of spam infected email messages detected on each day during the last one week.

Query	Retrieves information on...
MSME 85 : Spam detection history	All spam infected email messages detected. It displays a pie-chart representing the number of email messages by the type of spam detected.
MSME 85 : Spam detection today	The spam infected email messages detected as on date. It displays a pie-chart representing the number of email messages by the type of spam detected.
MSME 85 : Top 10 Attachment Types	The top 10 attachment types by their number of detections, which have triggered any rules.
MSME 85 : Top 10 Detected Viruses	The top 10 viruses by their number of detections.
MSME 85 : Top 10 Infected Exchange Servers	The top 10 Microsoft Exchange servers by number of infected email messages detected.
MSME 85 : Top 10 Unwanted Programs	The top 10 potentially unwanted programs by their number of detections.
MSME 85 : Top 10 Virus Recipients	The top 10 email addresses that received the maximum number of virus infected email messages.
MSME 85 : Top 10 Virus Senders	The top 10 email addresses that sent the maximum number of virus infected email messages.
MSME 85 : Unwanted Content Detected History	The potentially unwanted content detected in email messages.
MSME 85 : Virus Cleaned Today	The number of virus infected email messages cleaned as on current date.
MSME 85 : Virus Detection history	The number of virus infected email messages detected.
MSME 85 : Virus Detection Today	The number of virus infected email messages detected as on current date.
MSME 85 : Viruses detected in the last one week	The number of virus infected email messages detected on each day during the last one week.

Custom query filters

You can create custom queries with MSME specific filters to retrieve information on MSME data.

Filter	Filters the results based on...
DAT Version (McAfee Security for Microsoft Exchange)	The version of the virus signature files installed on the client systems.
Engine Version (McAfee Security for Microsoft Exchange)	The version of the scanning engine software installed on the client systems.
Hotfix/Patch Version (McAfee Security for Microsoft Exchange)	The patch version of the MSME software installed on the client systems.
Language (McAfee Security for Microsoft Exchange)	The language of the MSME software installed on the client systems.
Product Version (McAfee Security for Microsoft Exchange)	The version of the MSME software installed on the client systems.
Service Pack (McAfee Security for Microsoft Exchange)	The version of the Service Pack installed on the client systems.

Run a default query

Run the predefined MSME queries to generate reports based on MSME data.

Task

- 1 Log on to ePolicy Orchestrator as administrator.
- 2 Complete these steps according to your version of ePolicy Orchestrator

Version 4.6	Version 5.0 and 5.1
1 Click Menu Reporting Queries .	1 Click Menu Reporting Queries & Reports .
2 From Shared Groups in the Groups pane, select McAfee Security for Microsoft Exchange Reports .	2 From Shared Groups in the Groups pane, select MSME85REPORTS .

- 3 Select a query from the **Queries** list, then click **Run**. In the query result page, click any item in the results to drill down further.



To generate custom reports, duplicate a predefined query, then modify it per your requirements. For detailed instructions on working with queries, see the product guide for your version of ePolicy Orchestrator software.

- 4 Click **Close** when finished.

Filter events

Specify which MSME events generated from the client systems are to be forwarded to the server.

By default, all MSME events are enabled. Filter events based on the bandwidth used in your environment, and event-based queries required.

For more details on event filtering, see the product guide for your version of the ePolicy Orchestrator software.

Task

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu** | **Configuration** | **Server Settings**, select **Event filtering**, then click **Edit** at the bottom of the page.
- 3 Select **All events to the server** to forward all events to the ePolicy Orchestrator server, or select **Only selected events to the server** and select the MSME specific client events that you want to forward.

MSME events are prefixed with **McAfee Security for Microsoft Exchange** such as these:

- 34150: McAfee Security for Microsoft Exchange Packer detected (High)
- 34151: McAfee Security for Microsoft Exchange Phish detected (High)
- 34152: McAfee Security for Microsoft Exchange Mail size filter rule triggered (Medium)
- 34153: McAfee Security for Microsoft Exchange Signed content detected (Medium)
- 34154: McAfee Security for Microsoft Exchange Encrypted content detected (Medium)
- 34155: McAfee Security for Microsoft Exchange Corrupted content detected (Medium)
- 34156: McAfee Security for Microsoft Exchange Denial of service triggered (High)
- 34157: McAfee Security for Microsoft Exchange Protected content triggered (Medium)

- 34158: McAfee Security for Microsoft Exchange Password protected content detected (Medium)
- 34159: McAfee Security for Microsoft Exchange Blocked mime type detected (Medium)
- 34160: McAfee Security for Microsoft Exchange statistics and average scan time (Info)

4 Click **Save**.

The selected events are forwarded at the next agent-server communication.

See also

[Run a default query on page 159](#)

Configure automatic responses

Configure and schedule the MSME product health alerts to notify you on the product status.

Before you begin

Configure the **Mail Notifications** policy with the **Alert ePolicy Orchestrator** option as enabled.

For more details on automatic responses, see the product guide for your version of the ePolicy Orchestrator software.

Task

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Automation | Automatic Responses**, then click **Edit** next to **MSME 85 : Product Health Alert Notification**. Alternatively, duplicate **MSME 85 : Product Health Alert Notification** and edit its copy to retain the default values in the predefined notification.
- 3 In the **Description** step, select **Enable**, then click **Next**.
- 4 In the **Filter** step, select **Threat Action Taken** from available properties, select an appropriate comparison criteria, select the value as **MSME85PHA**, then click **Next**.



You can also select other appropriate filters, as required.

- 5 In the **Aggregation** step, select the appropriate aggregation, grouping, and throttling options, as required, then click **Next**.
- 6 In the **Actions** step, select **Send Email**, complete these options, then click **Next**.
 - **Recipients** — Email address of the health alert recipients.
 - **Importance** — Importance of the email notification: **High**, **Medium**, or **Low**.
 - **Subject** — Subject line for the email notification. Insert variables to include dynamic content. For example, event description.
 - **Body** — Body text of the email notification. Update the existing body text template, as required. The template uses variables to include dynamic content.
- 7 Review the summary, then click **Save**.

The selected recipients are notified, as configured.

See also

[Manage policies on page 151](#)

[Enable product health alerts on page 126](#)

Remove the software

Remove the MSME client software and extensions to remove the software and its features.

To completely remove the MSME software and its features from your environment, remove them in this order:

- 1 (If installed) Remove the McAfee Anti-spam software from the clients.
- 2 Remove the MSME client software from the clients.
- 3 (If installed) Remove the MSME reporting extension.
- 4 Remove the MSME software extension from ePolicy Orchestrator.

Tasks

- [Remove the McAfee Anti-spam software from clients on page 161](#)
Create a client task to remove McAfee Anti-spam software from the managed Microsoft Exchange servers.
- [Remove the client software on page 162](#)
Create a client task to remove MSME client software from the managed Microsoft Exchange servers.
- [Remove the software extension on page 162](#)
Remove the MSME extensions from the ePolicy Orchestrator server.

Remove the McAfee Anti-spam software from clients

Create a client task to remove McAfee Anti-spam software from the managed Microsoft Exchange servers.

Task

For option definitions, click ? in the interface.

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree**, then select the required group or systems.
- 3 Click the **Assigned Client Tasks** tab, then click **Actions | New Client Task Assignment**. The **Client Task Assignment Builder** page appears.
- 4 Define these options, then click **Create New Task**.
 - a For **Product**, select **McAfee Agent**
 - b For **Task Type**, select **Product Deployment**.
- 5 Type a name for the task, and any notes, then click **Save**. The task is listed in the **Task Name**.
- 6 On the **Create New Task** page, type a name for the task, and any notes.
- 7 Select **Windows** as a target platform.
- 8 In **Products and components**, select **McAfee Security for Microsoft Exchange (x64) - xxxxxxxx 8.5.0.xxxx**, select **Remove** as action, select the language, then click **Save**. The task is listed in the **Task Name**.
- 9 Select the task, then click **Next**.
- 10 Schedule the task to run immediately, then click **Next** to view a summary of the task.
- 11 Review the summary of the task, then click **Save**.

- 12 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
- 13 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

Remove the client software

Create a client task to remove MSME client software from the managed Microsoft Exchange servers.

Before you begin

When McAfee Anti-spam add-on has been deployed to the clients, remove it before removing the MSME client software.

Task

For option definitions, click ? in the interface.

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree**, then select the required group or systems.
- 3 Click the **Assigned Client Tasks** tab, then click **Actions | New Client Task Assignment**. The **Client Task Assignment Builder** page appears.
- 4 Define these options, then click **Create New Task**.
 - a For **Product**, select **McAfee Agent**
 - b For **Task Type**, select **Product Deployment**.
- 5 Type a name for the task, and any notes, then click **Save**. The task is listed in the **Task Name**.
- 6 On the **Create New Task** page, type a name for the task, and any notes:
- 7 Select **Windows** as a target platform.
- 8 In **Products and components**, select **McAfee Security for Microsoft Exchange (x64) - xxxxxxxx 8.5.0.xxxx**, select **Remove** as action, select the language, then click **Save**. The task is listed in the **Task Name**.
- 9 Select the task, then click **Next**.
- 10 Schedule the task to run immediately, then click **Next** to view a summary of the task.
- 11 Review the summary of the task, then click **Save**.
- 12 In the **System Tree** page, select the systems or groups where you assigned the task, then click **Wake Up Agents**.
- 13 In the **Wake Up McAfee Agent** screen, select **Force complete policy and task update**, then click **OK**.

Remove the software extension

Remove the MSME extensions from the ePolicy Orchestrator server.

Before you begin

If MSME reports extension is installed, remove it before removing the product extension.

Task

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 To remove the product extension, click **Menu | Software | Extensions**.
- 3 From the left pane, select **McAfee Security for Microsoft Exchange**.

The MSME extensions that are installed are displayed in the right pane.

- 4 Click the **Remove** button next to the MSME extension, select **Force removal, bypassing any checks or errors**, then click **OK**.

Remove the reports extension **McAfee Security for Microsoft Exchange Reports 8.5** (MSME85REPORTS.ZIP) first. Then repeat this step to remove the product extension **McAfee Security for Microsoft Exchange 8.5** (MSME____8500.ZIP).

9

Troubleshooting

Determine and troubleshoot issues while using MSME. Learn about the available performance counters and important registry keys associated with this product.

Contents

- ▶ *Default Vs. Enhanced configuration settings*
- ▶ *Important registry keys*

Default Vs. Enhanced configuration settings

Based on your requirement you can configure MSME to perform for maximum performance or maximum protection.

To modify your MSME configuration settings, go to **Settings & Diagnostics | Import and Export Configuration**. You can use:

- **Restore Default** — To configure MSME for maximum performance.
- **Restore Enhanced** — To configure MSME for maximum protection.

Table 9-1 Differences between Default and Enhanced configuration

Feature	Default	Enhanced
Message reputation	Disabled	Enabled
IP reputation	Disabled	Enabled
Maximum nesting level	10	50
Password Protected file	Allow through	Replace and quarantine
Protected file	Allow through	Replace and quarantine
File filter	Disabled	Enabled with default rule (*.exe, *.com, *.bat, *.scr)
Encrypted file	Allow through	Replace and quarantine
Corrupted file	Allow through	Replace and quarantine
Mail URL Reputation	Disabled	Enabled only for on-access scanning policies.

Important registry keys

Create these registry keys when the significance matches with your requirements.

Table 9-2 MSME – Important registry keys

Registry Key	Path	Significance
Name: DigestMail Type: DWORD Value: 1	HKEY_LOCAL_MACHINE \SOFTWARE \Wow6432Node \McAfee\MSME \ADUserCache	Maintains a cache of User Alias Vs SMTP address, which is used when MSME is integrated with MQM and the same address is used for Digest mail feature.
Name: ODUserID Type: REG_SZ Value: [Example: <admin@domain.com>]	HKEY_LOCAL_MACHINE \SOFTWARE \Wow6432Node \McAfee\MSME \E2007	Valid only for all Exchange Mailbox servers. Should be the email address of the On-demand user created by the product, used for interacting with Exchange web services for getting mail data from exchange database.
Name: EWSUrl Type: REG_SZ Value: https://<IP address>/EWS/ Exchange.asmx	HKEY_LOCAL_MACHINE \SOFTWARE \Wow6432Node \McAfee\MSME \OnDemand	Valid only for Exchange 2010 Mailbox servers. This is the URL used to connect to Exchange web services hosted by CAS server. This value is populated by powershell script GetHubTxDetails.ps1 during installation and also whenever MSME service is restarted.
Name: SCLJunkThreshold Type: DWORD Default value: 4	HKEY_LOCAL_MACHINE \SOFTWARE \Wow6432Node \McAfee\MSME \AntiSpam	Valid only for Exchange 2010 Mailbox servers. This is the SCL junk threshold, which is retrieved from AD and is at organization level. Any score above this value will be treated as Junk mail, which helps in Junk email routing on Exchange 2007/2010 Hub servers. This value is populated by powershell script GetSCLJunkThreshold.ps1 during installation, and also after some frequency.

10 Frequently asked questions

Provides answers to common situations that you might encounter when installing or using the product and contains troubleshooting information in the form of frequently asked questions.



To view an updated list of questions associated with this release, see the McAfee KnowledgeBase article [KB76886](#).

Contents

- ▶ *General*
- ▶ *Installation*
- ▶ *Policy Manager*
- ▶ *Settings and diagnostics*
- ▶ *McAfee Anti-Spam add-on component*
- ▶ *Regular Expressions (regex)*

General

Here are answers to general frequently asked questions.

Can email delivery be prioritized?

No. It cannot be prioritized, as this is an Exchange server task.

Do I still need to enable anonymous access to exchange server receive connector?

MSME does not require anonymous access to exchange receive connector. The on-demand user takes care of these functions. For more information on configuring anonymous access settings, see McAfee KnowledgeBase article [KB81752](#).

If an email is scanned in the Hub Transport server, will it be scanned in the Mailbox server?

It depends. If the email is scanned on the Hub server and has the same Anti-Virus (AV) stamp, then it will not be scanned on the Mailbox server. If the AV stamp differs either in terms of AV vendor or in terms of Engine/DAT version, it will be scanned on the Mailbox server.

Why should I use "Run as administrator" option in Windows 2008, to open the MSME user interface?

Due to security reasons, MSME will not be able to communicate with the RPC servers. This is due to the SID having no permission to do Inter-process communication (IPC) with the RPC process.

Under which executable does the scanning modules of MSME gets loaded across all Exchange versions?

The `RPCServ.exe` process loads all the scanning binaries. To find the process id of the scanner process, check the command line in **Task Manager** and see which `RPCServ.exe` process has the command line parameter: `/EVENTNAME:Global\MSME_scanner_RPCEvent`.

What is the optimum MSME configuration?

The configurations are for **Enhanced protection** and **Maximum performance**. The default configuration is to have maximum performance.

What should I exclude if MSME and a file level anti-virus is installed on the same server?

Exclude all the MSME binary folders and sub-folders, Postgres database, Replication folders, Exchange folders, ePolicy Orchestrator events folder, and product log.

Where can I find more information about Email Security?

For product solutions on email security, see <http://www.mcafee.com/us/products/email-and-web-security/email-security.aspx>.

How do I access the product interface of the remote system?

To access the remote MSME standalone interface:

- 1 Launch **McAfee Security for Microsoft Exchange - Product Configuration**.
- 2 From the **Change Server** menu, click **New Connection**.
- 3 In the **Browse for Computer** dialog box, type the IP address of the remote system, then click **OK**

To access the remote MSME web interface:

- 1 Launch **McAfee Security for Microsoft Exchange - Product Configuration (Web Interface)**.
- 2 In the address bar, type: `https://<Remote system IP Address>/MSME/0409/html/index.htm`
- 3 Provide the login credentials when prompted.

Installation

Here are answers to frequently asked questions on MSME installation.

How do I perform a silent installation?

Execute the `Silent.bat` file in the download package. For information on customization, see the *Perform a silent installation*.

Can I Install McAfee Security for Microsoft Exchange 8.5 using the account that is not a domain administrator?

You can install. For more information, see McAfee KnowledgeBase article [KB82190](#).

What is the supported ePolicy Orchestrator version?

McAfee ePolicy Orchestrator 4.6, 5.0, and 5.1.

What is the supported McAfee Agent version?

McAfee Agent 4.6 or later.

On which port does the MSME configuration replication works?

This service doesn't work on ports, but it keeps monitoring the folders that are set by administrator using replication user interface.

Do I have to consider anything special while upgrading to MSME 8.5 from MSME 7.6 or 8.0 in a CCR or DAG environment?

No considerations. Follow the standalone installation steps.

Policy Manager

Here are answers to frequently asked questions on the **Policy Manager** feature.

How do I create and use email policies?

Always create policies on gateway servers using the SMTP addresses and on mailbox servers using Active Directory (AD) groups. On Mailbox server, designing policies based on SMTP addresses will be very costly, as the product does not get SMTP addresses and in order to resolve the same, AD queries are made. Doing this will slow down the performance on the Mailbox servers.

Do domain names in policies affect performance?

Yes. For detailed explanation, see the previous question *How do I create and use email policies*.

How does policy priority work?

Whenever a child policy gets satisfied first based on the priority of resolution, the next policy is never evaluated.

Is it beneficial to have multiple policies and will it affect the server performance?

Yes, this will affect performance. During policy evaluation, when the first child policy is not satisfied and next policy is evaluated, there may be AD queries which might have to be made, thus resulting in slow performance.

How do I configure MSME to block executable files at a granular level?

You can do this using the **File Filtering Rules** option. For example, let us see how to filter specific executable files such as the Windows executables.

- 1 From the product's user interface, click **Policy Manager | On-Access (Master Policy)**.
- 2 Under **Core-Scanners**, click **File Filtering** and enable this option.
- 3 Under **Options (Core Anti-Spam Settings)**, click **Edit**.
- 4 Under **Available rules** drop-down list, select **<Create a new rule...>**.
- 5 Specify a rule name and under **File category filtering**, select **Enable file category filtering**.
- 6 From **File categories** list, select **Other specific formats**.
- 7 From **Subcategories** list, select **Windows Executables**.
- 8 Click **Save**.

What type of file is detected as Packers or PUPs, and from where I can control this setting?

Packers and PUPs belong to the malicious content category that is detected based on the category. Packers generally are files that are compressed or packed using some algorithm and then get de-compressed on execution.

Control this setting from **Anti-Virus settings** in the MSME user interface.

Settings and diagnostics

Here are answers to frequently asked questions on the **Settings & Diagnostics** feature.

Does enabling caMcAfee GTI use email latency?

Yes, there will be latency due to the email validation by McAfee GTI.

How do I verify if Transport scanner is scanning for spam emails?

You can verify this from the product's user interface in either of these ways:

- From the **Recently Scanned items** page, see the mails scanned and check the policy used to scan the email. It should show **Gateway** under **Scanned by** field.
- From the **Detected Items** database, check if there are any spam emails detected. Finally verify if the emails are not through authenticated sessions, which are logged under **MSME Debug Logging**.

Can I export the Blacklists and Whitelists from one MSME server to another?

Yes, you can export the blacklists and whitelists from one MSME server to another. To do this:

- 1 From the product's user interface, click **Policy Manager | Gateway (Master Policy)**.
- 2 Under **Core-Scanners**, click **Anti-Spam**.
- 3 Under **Options (Core Anti-Spam Settings)**, click **Edit**.
- 4 Click the **Mail Lists** tab, and then click **Export** to save all Blacklisted and Whitelisted senders/recipients to a CSV file.

McAfee Anti-Spam add-on component

Here are answers to frequently asked questions on the Anti-Spam add-on component.

How do I update the Anti-spam engine manually?

Update registry key and place the new engine on the specified directory which is entered in registry under `SpamEngineVersion` registry key under `MSME\SystemState` registry. These two values should be in-sync. For example, if the engine version is 9039, create a directory with the name `9039` under `MSME\Bin\AntiSpam\Engine` and copy the engine file `masecore.dll` to this directory.

Can I edit the Anti-spam rules manually?

No.

What should I consider before adding an email address to the Blacklist?

- Make sure that McAfee Anti-Spam add-on component is installed.
- The Microsoft Exchange server must be a Transport server. For example, have an Exchange server with Edge Transport or Hub Transport role.
- Have an un-authenticated connection, where emails reach the server directly from internet.

How do I blacklist or whitelist an email address?

- 1 From the product's user interface, click **Policy Manager | Gateway (Master Policy)**.
- 2 Under **Core Scanners**, click **Anti-Spam**.
- 3 Under **Options (Core Anti-Spam Settings)**, click **Edit**.
- 4 Click the **Mail Lists** tab and then click **Add** for the required options such as Blacklisted or Whitelisted senders/recipients.

What should I do when few emails are not being detected as spam?

From **Settings & Diagnostics | Anti-Spam**, select **Enable message reputation** and apply the settings. Also, adjust the spam score to a value between 51 and 79, which will help with the detection rate.



The emails with a lower spam score (51–59) could still be legitimate, so tweaking the score is required.

Where can I get the Anti-spam add-on license?

You can download the `MSMEASA.ZIP` file from the McAfee download site, if you have valid McAfee Anti-spam grant number. If you do not have a valid Anti-spam grant number, call the McAfee Customer Service team.

Regular Expressions (regex)

Here are answers to frequently asked questions on the regular expressions (regex).

Does enabling regex cause email latency?

Yes, enabling regular expression causes email latency, as content scanning is a process intensive configuration.

Where do I find more information on regex?

Several websites on the Internet provide information on regular expressions.

To name a few, see:

- <http://www.regular-expressions.info/reference.html>
- <http://www.regexbuddy.com/regex.html>

How do I block certain Credit Card numbers and Social Security numbers using regex?

- 1 From the product's user interface, click **Policy Manager | Shared Resource**. The **Shared Resources** page appears.
- 2 In the **DLP and Compliance Dictionaries** tab, click **New Category** and specify a category name.
- 3 Click **OK**.
- 4 Under **DLP and Compliance Rules**, click **Create New**.

- Specify the Rule Name, Description and under Word or Phrase specify the regular expression.

Table 10-1 Example: How to validate Credit Card Numbers

Card type	Regular Expression	Description
Visa	<code>^4[0-9]{12}([0-9]{3})?*</code>	All Visa card numbers start with number 4. New cards have 16 digits. Old cards have 13.
MasterCard	<code>^5[1-5][0-9]{14}</code>	All MasterCard numbers start with the numbers 51 through 55. All have 16 digits.
American Express	<code>^3[47][0-9]{13}</code>	American Express card numbers start with 34 or 37 and have 15 digits.
Diners Club	<code>^3(?:0[0-5] [68][0-9])[0-9]{11}</code>	Diners Club card numbers begin with 300 through 305, 36 or 38. All have 14 digits. There are Diners Club cards that begin with 5 and have 16 digits. These are a joint venture between Diners Club and MasterCard, and should be processed like a MasterCard.
Discover	<code>^6(?:011 5[0-9]{2})[0-9]{12}</code>	Discover card numbers begin with 6011 or 65. All have 16 digits.
JCB	<code>^(?:2131 1800 35\d{3})\d{11}</code>	JCB cards beginning with 2131 or 1800 have 15 digits. JCB cards beginning with 35 have 16 digits.

Based on the example mentioned above, you can also create a similar regular expression for Social Security numbers. For more examples on regular expressions, refer <http://www.regular-expressions.info/examples.html>.

- Select the **Regular Expression** option and click **Save**.
- Add this to the **DLP and Compliance** policy in **Policy Manager** by clicking **Policy Manager | On-Access (Master Policy) | DLP and Compliance**.
- Under **Activation**, select **Enable**.
- Under **DLP and Compliance rules and associated actions**, click **Add rule**.
- Under **Select rules group**, select the regex rule that you created earlier from the drop-down list.
- Specify the action to take, when the rule is triggered.
- Click **Save**.

A

Using McAfee Security for Microsoft Exchange Access Control

Allow or deny access to the MSME user interface for specific users or groups.

Task

- 1 From the **Start** menu, click **Programs | McAfee | Security for Microsoft Exchange | Access Control**. The **Permissions for Access** dialog box appears.

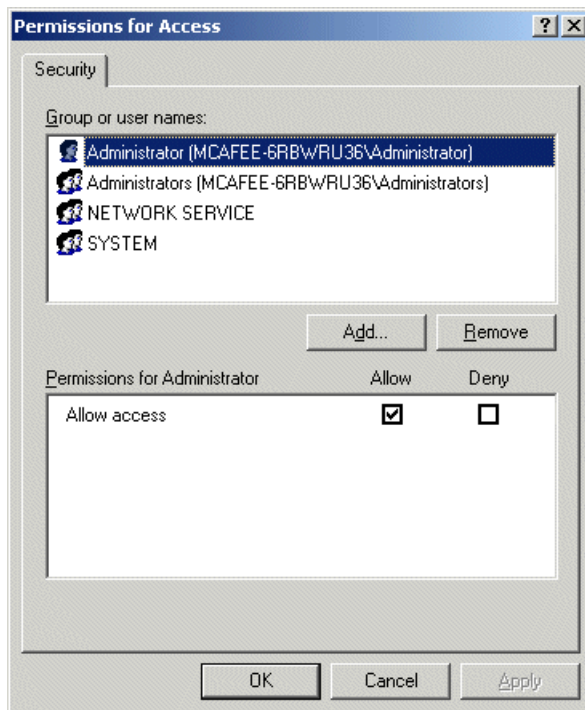


Figure A-1 Permissions for Access

- 2 From **Group or user names**, select the user you want to allow or deny access to the MSME user interface.
- 3 Click **OK**.

B

SiteList Editor

SiteList specifies the location from where automatic updates (including DAT file and scanning engines) are downloaded.

Access SiteList Editor

- From the **Start** menu, click **Programs | McAfee | Security for Microsoft Exchange | SiteList Editor**.

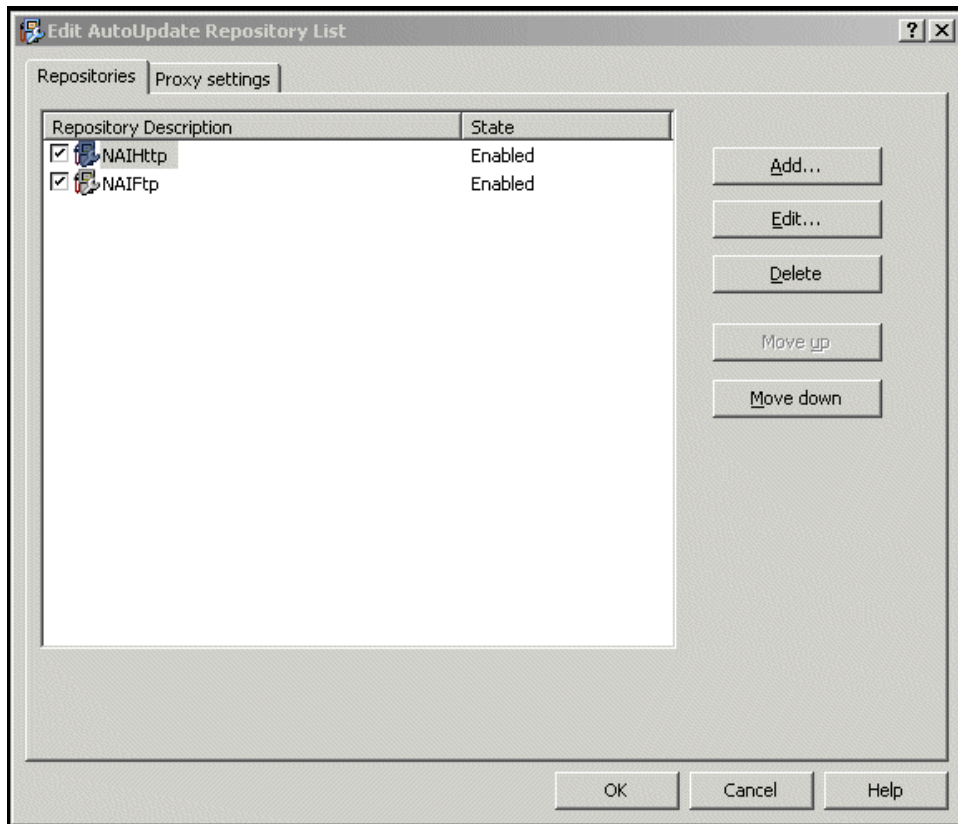


Figure B-1 Edit AutoUpdate Repository List

You can use these tabs:

- **Repositories** — To configure repository settings from where MSME can download automatic updates. By default, MSME uses a sitelist that points to a McAfee site for automatic updates, but you can also create alternative sitelists that point to a different location. For example, you might have copied the automatic updates to a local repository and created a sitelist that points your MSME systems to that local repository.
- **Proxy settings** — To configure the proxy server settings, so that MSME can connect to the Internet using this server, to download automatic updates.



Settings applied in the SiteList Editor are saved in the `SiteList.xml` file under `C:\ProgramData\McAfee\Common Framework\` directory.

Contents

- [Configure sitelist repository settings](#)
- [Configure sitelist proxy settings](#)

Configure sitelist repository settings

The **SiteList** specifies from where automatic updates are downloaded.

By default, McAfee Security for Microsoft Exchange uses a sitelist that points to a McAfee site for automatic updates, but you can use a sitelist that points to a different location. For example, you might have copied the automatic updates to a local repository and created a sitelist that points your McAfee Security for Microsoft Exchange systems to that local repository.

Task

- 1 Click **Start | Programs | McAfee | Security for Microsoft Exchange | SiteList Editor**. The **Edit AutoUpdate Repository List** dialog box appears.
- 2 From the **Repositories** tab, click **Add**. The **Repository Settings** dialog box appears.

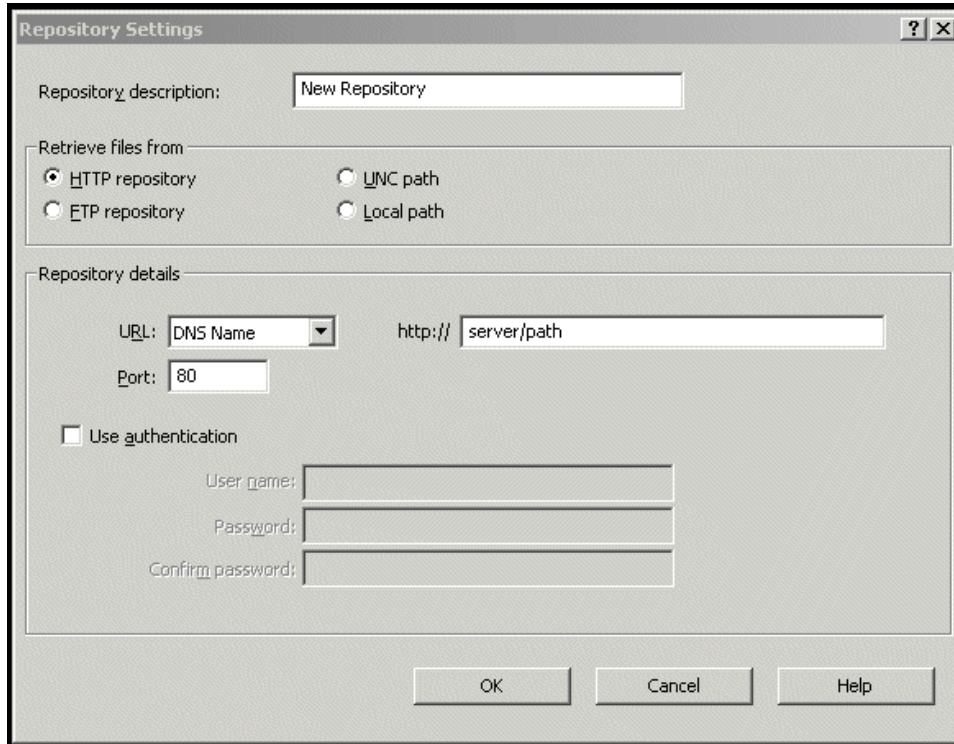


Figure B-2 Repository Settings

- 3 Select from the following Settings options:
 - **Repository Description** — To give a brief description of the repository.
 - **Retrieve files from** — To specify from which type of repository to retrieve the files. The available options are **HTTP repository**, **FTP repository**, **UNC Path**, and **Local Path**.
 - **URL** — To specify the URL of the repository.
 - **Port** — To specify the port number of the repository.
 - **Use Authentication** — To enable user authentication to access the repository.
- 4 Specify a user name and password for authentication of the repository and confirm the password by typing it again.
- 5 Click **OK** to add the new repository to the **Repository Description** list.
- 6 Click **OK** to close the **Edit AutoUpdate Repository List** dialog box.

Configure sitelist proxy settings

Configure these settings if your organization uses a proxy server to connect to the Internet, for MSME to download the product updates.

If your organization uses proxy servers for connecting to the Internet, you can select the **Proxy settings** option.

Task

- 1 Click **Start | Programs | McAfee | Security for Microsoft Exchange | SiteList Editor**.

The **Edit AutoUpdate Repository List** dialog box appears.

- 2 Click the **Proxy settings** tab.

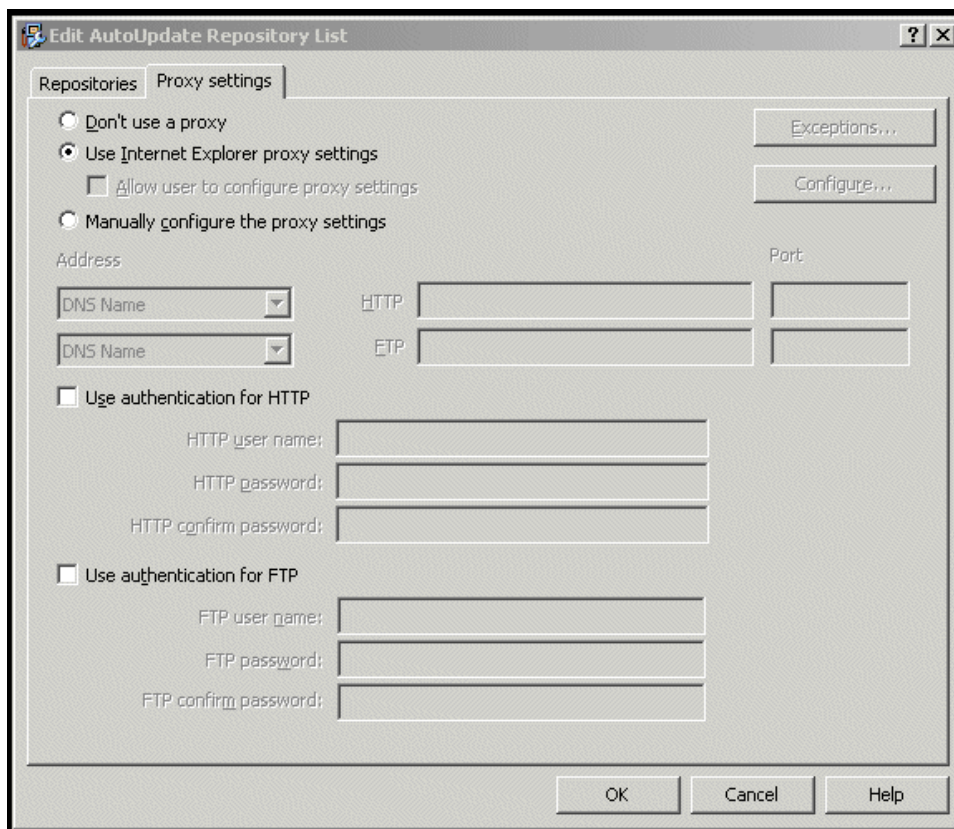


Figure B-3 Proxy settings

- 3 Select the **Use Internet Explorer proxy settings** or **Manually configure the proxy settings** option as required.
- 4 Type the IP address and port number of the HTTP or FTP server.
- 5 You can use the following options:
 - **Use Authentication** — To enable user authentication to access the proxy server.
 - **Username** — To specify a user name for authentication to access the proxy server.
 - **Password** — To specify a password.

- **Confirm Password** — To reconfirm the specified password.
- **Exceptions** — To bypass a proxy server for specific domains. Click **Exceptions**, then select **Specify Exceptions** and type the domains that need to be bypassed.

6 Click **OK**.

Index

- A**
 - about this guide [7](#)
 - access
 - SiteList Editor [175](#)
 - access control
 - configuring [173](#)
 - action to take
 - detected items [65](#)
 - actions
 - primary [79](#)
 - secondary [79](#)
 - to take [79](#)
 - add
 - filter [78](#)
 - scanner [78](#)
 - add resource to cluster group [29](#)
 - additional components [31](#)
 - advanced
 - policy view [71](#)
 - advanced search filters [53](#)
 - alert
 - creating new [83](#)
 - alert message
 - configuring settings [111](#)
 - alerts
 - configuring [82](#)
 - enabling product health [126](#)
 - anti-phishing scanner
 - configuring settings [102](#)
 - anti-spam
 - configure settings [128](#)
 - anti-spam add-on
 - faqs [170](#)
 - anti-spam component [32](#)
 - anti-spam scanner
 - configuring settings [99](#)
 - anti-virus component [32](#)
 - anti-virus scanner
 - configuring settings [91](#)
 - automatic update
 - schedule [40](#), [153](#)
 - available
 - scanners and filters [75](#)
- B**
 - background scan
 - configuring on-access settings [119](#)
 - banned file messages [58](#)
 - banned file types [58](#)
 - blacklist
 - exporting [101](#)
 - importing [101](#)
- C**
 - chart
 - configure settings [133](#)
 - check-in package [148](#)
 - Cluster Continuous Replication [29](#)
 - Cluster group [29](#)
 - cluster group resource [29](#)
 - comparison chart
 - scanners and filters [75](#)
 - configuration files [31](#)
 - configuration report task [156](#)
 - configuration reports [49](#)
 - email notification [52](#)
 - scheduling [50](#)
 - viewing [49](#)
 - configure
 - access control [173](#)
 - alerts [82](#)
 - anti-spam proxy settings [141](#)
 - DLP and Compliance Rules [85](#)
 - File Filtering Rules [88](#)
 - notification settings [124](#)
 - quarantine location [57](#)
 - scanners [81](#)
 - sitelist proxy settings [178](#)
 - sitelist repository settings [176](#)
 - configure on-access settings
 - background scan [119](#)
 - transport scan [120](#)
 - configure settings
 - alert message [111](#)
 - anti-phishing scanner [102](#)
 - anti-spam scanner [99](#)
 - anti-virus scanner [91](#)

configure settings (*continued*)

- corrupt content [103](#)
- DAT [139](#)
- disclaimer text [112](#)
- DLP and compliance scanner [93](#)
- encrypted content [104](#)
- export [139](#)
- file filtering [95](#)
- from another server [140](#)
- HTML files [110](#)
- import [139](#)
- local database [131](#)
- mail size filter [106](#)
- McAfee Quarantine Manager [129](#)
- MIME mail [108](#)
- password-protected files [105](#)
- protected content [104](#)
- scanner control [107](#)
- signed content [105](#)

contents, package [21](#)conventions and icons used in this guide [7](#)

core

- filters [74](#)
- scanners [74](#)

core scanner

- managing settings [90](#)

corrupt content

- configuring settings [103](#)

create

- new alert [83](#)
- new rule for new users [79](#)
- on-demand scan task [44](#)
- subpolicy [72](#)

D

dashboard

- configure settings [132](#)

Dashboard [33](#)

DAT settings

- configuring [139](#)

database

- optimizing [144](#)
- PostgreSQL [131](#)
- purging [144](#)

debug log

- configure settings [133](#)

default query [159](#)

default settings

- restoring [144](#)

default vs. enhanced

- settings [165](#)

denial of service [53](#)

detected items

- action to take [65](#)

detected items (*continued*)

- additional search options [63](#)
- comparison chart [62](#)
- configuring settings [129](#)
- primary search filters [60](#)
- search results [65](#)
- searching [64](#)
- viewing [57](#)

detection

- real-time [14](#)

detection name [53](#)detection types [58](#)

diagnostics

- configure settings [133](#)

disclaimer text

- configuring settings [112](#)

DLP and Compliance [58](#)

DLP and Compliance Rules

- configuring [85](#)

DLP and compliance scanner

- configuring settings [93](#)

documentation

- audience for this guide [7](#)
- product-specific, finding [8](#)
- typographical conventions and icons [7](#)

E

edit

- notification template [125](#)

EICAR test file [32](#)

emails

- how are they scanned [16](#)

encrypted content

- configuring settings [104](#)

error reporting service

- configure settings [137](#)

event log

- configure settings [135](#)

exchange server

- protecting your [14](#)
- supported roles [21](#)

exclude mailboxes [121](#)

existing configuration

- exporting [140](#)

export

- blacklists [101](#)
- configuring settings [139](#)
- existing configuration [140](#)
- whitelists [101](#)

extension check-in [148](#)**F**

faqs

- anti-spam add-on [170](#)

- faqs (*continued*)
 - general [167](#)
 - install [168](#)
 - Policy Manager [168](#)
 - regex [171](#)
 - regular expressions [171](#)
 - settings and diagnostics [169](#)
 - features
 - new [9](#)
 - product [11](#)
 - fields you can use, notification [126](#)
 - file filter
 - configuring settings [95](#)
 - File Filtering Rules
 - configuring [88](#)
 - filter
 - adding [78](#)
 - managing settings [103](#)
 - filters [74](#)
 - available [75](#)
 - folders exclusion
 - configuring settings [121](#)
 - frequently asked questions [167](#)
- G**
- general
 - faqs [167](#)
 - graph
 - configure settings [133](#)
 - graphical reports [52](#)
 - GTUBE test file [32](#)
- H**
- HTML files
 - configuring settings [110](#)
- I**
- import
 - blacklists [101](#)
 - configuring settings [139](#)
 - settings from another server [140](#)
 - sitelists [139](#), [141](#)
 - whitelists [101](#)
 - inbound emails
 - scanning [16](#)
 - information
 - product [40](#)
 - inheritance
 - policy view [71](#)
 - install
 - faqs [168](#)
 - modifying [143](#)
 - repairing [143](#)
 - installation
 - using wizard [22](#)
 - installed components [31](#)
 - internal emails
 - scanning [18](#)
 - introduction [9](#)
- K**
- keys
 - registry [166](#)
- L**
- license
 - product [39](#)
 - licenses
 - product [41](#)
 - list
 - filters [77](#)
 - scanners [77](#)
 - local database
 - quarantine using [131](#)
 - local database vs. MQM [57](#)
- M**
- mail size filter
 - configuring settings [106](#)
 - mail URL reputation [58](#)
 - configuration [96](#)
 - mailbox exclusion
 - configuring settings [121](#)
 - manage
 - filter settings [103](#)
 - miscellaneous settings [111](#)
 - quarantined data [57](#)
 - scanner settings [90](#)
 - manage using ePolicy Orchestrator [147](#)
 - prerequisites [147](#)
 - Master policy [72](#)
 - master repository [148](#)
 - McAfee Quarantine Manager
 - quarantine using [129](#)
 - McAfee ServicePortal, accessing [8](#)
 - McAfee Virtual Technician [32](#)
 - migrate policies
 - from ePolicy Orchestrator [148](#)
 - MIME [53](#)
 - MIME mail
 - configuring settings [108](#)
 - miscellaneous
 - managing settings [111](#)
 - modify
 - installation [143](#)
 - MQM vs. local database [57](#)

N

- new features [9](#)
- notification
 - settings [123](#)
- notification fields
 - using [126](#)
- notification template
 - editing [125](#)
- notifications
 - configuration report [52](#)
 - configuring [124](#)
 - status report [48](#)

O

- on-access settings [117](#)
 - configure VSAPI [118](#)
- on-demand
 - scanning [42](#)
- on-demand scan [42](#)
 - creating [44](#)
 - scheduling [44](#)
 - viewing [43](#)
- on-demand scan task [154](#)
- on-demand user
 - password reset [120](#)
- optimize
 - database [144](#)
- organizational threats [13](#)
- outbound emails
 - scanning [17](#)

P

- package contents [21](#)
- packer [53](#)
- password-protected files
 - configuring settings [105](#)
- phish [53](#), [58](#)
- policies
 - migrating [148](#)
 - prioritizing [71](#)
 - sorting [71](#)
- Policy Manager
 - faqs [168](#)
- policy settings
 - manage core scanners [90](#)
 - manage filters [103](#)
 - manage miscellaneous [111](#)
- policy view
 - advanced [71](#)
 - inheritance [71](#)
- PostgreSQL database [131](#)
- potentially unwanted program [53](#)
- potentially unwanted programs [58](#)
- pre-installation [19](#)

- primary
 - actions [79](#)
- prioritize
 - policies [71](#)
- product
 - license [39](#)
 - update [39](#)
- product features [11](#)
- product health alerts
 - enabling [126](#)
- product information [40](#)
- product log
 - configure settings [136](#)
- product logs
 - viewing [138](#)
- program
 - maintaining the [143](#)
- protect
 - exchange server [14](#)
- protected content
 - configuring settings [104](#)
- proxy settings
 - configuring anti-spam [141](#)
 - configuring sitelist [178](#)
- purge
 - database [144](#)
- purge DAT
 - schedule [156](#)

Q

- quarantine location
 - configuring [57](#)
- quarantined data
 - managing [57](#)
- quarantined items
 - action to take [65](#)
- queries
 - predefined [157](#)
- quick setup [28](#)

R

- real-time
 - detecting [14](#)
- recently scanned items [41](#)
- regex
 - faqs [171](#)
- registry keys
 - MSME [166](#)
- regular expressions
 - faqs [171](#)
- remove [145](#)
- remove extension [162](#)
- repair
 - installation [143](#)

- reports
 - graphical 52
- repository settings
 - configuring sitelist 176
- requirements
 - system 20
- restore
 - default settings 144
- roles supported
 - exchange server 21
- rule
 - creating new for specific users 79
- rules
 - DLP and Compliance 85
 - file filtering 88

S

- scan types
 - on-demand 42
- scanned items
 - recently 41
- scanner
 - adding 78
- scanner control
 - configuring settings 107
- scanners 74
 - available 75
 - configuring 81
- scanners and filters
 - comparison chart 75
 - listing 77
- schedule
 - automatic update 40
 - configuration reports 50
 - on-demand scan task 44
 - status reports 47
- scheduling tasks in ePolicy Orchestrator 153
- search
 - detected items 64
- search filters
 - comparison chart 62
 - primary 60
- search options
 - detected items 63
- secondary
 - actions 79
- ServicePortal, finding product documentation 8
- services 31
- setting policies in ePolicy Orchestrator 151
- settings
 - configure detected items 129
 - configure on-access 117
 - configuring anti-spam 128
 - configuring chart 133

- settings (*continued*)
 - configuring dashboard 132
 - configuring debug log 133
 - configuring diagnostics 133
 - configuring error reporting service 137
 - configuring event log 135
 - configuring graph 133
 - configuring local database 131
 - configuring McAfee Quarantine Manager 129
 - configuring product log 136
 - configuring user interface preferences 132
 - default vs. enhanced 165
 - notification 123
- settings and diagnostics
 - faqs 169
 - overview 115
- setup
 - quickly 28
- shared resource 81
 - configuring alerts 82
 - configuring DLP and Compliance Rules 85
 - configuring File Filtering Rules 88
 - configuring scanners 81
- signed content
 - configuring settings 105
- silent installation 25
- simple search filters 52
- Single Copy Cluster 29
- sitelist
 - importing 139
- SiteList
 - importing 141
- SiteList Editor
 - accessing 175
 - proxy settings 175
 - repository 175
- software
 - deployment 149
 - removing the 145
 - uninstalling the 145
 - upgrade 26
- software update
 - schedule 40
- sort
 - policies 71
- spam 58
- spam score 53
- specify
 - user 79
- statistical information 33
- statistics 33
- status report
 - schedule 155
- status reports 46
 - email notification 48

- status reports [46](#) (*continued*)
 - scheduling [47](#)
 - viewing [46](#)
- subject [53](#)
- subpolicies
 - creating [72](#)
- subpolicy [72](#)
- system
 - requirements [20](#)

T

- technical support, finding product information [8](#)
- test the installation [32](#)
- threats
 - to your organization [13](#)
- ticket number [53](#)
- time slots [89](#)
- transport scan
 - configuring on-access settings [120](#)
- type of scan
 - on-demand scan [42](#)
- types of
 - policy [72](#)
- types of detection [58](#)
- types of on-access scan
 - background [117](#), [119](#)
 - outbox [117](#)
 - proactive [117](#)
 - transport [117](#), [120](#)
 - VSAPI [117](#)

U

- uninstall [145](#)

- unwanted content [58](#)
- update
 - product [39](#)
 - software [40](#)
- updates
 - product version [39](#)
- user
 - specifying [79](#)
- user interface preferences
 - configure settings [132](#)
- using this guide [8](#)

V

- version
 - product [39](#)
- view
 - configuration reports [49](#)
 - detected items [57](#)
 - on-demand scan [43](#)
 - product logs [138](#)
 - status reports [46](#)
- viruses [58](#)
- VSAPI settings
 - configuring [118](#)

W

- what's new [9](#)
- whitelist
 - exporting [101](#)
 - importing [101](#)
- wildcards
 - examples [123](#)

