



GFI[®]

GFI MailEssentials[™]

ADMINISTRATOR GUIDE

Find out how you can manage and customize GFI MailEssentials. Tweak settings according to your requirements and troubleshoot any issues encountered.



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

GFI and GFI MailEssentials are trademarks or registered trademarks of GFI Software or its affiliates in the US and other countries. Any other trademarks contained herein are the property of their respective owners.

GFI MailEssentials is copyright of GFI Software. - 1999-2018 GFI Software. All rights reserved.

Document Version: 21

Last updated (month/day/year): 09/19/2018

Contents

1 Introduction	8
1.1 Terms and conventions used in this manual	8
1.2 GFI MailEssentials components	8
1.2.1 GFI MailEssentials scan engine	8
1.2.2 GFI MailEssentials web interface	8
1.2.3 GFI MailEssentials Switchboard	9
1.3 Inbound mail filtering	9
1.4 Outbound mail filtering	10
1.5 Email scanning and filtering engines	10
1.5.1 Malicious email scanning	10
1.5.2 Content filtering engines	11
1.5.3 Anti-spam filtering engines	11
1.5.4 Filters running at SMTP level	12
1.5.5 Other engines	12
1.6 Typical deployment scenarios	12
1.6.1 Installing directly on Microsoft® Exchange server	13
1.6.2 Installing on an email gateway or relay/perimeter server	13
1.7 End User Actions	15
2 Getting Started with GFI MailEssentials	16
2.1 System requirements	16
2.1.1 Hardware requirements	16
2.1.2 Software requirements	17
2.1.3 Virtualization	18
2.1.4 Antivirus and backup software	18
2.1.5 Firewall port settings	18
2.2 Pre-installation actions	19
2.2.1 Installing on the Microsoft® Exchange server	20
2.2.2 Installing on an email gateway or relay/perimeter server	20
2.2.3 Lotus Domino	23
2.3 Installation procedure	30
2.3.1 Important notes	30
2.3.2 Running the installation wizard	31
2.3.3 Installing GFI MailEssentials with GFI Directory	35
2.3.4 Post-Installation Wizard	37
2.4 Upgrading GFI MailEssentials	42
2.4.1 Upgrading from version 21	42
2.4.2 Upgrading from version 20	42
2.4.3 Upgrading from version 2015	43
2.4.4 Upgrading from version 2014	44
2.4.5 Upgrading from version 2012	45
2.5 Post-Install actions	45
2.5.1 Add engines to the Windows DEP Exception List	46
2.5.2 Test your installation	47
2.6 Obtaining a GFI MailEssentials subscription	48
2.6.1 Evaluating GFI MailEssentials for 30 days	49
2.6.2 I have a GFI Account and want to install GFI MailEssentials for the first time	49
2.6.3 Upgrading to a newer build or Service Release of the same version	49
2.6.4 Upgrading to a newer version of GFI MailEssentials	49
3 Monitoring status	50
3.1 Dashboard	50

3.1.1	Status and statistics	51
3.1.2	Email processing logs	53
3.1.3	Antivirus and anti-spam engine updates	56
3.1.4	Event logs	58
3.1.5	POP2Exchange activity	59
3.2	Reports	59
3.2.1	Enabling/Disabling reporting	59
3.2.2	Generating a report	60
3.2.3	Custom reports	63
3.2.4	Generating custom reports	64
3.2.5	Deleting custom reports	64
3.2.6	Searching the reporting database	64
3.2.7	Configuring reporting database	65
3.2.8	Maillnsights® report	68
4	Email Security	70
4.1	Virus Scanning Engines	70
4.1.1	Virus Scanning Priority	70
4.1.2	Avira	71
4.1.3	BitDefender	75
4.1.4	Kaspersky	79
4.1.5	Sophos	83
4.1.6	Cyren	87
4.2	Information Store Protection	91
4.2.1	Exchange Web Services (EWS) Settings	93
4.2.2	VSAPI Settings	93
4.3	Trojan and Executable Scanner	94
4.3.1	Configuring the Trojan & Executable Scanner	94
4.4	Email Exploit Engine	98
4.4.1	Configuring the Email Exploit Engine	98
4.4.2	Enabling/Disabling Email Exploits	101
4.5	HTML Sanitizer	102
4.5.1	Configuring the HTML Sanitizer	102
4.5.2	HTML Sanitizer Whitelist	103
4.5.3	HTML Santizer Domain\IP Exclusions	104
5	Anti-Spam	106
5.1	Anti-Spam filters	106
5.1.1	SpamRazer	107
5.1.2	Anti-Phishing	110
5.1.3	Directory Harvesting	112
5.1.4	Email blocklist	114
5.1.5	IP Blocklist	117
5.1.6	IP DNS Blocklist	119
5.1.7	URI DNS Blocklist	120
5.1.8	Sender Policy Framework	122
5.1.9	Anti-Spoofing	124
5.1.10	Greylist	126
5.1.11	Language Detection	128
5.1.12	Header Checking	129
5.1.13	Spam Keyword Checking	132
5.1.14	Bayesian Analysis	134
5.1.15	Whitelist	139
5.1.16	New Senders	143
5.2	Spam Actions - What to do with spam emails	145
5.2.1	Configuring Spam Actions	145

5.3	Sorting anti-spam filters by priority	147
5.4	SMTP Transmission Filtering	148
5.5	Spam Digest	150
5.5.1	Administrator spam digest	150
5.5.2	Recipient spam digest	150
5.6	Anti-Spam settings	152
5.6.1	Log file rotation	152
5.6.2	Anti-Spam Global Actions	153
5.6.3	DNS Server Settings	154
5.6.4	Remote Commands	155
5.6.5	Adding blocking reason to headers	157
5.7	SpamTag for Microsoft Outlook	158
5.7.1	Choosing SpamTag features	158
5.7.2	SpamTag requirements	161
5.7.3	Installing SpamTag manually	161
5.7.4	Installing SpamTag via GPO	162
5.7.5	Using SpamTag	164
5.8	Public Folder Scanning	164
5.8.1	Enabling Public folder Scanning	164
5.8.2	Using Public folder scanning	166
6	Content Filtering	168
6.1	Keyword Filtering	168
6.1.1	Creating a Keyword Filtering rule	168
6.1.2	Enabling/disabling Rules	173
6.1.3	Removing content filtering rules	173
6.1.4	Modifying an existing rule	174
6.1.5	Changing rule priority	174
6.2	Attachment Filtering	174
6.2.1	Creating an Attachment Filtering rule	174
6.2.2	Enabling/disabling rules	179
6.2.3	Removing attachment rules	179
6.2.4	Modifying an existing rule	179
6.2.5	Changing the rule priority	179
6.3	Advanced Content Filtering	180
6.3.1	Creating Advanced Content Filtering rules	180
6.3.2	Removing Rules	184
6.3.3	Enabling/Disabling Rules	184
6.3.4	Sorting Rules	184
6.4	Decompression Engine	185
6.4.1	Configuring the decompression engine filters	185
6.4.2	Enable/disable decompression filters	190
7	Quarantine	191
7.1	Important Notes	191
7.2	Searching the quarantine	191
7.3	Search Folders	196
7.3.1	Default Search Folders	196
7.3.2	Creating, editing and removing Custom Search Folders from Searches	198
7.3.3	Using the Search Folders node to auto-purge quarantined emails	198
7.4	Working with Quarantined emails	198
7.4.1	Viewing quarantined emails	198
7.4.2	Approving Quarantined Emails	201
7.4.3	Permanently Delete Quarantined Emails	201
7.5	Quarantine RSS Feeds	202
7.5.1	Enabling Quarantine RSS Feeds	202

7.5.2	Subscribing to Quarantine RSS feeds	203
7.5.3	Securing access to the GFI MailEssentials Quarantine RSS feeds	203
7.6	Quarantine Options	203
7.6.1	Spam Options	203
7.6.2	Malware Options	206
7.7	Quarantine Store Location and Public URL	209
8	Email Management	212
8.1	Disclaimers	212
8.1.1	Configuring Disclaimers	212
8.1.2	Disabling and enabling disclaimers	215
8.1.3	Sorting disclaimers by priority	215
8.2	Auto-Replies	215
8.2.1	Configuring auto-replies	216
8.3	List Server	217
8.3.1	Creating a newsletter or discussion list	217
8.3.2	Using Newsletters/Discussions	219
8.3.3	Configuring advanced newsletter/discussion list properties	220
8.4	Mail Monitoring	221
8.4.1	Adding new Mail Monitoring rules	221
8.4.2	How to use Mail Monitoring	222
8.4.3	Enabling/Disabling email monitoring rules	222
9	General Settings	224
9.1	Perimeter SMTP Server Settings	224
9.2	Administrator email address	225
9.3	Enabling/Disabling scanning modules	226
9.4	Proxy settings	227
9.5	Local domains	229
9.6	Managing local users	230
9.6.1	GFI MailEssentials installed in Active Directory mode	230
9.6.2	GFI MailEssentials installed in Remote Active Directory mode	230
9.6.3	GFI MailEssentials installed on the Microsoft® Exchange machine	230
9.6.4	GFI MailEssentials installed in SMTP mode	230
9.7	Remote Active Directory mode	231
9.8	Licensing	232
9.8.1	Editing License key	233
9.8.2	License key information	233
9.8.3	How to determine license requirements	233
9.9	SMTP Virtual Server bindings	233
9.9.1	Binding GFI MailEssentials to another other SMTP Virtual Server.	234
9.10	Product Updates	234
9.10.1	Viewing and installing downloaded updates	234
9.10.2	Disabling or modifying schedules	235
9.11	Access Control	236
9.12	Notification Templates	238
9.12.1	Editing Templates	239
10	Miscellaneous topics	243
10.1	Installation information	244
10.2	Virtual directory names	244
10.3	User interface mode	245
10.3.1	IIS Security Settings	246
10.4	GFI Directory mode	248
10.5	Failed emails	249
10.5.1	Reprocessing legitimate emails that fail	250

10.5.2 Failed emails notifications	250
10.6 Tracing	251
10.7 POP2Exchange - Download emails from POP3 server	253
10.7.1 Configuring POP3 downloader	253
10.7.2 Configure dial up connection options	255
10.8 Moving spam to user's mailbox folders	257
10.8.1 Microsoft® Exchange 2013/2016	257
10.8.2 Microsoft® Exchange 2010	258
10.9 Set a Microsoft® Exchange account	260
10.10 Exporting and importing settings manually	260
10.10.1 Export/Import settings via command line	263
10.11 Disabling email processing	265
10.12 Email backup before and after processing	266
10.13 Remoting ports	268
10.14 Monitoring Virus Scanning API	269
10.14.1 Performance monitor counters	270
11 GFI MailEssentials Multi-Server	272
11.1 Features synchronized by Multi-Server	272
11.2 Setting up Multi-Server	274
11.2.1 Configuring the master server	275
11.2.2 Configuring a slave server	276
11.2.3 Configuring the settings to synchronize	278
11.2.4 Configuring Reporting and Quarantine data centralization	280
12 Troubleshooting and support	282
12.1 Other troubleshooting resources	282
12.1.1 Knowledge Base	282
12.1.2 Web Forum	282
12.1.3 Request technical support	282
13 Glossary	283
14 Index	289

1 Introduction

The scope of this Administrator Guide is to help you install, run, configure and troubleshoot GFI MailEssentials on your network. The table below describes the contents of this guide.

Topics in this chapter:

1.1 Terms and conventions used in this manual	8
1.2 GFI MailEssentials components	8
1.3 Inbound mail filtering	9
1.4 Outbound mail filtering	10
1.5 Email scanning and filtering engines	10
1.6 Typical deployment scenarios	12
1.7 End User Actions	15

1.1 Terms and conventions used in this manual

Term	Description
>	Step by step navigational instructions to access a specific function.
Bold text	Items to select such as nodes, menu options or command buttons.
<i>Italics text</i>	Parameters and values that you must replace with the applicable value, such as custom paths and file names.
Code	Indicates text values to key in, such as commands and addresses.

For any technical terms and their definitions as used in this manual, refer to the [Glossary](#).

1.2 GFI MailEssentials components

1.2.1 GFI MailEssentials scan engine

The GFI MailEssentials scan engine analyzes the content of inbound, outbound and internal emails using a number of engines and filters. The result of the analysis identifies whether an email is to be blocked or allowed.

In Microsoft® Exchange environments, GFI MailEssentials also scans the Microsoft® Exchange Information Store.

1.2.2 GFI MailEssentials web interface

Through the GFI MailEssentials web interface, you can:

- » [Monitor email scanning activity](#)
- » [Manage scanning and filtering engines](#)
- » [Review and process quarantined emails](#)

- » Configure email management features
- » Generate reports

1.2.3 GFI MailEssentials Switchboard

Use the GFI MailEssentials Switchboard to configure:

- » How to launch the GFI MailEssentials user interface
- » Set Virtual Directory names for the web interface and RSS
- » Enable/Disable email processing
- » Enable/Disable tracing
- » Setting email backups before and after processing
- » Setting Quarantine Store location and Quarantine Public URL
- » Specifying a user account for 'Move to Exchange Folder' and Information Store Protection
- » Specifying Remoting Ports
- » Enable/Disable failed mail notifications

1.3 Inbound mail filtering

Inbound mail filtering is the process through which incoming emails are scanned and filtered before delivery to users.



Inbound emails are routed to GFI MailEssentials and processed as follows:

1. SMTP level filters (Directory Harvesting, Greylist, IP Blocklist & IP DNS Blocklist) can be executed before the email body is received.
2. The email is scanned by the malware and content filtering engines. Any email that is detected as containing malware is processed according to the actions configured. If an email is considered as safe, it then goes to the next stage.
3. The email is checked to see if it is addressed to a list in the list server. If the email matches a list, it will be processed by the list server.
4. The incoming email is filtered by the anti-spam filters. Any email that fails a spam filter check is processed as configured in the anti-spam actions. If an email goes through all the filters and is not identified as spam, it then goes to the next stage.
5. If configured, auto-replies are next sent to the sender.
6. If configured, email monitoring is next executed and the appropriate actions taken.
7. Email is next checked by the New Senders filter.
8. If email is not blocked by any scanning or filtering engine, it is sent to the user's mailbox.

1.4 Outbound mail filtering

Outbound mail filtering is the process through which emails sent by internal users are processed before sending them out over the Internet.



When sending an outbound email, this is routed to GFI MailEssentials and processed as follows:

1. The email is scanned by the malware and content filtering engines. Any email that is detected as containing malware is processed according to the actions configured. If an email is considered as safe, it then goes to the next stage.
2. Remote commands check and execute any remote commands in email, if any are found. If none are found, email goes to the next stage.
3. If configured, the applicable disclaimer is next added to the email.
4. If configured, email monitoring is next executed and the appropriate actions taken.
5. If enabled, Auto Whitelist adds the recipients' email addresses to the auto-whitelist. This automatically enables replies from such recipients to go to the sender without being checked for spam.
6. Email is sent to the recipient.

1.5 Email scanning and filtering engines

GFI MailEssentials contains a number of scanning and filtering engines to prevent malicious emails, spam and other unwanted emails from reaching domain users.

1.5.1 Malicious email scanning

The following engines scan and block emails containing malicious content.

Email scanning engine	Description
Virus Scanning Engines	GFI MailEssentials uses multiple antivirus engines to scan inbound, outbound and internal emails for the presence of viruses. GFI MailEssentials ships with Avira and BitDefender Virus Scanning Engines. You can also acquire a license for Kaspersky, Sophos & Cyren.
Information Store Protection	Use the Virus Scanning Engines to scan the Microsoft® Exchange mailbox databases and public folders for viruses.
Trojan & executable scanner	The Trojan and Executable Scanner analyzes and determines the function of executable files attached to emails. This scanner can subsequently quarantine any executables that perform suspicious activities (such as Trojans).
Email exploit engine	The Email Exploit Engine blocks exploits embedded in an email that can execute on the recipient's machine either when the user receives or opens the email.
HTML Sanitizer	The HTML Sanitizer scans and removes scripting code within the email body and attachments.

1.5.2 Content filtering engines

The following engines scan the content of emails, checking for parameters matching configured rules.

Email scanning engine	Description
Keyword Filtering	Keyword Filtering enables you to set up rules that filter emails with particular keywords or a combination of keywords in the body or subject of the email.
Attachment Filtering	Attachment Filtering allows you to set up rules to filter what types of email attachments to allow and block on the mail server.
Decompression engine	The Decompression engine extracts and analyzes archives (compressed files) attached to an email.
Advanced Content Filtering	Advanced Content filtering enables scanning of email header data and content using advanced configurable search conditions and regular expressions (regex).

1.5.3 Anti-spam filtering engines

The following engines scan and block spam emails.

Filter	Description	Enabled by default
SpamRazer	An anti-spam engine that determines if an email is spam by using email reputation, message fingerprinting and content analysis.	Yes
Anti-Phishing	Blocks emails that contain links in the message body pointing to known phishing sites or if they contain typical phishing keywords.	Yes
Directory Harvesting	Directory harvesting attacks occur when spammers try to guess email addresses by attaching well known usernames to your domain. The majority of the email addresses are non-existent.	Yes (only if GFI MailEssentials is installed in an Active Directory environment)
Email Blocklist	The Email Blocklist is a custom database of email addresses and domains from which you never want to receive emails.	Yes
IP Blocklist	The IP Blocklist is a custom database of IP addresses from which you never want to receive emails.	No
IP DNS Blocklist	IP DNS Blocklist checks the IP address of the sending mail server against a public list of mail servers known to send spam.	Yes
URI DNS Blocklist	Stops emails that contain links to domains listed on public Spam URI Blocklists.	Yes
Sender Policy Framework	This filter uses SPF records to stop email sent from forged IP addresses by identifying if the sender IP address is authorized.	No
Anti-Spoofing	Checks emails received with a sender email address claiming to originate from your own domain against a list of IP addresses by GFI MailEssentials. If the sender IP address is not on the list of own-domain server IP addresses, email is blocked.	No
Language Detection	Determines the language of the email body text and configurable to block certain languages.	No
Header Checking	The Header Checking filter analyses the email header to identify spam emails.	No

Filter	Description	Enabled by default
Spam Keyword Checking	This filter enables the identification of Spam based on keywords in the email being received.	No
Bayesian analysis	An anti-spam filter that can be trained to accurately determine if an email is spam based on past experience.	No

1.5.4 Filters running at SMTP level

The following engines scan and block emails during SMTP transmission before the email is received. For more information, refer to [SMTP Transmission Filtering](#) (page 148).

FILTER	DESCRIPTION	ENABLED BY DEFAULT
IP Blocklist	The IP Blocklist is a custom database of IP addresses from which you never want to receive emails.	No
Directory Harvesting	Directory harvesting attacks occur when spammers try to guess email addresses by attaching well known usernames to your domain. The majority of the email addresses are non-existent.	No
IP DNS Blocklist	IP DNS Blocklist checks the IP address of the sending mail server against a public list of mail servers known to send spam.	Yes
Greylist	The Greylist filter temporarily blocks incoming emails received from unknown senders. Legitimate mail systems typically try to send the email after a few minutes; spammers simply ignore such error messages.	No

1.5.5 Other engines

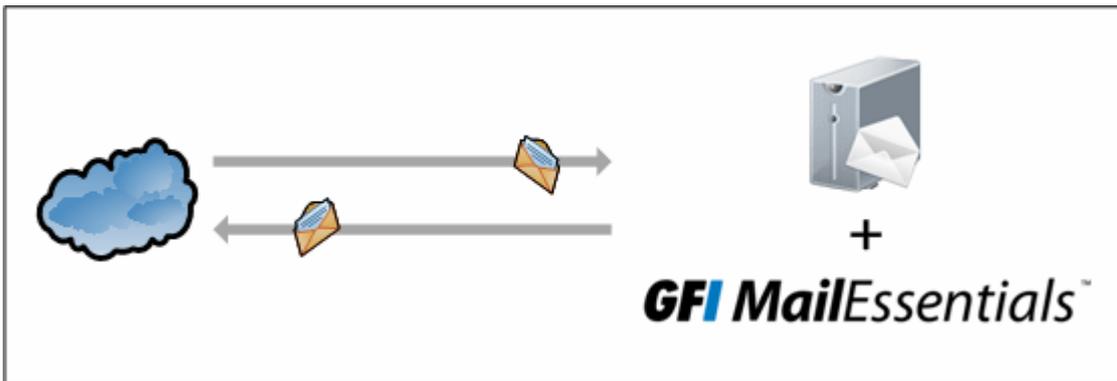
The following engines help to identify safe emails.

FILTER	DESCRIPTION	ENABLED BY DEFAULT
Whitelist	The Whitelist contains lists of criteria that identify legitimate email. Emails that match these criteria are not scanned by anti-spam filters and are always delivered to the recipient.	Yes
New Senders	The New Senders filter identifies emails that have been received from senders to whom emails have never been sent before.	No

1.6 Typical deployment scenarios

This chapter explains the different scenarios how GFI MailEssentials can be installed and configured.

1.6.1 Installing directly on Microsoft® Exchange server



Screenshot 1: Installing GFI MailEssentials on your Microsoft® Exchange server

You can install GFI MailEssentials directly on Microsoft® Exchange Server 2010 or later, without any additional configuration.

In Microsoft® Exchange 2010 environments, GFI MailEssentials can only be installed on the servers with the following roles:

- » Edge Server Role, or
- » Hub Transport Role, or
- » Hub Transport and Mailbox Roles - with this configuration GFI MailEssentials can also scan internal emails for viruses.

In Microsoft® Exchange 2013/2016, GFI MailEssentials can only be installed on the servers with the following roles:

- » Edge Transport role, or
- » Mailbox role.

NOTE

GFI MailEssentials supports a number of mail servers but can only be installed on the same machine as Microsoft® Exchange. For other mail servers, for example Lotus Domino, install GFI MailEssentials on a separate machine.

1.6.2 Installing on an email gateway or relay/perimeter server



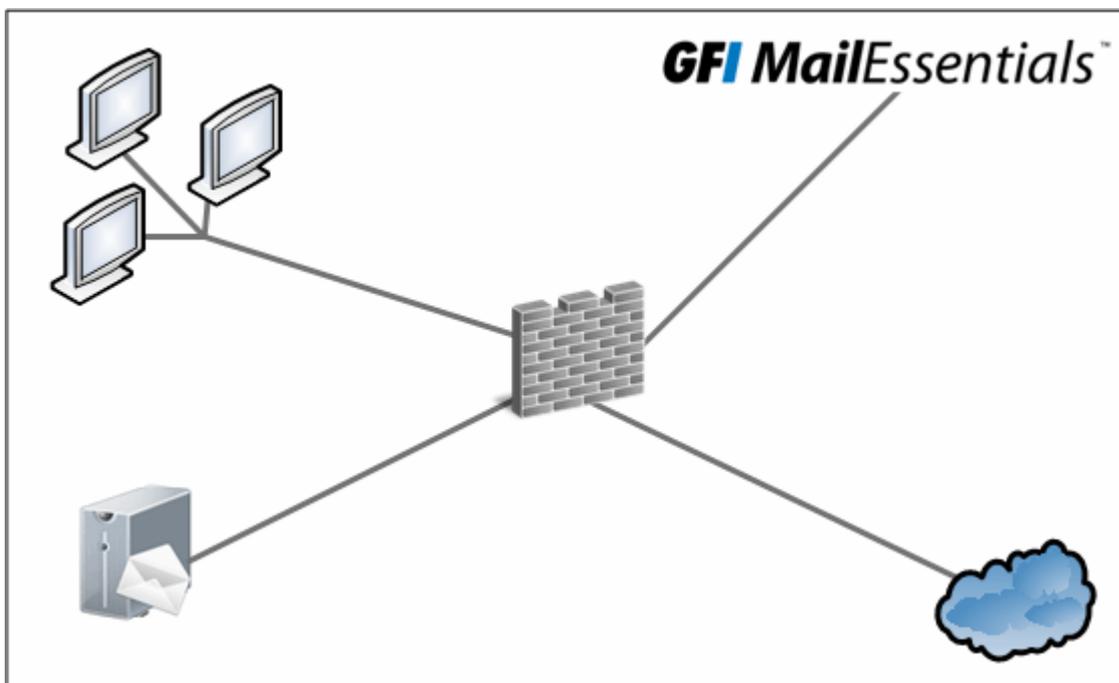
Screenshot 2: Installing GFI MailEssentials on a mail gateway/relay server

This setup is commonly used to filter spam on a separate machine, commonly installed in the DMZ. In this environment a server (also known as a gateway/perimeter server) is set to relay emails to the mail server. GFI MailEssentials is installed on the gateway/perimeter server so that spam and email malware is filtered before reaching the mail server.

This method enables you to filter out blocked emails before these are received on the mail server and reduce unnecessary email traffic. It also provides additional fault tolerance, where if the mail server is down, you can still receive email since emails are queued on the GFI MailEssentials machine.

When installing on a separate server (that is, on a server that is not the mail server), you must first configure that machine to act as a gateway (also known as “Smart host” or “Mail relay” server). This means that all inbound email must pass through GFI MailEssentials for scanning before being relayed to the mail server for distribution. For outbound emails, the mail server must relay all outgoing emails to the gateway machine for scanning before they are sent to destination.

If using a firewall, a good way to deploy GFI MailEssentials is in the DMZ. GFI MailEssentials will act as a smart host/mail relay server when installed on the perimeter network (also known as DMZ - demilitarized zone).



Screenshot 3: Installing GFI MailEssentials on a separate machine on a DMZ

NOTE

If GFI MailEssentials is installed on the perimeter server, you can use the anti-spam filters that run at SMTP level - Directory Harvesting and Greylist.

NOTE

In Microsoft® Exchange Server 2010 or later environments, mail relay servers in a DMZ can be running the Edge Transport Server Role.

NOTE

Configure the IIS SMTP Service to relay emails to your mail server and configure the MX record of your domain to point to the gateway machine. For more information, refer to [Installing on an email gateway or relay/perimeter server](#) (page 20).

1.7 End User Actions

GFI MailEssentials uses Active Directory groups to determine what is displayed to logged in users when they log into GFI MailEssentials. If the currently logged in user is part of the Administrators group, then GFI MailEssentials loads with all the configuration options that enable setting up GFI MailEssentials. If the currently logged in user is part of the users group, then GFI MailEssentials loads with only a limited number of options that enable the currently logged on user to administer his/her own quarantine and the personal whitelist/blocklists. The url used to log into GFI MailEssentials is always the same one, regardless of whether the currently logged on user is part of the administrator or user Active Directory group.

NOTE

User actions are only available if GFI MailEssentials is configured to use IIS mode. For more information, refer to [User interface mode](#) (page 245).

List of features available to user accounts:

Feature	Description
Personal Whitelist and Blocklist	Users may configure a complimentary list of whitelisted and blocklisted email addresses, over and above the list set up by the systems administrator. This feature is available only when the Personal Whitelist and/or Personal Blocklist are enabled. By default these options are not enabled.
Quarantine Search	Allows users to access and manage spam emails that were quarantined. Users can search through, view and then approve or delete quarantined emails. To make use of this feature, the action of anti-spam filters must be configured to quarantine spam emails. Users cannot manage quarantined malware emails due to the security risks involved.
SpamTag	Users can use the SpamTag addon in Microsoft Outlook to manage their preferences in management of spam emails. SpamTag must be installed on users' machine to be accessible via Microsoft Outlook. NOTE: This feature is not available to users in the GFI MailEssentials web interface. For more information, refer to SpamTag for Microsoft Outlook (page 158).
MailInsights®	MailInsights® is a reporting facility that gives a graphical presentation of the top 20 contacts that the user communicated with in the previous 30 days.

For more information on how end-users can use GFI MailEssentials, refer to the [GFI MailEssentials End User manual](#).

2 Getting Started with GFI MailEssentials

Want to try out GFI MailEssentials? This topic provides a quick list of actions to help you install and test the functionality of GFI MailEssentials.

- 1 Sign up to GFI MailEssentials**
Go to http://go.gfi.com/?pageid=ME_TRIALKEY and sign up for GFI MailEssentials. Follow the instructions to have your account created. After filling in the form you will be able to download the GFI MailEssentials installation executable. You will also receive a trial license key via email.
- 2 Prepare GFI MailEssentials server**
Common deployment methods include installing GFI MailEssentials on an email gateway, on a relay/perimeter server or directly on the Microsoft Exchange server. Choose a server within your network that meets or exceeds the GFI MailEssentials [system requirements](#) and configure mail routing depending on the placement of the server in the network. For more information, refer to [Typical deployment scenarios](#) (page 12).
- 3 Install GFI MailEssentials**
Run the GFI MailEssentials executable downloaded in step 1 above, on the server configured in step 2. After installing GFI MailEssentials, run the post-installation wizard which is automatically launched. For more information, refer to [Installation procedure](#) (page 30).
- 4 Launch the GFI MailEssentials Configuration**
Go to **Start > Programs > GFI MailEssentials > GFI MailEssentials Configuration** to launch the web-based interface where you can monitor, manage and configure GFI MailEssentials. Login with administrator credentials. Optimize your email protection system to ensure that it is effectively up and running. For more information, refer to [Post-Install actions](#) (page 45).
- 5 Test your installation**
GFI MailEssentials is now ready to start protecting and filtering your mail system from malicious and spam emails. Test your installation to ensure that GFI MailEssentials is working properly. For more information, refer to [Test your installation](#) (page 47).

2.1 System requirements

Before installing GFI MailEssentials, ensure that the system meets or exceeds the below requirements. If these requirements are not met, you may encounter problems during installation or in functionality.

2.1.1 Hardware requirements

The minimum hardware requirements for GFI MailEssentials are:

Component	Minimum	Recommended
Processor	2Ghz	2GHz with multiple cores
Available Memory (RAM)	1.2Gb	2Gb
Free Disk space	6Gb	10Gb

NOTE

Hardware requirements depend on a range of factors including email volume, and number of Anti Virus engines enabled in GFI MailEssentials. The requirements specified above are required for GFI MailEssentials only.

2.1.2 Software requirements

Supported Operating Systems

Install GFI MailEssentials on any 64-bit versions of the operating systems listed below.

Operating System	Supported Editions and notes
Microsoft® Windows Server 2016	Standard, Essentials and DataCenter editions. For more information refer to http://go.gfi.com/?pageid=ME_Win2016 .
Microsoft® Windows Server 2012	Standard, Essentials and DataCenter editions, including R2. For more information refer to http://go.gfi.com/?pageid=ME_Win2012 .
Windows® Server 2008 R2	Standard or Enterprise, For more information refer to http://go.gfi.com/?pageid=ME_Win2008 .
Windows® Small Business Server 2011	Standard & Premium.

Supported Mail Servers

GFI MailEssentials can be installed on the following mail servers without any further configuration.

- » Microsoft® Exchange Server 2016
- » Microsoft® Exchange Server 2013
- » Microsoft® Exchange Server 2010

For more information, refer to [Installing on the Microsoft® Exchange server](#) (page 20).

GFI MailEssentials can also be installed in an environment with any SMTP compliant mail server. In this case, GFI MailEssentials should be installed on the gateway/perimeter server so spam is filtered before reaching the mail server.

For more information, refer to [Installing on an email gateway or relay/perimeter server](#) (page 20).

Supported Internet browsers

GFI MailEssentials can be used with the following Internet browsers:

Browser	Version
Microsoft Internet Explorer	8 or later
Google Chrome	22 or later
Mozilla Firefox	16 or later

Other required components

Component	Notes
Internet Information Services (IIS®) World Wide Web service	
Internet Information Services (IIS®) SMTP service	Except when installing on Microsoft® Exchange 2010 or later server
Microsoft.NET® Framework 4	

Component	Notes
WCF HTTP Activation	Required when using SpamTag plugin for Microsoft Outlook
Windows® Authentication role and Static Content services	Required when installing on Microsoft® Windows Server 2008 R2 or later
Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1	Required when installing on Microsoft Exchange 2010 or later.
Microsoft XML core services	Installed automatically by GFI MailEssentials when installing on a US/UK English operating system.
MSMQ - Microsoft® Messaging Queuing Service	For more information refer to: <ul style="list-style-type: none"> • Windows Server 2016 • Windows Server 2012 • Windows Server 2008 • Windows Server 2003

2.1.3 Virtualization

GFI MailEssentials can be installed in a virtual environment that meets the requirements of a non-virtual environment, as defined in the previous sections.

VMware and Hyper-V are the only supported platforms for virtualization.

2.1.4 Antivirus and backup software

Antivirus and backup software scanning may cause GFI MailEssentials to malfunction. This occurs when such software denies access to certain files required by GFI MailEssentials.

Disable third party antivirus and backup software from scanning the following folders:

Folders to be excluded from antivirus scanning
<..\Program Files (x86)\Common Files\GFI>
<GFI MailEssentials installation path>\GFI\MailEssentials\
<..\Inetpub\mailroot> - if installed on a gateway machine.
<i>TransportRoles</i> folder located in the default Microsoft® Exchange installation path when GFI MailEssentials is installed on the same machine as Microsoft® Exchange 2010 or later.

2.1.5 Firewall port settings

Configure your firewall to allow the ports used by GFI MailEssentials.

Port	Description
53 - DNS	Used by the following anti-spam filters: <ul style="list-style-type: none"> » IP DNS Blocklist » SpamRazer » URI DNS Blocklist

Port	Description
80 - HTTP	<p>Used by GFI MailEssentials to download product patches and updates for:</p> <ul style="list-style-type: none"> » SpamRazer » Anti-Phishing » Bayesian Analysis » Antivirus definition files » Trojan and executable scanner » Email Exploit engine <p>GFI MailEssentials downloads from the following locations:</p> <ul style="list-style-type: none"> » meupdate.gfi.com » support.gfi.com » *.mailshell.net » *.rules.mailshell.net » spamrazer.gfi.com » db11.spamcatcher.net » gfi-downloader-137146314.us-east-1.elb.amazonaws.com » cdnupdate.gfi.com » cdnpatches.gfi.com <p>NOTE: GFI MailEssentials can also be configured to download updates through a proxy server. For more information, refer to Proxy settings (page 227).</p>
9090, 9091 - Remoting	<p>These ports are used for inter-process communication. No firewall configuration is required to allow connections to or from the remoting ports since all the GFI MailEssentials processes run on the same server.</p> <p>NOTE: Ensure that no other applications (except GFI MailEssentials) are listening on these ports. If other applications are using this ports, these ports can be changed. For more information, refer to Remoting ports (page 268).</p>
9095, 9096 - Multi-Server	<p>These TCP ports are used for communications between GFI MailEssentials servers that are joined to the Multi-Server network. Ensure that the master and all salve servers can communicate together via these ports.</p>
389/636 - LDAP/LDAPS	<p>This port is used in these scenarios:</p> <ul style="list-style-type: none"> » Remote Active Directory mode - When the GFI MailEssentials server is not joined to an Active Directory domain, but retrieves the list of users from a remote Active Directory instance. » GFI Directory mode - When the GFI MailEssentials server is not joined to an Active Directory domain, but retrieves the list of users from GFI Directory instance. » Microsoft® Exchange environment - Required if the server running GFI MailEssentials does not have access to or cannot get list of users from Active Directory, for example, in a DMZ environment or other environments which do not use Active Directory. » Lotus Domino mail server environment - Required to get email addresses from Lotus Domino server. » Other SMTP mail server environments - Required to get email addresses from SMTP server.
61000	<p>TCP port used for the communication between GFI MailEssentials and GFI Directory. If the GFI Directory is used, ensure that no other applications (except GFI MailEssentials) are listening on this port. This ports can be changed from the Switchboard. For more information, refer to GFI Directory mode (page 248).</p>

2.2 Pre-installation actions

Before installing GFI MailEssentials, prepare your environment for deployment.

Topics in this chapter:

- » [Installing on the Microsoft Exchange server](#)
- » [Installing on an email gateway or relay/perimeter server](#)
- » [Lotus Domino](#)

2.2.1 Installing on the Microsoft® Exchange server

When installing GFI MailEssentials on the same server as Microsoft® Exchange 2010 or later, no pre-install actions or configurations are required.

In Microsoft® Exchange 2010 environments, GFI MailEssentials can only be installed on the servers with the following roles:

- » Edge Server Role, or
- » Hub Transport Role, or
- » Hub Transport and Mailbox Roles - with this configuration GFI MailEssentials can also scan internal emails for viruses.

In Microsoft® Exchange 2013/2016, GFI MailEssentials can only be installed on the servers with the following roles:

- » Edge Transport role, or
- » Mailbox role.

2.2.2 Installing on an email gateway or relay/perimeter server

GFI MailEssentials can be installed:

- » On a perimeter server (for example, in a DMZ)
- » As a mail relay server between the perimeter (gateway) SMTP server and mail server.

This setup is commonly used to filter spam on a separate machine, commonly installed in the DMZ. In this environment a server (also known as a gateway/perimeter server) is set to relay emails to the mail server. GFI MailEssentials is installed on the gateway/perimeter server so that spam and email malware is filtered before reaching the mail server.

GFI MailEssentials uses the IIS SMTP service as its SMTP Server and therefore the IIS SMTP service must be configured to act as a mail relay server. To do this:

- » [Step 1: Enable IIS SMTP Service](#)
- » [Step 2: Create SMTP domains for email relaying](#)
- » [Step 3: Enable email relaying to your mail server](#)
- » [Step 4: Secure your SMTP email-relay server](#)
- » [Step 5: Enable your mail server to route emails via gateway](#)
- » [Step 6: Update your domain MX record to point to mail relay server](#)
- » [Step 7: Test your new mail relay server](#)

Step 1: Enable IIS SMTP Service

1. Launch Windows Server Manager.
2. Navigate to the **Features** node and select **Add Features**.
3. From the **Add Features Wizard** select **SMTP Server**.

NOTE

The SMTP Server feature might require the installation of additional role services and features. Click **Add Required Role Services** to proceed with installation.

4. In the following screens click **Next** to configure any required role services and features, and click **Install** to start the installation.
5. Click **Close** to finalize configuration.

Step 2: Create SMTP domain(s) for email relaying

1. Go to **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the left pane, expand the respective server node. Right click **Default SMTP Virtual Server** and select **Properties**.
4. Expand **Default SMTP Virtual Server** node.
5. Right-click **Domains** and select **New > Domain**.
6. Select **Remote** and click **Next**.
7. Specify organization domain name (for example, test.mydomain.com) and click **Finish**.

Step 3: Enable email relaying to your mail server

1. Right click on the new domain and select **Properties**.
2. Select **Allow the Incoming Mail to be Relayed to this Domain**.
3. Select **Forward all mail to smart host** and specify the IP address of the server managing emails in this domain. IP address must be enclosed in square brackets, for example, [123.123.123.123], to exclude them from all DNS lookup attempts.
4. Click **OK** to finalize your configuration.

Step 4: Secure your SMTP email-relay server

If unsecured, your mail relay server can be exploited and used as an open relay for spam. To prevent this, it is recommended that you specify which mail servers can route emails through this mail relay server (for example, allow only specific servers to use this email relaying setup). To achieve this:

1. Go to **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the left pane, expand the respective server node. Right-click on **Default SMTP Virtual Server** and select **Properties**.
3. From the **Access** tab, select **Relay**.
4. Select **Only the list below** and click **Add**.
5. Specify IP(s) of the internal mail server(s) that are allowed to route emails through your mail relay server. You can specify:
 - » Single computers - Authorize one specific machine to relay email through this server. Use the DNS Lookup button to lookup an IP address for a specific host.
 - » Group of computers - Authorize specific computer(s) to relay emails through this server.
 - » Domain - Allow all computers in a specific domain to relay emails through this server.

NOTE

The **Domain** option adds a processing overhead that can degrade SMTP service performance. This is due to the reverse DNS lookup processes triggered on all IP addresses (within that domain) that try to route emails through this relay server.

Step 5: Enable your mail server to route emails via GFI MailEssentials

SMTP/POP3 mail server

Configure your mail server to route all inbound and outbound email through GFI MailEssentials. In the configuration program of your mail server, use the option to relay all outbound email via another mail server (this option is usually called something similar to **Forward all messages to host**. Enter the computer name or IP of the machine running GFI MailEssentials. Save the new settings and restart your mail server.

Lotus Notes

For more information on how to setup Lotus Domino routing, refer to [Installation Guide \(Domino\)](#).

Step 6: Update your domain MX record to point to mail relay server

Update the MX record for your domain to point to the IP of the new mail relay server. If your DNS server is managed by your ISP, ask your ISP to update the MX record for you.

NOTE

If the MX record is not updated, all emails will be routed directly to your email server - hence bypassing GFI MailEssentials.

Verify that MX record has been successfully updated

To verify whether MX record is updated:

1. From command prompt key in `nslookup` and hit **Enter**.
2. Key in `set type=mx` and hit **Enter**.
3. Specify your mail domain name and hit **Enter**.

The MX record should return the IP addresses of the mail relay servers.

Step 7: Test your new mail relay server

Before proceeding to install GFI MailEssentials, verify that your new mail relay server is working correctly.

Test IIS SMTP inbound connection

1. Send an email from an 'external' account (example, from a Gmail account) to an internal email address/user.
2. Ensure that intended recipient received the test email in the respective email client.

Test IIS SMTP outbound connection

1. Send an email from an 'internal' email account to an external account (example, to a Gmail account).
2. Ensure that the intended recipient/external user received the test email.

NOTE

You can also use Telnet to manually send the test email and obtain more troubleshooting information. For more information refer to:

http://go.gfi.com/?pageid=ME_TelnetPort25

2.2.3 Lotus Domino

Information on using GFI MailEssentials with Lotus Domino.

- » [Lotus Domino incompatibilities](#)
- » [Installation information for Lotus Domino](#)
- » [Lotus Domino Anti Spam Folder Configuration](#)

Lotus Domino incompatibilities

Internal memos/emails are not scanned

GFI MailEssentials does not scan internal memos/emails sent by Lotus Domino since the Lotus Domino's sender/receiver format is not in a compatible format. When internal memos/emails are passed into GFI MailEssentials, these end up in the queue and are not processed.

NOTE

Do not pass internal memos/emails through GFI MailEssentials.

GFI MailEssentials List Server will not work with Lotus Domino

Creating Newsletters or discussion lists will not work for the internal domain of Lotus Domino. This option should not be used. If used, Lotus Domino users will not be able to send emails to the list.

GFI MailEssentials Installation Guide for Lotus Domino

Use the information in this section to install and configure Lotus Domino with GFI MailEssentials. Install GFI MailEssentials on a separate machine then Lotus Domino, as seen on the figure below.



Figure 1: GFI MailEssentials installation on a separate server than Lotus Domino

Install GFI MailEssentials by running the GFI MailEssentials installation file and following the onscreen instructions. For more information, refer to [Getting Started with GFI MailEssentials](#) (page 16).

If GFI MailEssentials is installed on a machine where Active Directory is present, one may encounter the dialog box below. Select **No, I do not have Active Directory...** to install GFI MailEssentials in SMTP mode.

Configure the machine where GFI MailEssentials is installed to act as a gateway (also known as "Smart host" or "Mail relay" server) for all email. Effectively, all inbound email must pass through this machine before relayed to the mail server for distribution (it is the first to receive all emails destined for your mail server).

The same applies for outbound emails; mail server must relay all outgoing emails to the gateway machine for scanning before these are sent to external recipients via Internet (it must be the last 'stop' for emails destined for the Internet). In this way, GFI MailEssentials checks all inbound and outbound mail before it is delivered to the recipients.

The MX record of your domain must point to the mail relay server

NOTE

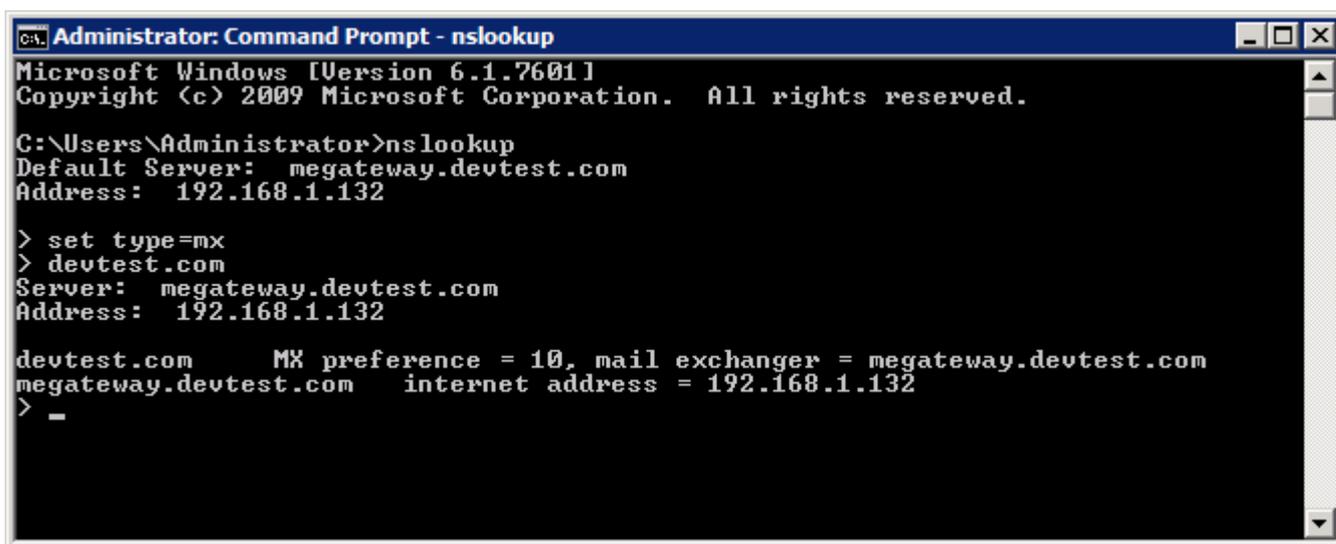
If your ISP manages the DNS server, ask this provider to update it for you.

Since the new mail relay server must first receive all inbound email, update the MX record of your domain to point to the IP of the new mail relay/Gateway server.

Verify the MX record of your DNS server as follows:

1. From command prompt, type `nslookup` and press **Enter**.
2. Type `set type=mx` and press **Enter**.
3. Type your mail domain and press **Enter**.

The MX record should return a single IP that corresponds to the IP address of the machine running GFI MailEssentials.



```
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup
Default Server: megateway.devtest.com
Address: 192.168.1.132

> set type=mx
> devtest.com
Server: megateway.devtest.com
Address: 192.168.1.132

devtest.com MX preference = 10, mail exchanger = megateway.devtest.com
megateway.devtest.com internet address = 192.168.1.132
> -
```

Screenshot 4: Verifying the MX record of the DNS

4. Test the new mail relay server. Before proceeding to install GFI MailEssentials, verify that the new mail relay server is working correctly.
5. Test the IIS SMTP inbound connection of the mail relay server by sending an email from an external account to an internal user (use web-mail, for example **mail.live.com**, if you do not have an external account available). Verify that the email client received the email.
6. Test the IIS SMTP outbound connection of your mail relay server by sending an email to an external account from an email client. Verify that the external user received the email.

NOTE

Alternatively, instead of an email client, send email manually through Telnet. This will give you more troubleshooting information.

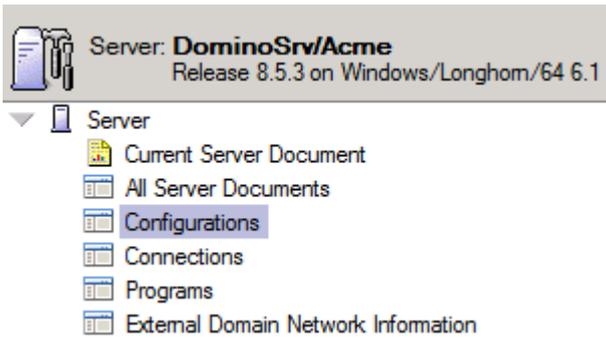
For more information, refer to:

<http://support.microsoft.com/support/kb/articles/Q153/1/19.asp>

Configuring Lotus Domino to send outbound emails through GFI MailEssentials

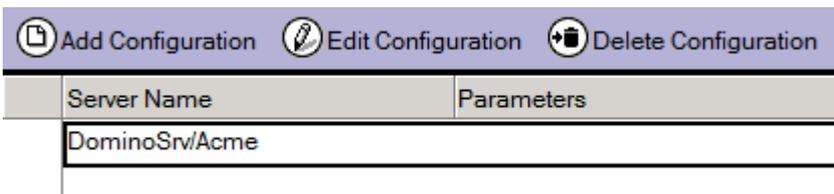
To direct all outgoing emails to the server where GFI MailEssentials is installed, Lotus Domino needs to be configured as below.

1. From the Lotus Domino Administrator, click **Configuration** tab and select **Server > Configurations**.



Screenshot 5: Lotus Domino Administrator - click Configurations option.

2. After configuration section is selected, main window will show the configuration of the server. Select desired server and click **Edit configuration**.

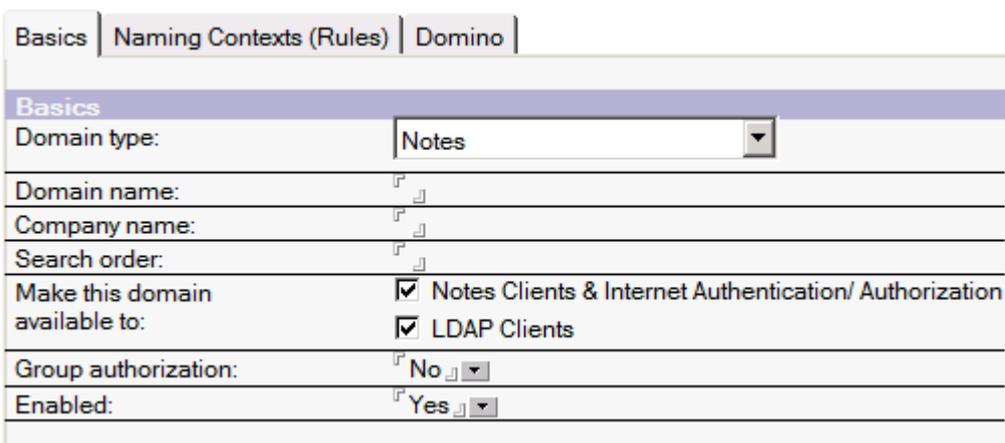


Screenshot 6: Click Edit Configuration

From the configuration document page, select **Router/SMTP** tab and ensure that **Basics** is selected. Double click on content to enable edit mode. Select **Relay host for messages leaving the local internet domain** and enter the IP Address of the machine that GFI MailEssentials is installed. Click **Save and Close** to save configuration document.

Lotus Domino LDAP Settings

From Lotus Domino, enable Directory Catalog and Directory Assistance. In the Directory Assistance database, click **Add Directory Assistance** to create a new Assistance document. In the document, one must enable the LDAP clients under **Make this domain available to** as follows:-



Screenshot 7: Lotus Domino LDAP Settings

In the server configuration one must edit the credentials under the configuration. Anonymous authentication must be enabled so that GFI MailEssentials can access the Lotus Domino LDAP.

SSL settings

SSL key file name:	keyfile.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept SSL site certificates:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Accept expired SSL certificates:	<input checked="" type="radio"/> Yes <input type="radio"/> No
SSL ciphers:	RC4 encryption with 40-bit key and MD5 MAC RC4 encryption with 128-bit key and MD5 MAC RC4 encryption with 128-bit key and SHA-1 MAC DES encryption with 56-bit key and SHA-1 MAC Triple DES encryption with 168-bit key and SHA-1 MAC
<input type="button" value="Modify"/>	
Enable SSL V2: (SSL V3 is always enabled)	<input type="checkbox"/> Yes

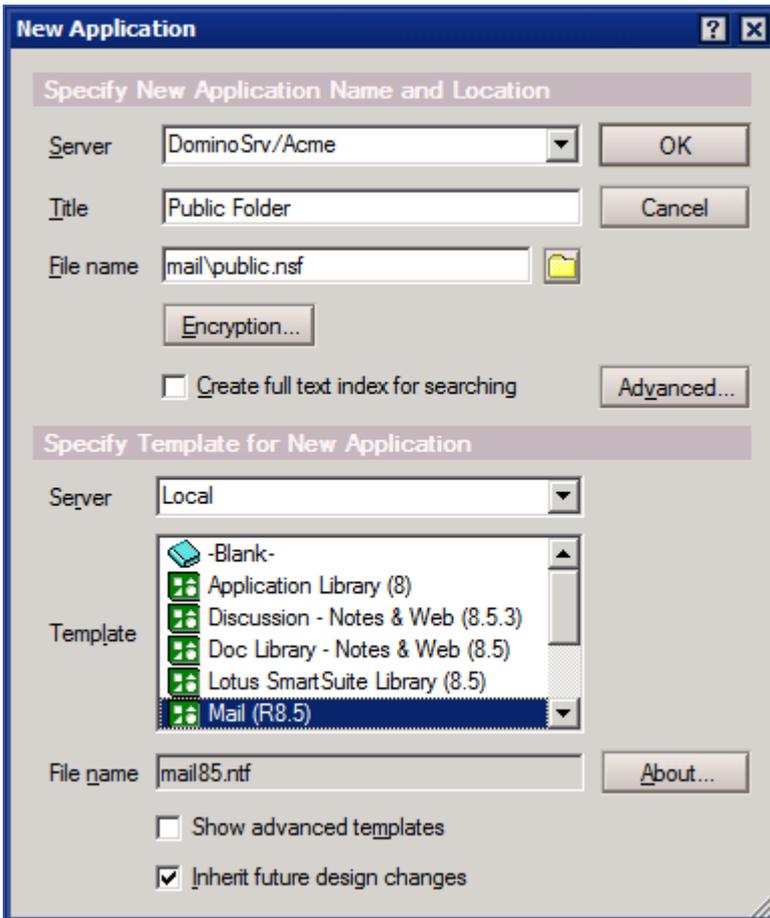
Directory (LDAP)

TCP/IP port number:	389
TCP/IP port status:	Enabled
Enforce server access settings:	No
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	636
SSL port status:	Disabled
Authentication options:	
Client certificate:	No
Name & password:	No
Anonymous:	Yes

Screenshot 8: Enable Anonymous Authentication

Lotus Domino Anti Spam Folder Configuration

1. From Lotus Notes Administrator, create a database with the normal MAIL85.NTF template, that is used as the public folder. When the database is created, right click the database from the files section and select **Access Control**. Configure the user or group or server to have access on the database.



Screenshot 9: Create a new database

2. Convert the database using the server console by typing:

```
load convert -e -h mail\public.nsf
```

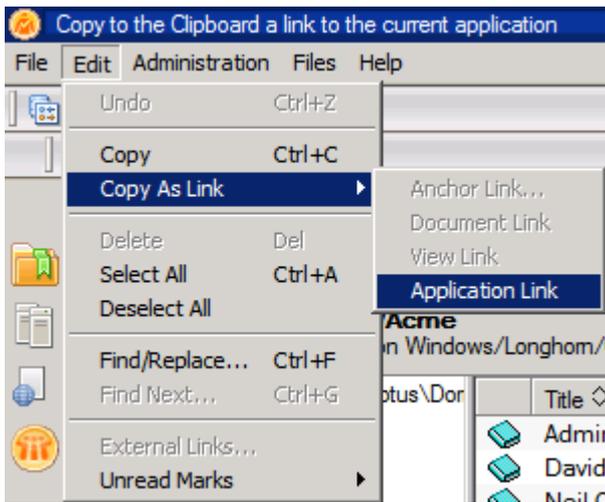
Command should display the following results.

```
load convert -e -h mail\public.nsf

[0A34:0002-06F4] 19/09/2012 16:48:43 Mail Conversion Utility starting
[0A34:0002-06F4] 19/09/2012 16:48:43 Mail Convert: Started enabling NSF support for IMAP
in 'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43 Mail Convert: Finished enabling NSF support for IMAP
in 'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43 Mail Convert: Started adding IMAP specific items in
'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43 Mail Convert: Finished adding IMAP specific items in
'mail\public.nsf'. 0 messages succeeded, 0 messages failed.
[0A34:0002-06F4] 19/09/2012 16:48:43 Mail Conversion Utility shutdown
```

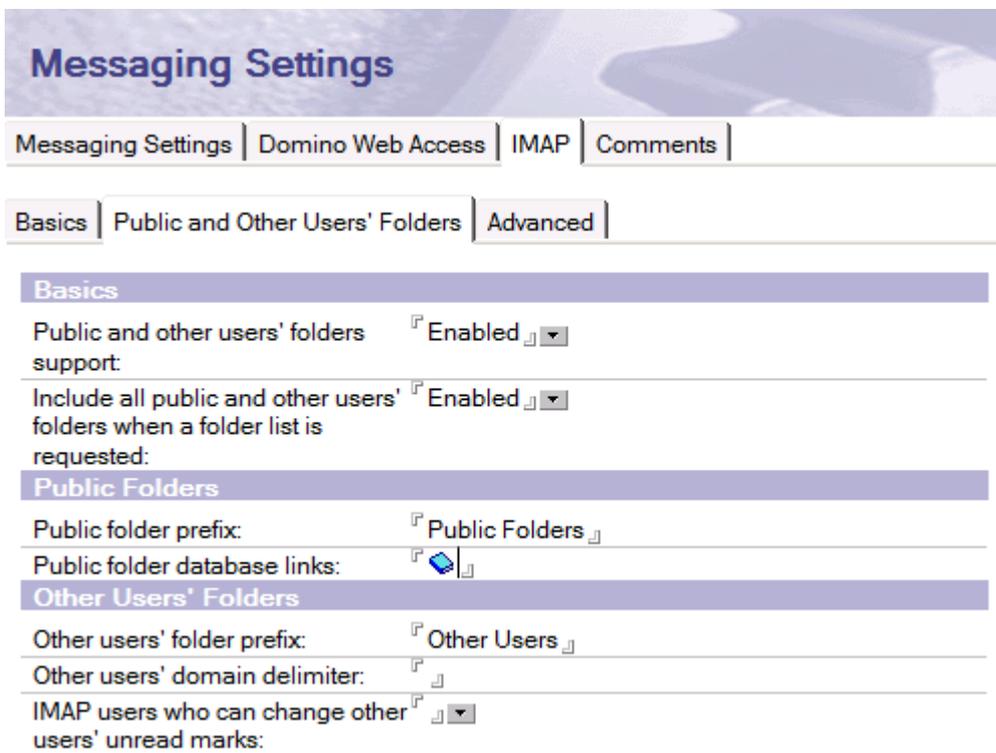
Screenshot 10: Load convert result

3. On completion, ensure that the database is accessible from IMAP service. From the Lotus Notes Administrator, go to **Configuration**, and select the **Files** tab. Highlight the database of the public folder, click **Edit**, select **Copy as Link** and click **Application Link**.



Screenshot 11: Copy to the clipboard a link to the current application

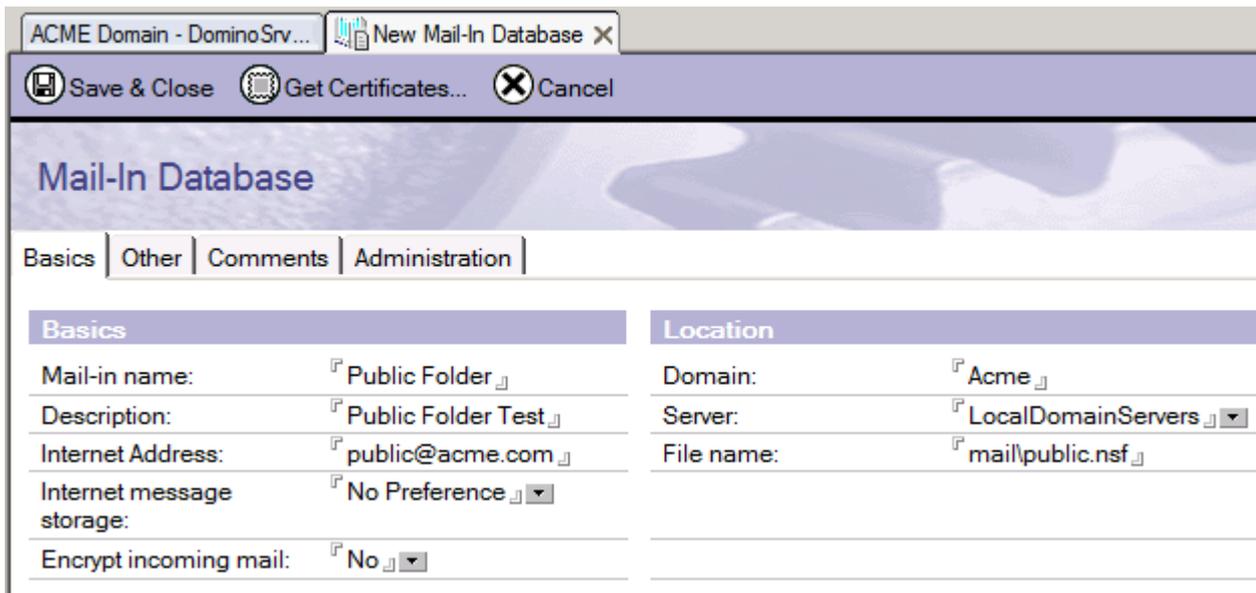
4. From the configuration, go to **Messaging Settings** and select **IMAP** tab.



Screenshot 12: Include all public and other users' folders when a folder list is requested

5. Select **Public and Other Users' Folders** tab. Right click and paste on the **Public Folders Database Links** and enable the **Include all public and other users folders when a folder list is requested**.

6. Save and close the document.



Screenshot 13: New mail-in database

7. From the Lotus Notes Administrator, configure the folder for mail usage. Go to **People and Groups** and select **Mail-In Database**. Create a new Mail-in Database and in the whole directory path enter the full path (for example, Mailpublic.nsf).
8. Save and close the document.
9. From the GFI MailEssentials web interface, expand **AntiSpam** and select **AntiSpam Settings**.
10. On the right hand pane, select **Public Folder Scanning** tab and select **Enable Public Folder Scanning**.
11. From the **IMAP configuration** section, enter the IMAP server (your Lotus Domino server, Port and the credentials of the user to access the folder).

NOTE

The test button will not function.

12. Click **Apply** to save modifications.

DNS Server	Public Folder Scanning	Remote Commands
Anti-spam logging		Global Actions
 Configure use of public folders for classification of emails		
Public Folder Scanning Settings		
<input checked="" type="checkbox"/> Enable Public Folder Scanning Scanning interval: <input type="text" value="2"/> hours Poll public folders via: <input type="text" value="IMAP"/> <input type="button" value="Scan now"/>		
IMAP configuration		
Server: <input type="text" value="192.168.1.205"/>	Port: <input type="text" value="143"/>	<input type="checkbox"/> Use SSL
Username: <input type="text" value="Administrator"/>	Password: <input type="password" value="••••••"/>	<input type="button" value="Test"/>
NOTE: IMAP cannot be used to access Exchange 2007/2010/2013 Public Folders		

Screenshot 14: Enable Public Folder Scanning

13. From the registry , change values to use this function. From the registry select HKEY_LOCAL_MACHINE\SOFTWARE\GFI\ME12\ATTENDANT\RPFOLDERS : 5 and create the following Key String Value as follows:

Name/Value

SharedNamespace Public Folders\\Public Folder

FolderDelimiter \\

2.3 Installation procedure

This section describes how to run the installation of GFI MailEssentials.

2.3.1 Important notes

» If you are currently using a previous version of GFI MailEssentials, you can upgrade your current installation while at the same time retaining all your existing configuration settings. Upgrade is not reversible; you cannot downgrade to the previous version after upgrading. For more information, refer to [Upgrading GFI MailEssentials](#) (page 42).

» GFI MailEssentials 21 and later offers two types of licensing services:

- Using the GFI Account credentials. The username and password are retrieved from [GFI Accounts](#) and assigned to the user in the moment of the registration of the account.
- Using a license key. When upgrading to a new major release you also need to upgrade your license key. For more information, refer to [Obtaining a GFI MailEssentials subscription](#) (page 48).

» GFI MailEssentials installation restarts Microsoft® Exchange or Microsoft IIS® SMTP services. This is required to allow GFI MailEssentials components to register correctly. It is recommended to install GFI MailEssentials at a time when restarting these services has the least impact on your network.

» Before running installation wizard, ensure that:

- You are logged on using an account with administrative privileges.
- The machine where GFI MailEssentials is going to be installed, meets the specified system requirements. For more information, refer to [System requirements](#) (page 16).
- Configure your firewall to allow GFI MailEssentials to connect to GFI servers. For more information, refer to [Firewall port settings](#) (page 18).
- Disable third-party antivirus and backup software from scanning folders used by GFI MailEssentials. For more information, refer to [Antivirus and backup software](#) (page 18).
- If installing GFI MailEssentials on an email gateway or relay/perimeter server, configure that machine to act as a gateway. For more information, refer to [Installing on an email gateway or relay/perimeter server](#) (page 20).
- Save any pending work and close all open applications on the machine.

2.3.2 Running the installation wizard

1. Right-click the GFI MailEssentials installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

2. Launch the GFI MailEssentials installer.

3. Select the language to use with this installation of GFI MailEssentials. Accept the terms and conditions and click **Next**.

NOTE

Language selection is not reversible. You will need to reinstall GFI MailEssentials to change the language selected at this stage.

Screenshot 15: Specifying a GFI account or a license key

4. In the **Username** and **Password** fields, enter your [GFI Accounts](#) area credentials or the account used when signing up to download GFI MailEssentials. Click **Login** to retrieve the license keys registered to your account. Choose a key from the Available keys drop-down. If you do not have a GFI account, click **Sign up** and fill in the registration form. You may also manually specify a license key in the **Manually Enter a License Key** field. Click **Next**. For more information, refer to [Obtaining a GFI MailEssentials subscription](#) (page 48).

5. Select the mode that GFI MailEssentials will use to retrieve the list of email users. The selected user mode cannot be changed after installation. The list of modes available depends on the environment where GFI MailEssentials is installed.

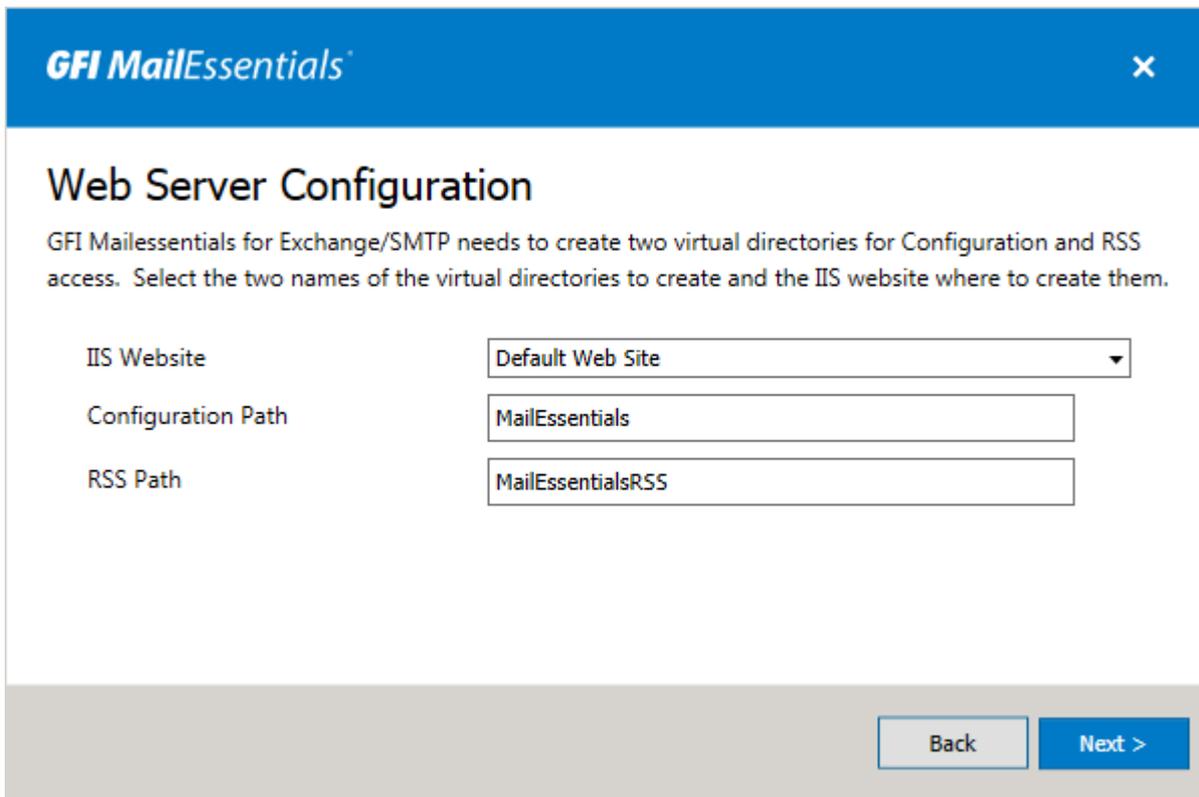
Option	Description
Active Directory	This option is only available when installing GFI MailEssentials on a machine that is joined to an Active Directory domain. GFI MailEssentials retrieves the list of mail-enabled users from Active Directory. Selecting this option means that GFI MailEssentials is being installed behind your firewall and that it has access to the Active Directory containing ALL your email users.
SMTP	Select this mode if an Active Directory domain is not available or if you would like to manage the list of users manually. In this mode, GFI MailEssentials automatically populates the list of local users using the sender's email address in outbound emails. The list of users can also be managed from the GFI MailEssentials General Settings node. For more information, refer to Managing local users (page 230).

Option	Description
Remote Active Directory	Option only available when installing GFI MailEssentials on a machine that is NOT joined to an Active Directory domain. In this mode, GFI MailEssentials retrieves the list of users from a remote Active Directory domain, even though the GFI MailEssentials server is not joined to a domain. This mode can be used for example, when installing GFI MailEssentials in a DMZ, before the firewall that separates your internal and external networks. In this example, the GFI MailEssentials server is typically not joined to the internal domain. In this mode, all other features of GFI MailEssentials function similarly to when GFI MailEssentials is joined to a domain. When choosing this option, in the next screen specify the details of the Remote Domain Controller to use. Ensure that GFI MailEssentials can communicate with this server using LDAP, which by default uses port 389 (or port 636 when using an SSL certificate).
GFI Directory	Option only available when installing GFI MailEssentials on a machine that is not joined to an Active Directory domain. In this mode, GFI MailEssentials connects and fetches users from GFI Directory. This mode is best suited for installations that do not have Active Directory yet want the features and functionalities that a user directory offers. When this option is selected, you need to enter the details to connect with a separate instance of GFI Directory. For more information, refer to Installing GFI MailEssentials with GFI Directory (page 35).

6. Click **Next**.

7. Configure the Administrator Email Address and the SMTP Server Configuration.

Option	Description
Administrator Email Address	Specify the administrator email address to use for notifications about product status.
SMTP Server Setup	Select the SMTP Server that GFI MailEssentials binds to. By default, GFI MailEssentials binds to your Default SMTP Virtual Server. If you have multiple SMTP virtual servers on your domain, you can bind GFI MailEssentials to any available SMTP virtual server. NOTES 1. If you are installing on a Microsoft® Exchange Server 2010 or later machine this option is not shown since Microsoft® Exchange has its own built-in SMTP server. 2. After installation, you can still bind GFI MailEssentials to another SMTP virtual server from the GFI MailEssentials Configuration. For more information, refer to SMTP Virtual Server bindings (page 233).



Screenshot 16: Web server and virtual directory details

8. In the **Web Server Setup** dialog, configure the following options:

NOTE

Default settings are typically correct for most installations.

Option	Description
IIS Website	Select the website where you want to host the GFI MailEssentials virtual directories.
Configuration Path	Specify a name for the GFI MailEssentials virtual directory.
RSS Path	Specify a name for the GFI MailEssentials Quarantine RSS feeds virtual directory.

9. Click **Next**.

10. Select a folder to install GFI MailEssentials and click **Next**. When the installation is an upgrade, GFI MailEssentials installs in the same location as the previous installation.

11. Click **Install** to start the installation process. If you are prompted to restart the SMTP services, click **Yes**.

12. On completion, click **Finish**.

NOTE

For new installations, setup automatically launches the Post-Installation Wizard. For more information, refer to [Post-Installation Wizard](#) (page 37).

2.3.3 Installing GFI MailEssentials with GFI Directory

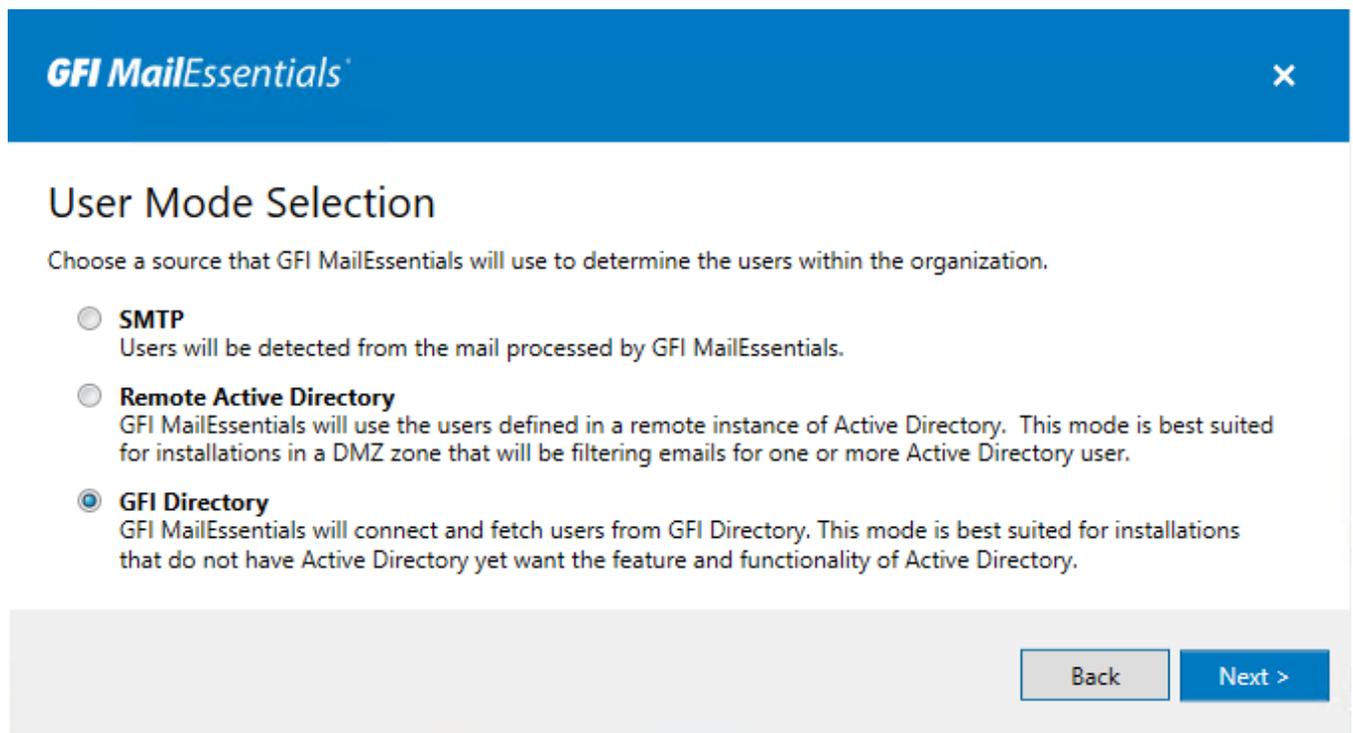
GFI MailEssentials can retrieve users from a remote GFI Directory instance. This mode is best suited for installations that do not have Active Directory yet but want the features and functionalities that a user directory offers.

For more information about how to install, use and manage users in GFI Directory, go to <http://go.gfi.com/?pageid=directory2.0UserHelp>.

The process to configure GFI MailEssentials to work with GFI Directory consists of three steps:

Step 1 - Selecting GFI Directory during the installation of GFI MailEssentials

1. During the installation of GFI MailEssentials, choose the GFI Directory option in the user mode selection.



Screenshot 17: GFI Directory option during installation

2. Key in the necessary information to connect with GFI Directory.

GFI MailEssentials ×

GFI Directory Configuration

Enter the details to connect to the local or remote GFI Directory instance

GFI Directory server: Use SSL

Username:

Password:

GFI Directory port:

Screenshot 18: Settings to connect with GFI Directory

To connect with GFI Directory:

Options	Description
GFI Directory server	FQDN or IP of the server where the GFI Directory is installed. Use localhost when GFI Directory is installed on the same machine.
LDAP port	Port used for LDAP queries to GFI Directory. The default port is 389. This port must be open on the firewall.
Use SSL	Select this option to use an SSL certificate to encrypt LDAP queries to GFI Directory. When this option is selected, the LDAP port is automatically changed to 636. This port must be open on the firewall.
Username	The username used to connect to GFI Directory. Use the same format used when logging into GFI Directory. NOTE When GFI Directory is installed on a separate machine, both GFI Directory and GFI MailEssentials machine must use the same user and password.
Password	The password used to connect to GFI Directory. Ensure that the password is not set to expire and does not change. NOTE When GFI Directory is installed on a separate machine, both GFI Directory and GFI MailEssentials machine must use the same user and password.
GFI Directory port	By default 61000. This port must be open on the firewall. This setting can be changed later from the GFI MailEssentials Switchboard. For more information, refer to GFI Directory mode (page 248).

3. Click **Next**.

4. Key in the following information:

Field	Description
Administrator email address	GFI MailEssentials uses the administrator email address to send notifications about the product status.
SMTP Server configuration	Select the SMTP server virtual instance which GFI MailEssentials should bind to. The selected SMTP server will be monitored for all mail traffic.

5. Click **Next** to continue with the GFI MailEssentials installation wizard.

Step 2 - Configuring GFI Directory Server WCF port

On the machine where GFI Directory is installed perform the following actions:

1. Navigate to <GFI MailEssentials install directory>\Directory\Data
2. Open `product.config` on a notepad or any other text editor.
3. Find `WCFSecurityTCPPortName` and change it from 0 to whatever port you want. If available you can use 61001.
4. Ensure that the value of `WCFSecurityPluginName` is set to `DSecurity`.
5. Save and close the file.

Step 3 - Configuring GFI MailEssentials WCF port

The last step is to configure GFI MailEssentials to use the same port set for the GFI Directory in the previous step. You can do this:

» During installation:

Choose GFI Directory option and provide the same port number when configuring the GFI Directory settings.

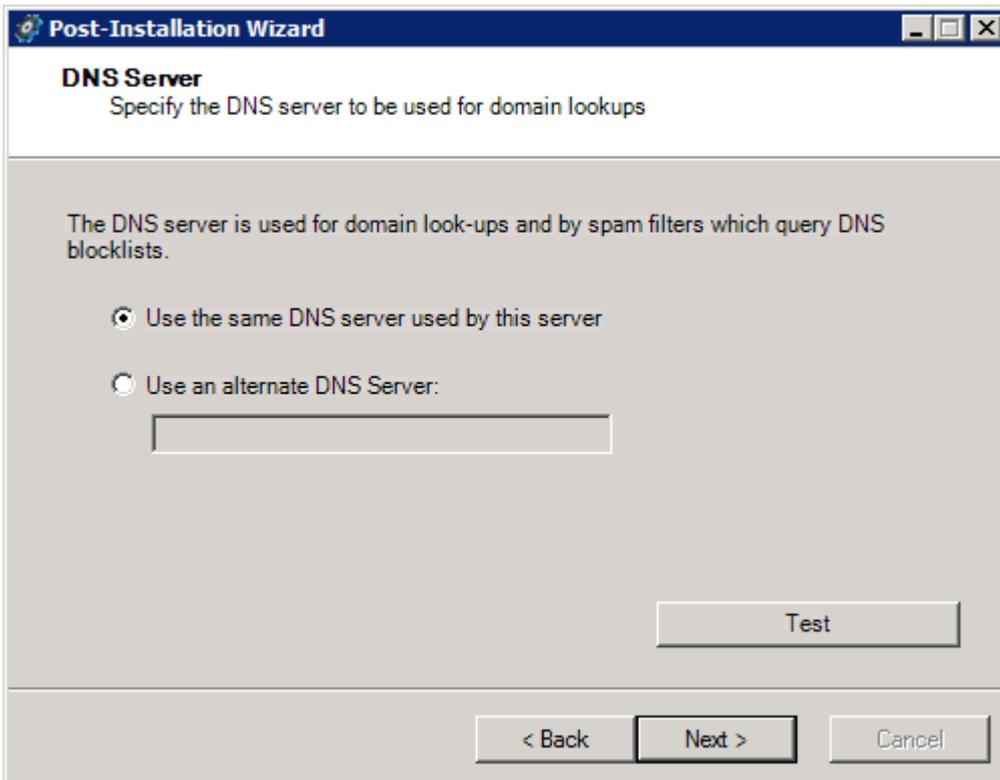
» When already installed:

Open the [GFI MailEssentials Switchboard](#) and configure the **WCF Port** to use the same port configured on the GFI Directory.

2.3.4 Post-Installation Wizard

The post-installation wizard loads automatically after installing GFI MailEssentials the first time. It enables configuration of the most important settings of GFI MailEssentials.

1. Click **Next** in the welcome page.

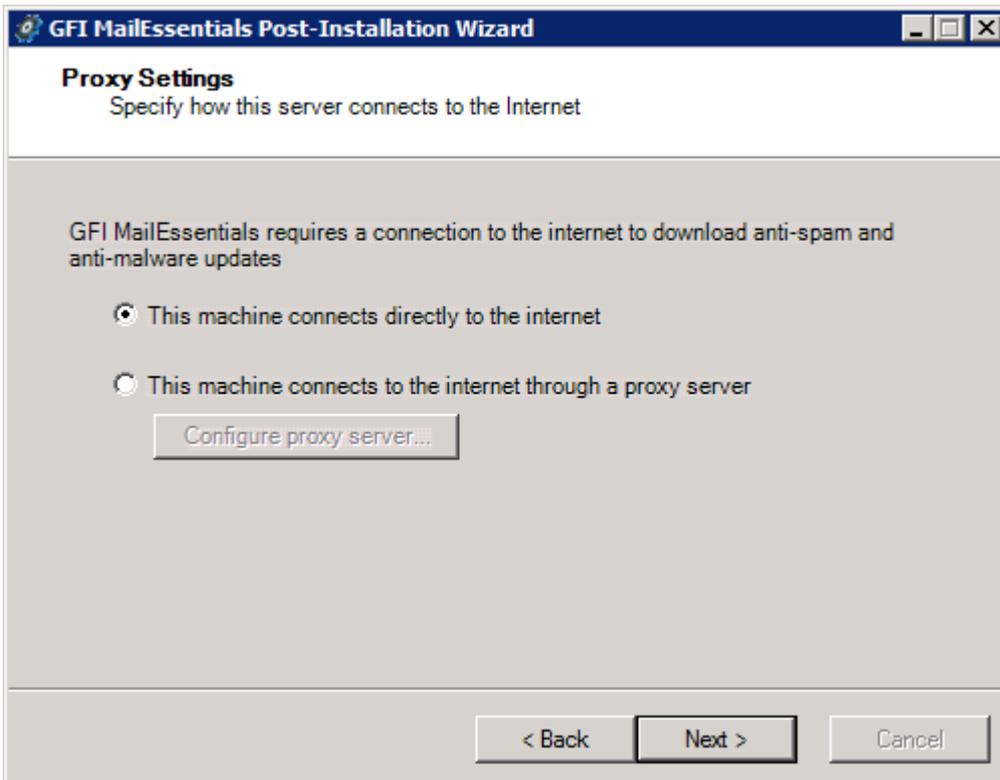


Screenshot 19: DNS Server settings

2. In the DNS Server dialog, select:

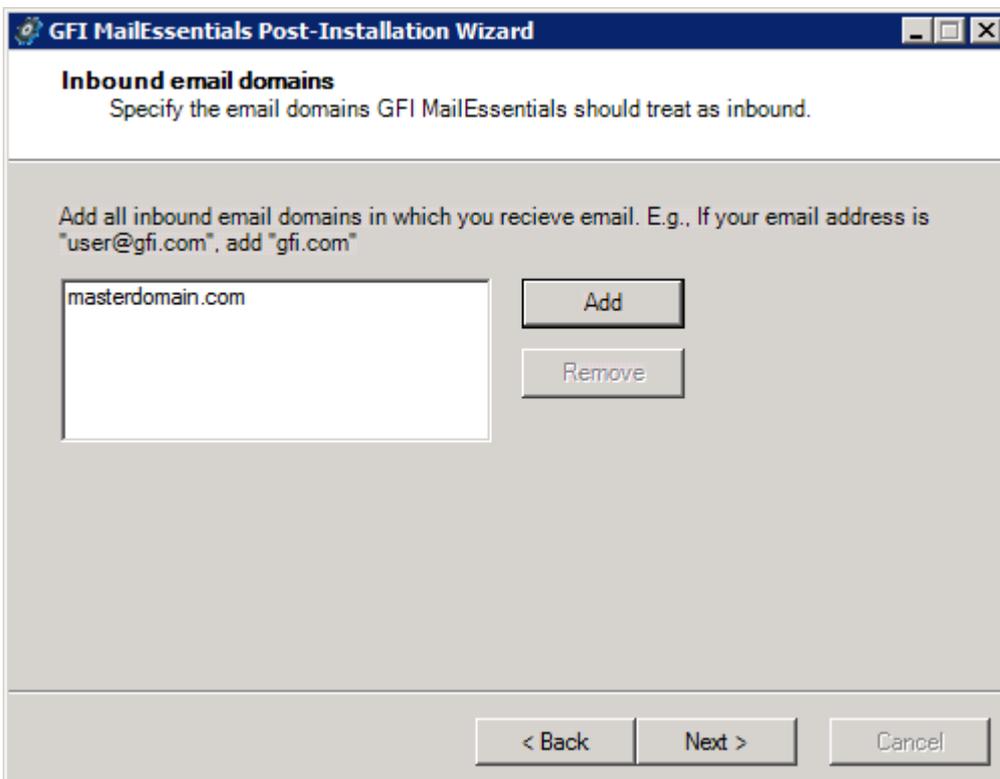
Option	Description
Use the same DNS server used by this server	Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
Use an alternate DNS server	Select this option to specify a custom DNS server IP address.

Click **Test** to test connection with the specified DNS server. If test is unsuccessful, specify another DNS server. Click **Next**.



Screenshot 20: Proxy settings

3. In the **Proxy Settings** dialog, specify how GFI MailEssentials connects to the Internet. If the server connects through a proxy server click **Configure proxy server...** and specify proxy settings. Click **Next**.

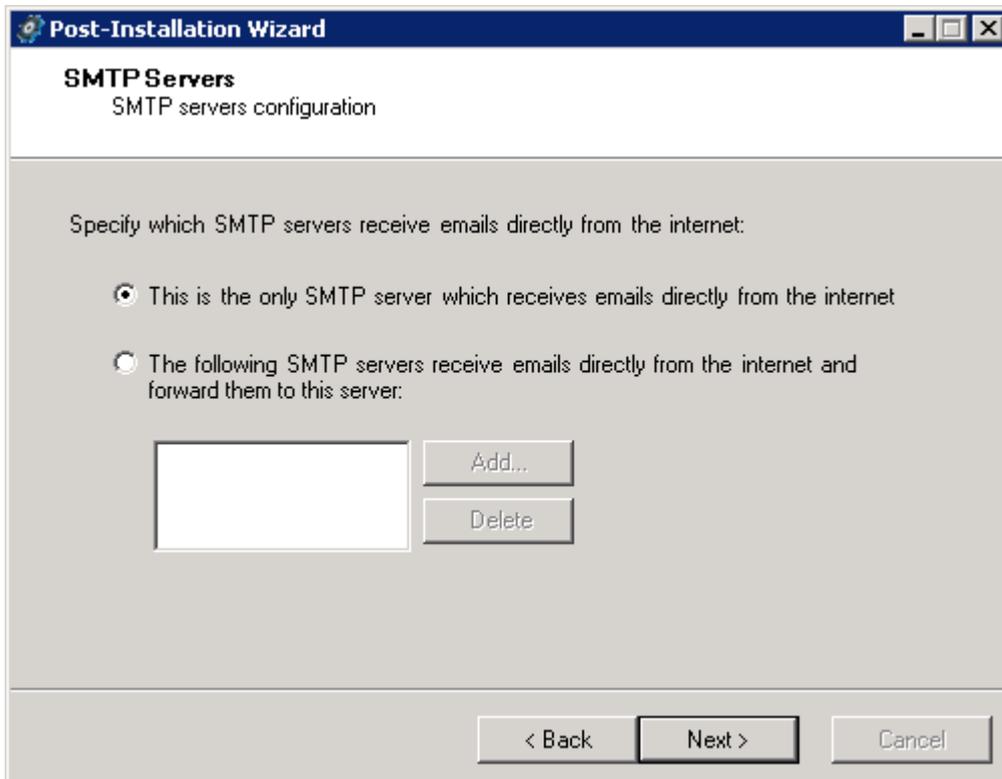


Screenshot 21: Inbound email domains

4. In the **Inbound email domains** dialog specify all the domains to scan for viruses and spam. Any local domains that are not specified in this list will not be scanned. Click **Next**.

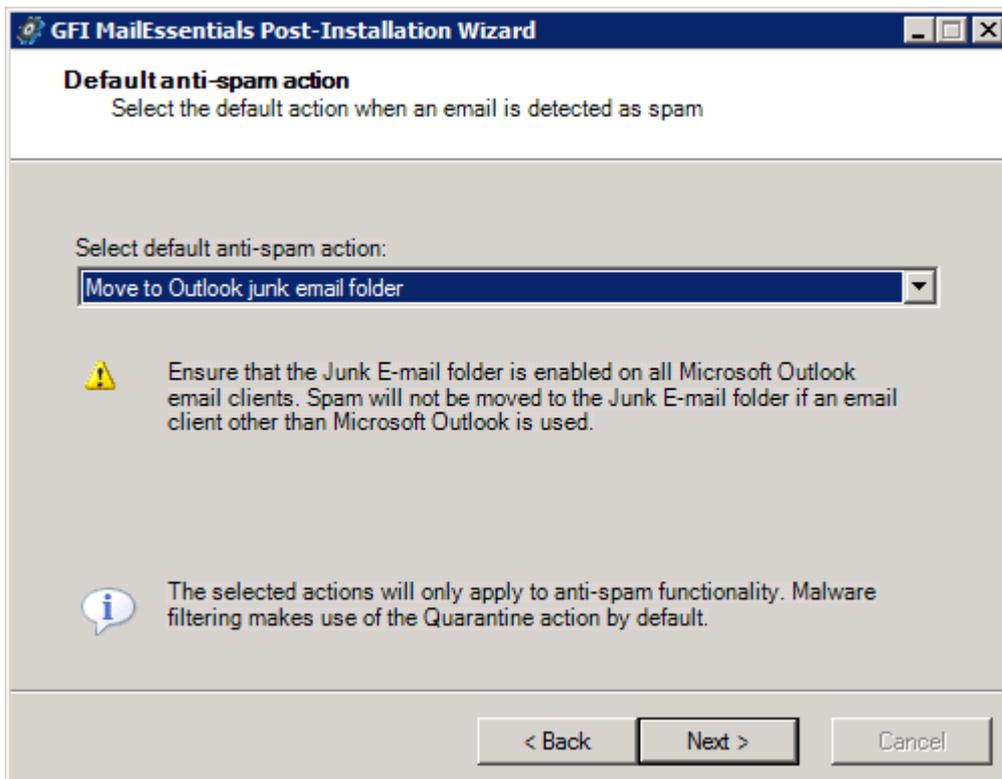
NOTE

When adding domains, select **Obtain domain's MX records and include in perimeter servers list** to retrieve the domain's MX records and automatically add them to the perimeter SMTP servers list (configured in the next step).



Screenshot 22: SMTP Server settings

5. In the **SMTP Servers** dialog specify how the server receives external emails. If emails are routed through other servers before they are forwarded to GFI MailEssentials, add the IP address of the other servers in the list. For more information about perimeter SMTP servers refer to: http://go.gfi.com/?pageid=ME_PerimeterServer. Click **Next**.



Screenshot 23: Selecting the default anti-spam action to use

6. In the **Default anti-spam action** dialog select the default action to be taken when emails are detected as spam. This action applies to anti-spam filters only. Malware filters automatically quarantine blocked emails. For more information, refer to [Email scanning and filtering engines](#) (page 10).

NOTE

When installing on Microsoft® Exchange 2010 or later, and the default action selected is **Move to sub folder in recipient's Exchange mailbox**, a user with impersonation rights must be created. Select whether to let GFI MailEssentials automatically create the user or manually specify the credentials and click **Set access rights** to assign the required rights to the specified user. This user must be dedicated to this feature only and the credentials must not be changed. For more information, refer to [Set a Microsoft® Exchange account](#) (page 260).

Click **Next**.

7. When installing on Microsoft® Exchange Server 2010 or newer, the list of Microsoft® Exchange server roles detected and GFI MailEssentials components required is displayed. Click **Next** to install the required GFI MailEssentials components.

8. Click **Finish** to finalize the installation.

GFI MailEssentials installation is now complete and the email protection system is up and running.

Next step: Optimize your protection system to ensure that it is effectively up and running. For more information, refer to [Post-Install actions](#) (page 45).

NOTE

To re-run the Post-Installation wizard, from command prompt, navigate to the GFI MailEssentials installation folder and run the following command:

```
e2k7wiz.exe clean
```

2.4 Upgrading GFI MailEssentials

Choose your current GFI MailEssentials version for notes and instructions on how to upgrade to the latest version while retaining all settings:

- » [GFI MailEssentials 21](#)
- » [GFI MailEssentials 20](#)
- » [GFI MailEssentials 2015](#)
- » [GFI MailEssentials 2014](#)
- » [GFI MailEssentials 2012](#)

To determine your current version number open the GFI MailEssentials web interface and navigate to **General Settings > About**.

2.4.1 Upgrading from version 21

This topic describes how to upgrade a GFI MailEssentials 21 installation to the latest version while retaining all settings.

Important notes before upgrading

- » Ensure your server meets the [system requirements](#).
- » Upgrade is not reversible; you cannot downgrade to the previous version after upgrading.
- »

Export the GFI MailEssentials settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to [Exporting and importing settings manually](#) (page 260).

- » Save any pending work and close all open applications on the machine before starting the upgrade.
- » Log on to your current GFI MailEssentials server as an Administrator or using an account with administrative privileges.

Upgrade procedure

1. Download the latest build of GFI MailEssentials on the server where GFI MailEssentials is currently installed. Go to [this link](#), click **Login** and key in your GFI Account credentials.
2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Launch the installer.
4. Follow the wizard steps to start the upgrade installation. The new version of GFI MailEssentials is automatically installed in the same directory as the previously installed version.
5. If GFI MailEssentials is installed on a server that also includes Microsoft® Exchange, the Post Installation wizard displays the list of Microsoft® Exchange server roles detected and the GFI MailEssentials components required. Click **Next** to install the required components and complete the wizard.
6. On upgrade completion, [test](#) mail flow and mail filtering.

2.4.2 Upgrading from version 20

This topic describes how to upgrade a GFI MailEssentials 20 installation to the latest version while retaining all settings.

Important notes before upgrading

- » Ensure your server meets the [system requirements](#).
- » Upgrade is not reversible; you cannot downgrade to the previous version after upgrading.
- » Export the GFI MailEssentials settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to [Exporting and importing settings manually](#) (page 260).
- » Save any pending work and close all open applications on the machine before starting the upgrade.
- » Log on to your current GFI MailEssentials server as an Administrator or using an account with administrative privileges.
- » Log in to the [GFI Customer Area](#) to get a new license key. Click the blue key icon on the right and select **Upgrade License Key**, or click **Renewal** to extend your maintenance agreement.

Upgrade procedure

1. Download the latest build of GFI MailEssentials on the server where GFI MailEssentials is currently installed. Go to [this link](#), click **Login** and key in your GFI Account credentials.
2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Launch the installer.
4. Follow the wizard steps to start the upgrade installation. The new version of GFI MailEssentials is automatically installed in the same directory as the previously installed version.
5. If GFI MailEssentials is installed on a server that also includes Microsoft[®] Exchange, the Post Installation wizard displays the list of Microsoft[®] Exchange server roles detected and the GFI MailEssentials components required. Click **Next** to install the required components and complete the wizard.
6. On upgrade completion, [test](#) mail flow and mail filtering.

2.4.3 Upgrading from version 2015

This topic describes how to upgrade a GFI MailEssentials 2015 installation to the latest version while retaining all settings.

Important notes before upgrading

- » Ensure your server meets the [system requirements](#).
- » Upgrade is not reversible; you cannot downgrade to the previous version after upgrading.
- » Export the GFI MailEssentials settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to [Exporting and importing settings manually](#) (page 260).
- » Save any pending work and close all open applications on the machine before starting the upgrade.
- » Log on to your current GFI MailEssentials server as an Administrator or using an account with administrative privileges.
- » Log in to the [GFI Customer Area](#) to get a new license key. Click the blue key icon on the right and select **Upgrade License Key**, or click **Renewal** to extend your maintenance agreement.

Upgrade procedure

1. Download the latest build of GFI MailEssentials on the server where GFI MailEssentials is currently installed. Go to [this link](#), click **Login** and key in your GFI Account credentials.
2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Launch the installer.
4. Follow the wizard steps to start the upgrade installation. The new version of GFI MailEssentials is automatically installed in the same directory as the previously installed version.
5. If GFI MailEssentials is installed on a server that also includes Microsoft® Exchange, the Post Installation wizard displays the list of Microsoft® Exchange server roles detected and the GFI MailEssentials components required. Click **Next** to install the required components and complete the wizard.
6. On upgrade completion, [test](#) mail flow and mail filtering.

2.4.4 Upgrading from version 2014

This topic describes how to upgrade a GFI MailEssentials 2014 installation to the latest version while retaining all settings.

Important notes before upgrading

- » Ensure your server meets the [system requirements](#).
- » Upgrade is not reversible; you cannot downgrade to the previous version after upgrading.
- » Export the GFI MailEssentials settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to [Exporting and importing settings manually](#) (page 260).
- » Save any pending work and close all open applications on the machine before starting the upgrade.
- » Log on to your current GFI MailEssentials server as an Administrator or using an account with administrative privileges.
- » As from GFI MailEssentials 2015, the Anti-spam Synchronization Agent feature has been deprecated and is now replaced with the GFI MailEssentials [Multi-Server](#) feature. This needs to be reconfigured manually after installation upgrade.
- » Log in to the [GFI Customer Area](#) to get a new license key. Click the blue key icon on the right and select **Upgrade License Key**, or click **Renewal** to extend your maintenance agreement.

Upgrade procedure

1. Download the latest build of GFI MailEssentials on the server where GFI MailEssentials is currently installed. Go to [this link](#), click **Login** and key in your GFI Account credentials.
2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Launch the installer.
4. Follow the wizard steps to start the upgrade installation. The new version of GFI MailEssentials is automatically installed in the same directory as the previously installed version.

5. If GFI MailEssentials is installed on a server that also includes Microsoft® Exchange, the Post Installation wizard displays the list of Microsoft® Exchange server roles detected and the GFI MailEssentials components required. Click **Next** to install the required components and complete the wizard.
6. On upgrade completion, [test](#) mail flow and mail filtering.

2.4.5 Upgrading from version 2012

This topic describes how to upgrade a GFI MailEssentials 2012 installation to the latest version while retaining all settings.

Important notes before upgrading

- » A direct upgrade from GFI MailEssentials 2012 to the latest version is not possible. To overcome this limitation, you can first upgrade GFI MailEssentials from version 2012 to version 2014. After that, upgrade from version 2014 to the latest version.
- » Ensure your server meets the [system requirements](#).
- » Upgrade is not reversible; you cannot downgrade to the previous version after upgrading.
- » Export the GFI MailEssentials settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to [Exporting and importing settings manually](#) (page 260).
- » Save any pending work and close all open applications on the machine before starting the upgrade.
- » Log on to your current GFI MailEssentials server as an Administrator or using an account with administrative privileges.
- » Log in to the [GFI Customer Area](#) to get a new license key. Click the blue key icon on the right and select **Upgrade License Key**, or click **Renewal** to extend your maintenance agreement.

Upgrade procedure

1. Download the GFI MailEssentials 2014 installer on the server where GFI MailEssentials is currently installed. The 32-bit installer is available from <http://cdndf.gfi.com/mailessentials2014.exe>, while the 64-bit version can be downloaded from http://cdndf.gfi.com/mailessentials2014_x64.exe
2. Right-click the newly downloaded installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.
3. Launch the installer.
4. Follow the wizard steps to start the upgrade installation. The new version of GFI MailEssentials is automatically installed in the same directory as the previously installed version.
5. If GFI MailEssentials is installed on a server that also includes Microsoft® Exchange, the Post Installation wizard displays the list of Microsoft® Exchange server roles detected and the GFI MailEssentials components required. Click **Next** to install the required components and complete the wizard.
6. When the upgrade from version 2012 to version 2014 is complete, you can proceed to upgrade version 2014 to the latest version. For more information, refer to [Upgrading from version 2014](#) (page 44).
7. On upgrade completion, [test](#) mail flow and mail filtering.

2.5 Post-Install actions

To ensure GFI MailEssentials scanning and filtering system is effectively up and running, perform the following post-install actions:

Action	Description
Add GFI MailEssentials scanning engines to the Windows DEP Exception List.	<p>Data Execution Prevention (DEP) is a set of hardware and software technologies that perform memory checks to help prevent malicious code from running on a system. If you installed GFI MailEssentials on an operating system that includes DEP, you will need to add the GFI MailEssentials scanning engine (GFiScanM.exe) and the Kaspersky Virus Scanning Engine (kavss.exe) executables.</p> <p>NOTE This is required only when installing on Microsoft® Windows Server 2003 SP 1 or SP 2.</p> <p>For more information, refer to Add engines to the Windows DEP Exception List (page 46).</p>
Launch GFI MailEssentials Configuration	Go to Start > Programs > GFI MailEssentials > GFI MailEssentials Configuration .
Enable Directory Harvesting	Directory harvesting attacks occur when spammers try to guess email addresses by attaching well known usernames to your domain. The majority of the email addresses are non-existent. This filter is enabled by default if GFI MailEssentials is installed in an Active Directory Environment. For more information, refer to Directory Harvesting (page 112).
Enable Greylist	The Greylist filter temporarily blocks incoming emails received from unknown senders. Legitimate mail systems typically try to send the email after a few minutes; spammers simply ignore such error messages. This filter is not enabled by default. For more information, refer to Greylist (page 126).
Configure Whitelists	The Whitelist contains lists of criteria that identify legitimate email. Emails that match these criteria are not scanned by anti-spam filters and are always delivered to the recipient. For more information, refer to Whitelist (page 139).
Test your installation	After configuring all post-install actions, GFI MailEssentials is ready to start protecting and filtering your mail system from malicious and spam emails. Test your installation to ensure that GFI MailEssentials is working properly. For more information, refer to Test your installation (page 47).

2.5.1 Add engines to the Windows DEP Exception List

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform memory checks to help prevent malicious code from running on a system.

If you installed GFI MailEssentials on an operating system that includes DEP, you will need to add the GFI MailEssentials scanning engine (**GFiScanM.exe**) and the Kaspersky Virus Scanning Engine (**kavss.exe**) executables.

NOTE

This is required only when installing on Microsoft® Windows Server 2003 SP 1 or SP 2.

To add the GFI executables in the DEP exception list:

1. From **Control Panel** open the **System** applet.
2. From the **Advanced** tab, under the **Performance** area, click **Settings**.
3. Click **Data Execution Prevention** tab.
4. Click **Turn on DEP for all programs and services except those I select**.
5. Click **Add** and from the dialog box browse to: **<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity**, and choose **GFiScanM.exe**.

- Click **Add** and from the dialog box browse to: **<GFI MailEssentials installation path>\GFI\MailEssentials\AntiVirus\Kaspersky**, and choose **kavss.exe**.
- Click **Apply** and **OK** to apply the changes.
- Restart the **GFI MailEssentials Autoupdater** service and the **GFI MailEssentials AV Scan Engine** services.

2.5.2 Test your installation

After configuring all post-install actions, GFI MailEssentials is ready to start protecting and filtering your mail system from malicious and spam emails.

Ensure that GFI MailEssentials blocks unwanted emails. To do this, send inbound and outbound test emails that are purposely composed in such a way that they are blocked by GFI MailEssentials.

Step 1: Create a Content Filtering rule

- Launch the GFI MailEssentials console.
- Go to **GFI MailEssentials > Content Filtering > Keyword Filtering** node.
- Click **Add Rule...**

General	Body	Subject	Actions	Users/Folders
 Keyword Filtering				
Rule name: Provide a friendly name for this rule: <input type="text" value="New Keyword Filtering Rule"/>				
Email checking Select to which emails this rule applies: <input checked="" type="checkbox"/> Inbound emails <input checked="" type="checkbox"/> Outbound emails <input checked="" type="checkbox"/> Internal emails				
PGP Encryption This rule can be set to block any PGP encrypted mail. Enable or disable this option below: <input type="checkbox"/> Block PGP encrypted emails				

Screenshot 24: Creating a test rule on Keyword filtering

- In **Rule name** type `Test Rule`.
- From the **Subject** tab, select **Block emails if content is found matching these conditions (message subject)**.
- In **Edit Condition** type `Threat test` and click **Add Condition**.

- From **Actions** tab, enable **Block email and perform this action** and select **Quarantine email**.
- Click **Apply** to save the rule.

Step 2: Send an inbound test email

- From an external email account, create a new email and type `Threat test` as the subject.
- Send the email to one of your internal email accounts.

Step 3: Send an outbound test email

- From an internal email account, create a new email and type `Threat test` as the subject.
- Send the email to an external email account.

Step 4: Confirm that test emails are blocked

Verify that both inbound and outbound test emails are blocked and quarantined. To do this:

- From GFI MailEssentials, go to **Quarantine > Today**.
- Ensure that both inbound and outbound test emails are listed in **Malware and Content** tab, reason being: **Triggered rule "Test rule"**.

The screenshot shows the 'Malware and Content (3)' tab selected. Below the header, there are buttons for 'Approve', 'Delete', and 'Rescan', and an 'Item Source' dropdown menu set to 'View All'. A table lists three blocked items:

<input type="checkbox"/>	Date	Sender	Recipients	Subject	Module	Reason	Source
<input type="checkbox"/>	3/27/2012 1:43:50 PM	administrator@tcdomainb.com	jsmith@tcdomainb.com	Threat test	Keyword Filtering	Triggered rule "Test rule"	Gateway (SMTP)
<input type="checkbox"/>	3/27/2012 1:43:28 PM	administrator@tcdomainb.com	administrator@tcdomainb.com	Threat test	Keyword Filtering	Triggered rule "Test rule"	Gateway (SMTP)
<input type="checkbox"/>	3/27/2012 1:43:07 PM	administrator@tcdomainb.com	administrator@tcdomainb.com	Threat test	Keyword Filtering	Triggered rule "Test rule"	Gateway (SMTP)

Below the table, there are navigation controls (back, forward, page 1 of 1), a 'Page size: 10' dropdown, and a '3 items in 1 pages' indicator. At the bottom, there are buttons for 'Approve', 'Delete', and 'Rescan'.

Screenshot 25: Test email blocked by Test rule

NOTE

When test is completed successfully, delete or disable **Test rule** created in step 1.

2.6 Obtaining a GFI MailEssentials subscription

During the GFI MailEssentials installation, you are requested to key in your GFI account credentials or a license key.

Choose the procedure that best describes your scenario for information on how to obtain a subscription:

2.6.1 Evaluating GFI MailEssentials for 30 days

For a free GFI MailEssentials trial for 30 days:

1. Fill in the registration form at: <https://www.gfi.com/products-and-solutions/email-and-messaging-solutions/gfi-mailessentials/download>
2. Check your mail box and open the email received from noreply@gfi.com.
3. Click the link provided to confirm your account details and to create a password for your GFI Account.
4. After confirming your account details, the installer is automatically downloaded.
5. During the installation process, provide your GFI account credentials.

2.6.2 I have a GFI Account and want to install GFI MailEssentials for the first time

During installation, key in the username and password associated with your account and verify that the account is valid.

Your license status can also be verified from the GFI Accounts Portal. Login to <https://accounts.gfi.com> and click **My products**. Select GFI MailEssentials to check the status of your license.

2.6.3 Upgrading to a newer build or Service Release of the same version

When upgrading GFI MailEssentials to a build of the same version, such as when installing a Service Release, you have two options to enter a license:

- » Enter your GFI account credentials.
- » Select a license key from the **Available keys** list.

If you don't have access to your previous license key but you have a GFI account, you can retrieve the license key from the GFI Accounts portal. Login to <https://accounts.gfi.com> and click **My products**. Select GFI MailEssentials to retrieve your license key.

2.6.4 Upgrading to a newer version of GFI MailEssentials

When upgrading your current installation to a newer major version, there are two scenarios:

- » If using GFI Accounts, enter your credentials.
- » If using a license key, upgrade your key:

Log in to the GFI Customer Area on <https://customers.gfi.com/>.

- If you have a valid GFI MailEssentials maintenance agreement, click the blue key icon on the right and select **Upgrade License Key** to upgrade your license key. Then, key in your upgraded license key when running the installation wizard.
- If you do not have a valid GFI MailEssentials maintenance agreement, click on the blue key icon on the right and select **Renewal**. Renew your maintenance agreement. On completion a new license key is available. Then, key in your upgraded license key when running the installation wizard.

3 Monitoring status

GFI MailEssentials enables monitoring of your email activity in real time or by generating reports of email activity for a particular time period.

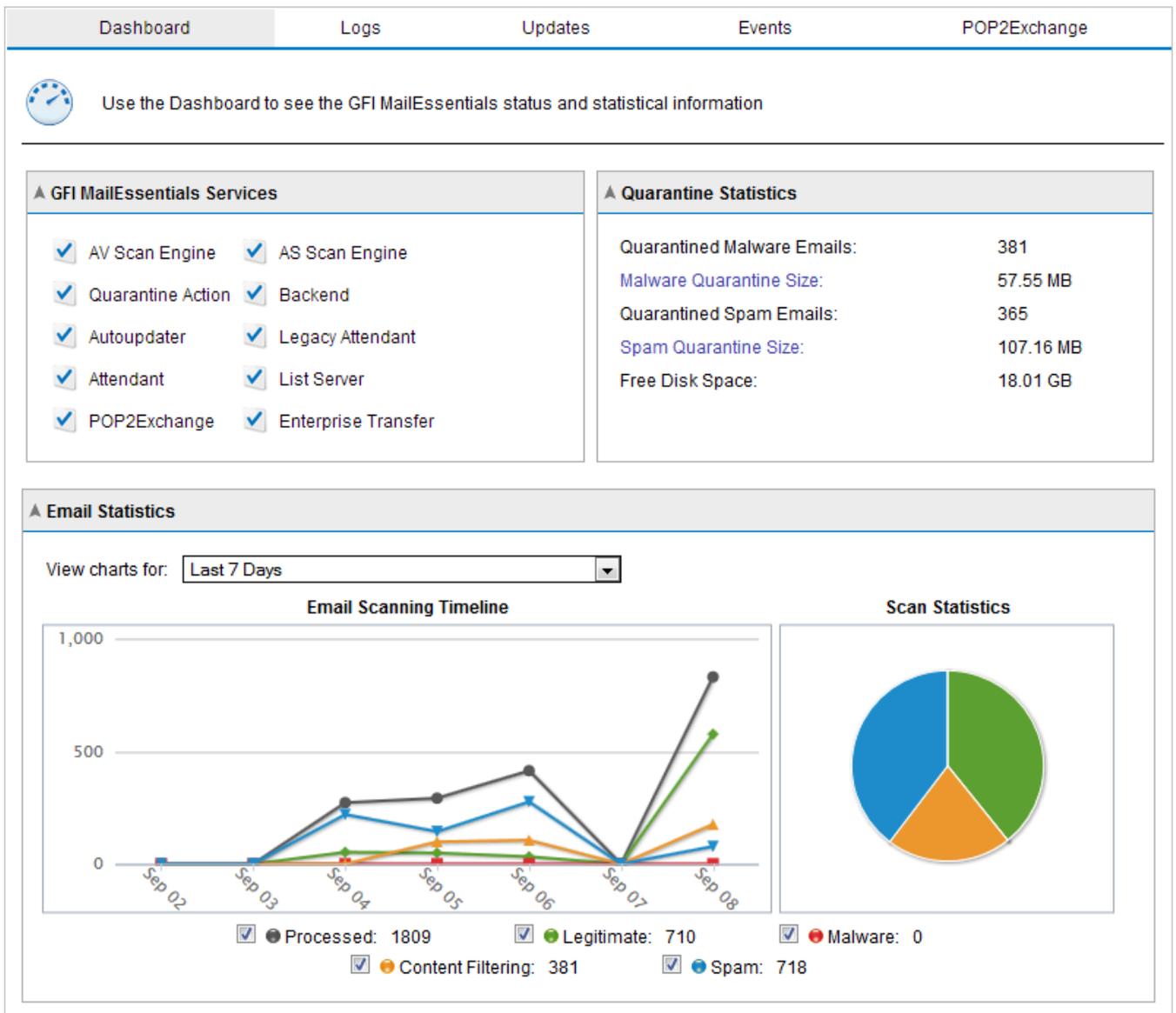
Monitoring module	Description
Dashboard	<p>The GFI MailEssentials Dashboard provides real time information that enables you to monitor the product. To access the Dashboard, go to GFI MailEssentials > Dashboard. This includes:</p> <ul style="list-style-type: none">» Important statistical information about blocked emails. For more information, refer to Status and statistics (page 51).» Status of GFI MailEssentials services. For more information, refer to Services (page 52).» Graphical presentation of email activity. For more information, refer to Charts (page 53).» List of emails processed. For more information, refer to Email processing logs (page 53).» Status of software updates. For more information, refer to Antivirus and anti-spam engine updates (page 56).» Record of important GFI MailEssentials events. For more information, refer to Event logs (page 58).» Log of POP2Exchange activities. For more information, refer to POP2Exchange activity (page 59).
Reports	<p>GFI MailEssentials enables you to create reports based on data logged to database. To access Reporting, go to GFI MailEssentials > Reporting.</p> <ul style="list-style-type: none">» Enabling reporting - For more information, refer to Enabling/Disabling reporting (page 59).» Configure reporting database - For more information, refer to Configuring reporting database (page 65).» Generate reports - For more information, refer to Generating a report (page 60).» Custom reports - Save custom report parameters and generate on a schedule. For more information, refer to Custom reports (page 63).» Search the reporting database - For more information, refer to Searching the reporting database (page 64).

3.1 Dashboard

The GFI MailEssentials **Dashboard** provides real time information that enables you to monitor the product. To access the Dashboard, go to **GFI MailEssentials > Dashboard**. This includes:

- » Important statistical information about blocked emails. For more information, refer to [Status and statistics](#) (page 51).
- » Status of GFI MailEssentials services. For more information, refer to [Services](#) (page 52).
- » Graphical presentation of email activity. For more information, refer to [Charts](#) (page 53).
- » List of emails processed. For more information, refer to [Email processing logs](#) (page 53).
- » Status of software updates. For more information, refer to [Antivirus and anti-spam engine updates](#) (page 56).
- » Record of important GFI MailEssentials events. For more information, refer to [Event logs](#) (page 58).
- » Log of POP2Exchange activities. For more information, refer to [POP2Exchange activity](#) (page 59).

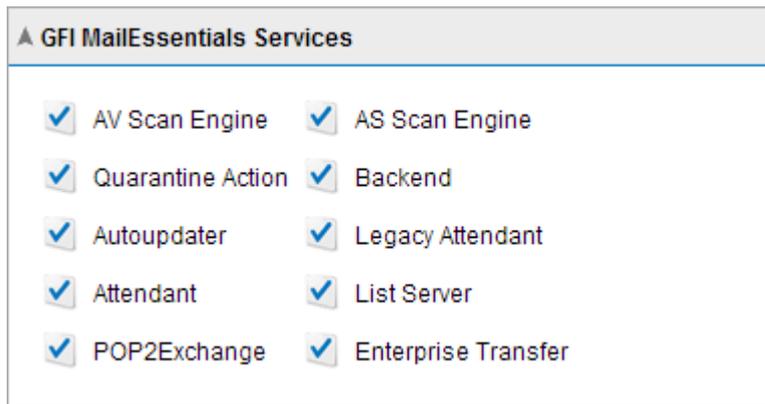
3.1.1 Status and statistics



Screenshot 26: The GFI MailEssentials Dashboard

To open the Dashboard, go to **GFI MailEssentials > Dashboard**. This page displays statistics, status of services and a graphical presentation of email activity. More details on these sections are provided below.

Services



Screenshot 27: The GFI MailEssentials Services

The **Services** area displays the status of GFI MailEssentials services.

»  - Indicates that the service is started.

»  - Indicates that the service is stopped. Click this icon to start a stopped service.

You can also start or stop services from the Microsoft® Windows Services console. To launch the Services console, go to **Start > Run**, type `services.msc` and click **OK**.

Quarantine Statistics

A screenshot of the Quarantine Statistics console. The title bar reads 'Quarantine Statistics'. Below the title bar, there is a table with two columns: 'Statistic title' and 'Value'. The table contains the following data:

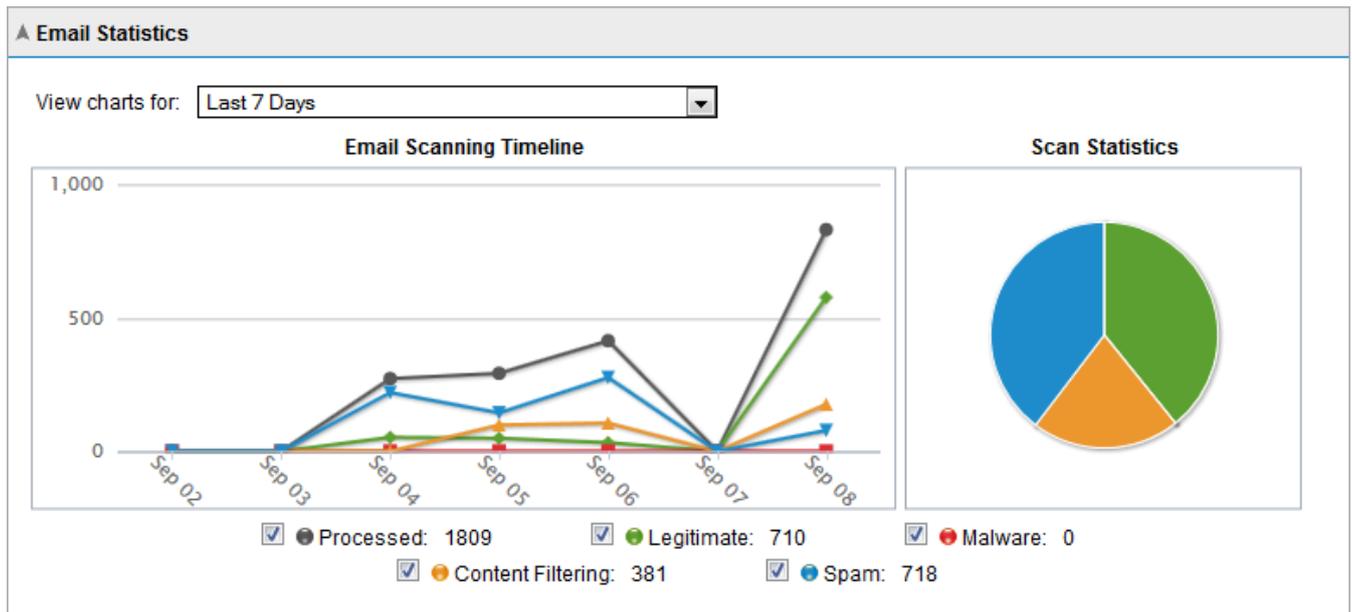
Statistic title	Value
Quarantined Malware Emails:	381
Malware Quarantine Size:	57.55 MB
Quarantined Spam Emails:	365
Spam Quarantine Size:	107.16 MB
Free Disk Space:	18.01 GB

Screenshot 28: Quarantine statistics

The **Quarantine Statistics** area displays the following statistical information:

Statistic title	Description
Quarantined Malware Emails	Number of emails blocked by Email Security and Content Filtering engines, and stored in the Malware Quarantine Store.
Malware Quarantine Size	Size on disk of the Malware Quarantine Store database.
Quarantined Spam Emails	Number of emails blocked by anti-spam engines and stored in the Spam Quarantine Store.
Spam Quarantine Size	Size on disk of the Spam Quarantine Store database.
Free disk space	Free space on the disk where quarantine stores are saved.

Charts



Screenshot 29: Dashboard charts

The **Charts** area displays graphical information about emails processed by GFI MailEssentials. Select the time period from the drop-down list to display information for that period in the charts.

Area	Description
View charts for	Enables you to select a period for which to view charts. Available options are: <ul style="list-style-type: none"> » Last 6 hours » Last 24 hours » Last 48 hours » Last 7 days
Email scanning timeline (time graph)	Shows a time graph in intervals for the time period selected. The graph shows the number of processed, legitimate, malware, content filtering and spam emails.
Scan statistics (pie chart)	A graphical distribution of the total number of safe, quarantined and failed emails for the time period selected.
Legend	The legend shows the color used in graphs and the count of each category.

3.1.2 Email processing logs

From GFI MailEssentials Configuration, you can monitor all processed emails in real time. Likewise, you can add recipients and senders to the whitelist or blocklist.

Dashboard **Logs** Updates Events POP2Exchange

The Logs show all the email scanning activity in chronological order

▲ Filters

Sender: Subject: Scan Result:

Recipient: From: To:

Modules:

Show entries

	Date/Time	Sender	Recipient(s)	Subject	Scan Result	View
	07/09/2013 11:57:27	safe@safesender.com	administrator@domaina.tcv	Test Subject	Ok	Details
	07/09/2013 11:41:04	spam@spam2domain.com	administrator@domaina.tcv	◆省下利息讓您輕鬆過生活◆	Blocked [SpamRazer]	Details
	07/09/2013 11:41:04	spam@spam2domain.com	administrator@domaina.tcv	◆省下利息讓您輕鬆過生活◆	Blocked [SpamRazer]	Details
	07/09/2013 11:41:04	spam@spam2domain.com	administrator@domaina.tcv	◆省下利息讓您輕鬆過生活◆	Blocked [SpamRazer]	Details
	07/09/2013 11:41:04	spam@spam2domain.com	administrator@domaina.tcv	◆省下利息讓您輕鬆過生活◆	Blocked [SpamRazer]	Details
	07/09/2013 11:41:03	spam@spam2domain.com	administrator@domaina.tcv	★★★網路行銷專家 快速曝光產品 增加網站流量★★★	Quarantined [Email Blocklist]	Details
	07/09/2013 11:41:03	spam@spam2domain.com	administrator@domaina.tcv	◆省下利息讓您輕鬆過生活◆	Blocked [SpamRazer]	Details
	07/09/2013 11:41:02	spam@spam2domain.com	administrator@domaina.tcv	◆省下利息讓您輕鬆過生活◆	Blocked [SpamRazer]	Details
	07/09/2013 11:41:02	spam@spam2domain.com	administrator@domaina.tcv	◆省下利息讓您輕鬆過生活◆	Blocked [SpamRazer]	Details
	07/09/2013 11:41:01	spam@spam2domain.com	administrator@domaina.tcv	★★★網路行銷專家 快速曝光產品 增加網站流量★★★	Quarantined [Email Blocklist]	Details

Showing 1 to 10 of 1,809 entries

Screenshot 30: Email processing logs

Navigate to **GFI MailEssentials > Dashboard** and select the **Logs** tab to display the list of processed emails. The following details are displayed for each email processed:

- » Date/Time
- » Sender
- » Recipient(s)
- » Subject
- » Scan Result - shows the action taken on the email. The below table defines each action.

Action	Description
OK	Email is not blocked by GFI MailEssentials, and is delivered to its intended recipients.
Quarantined	Email is blocked by an engine or a filter that has the action set to Quarantine. Click Quarantine to review the email.
	<p>NOTE</p> <p>The email cannot be previewed in quarantine if it was manually deleted from quarantine.</p>
Blocked	Email is blocked by an engine or filter. Action taken is as configured for that particular engine.
Deleted	Email is blocked by an engine or filter with the action set to delete detected emails.
Failed	Email that could not be scanned by GFI MailEssentials. Email is moved to one of the following folder: <code><GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\FailedMails\ <GFI MailEssentials installation path>\GFI\MailEssentials\AntiSpam\FailedMails\ For more information, refer to Failed emails (page 249).</code>

Working with the email processing logs

Senders and recipients can be added to the whitelist or blocklist directly from the processing logs page. For more information refer to [Whitelist](#) and [Blocklist](#).

To action an email right-click any log entry. The following actions can be taken from the context menu:

Action	Description
Details	Shows more detailed information about the email.
Add Sender to Whitelist	Adds the sender to the Whitelist. Emails from this sender bypass all the spam filters.
Add Sender to Blocklist	Adds the sender to the Blocklist. Emails from this sender are classified as spam.
Add Recipient to Whitelist	Adds the recipient to the Whitelist. Emails sent to this recipient bypass all the spam filters.
Add Recipient to Blocklist.	Adds the recipient to the Blocklist. Emails to this recipient are automatically classified as spam.

Filtering the email processing logs

Filtering the email processing logs simplifies the reviewing process by providing the possibility to find particular emails.

▲ Filters

Sender: Subject: Scan Result:

Recipient: From: To:

Modules:

[Clear Filters](#)

Screenshot 31: Email processing logs filter

From the **Filter** area, specify any of the following criteria:

Filter	Description
Sender	Specify the full or part of an email address to display only the emails sent by matching senders.
Recipient	Specify the full or part of an email address to display only the emails sent to matching recipients.

Filter	Description
Subject	Specify the full or part of an email subject to display only the emails with a matching subject.
Scan result	From the drop-down list, select whether to display only emails with a particular scan result (for example, quarantined emails only)
From & To	Specify a date and time range to display emails processed during that particular period.
Modules	Show only emails that were blocked by particular engines or filters.

NOTE

Click **Clear Filters** to remove specified filters and to show all email logs.

3.1.3 Antivirus and anti-spam engine updates

The updates of antivirus and antispam scanning engines can be monitored from a central page. Go to **GFI MailEssentials > Dashboard** and select the **Updates** tab to review the status, date and time when scanning engines were last updated.

Dashboard Logs **Updates** Events POP2Exchange

 GFI MailEssentials checks for and downloads updates for anti-virus engines and for spam filters

▲ Anti-Virus Definition Updates

	Anti-virus engine	Last Update	Status
	Avira AntiVirus	7/20/2017 2:17:36 PM	 Downloading... (in progress)
	BitDefender AntiVirus	7/20/2017 2:18:39 PM	 No updates currently in progress (last update succeeded)
	Kaspersky AntiVirus	7/20/2017 1:06:29 PM	 No updates currently in progress (last update succeeded)
	Cyren AntiVirus	7/20/2017 1:25:42 PM	 No updates currently in progress (last update failed)
	Sophos AntiVirus	7/20/2017 1:25:13 PM	 No updates currently in progress (last update succeeded)

Update all engines

▲ Anti-Spam Definition Updates

	Anti-spam engine	Last Update	Status
	SpamRazer	7/20/2017 1:06:29 PM	 No updates currently in progress (last update succeeded)
	Anti-Phishing	7/20/2017 2:18:39 PM	 No updates currently in progress (last update succeeded)
	Bayesian	7/20/2017 1:06:29 PM	 No updates currently in progress (last update succeeded)

Update all engines

Screenshot 32: Virus scanning engines updates

Click **Update all engines** to check for, and download all updates.

The updates are checked for, and downloaded, as configured in the engines' configuration pages. Go to the configuration page of each engine and navigate to the **Updates** tab to configure update settings.

NOTES

Updates for each engine are checked for and downloaded sequentially (one engine update at a time). If you experience problems when downloading updates, check your firewall settings to ensure that exceptions for the URLs used for updates are in place. For more information, refer to [Firewall port settings](#) (page 18).

3.1.4 Event logs

Dashboard Logs Updates **Events** POP2Exchange

Event Logging

▲ Events

Show entries

	Date	Event ID	Subject	Details
	03/01/2014 10:43:43	1027	GFI MailEssentials - Anti-Phishing data updated.	Details
	03/01/2014 10:42:32	1027	GFI MailEssentials - Anti-Phishing data updated.	Details

Showing 1 to 2 of 2 entries

First Previous **1** Next Last

Screenshot 33: Event logs

From GFI MailEssentials Configuration, you can monitor important events related to the functionality of GFI MailEssentials. Examples of instances that trigger events:

- » completion of anti-spam engine updates
- » reporting database reaches 1.7GB and GFI MailEssentials rolls over to a new database
- » less than 1GB free disk space on partition where quarantine is stored

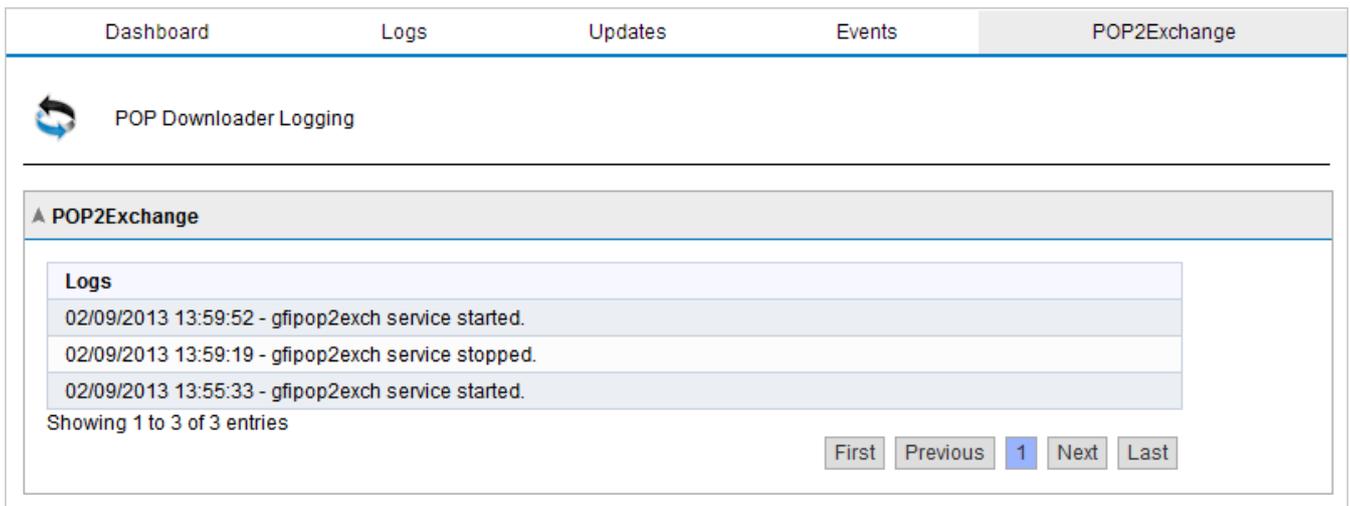
Navigate to **GFI MailEssentials > Dashboard** and select the **Events** tab to display the list of events. The following information is displayed for each event:

- » Date/Time
- » Event ID - an identifier is assigned to each type of GFI MailEssentials event.
- » Subject

Click **Details** to show more information about a particular event.

GFI MailEssentials events are also available from the Windows Event Viewer under **Applications and Services Logs > GFI MailEssentials**.

3.1.5 POP2Exchange activity



Dashboard Logs Updates Events POP2Exchange

POP Downloader Logging

▲ POP2Exchange

Logs
02/09/2013 13:59:52 - gfipop2exch service started.
02/09/2013 13:59:19 - gfipop2exch service stopped.
02/09/2013 13:55:33 - gfipop2exch service started.

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

Screenshot 34: POP2Exchange log

From GFI MailEssentials, you can monitor the activity of POP2Exchange in real time. Navigate to **GFI MailEssentials > Dashboard** and select the **POP2Exchange** tab.

NOTE

POP2Exchange is configurable from the Email Management Tools console. For more information, refer to [POP2Exchange - Download emails from POP3 server](#) (page 253).

3.2 Reports

GFI MailEssentials enables you to create reports based on data logged to database.

To access Reporting, go to **GFI MailEssentials > Reporting**.

- » **Enabling reporting** - For more information, refer to [Enabling/Disabling reporting](#) (page 59).
- » **Configure reporting database** - For more information, refer to [Configuring reporting database](#) (page 65).
- » **Generate reports** - For more information, refer to [Generating a report](#) (page 60).
- » **Custom reports** - Save custom report parameters and generate on a schedule. For more information, refer to [Custom reports](#) (page 63).
- » **Search the reporting database** - For more information, refer to [Searching the reporting database](#) (page 64).

3.2.1 Enabling/Disabling reporting

By default, Reporting is enabled and email activity data is logged to a Firebird database (.fdb) located in folder:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\data\
```

Go to **Reporting > Settings** node and check or uncheck **Enable Reporting** to enable or disable reporting respectively.

3.2.2 Generating a report

1. From GFI MailEssentials configuration, go to **GFI MailEssentials > Reporting > Reports**.

Report List Custom Reports

 Use this page to generate reports and select what data to show in the reports.

Reports lists

Select report to generate:

Email Direction [View Report Preview](#)

Description:

Reporting filtering

Date filtering:

Last 30 Days

Custom FROM date Custom TO date

04/08/2013 02/09/2013

Email direction filtering:

All email directions (inbound, outbound, internal)

Email address filtering:

Reporting grouping

Grouping:

Group by Week

Generate **Save As Custom**

Screenshot 35: Creating a report

2. From the **Report List** tab, configure the following report options:

Option	Description
Select report to generate:	<p>Select the type of report to generate:</p> <ul style="list-style-type: none"> » Email Direction - shows total emails processed for each email direction - Inbound, Outbound and Internal. » Email Direction Chart - graphically shows total emails processed for each email direction - Inbound, Outbound and Internal. » Emails Blocked - shows total emails blocked by anti-spam and anti-malware filters for each email direction (Inbound, Outbound and Internal) out of all emails processed. » Emails Blocked Graph - graphically shows total emails blocked by anti-spam and anti-malware filters for each email direction (Inbound, Outbound and Internal) out of all emails processed. » Spam Filter - shows the total number of emails blocked by each anti-spam filter. » Spam Filter Graph - graphically shows the total number of emails blocked by each anti-spam filter. » User Report - shows the number of blocked and allowed emails for each email address. » User Report (Active Users) - shows the number of blocked and allowed emails for email addresses that were active during the selected report period. <p>Click View Report Preview to preview how report looks like.</p>
Date filtering	<p>Select report date range. When selecting Custom date range, specify the period to display data for, from the Custom from date and Custom to date calendar controls.</p>
Email direction filtering	<p>Select a particular email direction to display data for or select All email directions (inbound, outbound, internal) to display data for all directions.</p>
Email address filtering	<p>Key in an email address to display report information for that particular email address only.</p>
Report Grouping	<p>Specify how to group data. Available options are:</p> <ul style="list-style-type: none"> » Group by Day » Group by Week » Group by Month » Group by Year

3. Click **Generate** to build and display the report or **Save as Custom** to save report settings for reuse at a later time.

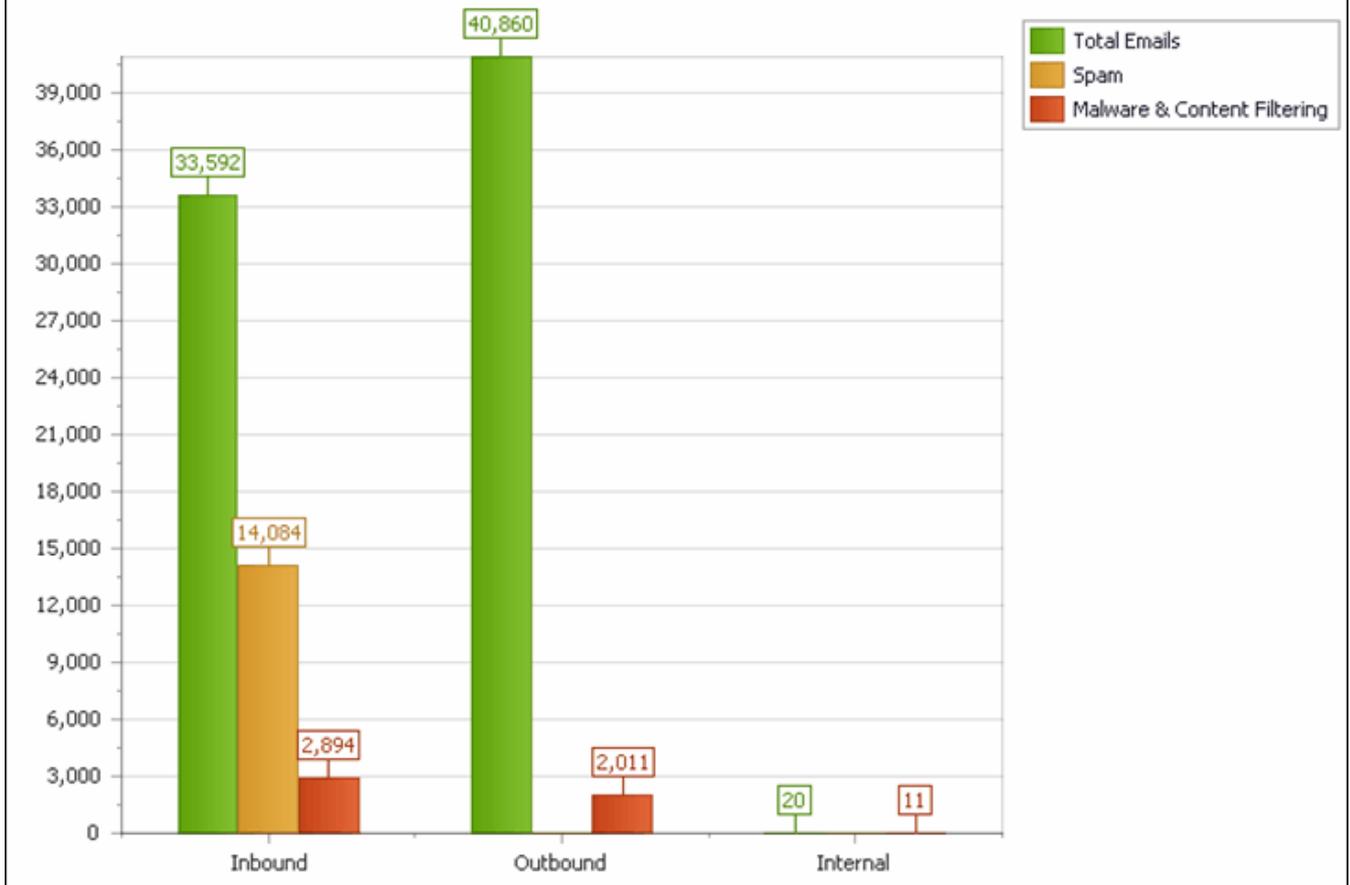
Emails Blocked Graph

From: Monday, February 27, 2012

User: All

To: Tuesday, March 27, 2012

Direction: All



Screenshot 36: Emails blocked graph report

Report functions

Use the report top toolbar to do the following functions:

Function	Icon	Description
Print		Click to print report.
Print current page		Click to print the page that is currently displayed.
Navigate		Use this toolbar to navigate through report pages.
Save		Select format to save report in and click Save . Specify location where to save report.

3.2.3 Custom reports

Custom reports enable you to save specific report parameters (for example, a report type for a specific time/date period) and to have it generated on a schedule. Use this feature to automate report generation.

Creating new custom reports

1. From GFI MailEssentials configuration, go to **GFI MailEssentials > Reporting > Reports**.
2. Select **Custom Reports** tab and click **New**.
3. In **Report Name**, key in a friendly name for the report.
4. Configure the following options:

Option	Description
Select report to generate:	Select the type of report to generate: <ul style="list-style-type: none">» Email Direction - shows total emails processed for each email direction - Inbound, Outbound and Internal.» Email Direction Chart - graphically shows total emails processed for each email direction - Inbound, Outbound and Internal.» Emails Blocked - shows total emails blocked by anti-spam and anti-malware filters for each email direction (Inbound, Outbound and Internal) out of all emails processed.» Emails Blocked Graph - graphically shows total emails blocked by anti-spam and anti-malware filters for each email direction (Inbound, Outbound and Internal) out of all emails processed.» Spam Filter - shows the total number of emails blocked by each anti-spam filter.» Spam Filter Graph - graphically shows the total number of emails blocked by each anti-spam filter.» User Report - shows the number of blocked and allowed emails for each email address.» User Report (Active Users) - shows the number of blocked and allowed emails for email addresses that were active during the selected report period. Click View Report Preview to preview how report looks like.
Date filtering	Select report date range. When selecting Custom date range , specify the period to display data for, from the Custom from date and Custom to date calendar controls.
Email direction filtering	Select a particular email direction to display data for or select All email directions (inbound, outbound, internal) to display data for all directions.
Email address filtering	Key in an email address to display report information for that particular email address only.
Report Grouping	Specify how to group data. Available options are: <ul style="list-style-type: none">» Group by Day» Group by Week» Group by Month» Group by Year

5. Optionally, enable **Send every** checkbox and configure a date/time combination to have the report generated at a specific date and time. Click **Add Rule** to save report generation time.

NOTE

To delete a rule, select an existing report generation time and click **Delete**.

6. Select whether to send report by email or save it to disk. To send report by email, select **Send by email** and provide the email address to where the email is sent. To save report to disk, select **Save to Disk** and provide a location where file will be saved. Select the format of the report in the **File Type** box.
7. Click **Save** to save newly created report.

3.2.4 Generating custom reports

To generate a custom report:

1. From GFI MailEssentials configuration, go to **GFI MailEssentials > Reporting > Reports**.
2. From the **Custom Reports** tab, select a report to generate.
3. Click **Generate**.

3.2.5 Deleting custom reports

To delete a custom report:

1. From GFI MailEssentials configuration, go to **GFI MailEssentials > Reporting > Reports**.
2. From the **Custom Reports** tab, select a report to delete.
3. Click **Delete**.

3.2.6 Searching the reporting database

GFI MailEssentials stores some properties of all emails processed in the reporting database. GFI MailEssentials enables you to search the reporting database, to find processed emails. To search the reporting database:

1. From GFI MailEssentials Configuration, go to **GFI MailEssentials > Reporting > Search**.

Search Email

 Use this page to search for emails in the reporting database.

Specify search date range:

Specify the days through which to search for emails sent and received by users:

Start Date:  End Date: 

User	Total Emails
<input type="text" value=""/> 	<input type="text" value=""/> 
 administrator@domaina.tcv	1384
 jsmith@domaina.tcv	1

Click an email address to view emails sent/received.

Screenshot 37: Searching the reporting database

2. Specify search criteria:

Search criteria	Description
Start date & End date	Select date range to filter emails from that period. Click Search .
User	Filter email address results. Key in number and click  to specify conditions.
Total emails	Filter users by the amount of emails processed. Key in number and click  to specify conditions.

3. The list of matching users is displayed. Click an email address to view detailed report of emails processed for that email address.

 administrator@domaina.tcv

	Date	Sender	Received	Subject	Size
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
	03/09/2013	spam@spam2domain.com	administrator@domaina.tcv	Energy Issues	188803
	03/09/2013	spam@spam2domain.com	administrator@domaina.tcv	DJ FERC To Lower Price Cap In Calif PwrOrder-Commissioners	8854
	03/09/2013	spam@spam2domain.com	administrator@domaina.tcv	Energy Issues	175289
	03/09/2013	spam@spamdomain.com	administrator@domaina.tcv	Test Subject	903
	03/09/2013	administrator@domaina.tcv	spam@spamdomain.com	RE: This is a blocked outbound email	5633
	03/09/2013	administrator@domaina.tcv	dhe@gkl.nu	RE: This is a blocked outbound email	4982
	03/09/2013	administrator@domaina.tcv	jsmith@domaina.tcv	blocked by content filtering	3965
	03/09/2013	administrator@domaina.tcv	spam@spamdomain.com	This is a blocked outbound email	4039

... 86 87 88 89 90 91 92 93 94 95 Page 95 of 95, items 1505 to 1520 of 1520.

Export report to file: **Export** **Close**

Screenshot 38: Reports database search results

4. (Optional) From the report, filter the data by email direction, sender, recipient or subject.

5. To export the report to another format, select format and click **Export**.

3.2.7 Configuring reporting database

By default, GFI MailEssentials uses a Firebird database **reports.fdb** located in:

`<GFI MailEssentials installation path>\GFI\MailEssentials\data\`

You can also use a Microsoft® SQL Server database for reports.

- » [Configuring a Firebird database backend](#)
- » [Configuring a Microsoft® SQL Server database backend](#)
- » [Configuring database auto-purging](#)

Configuring a Firebird database backend

Reporting Auto Purge

 Configure reporting database.

Use this node to enable and use GFI MailEssentials Reporting. This enables you to use the data collected by GFI MailEssentials and generate various reports.

Enable Reporting

Current Database Settings

Current type : Firebird

Current location : C:\Program Files (x86)\GFI\MailEssentials\data\reports.fdb

New Database Settings

Database type

Firebird SQL Server

Enter a valid path to an existing database below or specify a new location/filename to have a new database created automatically.

File : C:\Program Files (x86)\GFI\MailEssentials\data\reports.fdb

Screenshot 39: Configuring a Firebird database backend

1. Navigate to **Reporting > Settings**.
2. From the **Database Type** box, select **Firebird**.
3. Key in the complete path including file name and .fdb extension of the database file. If you only specify a file name, the database file is created in the following default path:

`<GFI MailEssentials installation path>\GFI\MailEssentials\data\`

4. Click **Apply**.

NOTE

An email notification is sent to the administrator when the database reaches 7GB since this may impact performance. If this is the case it is recommended to use [Auto-Purging](#) to remove emails older than a particular date.

Configuring a Microsoft® SQL Server database backend

1. Create a new database in Microsoft® SQL Server.
2. Create a dedicated user/login in Microsoft® SQL Server, mapped to the newly created database. Grant the user full access to all server and database roles and permissions.
3. In GFI MailEssentials navigate to **Reporting > Settings**.

New Database Settings

Database type

Firebird SQL Server

SQL server reporting

Detected server : DBServer\SQL

Manually specified server :

User : administrator

Password : ●●●●●●●●

Get Database List

Database :

Screenshot 40: Configuring SQL Server Database backend

4. From the **Database Type** box, select **SQL Server**.
5. Select **Detected server** to select an automatically detected SQL Server from the list. If the server is not detected, select **Manually specified server** and key in the Microsoft® SQL Server host name or IP address.
6. Key in the credentials with permissions to read/write to the database.
7. Click **Get Database List** to extract the list of databases from the server.
8. From the **Database** list, select the database created for GFI MailEssentials Reporting.
9. Click **Apply**.

Configuring database auto-purging

You can configure GFI MailEssentials to automatically delete (auto-purge) records from the database that are older than a particular period.

By default Auto-Purging is configured to delete data older than 12 months.

To enable auto-purging:

1. Navigate to **Reporting > Settings** and select **Auto-purge** tab.
2. Select **Enable Auto-Purging** and specify how long items in database should be stored in months .
3. Click **Apply**.

NOTE

Auto-purging is applied only to the current database configured in the Reporting tab.

3.2.8 Maillnsights® report

Maillnsights® is a reporting facility that uses the data in the reporting database to deliver information related to email usage and trends.

GFI MailEssentials provides the Communication Flow report which gives a graphical presentation of emails exchanged between selected users/groups and their contacts. Other [Maillnsights®](#) reports can be generated using [GFI MailArchiver](#).

Communication Flow report

The Communication Flow report shows the top 20 contacts that a user communicated with in the previous 30 days.

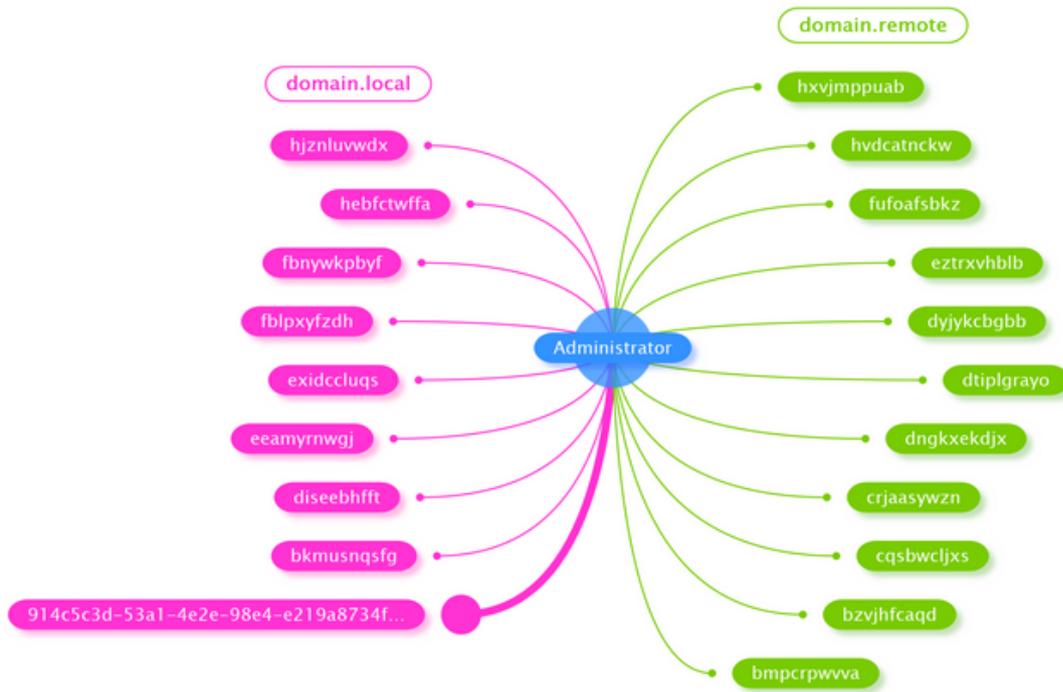
1. Navigate to **Reporting > Maillnsights** and select the **Communication Flow** tab.
2. Administrators can generate the report for any email user. Click **Search** to select an email user and click **Generate** to start building the report.

The generated report displays the data for the selected user as follows:

Totals	The top area of the report shows the total statistics of communication flow in the previous 30 days. <ul style="list-style-type: none">» Total Contacts - the total number of email addresses with whom the user had email communications.» Total Internal - total number of internal users with whom the user had communications.» Top Internal - the internal email address with whom the selected user communicated the most.» Total External - total number of external users with whom the user had communications.» Top External - the external email address with whom the selected user communicated the most.
Graph	The selected user is displayed as a single entity in the middle of the graph. Contacts are segregated by domains. Each domain cluster is shown in different color. Edge width between the nodes shows the strength of the email relation between different entities.
Top 20 contacts	The top 20 contacts with whom the selected user communicated the most. Color codes indicate the different contacts' domains. The table indicates the total number of sent & received emails with that contact, together with the date and time when the last email communication occurred.

Top 20 Contacts - Last 30 days

Total Contacts	Total Internal	Top Internal	Total External	Top External
20	20	914c5c3d-53a1-4e2e-98e4-e219a8734f78@domain.local	0	
100% of Total Contacts	100% of Total Contacts	5	0% of Total Contacts	0



Screenshot 41: MailInsights® Communication Flow report

4 Email Security

The security filters of GFI MailEssentials offer protection against virus-infected and other malicious emails.

Topics in this chapter:

4.1 Virus Scanning Engines	70
4.2 Information Store Protection	91
4.3 Trojan and Executable Scanner	94
4.4 Email Exploit Engine	98
4.5 HTML Sanitizer	102

4.1 Virus Scanning Engines

GFI MailEssentials uses multiple antivirus engines to scan inbound, outbound and internal emails for the presence of viruses. GFI MailEssentials ships with Avira and BitDefender Virus Scanning Engines. You can also acquire a license for Kaspersky, Sophos & Cyren.

This chapter describes how to configure Virus Scanning Engines, updates, actions and the scanning sequence.

4.1.1 Virus Scanning Priority

GFI MailEssentials uses third-parties antivirus engines to scan emails for malicious threats.

Apply
Cancel

Virus Scanning

Virus Scanning Engines

Virus Scanning Engines Status

Use this page to review the virus scanning engine status and to configure their order of execution.

	Virus Scanning Engine	Status	License	Priority		
	Avira Anti-Virus	Gateway scanning: Enabled	Licensed	0	↑	↓
	BitDefender Anti-Virus	Gateway scanning: Enabled	Licensed	1	↑	↓
	Kaspersky Anti-Virus	Gateway scanning: Enabled	Licensed	2	↑	↓
	Cyren Anti-Virus	Gateway scanning: Enabled	Licensed	3	↑	↓
	Sophos Anti-Virus	Gateway scanning: Enabled	Licensed	4	↑	↓

Virus Scanning Optimizations

Stop virus scanning the current item, if viruses are detected by:
 virus scanners

Stop all further scanning (including non-virus related threats scanning)

Screenshot 42: Virus Scanning Engine priority list

Administrators can have an overview of the antivirus engines' statuses and alter the order used to scan the emails. GFI MailEssentials scans the emails in the order set on the **Virus Scanning Engine Status** from top to bottom.

To reorder the antivirus priority list:

1. Go to **Email Security > Virus Scanning Engines**.
2. Click the icon to increase or the icon to decrease the priority of the engine.
3. Click **Save**.

Administrators can also optimize the virus scanning by checking or unchecking the following options:

- » Stop virus scanning the current item, if viruses are detected by a specified number of virus scanners.
- » Stop all further scanning, including non-virus related threats scanning.

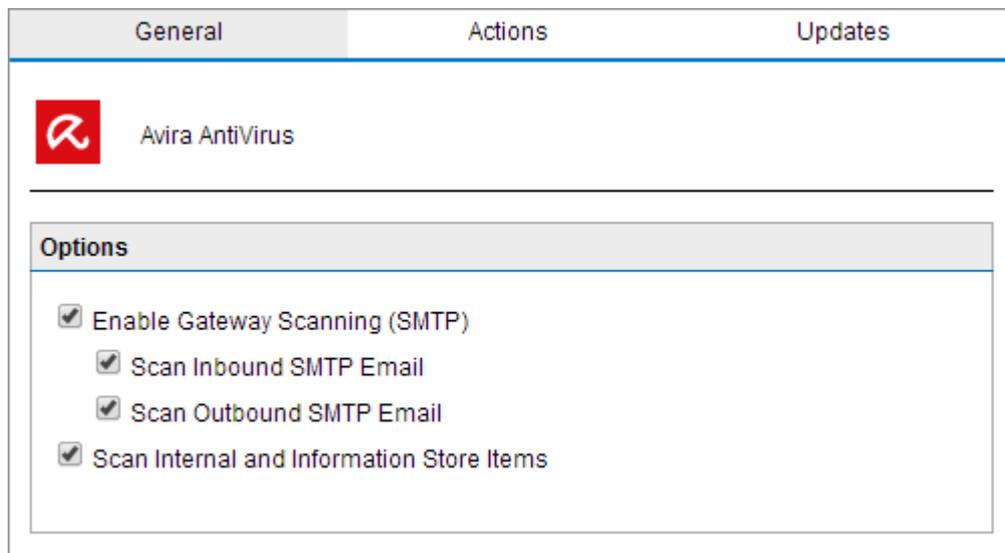
4.1.2 Avira

GFI MailEssentials uses Avira antivirus to scan inbound, outbound and internal email for viruses. The Avira license is included in the GFI MailEssentials license.

Emails found containing virus during a scan are handled according to the action set for the engine that detected the virus.

To configure the Avira settings:

1. Go to **Email Security > Virus Scanning Engines > Avira**.



Screenshot 43: Avira configuration

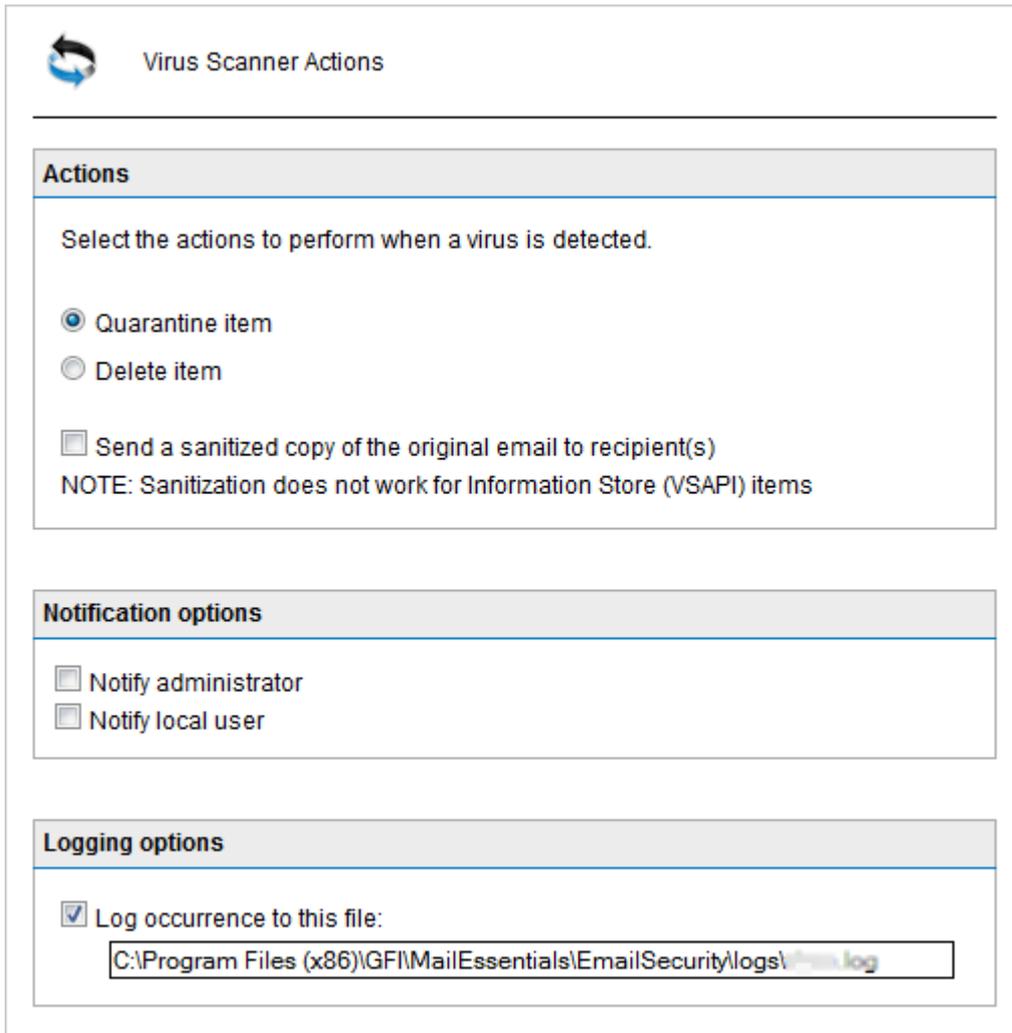
2. Select the **Enable Gateway Scanning (SMTP)** check box to scan emails using this Virus Scanning Engine.
3. Select whether to scan inbound and/or outbound emails using this Virus Scanning Engine.

Option	Description
Scan Inbound SMTP email	Check this option to scan incoming emails.
Scan Outbound SMTP email	Check this option to scan outgoing emails.

4. If Information Store Protection is enabled, you have the option to scan internal emails and the Information Store Items. Check **Scan Internal and Information Store Items**. For more information, refer to [Information Store Protection](#) (page 91).

NOTE

On this page you can also review the antivirus engine licensing and version information.



Screenshot 44: Virus scanning engine actions

5. From the **Actions** tab, choose the action to be taken when an email is blocked:

Action	Description
Quarantine item	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve or delete) all the quarantined emails. For more information, refer to Quarantine (page 191).
Delete item	Deletes infected emails.
Send a sanitized copy of the original email to recipient(s)	When this option is enabled, GFI MailEssentials removes malicious content from emails and attaches a text file indicating that the email contained malicious content. The email is then forwarded to its intended recipients.

6. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

7. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

General Actions Updates

Configure the Automatic Updates For This Profile

Automatic update options

Configure the automatic update options.

Automatically check for updates

Downloading option:
Check for updates and download ▾

Download time interval:
1 hour(s)

Last update:
Never

Update options

Enable email notifications upon successful updates

NOTE: Notifications for unsuccessful updates will always be sent.

Click the buttons below to either trigger the update process manually or force a clean full update of the antivirus engine files.

Download updates

Force full update

Update Status

No updates currently in progress (last update succeeded)

Screenshot 45: Engine Updates tab

8. In the **Updates** tab, check **Automatically check for updates** to enable automatic updating for the selected engine.

9. From the **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option does NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

10. Specify how often you want GFI MailEssentials to check and download updates for this engine, by specifying an interval value in hours.

11. From **Update options** area, check **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

NOTE

An email notification is always sent when an update fails.

12. To force the most recent updates you have two options:

Option	Description
Download updates	Trigger the update process manually. It is an incremental update where only the most recent definitions are updated.
Force full updates	This option forces a new version of the engine to be downloaded and replaced. This option is slower and consumes more bandwidth.

13. Click **Apply**.

4.1.3 BitDefender

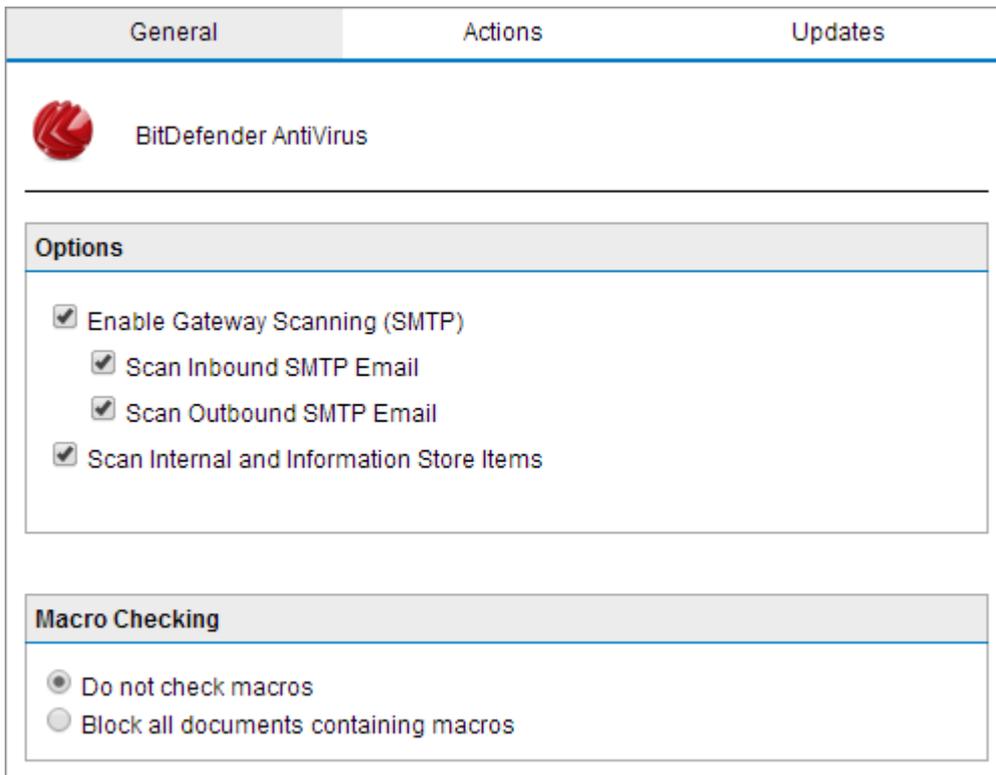
GFI MailEssentials uses BitDefender antivirus to scan inbound, outbound and internal email for viruses.

The BitDefender license is included in the GFI MailEssentials license.

Emails found containing virus during a scan are handled according to the action set for the engine that detected the virus.

To configure the BitDefender settings:

1. Go to **Email Security > Virus Scanning Engines > BitDefender**.



Screenshot 46: BitDefender configuration

2. Select the **Enable Gateway Scanning (SMTP)** check box to scan emails using this Virus Scanning Engine.
3. Select whether to scan inbound and/or outbound emails using this Virus Scanning Engine.

Option	Description
Scan Inbound SMTP email	Check this option to scan incoming emails.
Scan Outbound SMTP email	Check this option to scan outgoing emails.

4. If Information Store Protection is enabled, you have the option to scan internal emails and the Information Store Items. Check **Scan Internal and Information Store Items**. For more information, refer to [Information Store Protection](#) (page 91).

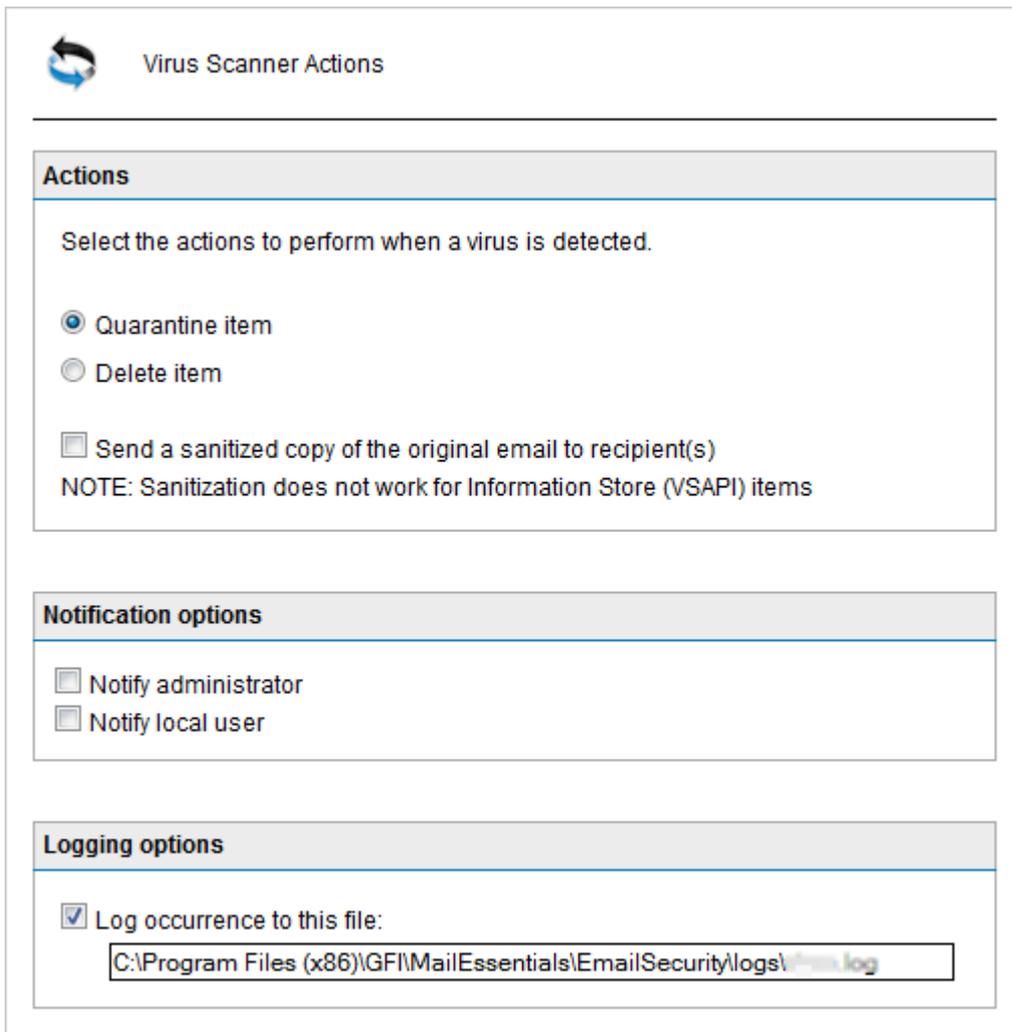
5. BitDefender can also be used to block emails with attachments that contain macros. Enable this feature from the **Macro Checking** area by selecting **Block all documents containing macros**.

NOTE

If Macro Checking is disabled, GFI MailEssentials still scans for and blocks Macro Viruses.

NOTE

On this page you can also review the antivirus engine licensing and version information.



Screenshot 47: Virus scanning engine actions

6. From the **Actions** tab, choose the action to be taken when an email is blocked:

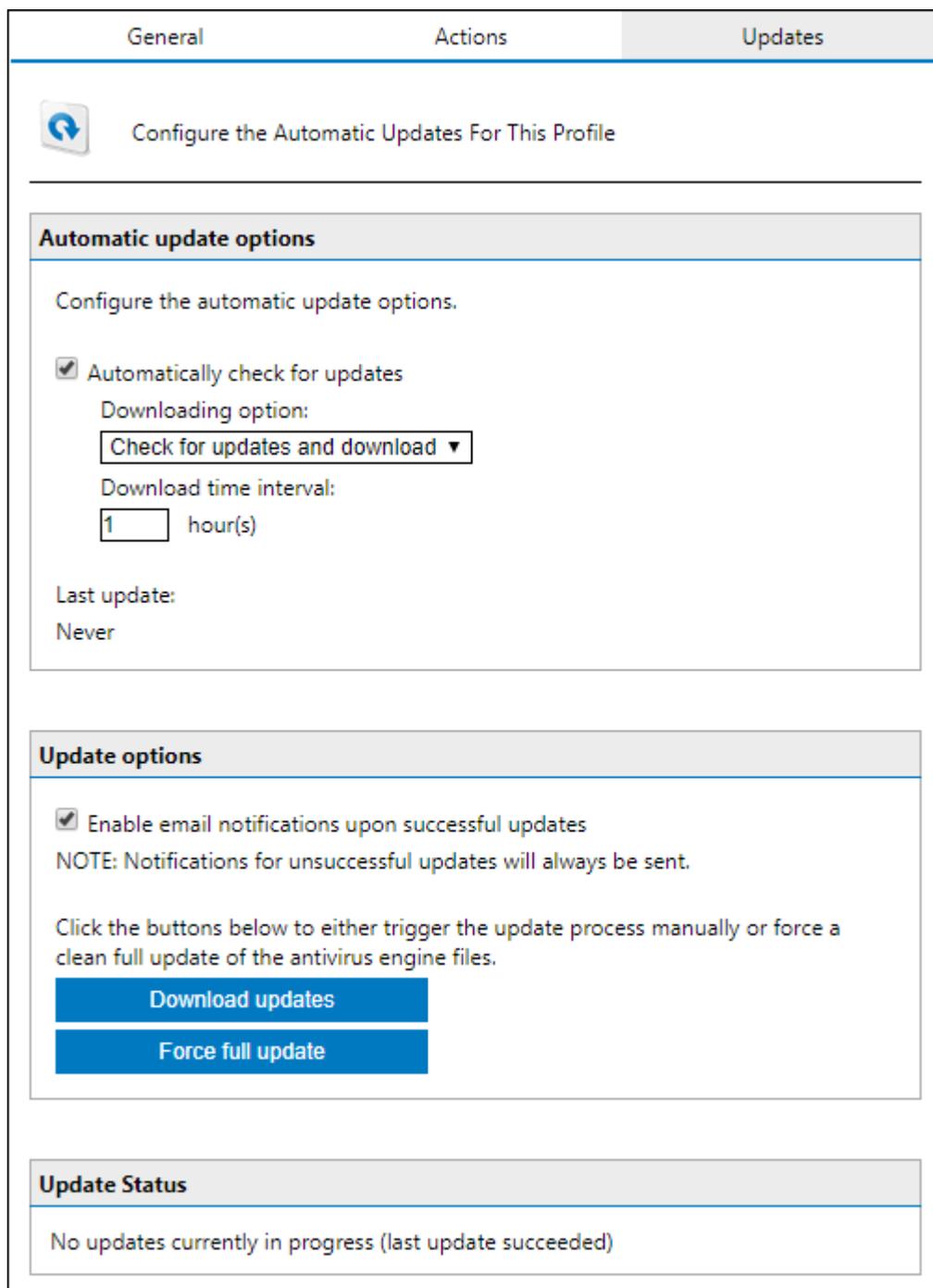
Action	Description
Quarantine item	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve or delete) all the quarantined emails. For more information, refer to Quarantine (page 191).
Delete item	Deletes infected emails.
Send a sanitized copy of the original email to recipient(s)	When this option is enabled, GFI MailEssentials removes malicious content from emails and attaches a text file indicating that the email contained malicious content. The email is then forwarded to its intended recipients.

7. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```



Screenshot 48: Engine Updates tab

9. In the **Updates** tab, check **Automatically check for updates** to enable automatic updating for the selected engine.

10. From the **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option does NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

11. Specify how often you want GFI MailEssentials to check and download updates for this engine, by specifying an interval value in hours.

12. From **Update options** area, check **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

NOTE

An email notification is always sent when an update fails.

13. To force the most recent updates you have two options:

Option	Description
Download updates	Trigger the update process manually. It is an incremental update where only the most recent definitions are updated.
Force full updates	This option forces a new version of the engine to be downloaded and replaced. This option is slower and consumes more bandwidth.

14. Click **Apply**.

4.1.4 Kaspersky

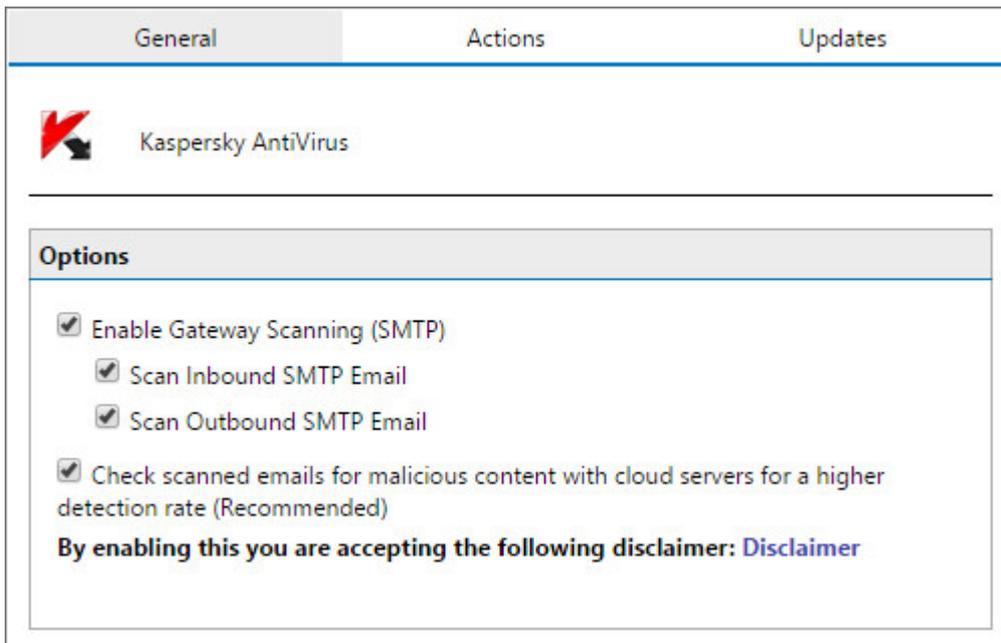
GFI MailEssentials uses Kasperky antivirus to scan inbound, outbound and internal email for viruses.

The Kaspersky license needs be acquired separately from the GFI MailEssentials license.

Emails found containing virus during a scan are handled according to the action set for the engine that detected the virus.

To configure the Kaspersky settings:

1. Go to **Email Security > Virus Scanning Engines > Kaspersky**.



Screenshot 49: Kaspersky configuration

2. Select the **Enable Gateway Scanning (SMTP)** check box to scan emails using this Virus Scanning Engine.
3. Select whether to scan inbound and/or outbound emails using this Virus Scanning Engine.

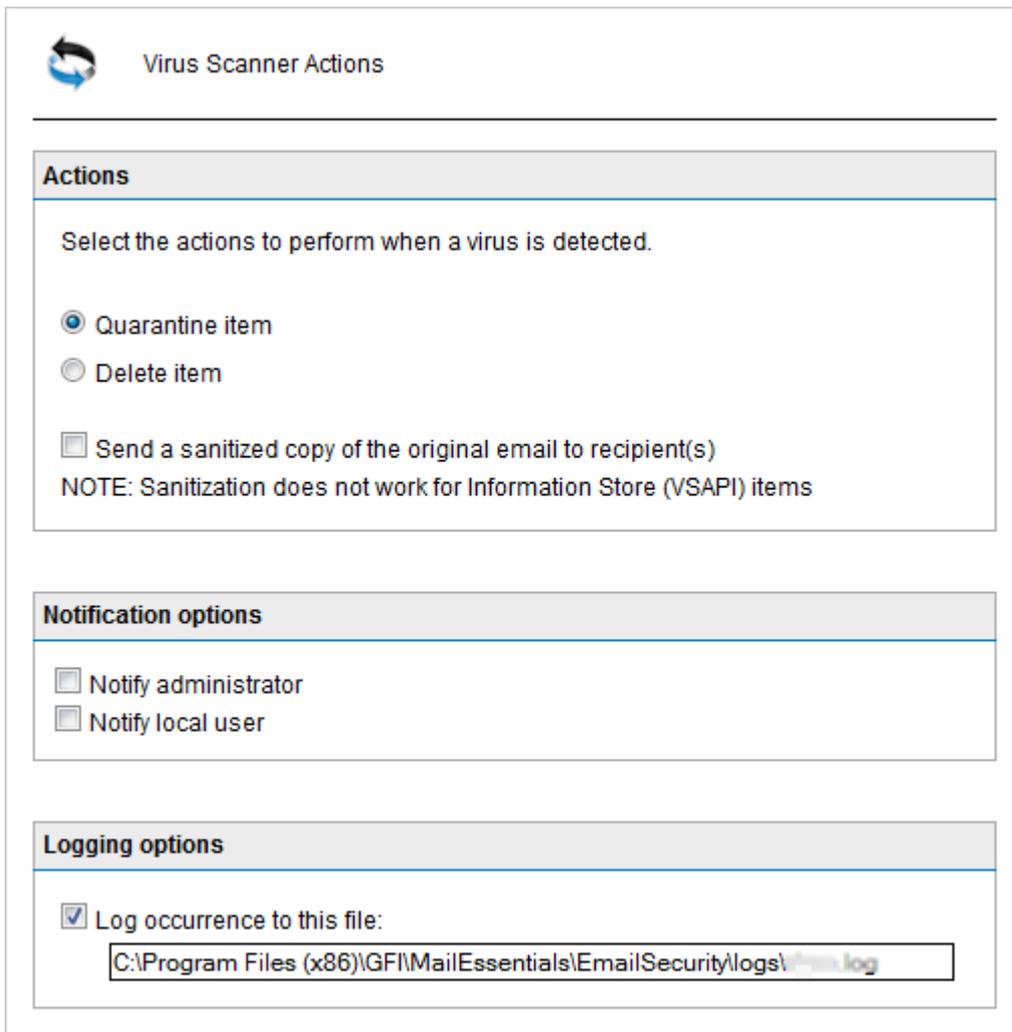
Option	Description
Scan Inbound SMTP email	Check this option to scan incoming emails.
Scan Outbound SMTP email	Check this option to scan outgoing emails.

4. If Information Store Protection is enabled, you have the option to scan internal emails and the Information Store Items. Check **Scan Internal and Information Store Items**. For more information, refer to [Information Store Protection](#) (page 91).

5. Select **Check scanned emails for malicious content with cloud server for a higher detection rate** to enable zero-hour virus detection. When an executable attachment is found, this feature creates a hash key based on the attachment and sends the key to a Kaspersky cloud service to be compared with well-known malicious hashes. This feature offers a more secure environment where viruses can be detected quicker, since it does not rely on updates of the antivirus engine. When this feature is enabled, you may experience a slight delay in email delivery of inbound emails. Note that by enabling to use this feature, you will be accepting the Kaspersky disclaimer shown when you click the link **Disclaimer**.

NOTE

On this page you can also review the antivirus engine licensing and version information.



Screenshot 50: Virus scanning engine actions

6. From the **Actions** tab, choose the action to be taken when an email is blocked:

Action	Description
Quarantine item	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve or delete) all the quarantined emails. For more information, refer to Quarantine (page 191).
Delete item	Deletes infected emails.
Send a sanitized copy of the original email to recipient(s)	When this option is enabled, GFI MailEssentials removes malicious content from emails and attaches a text file indicating that the email contained malicious content. The email is then forwarded to its intended recipients.

7. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

General Actions Updates

Configure the Automatic Updates For This Profile

Automatic update options

Configure the automatic update options.

Automatically check for updates

Downloading option:
Check for updates and download ▾

Download time interval:
1 hour(s)

Last update:
Never

Update options

Enable email notifications upon successful updates
NOTE: Notifications for unsuccessful updates will always be sent.

Click the buttons below to either trigger the update process manually or force a clean full update of the antivirus engine files.

Download updates

Force full update

Update Status

No updates currently in progress (last update succeeded)

Screenshot 51: Engine Updates tab

9. In the **Updates** tab, check **Automatically check for updates** to enable automatic updating for the selected engine.

10. From the **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option does NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

11. Specify how often you want GFI MailEssentials to check and download updates for this engine, by specifying an interval value in hours.

12. From **Update options** area, check **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

NOTE

An email notification is always sent when an update fails.

13. To force the most recent updates you have two options:

Option	Description
Download updates	Trigger the update process manually. It is an incremental update where only the most recent definitions are updated.
Force full updates	This option forces a new version of the engine to be downloaded and replaced. This option is slower and consumes more bandwidth.

14. Click **Apply**.

4.1.5 Sophos

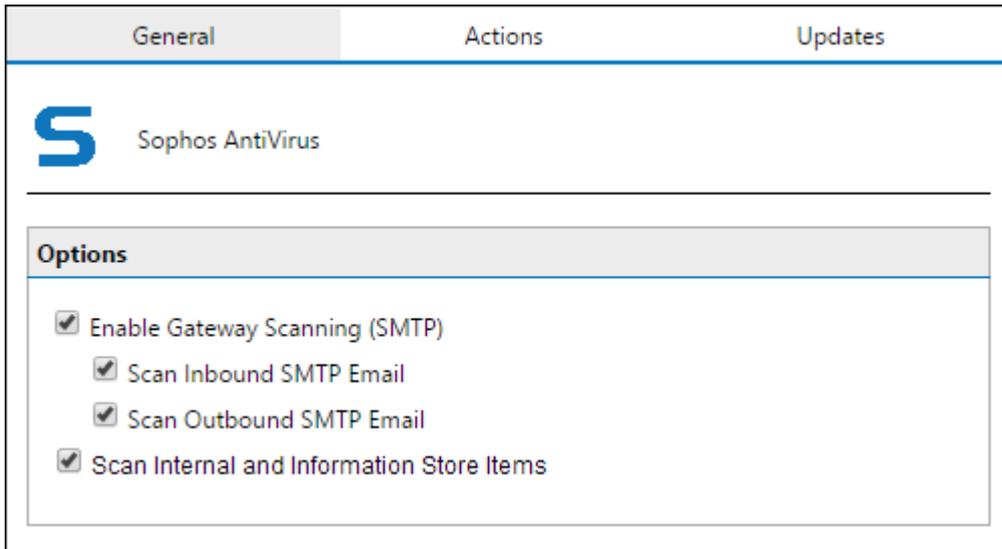
GFI MailEssentials uses Sophos antivirus to scan inbound, outbound and internal email for viruses.

The Sophos license is acquired separately from the GFI MailEssentials license.

Emails found containing virus during a scan are handled according to the action set for the engine that detected the virus.

To configure Sophos settings:

1. Go to **Email Security > Virus Scanning Engines > Sophos**.



Screenshot 52: Sophos configuration

2. Select the **Enable Gateway Scanning (SMTP)** check box to scan emails using this Virus Scanning Engine.

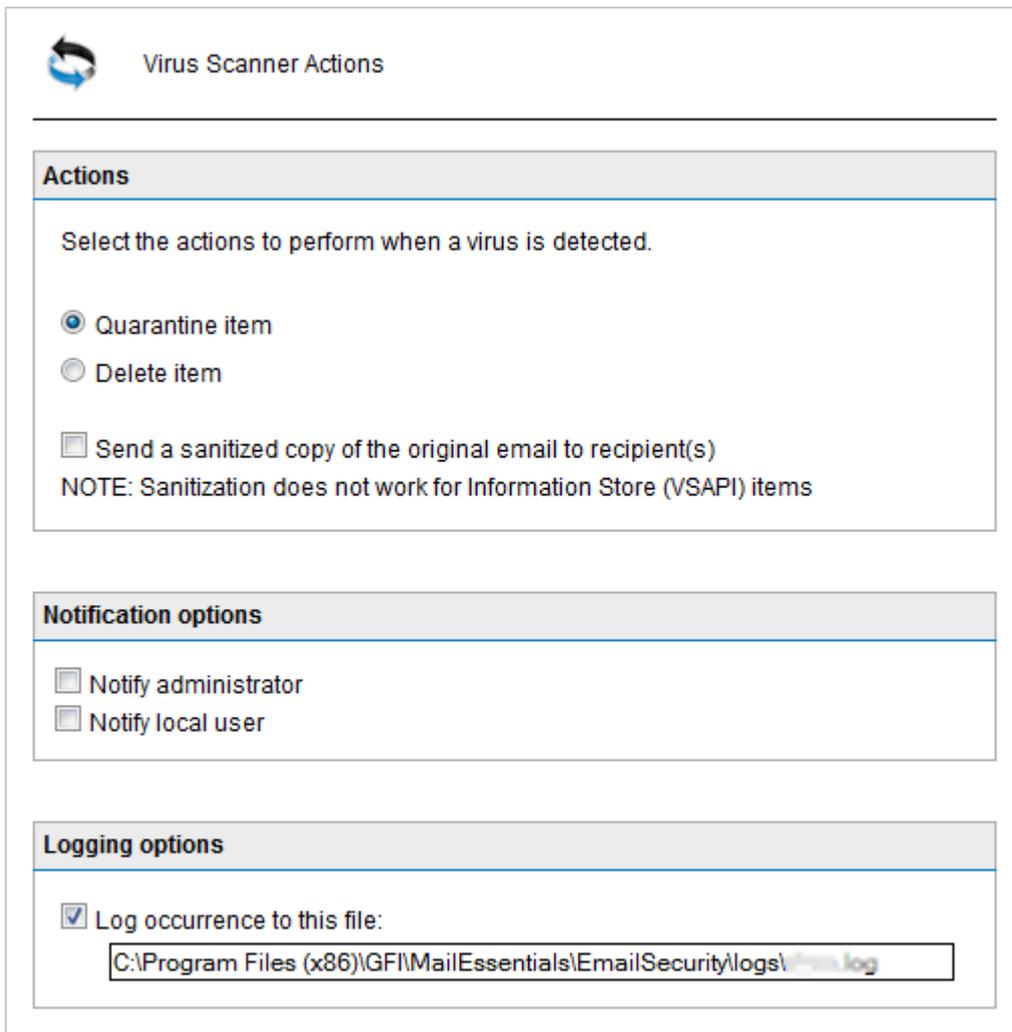
3. Select whether to scan inbound and/or outbound emails using this Virus Scanning Engine.

Option	Description
Scan Inbound SMTP email	Check this option to scan incoming emails.
Scan Outbound SMTP email	Check this option to scan outgoing emails.

4. If Information Store Protection is enabled, you have the option to scan internal emails and the Information Store Items. Check **Scan Internal and Information Store Items**. For more information, refer to [Information Store Protection](#) (page 91).

NOTE

On this page you can also review the antivirus engine licensing and version information.



Screenshot 53: Virus scanning engine actions

5. From the **Actions** tab, choose the action to be taken when an email is blocked:

Action	Description
Quarantine item	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve or delete) all the quarantined emails. For more information, refer to Quarantine (page 191).
Delete item	Deletes infected emails.
Send a sanitized copy of the original email to recipient(s)	When this option is enabled, GFI MailEssentials removes malicious content from emails and attaches a text file indicating that the email contained malicious content. The email is then forwarded to its intended recipients.

6. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

7. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

General Actions Updates

Configure the Automatic Updates For This Profile

Automatic update options

Configure the automatic update options.

Automatically check for updates

Downloading option:
Check for updates and download ▾

Download time interval:
1 hour(s)

Last update:
Never

Update options

Enable email notifications upon successful updates

NOTE: Notifications for unsuccessful updates will always be sent.

Click the buttons below to either trigger the update process manually or force a clean full update of the antivirus engine files.

Download updates

Force full update

Update Status

No updates currently in progress (last update succeeded)

Screenshot 54: Engine Updates tab

8. In the **Updates** tab, check **Automatically check for updates** to enable automatic updating for the selected engine.

9. From the **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option does NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

10. Specify how often you want GFI MailEssentials to check and download updates for this engine, by specifying an interval value in hours.

11. From **Update options** area, check **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

NOTE

An email notification is always sent when an update fails.

12. To force the most recent updates you have two options:

Option	Description
Download updates	Trigger the update process manually. It is an incremental update where only the most recent definitions are updated.
Force full updates	This option forces a new version of the engine to be downloaded and replaced. This option is slower and consumes more bandwidth.

13. Click **Apply**.

4.1.6 Cyren

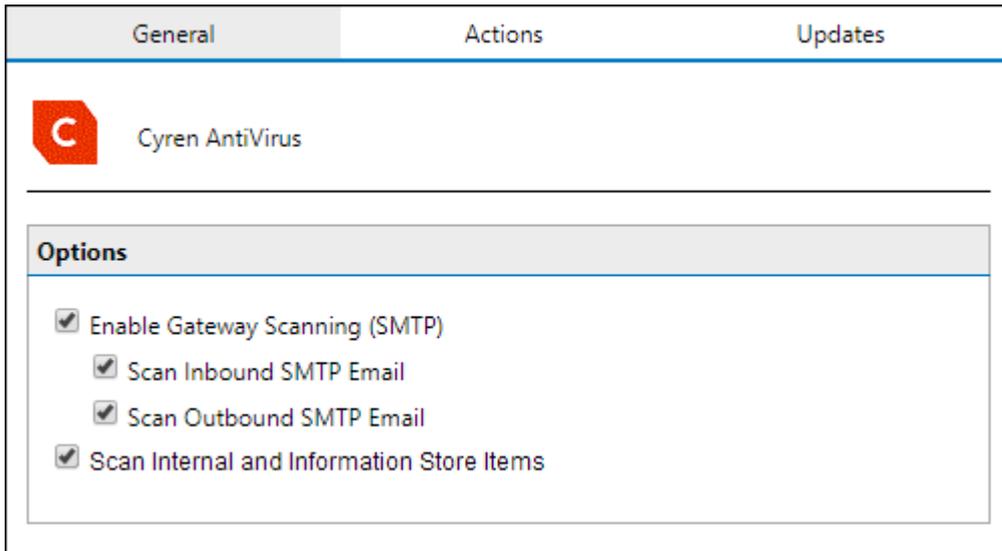
GFI MailEssentials uses Cyren antivirus to scan inbound, outbound and internal email for viruses.

The Cyren license is acquired separately from the GFI MailEssentials license.

Emails found containing virus during a scan are handled according to the action set for the engine that detected the virus.

To configure the Cyren settings:

1. Go to **Email Security > Virus Scanning Engines > Cyren**.



Screenshot 55: Cyren configuration

2. Select the **Enable Gateway Scanning (SMTP)** check box to scan emails using this Virus Scanning Engine.

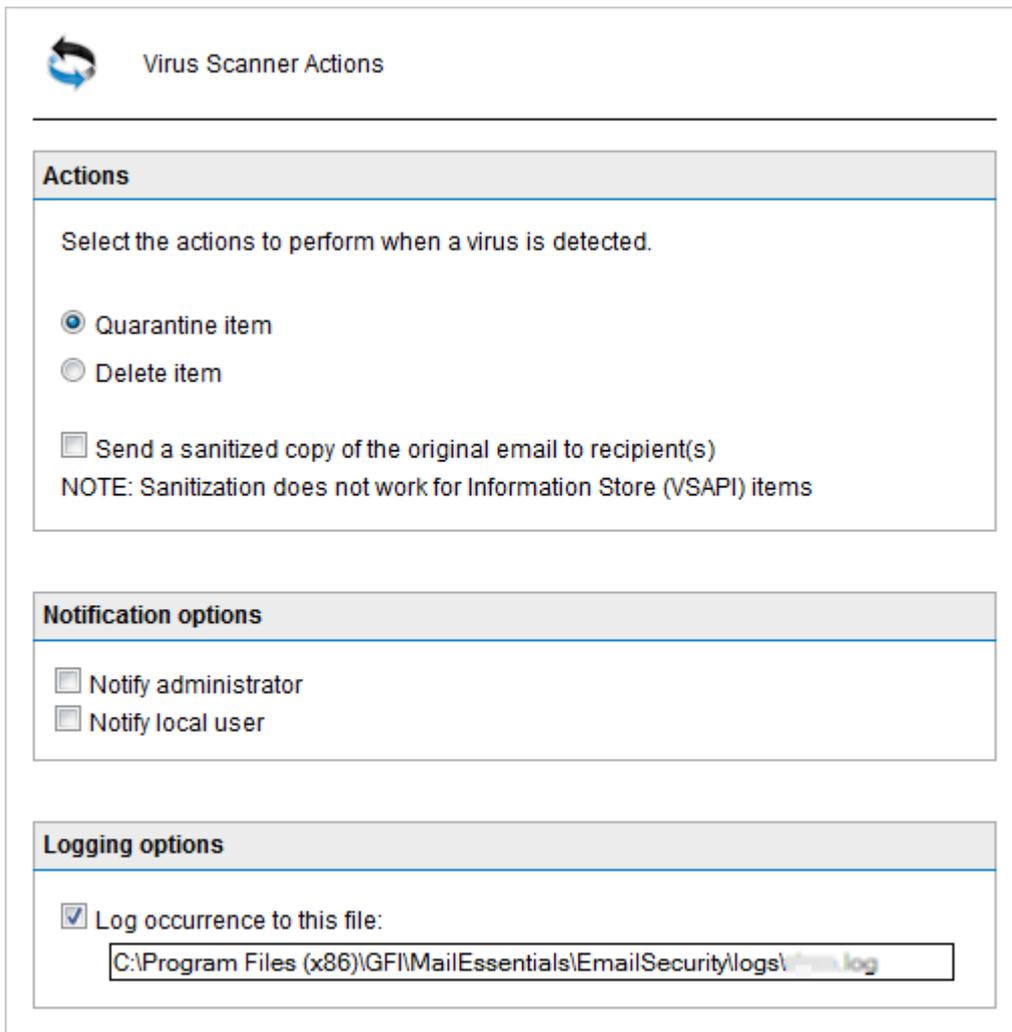
3. Select whether to scan inbound and/or outbound emails using this Virus Scanning Engine.

Option	Description
Scan Inbound SMTP email	Check this option to scan incoming emails.
Scan Outbound SMTP email	Check this option to scan outgoing emails.

4. If Information Store Protection is enabled, you have the option to scan internal emails and the Information Store Items. Check **Scan Internal and Information Store Items**. For more information, refer to [Information Store Protection](#) (page 91).

NOTE

On this page you can also review the antivirus engine licensing and version information.



Screenshot 56: Virus scanning engine actions

5. From the **Actions** tab, choose the action to be taken when an email is blocked:

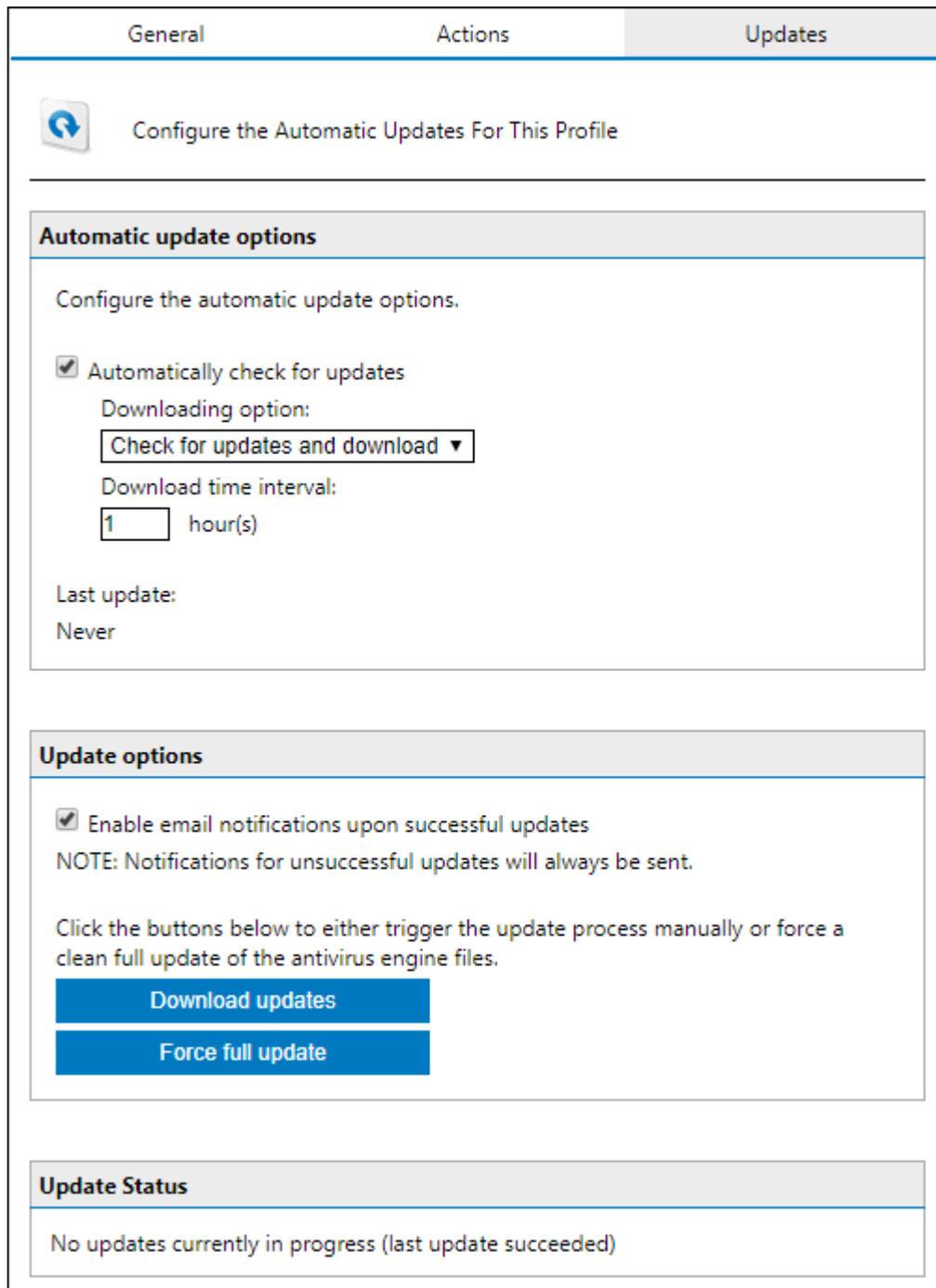
Action	Description
Quarantine item	Stores all infected emails detected by the selected Virus Scanning Engine in the Quarantine Store. You can subsequently review (approve or delete) all the quarantined emails. For more information, refer to Quarantine (page 191).
Delete item	Deletes infected emails.
Send a sanitized copy of the original email to recipient(s)	When this option is enabled, GFI MailEssentials removes malicious content from emails and attaches a text file indicating that the email contained malicious content. The email is then forwarded to its intended recipients.

6. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

7. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log



Screenshot 57: Engine Updates tab

8. In the **Updates** tab, check **Automatically check for updates** to enable automatic updating for the selected engine.

9. From the **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option does NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

10. Specify how often you want GFI MailEssentials to check and download updates for this engine, by specifying an interval value in hours.

11. From **Update options** area, check **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

NOTE

An email notification is always sent when an update fails.

12. To force the most recent updates you have two options:

Option	Description
Download updates	Trigger the update process manually. It is an incremental update where only the most recent definitions are updated.
Force full updates	This option forces a new version of the engine to be downloaded and replaced. This option is slower and consumes more bandwidth.

13. Click **Apply**.

4.2 Information Store Protection

Use the Virus Scanning Engines to scan the Microsoft® Exchange mailbox databases and public folders for viruses.

GFI MailEssentials can scan the Microsoft Exchange Information Store using two different protocols:

Protocol	Exchange versions	Description
Exchange Web Services (EWS)	<ul style="list-style-type: none"> » 2016 » 2013 » 2010 	<p>Information Store protection via Exchange Web Services retrieves email attachments from the Information Store via a predefined schedule. Attachments are then scanned by the Virus Scanning Engines and if malware is found, the attachment is removed from the email in the mailbox. GFI MailEssentials does not have to be installed on the Microsoft Exchange server to use EWS.</p> <p>NOTES:</p> <ul style="list-style-type: none"> » EWS may impact system performance so it is recommended to schedule scanning during off-peak hours. » A user account with access to all mailboxes is required to use EWS. For more information, refer to Set a Microsoft® Exchange account (page 260). » Unlike VSAPI, email attachments are scanned after these are stored in the mailbox so malicious attachments are not filtered from the Information Store until scan starts.

Protocol	Exchange versions	Description
Virus Scan API (VSAPI)	» 2010	VSAPI scans emails before these are stored in the Information Store, ensuring that malware is filtered out immediately before reaching the Information Store. VSAPI requires that GFI MailEssentials is installed on the Microsoft Exchange server. On a Microsoft® Exchange Server 2010 machine, the Mailbox Server Role and Hub Transport Server Role are required. NOTE: GFI MailEssentials cannot scan the Information Store if any other software is registered to use the Microsoft® Exchange VSAPI.

NOTE

Information Store Protection is only available when GFI MailEssentials is installed in Active Directory or Remote Active Directory modes. It is not available in SMTP mode or GFI Directory mode.

To enable Information Store Scanning and configure the scanning protocol:

1. Go to **Email Security > Information Store Protection**.



Screenshot 58: Information Store Protection node when both EWS & VSAPI are available

2. From **Information Store Virus Scanning** tab, select **Enable Information Store Virus Scanning**.
3. When GFI MailEssentials is installed on Microsoft Exchange 2010 with Mailbox Server and Hub Transport Server Roles, choose the protocol to use for scanning the Information Store - **VSAPI** or **Exchange Web Services**.
4. In the other tabs, configure the protocol options. Refer to [VSAPI Settings](#) or [Exchange Web Services \(EWS\) Settings](#)
5. Click **Apply**.

The status of the Virus Scanning Engines used to scan the Information Store is displayed in the table.

To disable a particular antivirus engine from Information Store Scanning, navigate to the Virus Scanning Engines page, select the antivirus engine and disable **Scan Internal and Information Store Items**.

4.2.1 Exchange Web Services (EWS) Settings

1. Go to the **EWS Settings** tab.
2. Configure the settings used to connect to Microsoft Exchange. EWS uses the Exchange account configured in the Switchboard to connect to the Information Store. For more information, refer to [Set a Microsoft® Exchange account](#) (page 260).

Option	Description
Microsoft Exchange Server URL	Choose Auto-Discovery to allow GFI MailEssentials to automatically find your Microsoft Exchange server. If Exchange is not discoverable, choose Manual to key in the Exchange Web Services (EWS) URL manually. The URL is usually composed in the following syntax: <code>https://<Exchange Hostname>/EWS/Exchange.asmx</code> NOTE: The Exchange Web Services (EWS) URL can also be retrieved by running this command in Exchange Management Shell: <code>Get-WebServicesVirtualDirectory Select name, *url* fl</code>
Test	Click to ensure that GFI MailEssentials can connect to the Microsoft Exchange Information Store using the provided details.
Scan Public Folders	Select to also scan items in Public Folders.
Simultaneous mailbox scans	Define the number of mailboxes to scan at the same time. The default number of simultaneous mailboxes is 1. Defining a higher number uses more system resources for scanning, but more items can get scanned in a shorter time.

3. In the **Scanning Schedule** area, define a schedule when to run Information Store Scanning. When the schedule is on, GFI MailEssentials goes through items that were not scanned in each mailbox. On scanning all new items in a mailbox, it starts scanning the next mailbox. When all mailboxes are scanned, it restarts scanning new items in the first mailbox again and repeats the process until the schedule is turned off. Choose the type of schedule to run:

- **Continuous scanning** - Run Information Store Protection via EWS without pause.
- **Timed interval** - Run scans in a defined schedule. Choose **Daily** to run scan everyday or **On the following day(s)** to run scan on selected days only. Define the time when to run the scan and the duration of the scan in hours.

NOTE

Scanning via EWS can be time consuming and uses considerable system resources, so it is recommended to run scans during off-peak hours only.

4. In the **Excluded Mailboxes** area, add any mailboxes which you do not want the Information Store Protection to scan.
5. Click **Apply**.

4.2.2 VSAPI Settings

1. Go to the **VSAPI Settings** tab.
2. (Optional) Select **Enable background scanning** to run Information Store Scanning in the background.

WARNING

Background scanning causes all the contents of the Information Store to be scanned. This can result in a high processing load on the Microsoft® Exchange server depending on the amount of items stored in the Information Store. It is recommended to enable this option only during periods of low server activity such as during the night.

3. Select a VSAPI scan method:

Scan Method	Description
On-access scanning	New items in the Information Store are scanned as soon as they are accessed by the email client. This introduces a short delay before the email client displays the contents of a new message.
Pro-active scanning	New items added to the Information Store are added to a queue for scanning. This is the default and recommended mode of operation, since in general the delay associated with on-access scanning is avoided.

NOTE
If an email client tries to access an item that is still in the queue, it allocates a higher scanning priority so that it is scanned immediately.

4. Click **Apply**.

4.3 Trojan and Executable Scanner

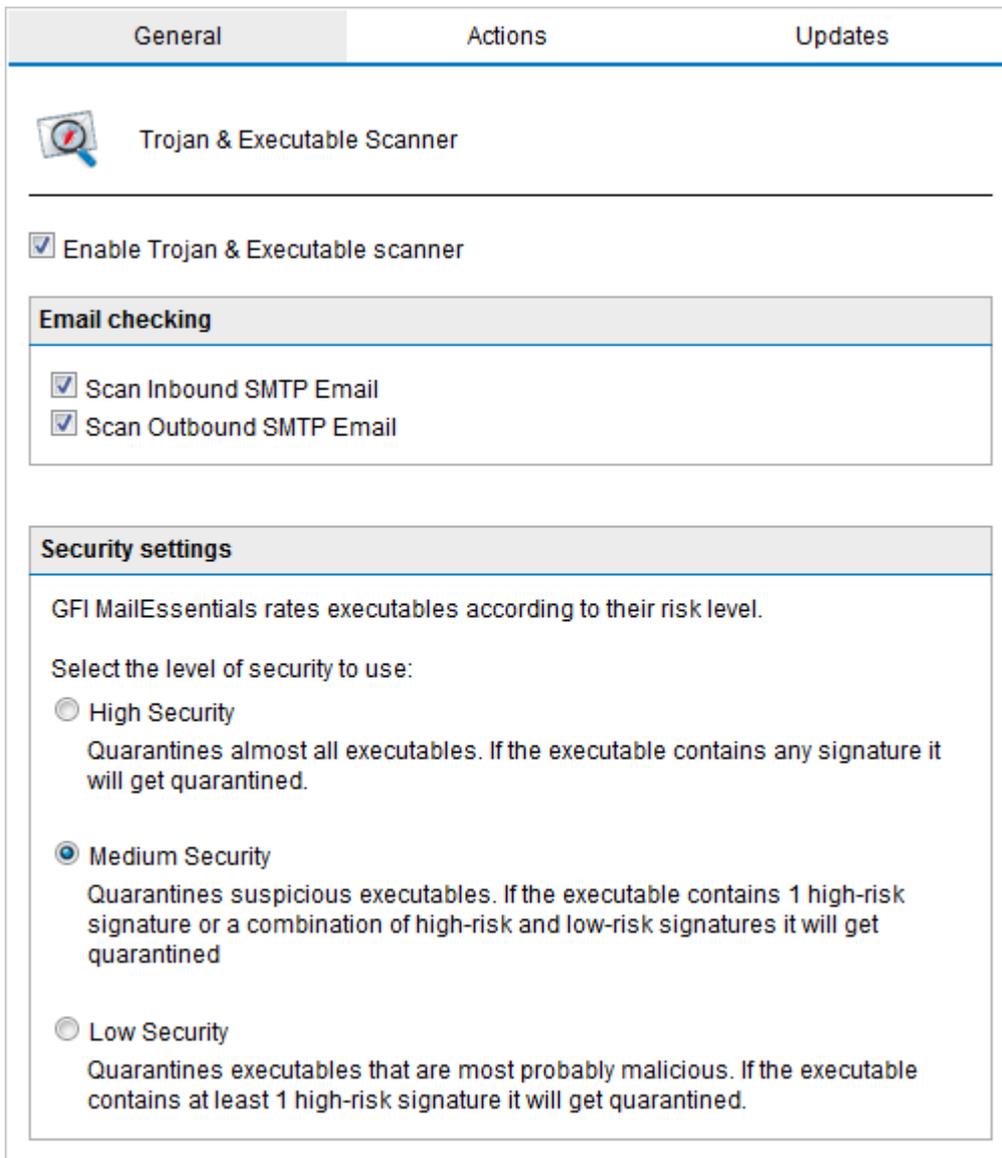
The Trojan and Executable Scanner analyzes and determines the function of executable files attached to emails. This scanner can subsequently quarantine any executables that perform suspicious activities (such as Trojans).

How does the Trojan & Executable Scanner work?

GFI MailEssentials rates the risk-level of an executable file by decompiling the executable, and detecting in real-time what the executable might do. Subsequently, it compares capabilities of the executable to a database of malicious actions and rates the risk level of the file. With the Trojan & Executable scanner, you can detect and block potentially dangerous, unknown or one-off Trojans before they compromise your network.

4.3.1 Configuring the Trojan & Executable Scanner

1. Go to **Email Security > Trojan & Executable Scanner**.



Screenshot 59: Trojan and Executable Scanner: General Tab

2. Select **Enable Trojan & Executable Scanner** to activate this filter.
3. In **Email checking** area, specify the emails to check for Trojans and other malicious executables by selecting:

Option	Description
Scan Inbound SMTP Email	Scan incoming emails for Trojans and malicious executable files.
Scan Outbound SMTP Email	Scan outgoing emails for Trojans and malicious executable files.

4. From the **Security settings** area, choose the required level of security:

Security Level	Description
High Security	Blocks all executables that contain any known malicious signatures
Medium Security	Blocks suspicious executables. Emails are blocked if an executable contains one high-risk signature or a combination of high-risk and low-risk signatures.

Security Level	Description
Low Security	Blocks only malicious executables. Emails are blocked if an executable contains at least one high-risk signature.

5. From **Actions** tab, configure the actions you want GFI MailEssentials to take on emails containing a malicious executable.

NOTE

Emails blocked by the Trojan & Executable Scanner are always quarantined.

6. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

7. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation
path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

General
Actions
Updates

Configure the Automatic Updates For This Profile

Automatic update options

Configure the automatic update options.

Automatically check for updates

 Downloading option:

 Download time interval:
 hour(s)

Last update:
 Never

Update options

Enable email notifications upon successful updates

NOTE: Notifications for unsuccessful updates will always be sent.

Click the buttons below to either trigger the update process manually or force a clean full update of the antivirus engine files.

Update Status

No updates currently in progress (last update succeeded)

Screenshot 60: Engine Updates tab

8. In the **Updates** tab, check **Automatically check for updates** to enable automatic updating for the selected engine.
9. From the **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option does NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

10. Specify how often you want GFI MailEssentials to check and download updates for this engine, by specifying an interval value in hours.

11. From **Update options** area, check **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

NOTE

An email notification is always sent when an update fails.

12. To force the most recent updates you have two options:

Option	Description
Download updates	Trigger the update process manually. It is an incremental update where only the most recent definitions are updated.
Force full updates	This option forces a new version of the engine to be downloaded and replaced. This option is slower and consumes more bandwidth.

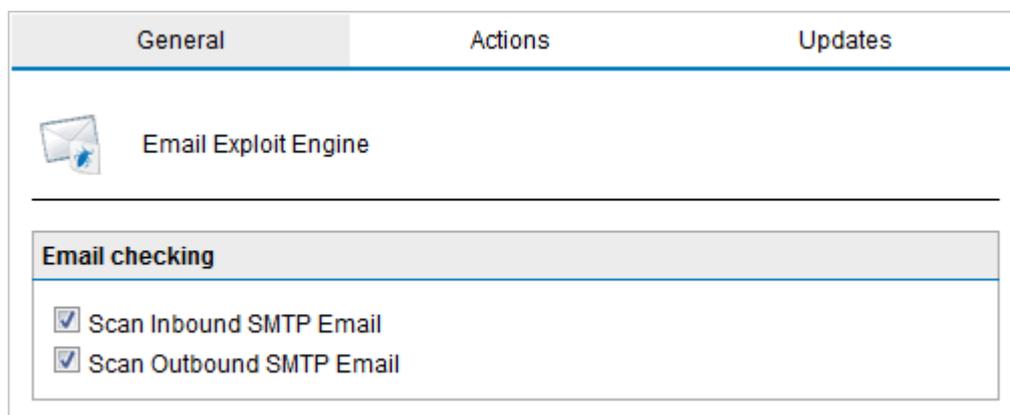
13. Click **Apply**.

4.4 Email Exploit Engine

The Email Exploit Engine blocks exploits embedded in an email that can execute on the recipient's machine either when the user receives or opens the email. An exploit uses known vulnerabilities in applications or operating systems to compromise the security of a system. For example, execute a program or command, or install a backdoor.

4.4.1 Configuring the Email Exploit Engine

1. Go to **Email Security > Email Exploit Engine**.



Screenshot 61: Email Exploit configuration

2. From the **General** tab, select whether to scan inbound and/or outbound emails.

Option	Description
Scan inbound SMTP emails	Select this option to scan incoming emails
Scan outbound SMTP emails	Select this option to scan outgoing emails

General	Actions	Updates
 Email Exploit Actions		
Actions		
Select the actions to perform when an exploit is detected.		
<input checked="" type="radio"/> Quarantine email <input type="radio"/> Delete email		
Notification options		
<input checked="" type="checkbox"/> Notify administrator <input type="checkbox"/> Notify local user		
Logging options		
<input checked="" type="checkbox"/> Log occurrence to this file: <input type="text" value="C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\logs\EmailExploit.log"/>		

Screenshot 62: Email Exploit Actions

3. From **Actions** tab, choose the action to take when an email is blocked:

Action	Description
Quarantine email	Stores all infected emails detected by the Email Exploit Engine in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Working with Quarantined emails (page 198).
Delete email	Deletes infected emails.

4. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

5. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

General Actions **Updates**

 Configure the Automatic Updates For This Profile

Automatic update options

Configure the automatic update options.

Automatically check for updates

Downloading option:

Download time interval:
 hour(s)

Last update:
 Never

Update options

Enable email notifications upon successful updates
 NOTE: Notifications for unsuccessful updates will always be sent.

Click the buttons below to either trigger the update process manually or force a clean full update of the antivirus engine files.

[Download updates](#)

[Force full update](#)

Update Status

No updates currently in progress (last update succeeded)

Screenshot 63: Engine Updates tab

- In the **Updates** tab, check **Automatically check for updates** to enable automatic updating for the selected engine.
- From the **Downloading option** list, select one of the following options:

Option	Description
Only check for updates	Select this option if you want GFI MailEssentials to just check for and notify the administrator when updates are available for this engine. This option does NOT download the available updates automatically.
Check for updates and download	Select this option if you want GFI MailEssentials to check for and automatically download any updates available for this engine.

- Specify how often you want GFI MailEssentials to check and download updates for this engine, by specifying an interval value in hours.
- From **Update options** area, check **Enable email notifications upon successful updates** to send an email notification to the administrator whenever the engine updates successfully.

NOTE

An email notification is always sent when an update fails.

- To force the most recent updates you have two options:

Option	Description
Download updates	Trigger the update process manually. It is an incremental update where only the most recent definitions are updated.
Force full updates	This option forces a new version of the engine to be downloaded and replaced. This option is slower and consumes more bandwidth.

- Click **Apply**.

4.4.2 Enabling/Disabling Email Exploits

- Go to **Email Security > Email Exploit Engine > Exploit List**

Email Exploit

Email Exploit Engine

Enable Selected Disable Selected

<input type="checkbox"/>	ID		Description	Status
<input type="checkbox"/>	1		CLS-ID File Extension (High alert)	Enabled
<input type="checkbox"/>	2		Iframe within an HTML email (Suspicious)	Enabled
<input type="checkbox"/>	3		Malformed File Extension (High alert)	Enabled
<input type="checkbox"/>	4		Java ActiveX Component Exploit (High alert)	Enabled
<input type="checkbox"/>	5		Mime header vulnerability (High alert)	Enabled
<input type="checkbox"/>	6		ASX buffer-overflow (High alert)	Enabled
<input type="checkbox"/>	7		Document.Open method Exploits (Possible intrusion attempt)	Enabled
<input type="checkbox"/>	8		Popup Object exploit (High alert)	Enabled
<input type="checkbox"/>	9		Object CODEBASE file execution (High alert)	Enabled
<input type="checkbox"/>	10		Local file reading/execution (Suspicious)	Enabled
<input type="checkbox"/>	11		Java security vulnerability (High alert)	Enabled
<input type="checkbox"/>	12		MSScriptControl.ScriptControl ActiveX scripting (High alert)	Enabled
<input type="checkbox"/>	13		Office XP ActiveX control exploit (Suspicious)	Enabled

Screenshot 64: Email Exploit List

2. Select the check box of the exploit(s) to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly.

4.5 HTML Sanitizer

The HTML Sanitizer scans and removes scripting code within the email body and attachments. It scans:

- » the email body of emails that have the MIME type set to “text/html”
- » all attachments of type **.htm** or **.html**.

4.5.1 Configuring the HTML Sanitizer

1. Go to **Email Security > HTML Sanitizer**.

HTML Sanitizer	Whitelist	Domain/IP Exclusions
 Configure HTML Sanitizer		
<p>This filter removes all scripting code from the HTML of emails and attachments (*.htm/*.html only). Content, layout and formatting are not altered. Emails are guaranteed to be received free of HTML Scripting code and are therefore safe for viewing.</p>		
<input checked="" type="checkbox"/> Enable the HTML Sanitizer		
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Email checking</p> <p>Select the emails you want the HTML Sanitizer to scan and clean:</p> <input checked="" type="checkbox"/> Scan Inbound SMTP Email <input checked="" type="checkbox"/> Scan Outbound SMTP Email </div>		

Screenshot 65: HTML Sanitizer configuration page

2. Enable the HTML Sanitizer by selecting **Enable the HTML Sanitizer** checkbox .
3. Select direction of emails:

Option	Description
Scan inbound SMTP emails	Scan and sanitize HTML scripts from all incoming emails.
Scan outbound SMTP emails	Scan and sanitize HTML scripts from all outgoing emails.

4. Click **Apply**.

4.5.2 HTML Sanitizer Whitelist

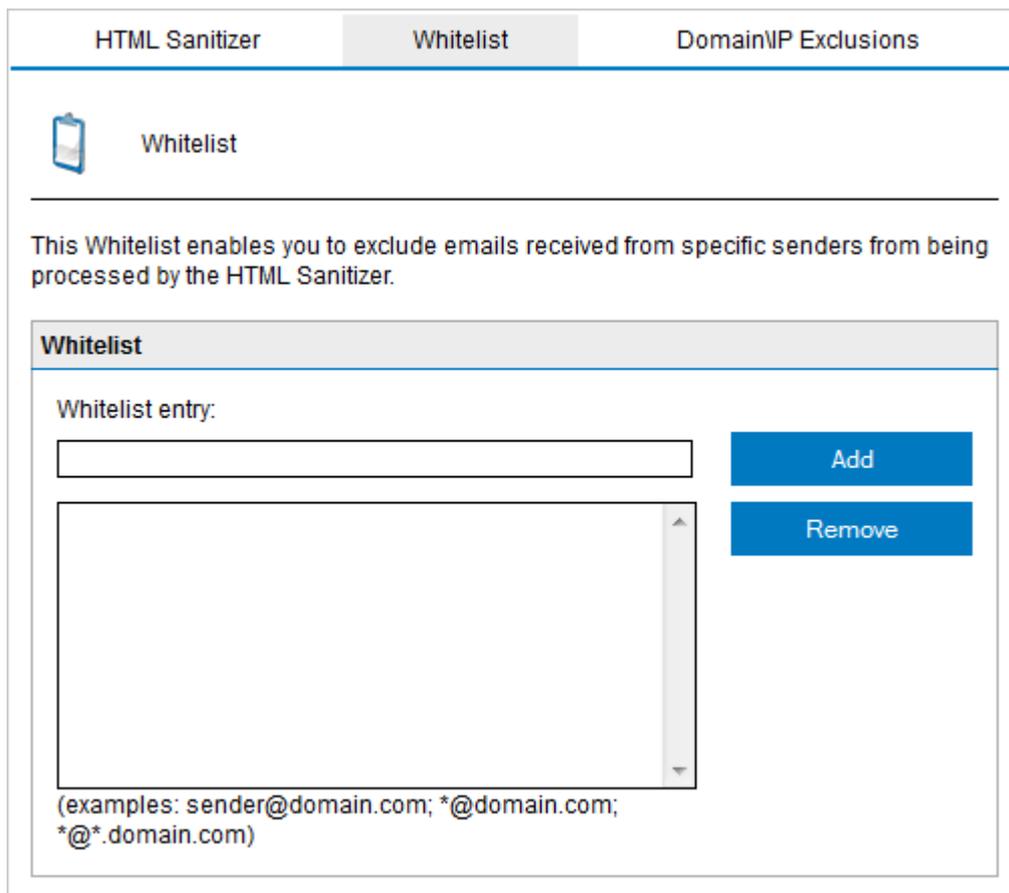
The HTML Sanitizer Whitelist can be configured to exclude emails received from specific senders.

NOTE

To exclude specific IP Addresses or domains, use the HTML Sanitizer Domain\IP Exclusions feature. For more information, refer to [HTML Santizer Domain\IP Exclusions](#) (page 104).

To manage senders in the HTML Sanitizer Whitelist:

1. Navigate to **Email Security > HTML Sanitizer** and select **Whitelist** tab.



Screenshot 66: HTML Sanitizer Whitelist page

2. In **Whitelist entry**, key in an email address, an email domain (for example, *@domain.com) or an email sub-domain (for example, *@*.domain.com) and click **Add**.

NOTE

To remove an entry from the HTML Sanitizer whitelist, select an entry and click **Remove**.

3. Click **Apply**.

4.5.3 HTML Santizer Domain\IP Exclusions

The HTML Santizer Domain\IP Exclusions feature enables administrators to specify IP addresses or domains to exclude from HTML Sanitizer. This will not simply use an IP address list; it can also support domain addresses, which are then resolved at runtime, so that all the IP addresses for the domain in question are obtained. This is done in two ways:

1. By default, the feature queries the MX records of the domain being processed
2. Optionally, you can choose to have the SPF record of the domain queried. If the domain doesn't have an SPF record, the SPF part is ignored and only the MX records are used.

If the IP address from where the email originated (the one which sent to the perimeter server) is an IP listed in the Domains\IPs exclusions tab or resolved from a domain in the same list, then the email is not processed by HTML Sanitizer. The exclusion list also accepts domains, resolves the domains' MX records and (optionally) checks the SPF record to get IP addresses.

To manage domains\IP exclusions in the HTML Sanitizer Whitelist:

1. Navigate to **Email Security > HTML Sanitizer** and select **Domains\IP exclusions** tab.

HTML Sanitizer Whitelist **Domain/IP Exclusions**

 Domain/IP Exclusions

The domain exclusions provide the ability to exclude HTML Sanitizing processing for MX records of a domain by specifying the domain name. Server ip addresses can also be specified.

Exclusions

Exclusion entry:

(Examples: domain.com, 192.168.1.1)

Query the SPF records of the specified domains for the list of the servers to exclude

Screenshot 67: Domain/IP Exclusions

2. Key in the domain or IP address to exclude and click **Add**.

NOTE

To remove an entry from the HTML Sanitizer Domain/IP Exclusions, select an entry and click **Remove**.

3. Optionally, select **Query the SPF records of the specified domains for the list of the servers to exclude**.

4. Click **Apply**.

5 Anti-Spam

The anti-spam filters included with GFI MailEssentials help detect and block unwanted emails (spam).

Topics in this chapter:

5.1 Anti-Spam filters	106
5.2 Spam Actions - What to do with spam emails	145
5.3 Sorting anti-spam filters by priority	147
5.4 SMTP Transmission Filtering	148
5.5 Spam Digest	150
5.6 Anti-Spam settings	152
5.7 SpamTag for Microsoft Outlook	158
5.8 Public Folder Scanning	164

5.1 Anti-Spam filters

GFI MailEssentials uses various scanning filters to identify spam:

Filter	Description	Enabled by Default
SpamRazer	An anti-spam engine that determines if an email is spam by using email reputation, message fingerprinting and content analysis.	Yes
Anti-Phishing	Blocks emails that contain links in the message body pointing to known phishing sites or if they contain typical phishing keywords.	Yes
Director Harvesting	Directory harvesting attacks occur when spammers try to guess email addresses by attaching well known usernames to your domain. The majority of the email addresses are non-existent.	Yes (only if GFI MailEssentials is installed in an Active Directory environment)
Email Blocklist	The Email Blocklist is a custom database of email addresses and domains from which you never want to receive emails.	Yes
IP Blocklist	The IP Blocklist is a custom database of IP addresses from which you never want to receive emails.	No
IP DNS Blocklist	IP DNS Blocklist checks the IP address of the sending mail server against a public list of mail servers known to send spam.	Yes
URI DNS Blocklist	Stops emails that contain links to domains listed on public Spam URI Blocklists.	Yes
Sender Policy Framework	This filter uses SPF records to stop email sent from forged IP addresses by identifying if the sender IP address is authorized.	No
Anti-Spoofing	Checks emails received with a sender email address claiming to originate from your own domain against a list of IP addresses by GFI MailEssentials. If the sender IP address is not on the list of own-domain server IP addresses, email is blocked.	No

Filter	Description	Enabled by Default
Greylist	The Greylist filter temporarily blocks incoming emails received from unknown senders. Legitimate mail systems typically try to send the email after a few minutes; spammers simply ignore such error messages.	No
Language Detection	Determines the language of the email body text and configurable to block certain languages.	No
Header Checking	The Header Checking filter analyses the email header to identify spam emails.	No
Spam Keyword Checking	This filter enables the identification of Spam based on keywords in the email being received.	No
Bayesian analysis	An anti-spam filter that can be trained to accurately determine if an email is spam based on past experience.	No
Whitelist	The Whitelist contains lists of criteria that identify legitimate email. Emails that match these criteria are not scanned by anti-spam filters and are always delivered to the recipient.	Yes
New Senders	The New Senders filter identifies emails that have been received from senders to whom emails have never been sent before.	No

5.1.1 SpamRazer

An anti-spam engine that determines if an email is spam by using email reputation, message fingerprinting and content analysis. SpamRazer is the primary anti-spam engine and is enabled by default on installation. Frequent updates are released for SpamRazer that will further decrease the response time to new trends of spam.

SpamRazer also includes Sender Policy Framework filtering which detects forged senders. It is recommended that senders publish their mail server in an SPF record. For more information on SPF and how it works, visit the Sender Policy Framework website at: <http://www.openspf.org>.

This filter also blocks NDR spam. For more information on NDR spam refer to http://go.gfi.com/?pageid=ME_NDRSpam

Configuring SpamRazer

NOTES

1. Disabling SpamRazer is **NOT** recommended.
2. GFI MailEssentials downloads SpamRazer updates from: ***.mailshell.net**

1. Go to **Anti-Spam > Anti-Spam Filters > SpamRazer**.

General
Updates
Actions

SpamRazer Configuration

SpamRazer is an anti-spam engine that determines if an email is spam through the use of email fingerprints, email reputation and content analysis.

Options

- Enable SpamRazer engine**
 Information about blocking descriptions returned by SpamRazer can be obtained from the following KB article:
<http://www.gfi.com/link/entry.aspx?page=skynet&id=KBID001896>
- Enable SpamRazer SPF (Recommended)**
 Enables SpamRazer to perform a Sender Policy Framework check as part of its checks. For more information, refer to:
http://go.gfi.com/?pageid=ME_SPFfilter

Licensing

SpamRazer Licensing Status: Evaluation license

Screenshot 68: SpamRazer Properties

2. From the **General** tab perform any of the following actions:

Option	Description
Enable SpamRazer engine	Enable or disable SpamRazer.
Enable SpamRazer SPF (Recommended)	Enable or disable Sender Policy Framework. It is recommended to enable this option and to have this filter running after the Email Whitelist.

General	Updates	Actions
 Automatic SpamRazer Updates		
Automatic update options		
Configure the automatic update options.		
<input checked="" type="checkbox"/> Automatically check for updates Update interval for spam detection rules: <input type="text" value="30"/> minutes (min: 5min, max: 30min)		
Update interval for SpamRazer engine: <input type="text" value="24"/> hours (min: 1hr, max: 24hr)		
Update options		
<input type="checkbox"/> Enable email notifications upon successful updates		
<input checked="" type="checkbox"/> Enable email notifications upon failed updates		
Last attempt: 02/09/2013 15:30:02 Last attempt result: Successful Current Version: 2013.09.02.10.47.45		
Click the button below to force the updater service to download the most recent updates.		
<input type="button" value="Download updates now..."/>		

Screenshot 69: SpamRazer Updates tab

3. From the **Updates** tab, perform any of the following actions:

Option	Description
Automatically check for updates	Configure GFI MailEssentials to automatically check for and download any SpamRazer updates. Specify the time interval in minutes when to check for spam detection rule and SpamRazer engine updates. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p>NOTE</p> <p>It is recommended to enable this option for SpamRazer to be more effective in detecting the latest spam trends.</p> </div>
Enable email notifications upon successful updates	Select this option to be informed via email when new updates are downloaded.

Option	Description
Enable email notifications upon failed updates	Select this option to be informed via email when a download or installation fails.
Download updates now...	Click to download updates.

NOTE

You can download updates using a proxy server. For more information, refer to [Proxy settings](#) (page 227).

- Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).
- Click **Apply**.

5.1.2 Anti-Phishing

Blocks emails that contain links in the message body pointing to known phishing sites or if they contain typical phishing keywords. Phishing is an email based social engineering technique aimed at having email users disclose personal details to spammers. A phishing email is most likely crafted to resemble an official email originating from a reputable business, for example a bank. Phishing emails will usually contain instructions requiring users to reconfirm sensitive information such as online banking details or credit card information. Phishing emails usually include a phishing Uniform Resource Identifier (URI) that the user is supposed to follow to key in some sensitive information on a phishing site. The site pointed to by the phishing URI might be a replica of an official site, but in reality it is controlled by whoever sent the phishing emails. When the user enters the sensitive information on the phishing site, the data is collected and used, for example, to withdraw money from bank accounts.

The Anti-Phishing filter detects phishing emails by comparing URIs present in the email to a database of URIs known to be used in phishing attacks. Phishing also looks for typical phishing keywords in the URIs.

The Anti-Phishing filter is enabled by default on installation.

Configuring Anti-Phishing

NOTE

Disabling Anti-Phishing is **NOT** recommended.

- Go to **Anti-Spam > Anti-Spam Filters > Anti-Phishing**.
- From the **General** tab, select/unselect **Check mail messages for URIs to known phishing sites** option to enable/disable Anti-Phishing.

General
Keywords
Updates
Actions

Phishing URI Realtime Blocklist (PURBL) Configuration

Check URI's in mail messages for typical phishing keywords

Keywords

Edit keywords:

Keyword list

Current keywords:

paypal
 ebay
 lloydsts
 barclays
 citifi
 citibank

Specify file from which to import keywords:

Screenshot 70: Anti-Phishing options

3. From the **Keywords** tab select any of the following options:

Option	Description
Check URI's in mail messages for typical phishing keywords	Enable/disable checks for typical phishing keywords
Add	Add keywords that trigger the Anti-Phishing filter. Key in a keyword and click Add to add a keyword to the Anti-Phishing filter
Update	Updates selected keywords. Select a keyword from the Current Keywords list, make any changes to keyword in Edit Keywords field and click Update .
Remove	Removes selected keywords from list. Select a keyword from the Current Keywords list, and click Remove .
Export	Exports current list to an XML format file.
Browse...	Enables importing of a previously exported keyword list. Click Browse , select a previously exported keyword file and click Import .

4. From the **Updates** tab, select any of the following options:

Option	Description
Automatically check for updates	Configure GFI MailEssentials to automatically check for and download any Anti-Phishing updates. Specify the time interval in minutes when to check for updates. NOTE It is recommended to enable this option for Anti-Phishing to be more effective in detecting the latest phishing trends.
Enable email notifications upon successful updates	Select/unselect checkbox to be informed via email when new updates are downloaded.
Enable email notifications upon failed updates	Select/unselect to be informed when a download or installation fails.
Download updates now...	Click to immediately download Anti-Phishing updates.

NOTE

You can download updates using a proxy server. For more information, refer to [Proxy settings](#) (page 227).

- Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).
- Click **Apply**.

5.1.3 Directory Harvesting

Directory harvesting attacks occur when spammers try to guess email addresses by attaching well known usernames to your domain. The majority of the email addresses are non-existent. Spammers send emails to randomly generated email addresses and while some email addresses may match real users, the majority of these messages are invalid and consequently floods the victim's email server.

GFI MailEssentials stops these attacks by blocking emails addressed to users not in the organizations' Active Directory or email server.

Directory harvesting can either be configured to execute when the full email is received or at SMTP level, that is, emails are filtered while they are being received. SMTP level filtering terminates the email's connection and therefore stops the download of the full email, economizing on bandwidth and processing resources. In this case the connection is terminated immediately and emails are not required to go through any other anti-spam filters.

This filter is enabled by default on installing GFI MailEssentials in an Active Directory Environment.

Directory Harvesting is set up in two stages as follows

[Stage 1 - Configuring Directory Harvesting properties](#)

[Stage 2 - Selecting if Directory Harvesting should be done during the SMTP transmission.](#)

Stage 1 - Configuring Directory Harvesting properties

- Go to **Anti-Spam > Anti-Spam Filters > Directory Harvesting**.

General
Actions



This plug-in checks if the SMTP recipients of incoming mail are real users or the result of a directory harvesting attack

Enable directory harvesting protection

Lookup options

Use native Active Directory lookups
 Use LDAP lookups

LDAP Settings

Server:

Port: Use SSL

Version: ▼

Base DN: ▼

Anonymous bind Update DN list

User:

Password:

* For security reasons, the length in the password box above does not necessarily reflect the true password length

Block if non-existent recipients equal or exceed:

Email address test

Email address:

Test

Screenshot 71: Directory Harvesting page

2. Enable/Disable Directory Harvesting and select the lookup method to use:

Option	Description
Enable directory harvesting protection	Enable/Disable Directory Harvesting.
Use native Active Directory lookups	Select option to retrieve the list of local users from Active Directory (or from a Remote AD if GFI MailEssentials is installed in Remote Active Directory mode).

Option	Description
Use LDAP lookups	Select this option when GFI MailEssentials is installed in SMTP mode and you want to retrieve the list of users from a separate Active Directory instance using LDAP. Key in your Active Directory server details. If your LDAP server requires authentication, unmark the Anonymous bind option and enter the authentication details that will be used by this feature.
	<p>NOTE</p> <p>Specify authentication credentials using Domain\User format (for example master-domain\administrator).</p>

3. In **Block if non-existent recipients equal or exceed**, specify the number of nonexistent recipients that will qualify the email as spam. Emails will be blocked by Directory Harvesting if all the recipients of an email are invalid, or if the number of invalid recipients in an email equals or exceeds the limit specified.

NOTE

Avoid false positives by configuring a reasonable amount in the **Block if non-existent recipients equal or exceed** edit box. This value should account for users who send legitimate emails with mistyped email addresses or to users no longer employed with the company. It is recommended that this value is at least **2**.

4. Provide an email address and click **Test** to verify Directory Harvesting settings. Repeat the test using a non-existent email address and ensure that Active Directory lookup fails.

5. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

NOTE

If Directory Harvesting is set to run at SMTP level, only the **Log rule occurrence to this file** option will be available in the **Actions** tab.

6. Click **Apply**.

Stage 2 - Selecting if Directory Harvesting should be done during the SMTP transmission.

1. Navigate to **Anti-spam > Filter Priority**, and select **SMTP Transmission Filtering** tab.

2. Click **Switch** to toggle the Directory Harvesting filtering between:

Option	Description
Filtering on receiving full email	Filtering is done when the whole email is received.
Filtering during SMTP transmission	Filtering is done during SMTP transmission by checking if the email recipients exist before the email body and attachment are received.
	<p>NOTE</p> <p>If this option is chosen, Directory Harvesting will always run before the other spam filters.</p>

3. Click **Apply**.

5.1.4 Email blocklist

The Email Blocklist is a custom database of email addresses and domains from which you never want to receive emails.

This filter is enabled by default on installing GFI MailEssentials.

Configuring Email Blocklist

1. Go to Anti-Spam > Anti-Spam Filters > Email Blocklist.

Blocklist Personal Blocklist Actions

 Specify which email addresses will be filtered for spam

Enable email blacklist

Blocklist Entry

Email Address/Domain:

Email Type:

Description:

Blocklist

Search

<input type="checkbox"/>	Email	Description
<input type="checkbox"/>	 *@list.adult-newsletter.com	
<input type="checkbox"/>	 *@sexymailer.com	

Specify the full path and filename of the file to use for importing:

Note: Import of list data cannot be performed unless the import list is on the server where GFI MailEssentials is installed.

Legend

Email MIME SMTP  Sender  Recipient

Screenshot 72: Email blacklist

2. From the **Blocklist** tab, configure the email addresses and domains to block.

Option	Description
Enable Email Blocklist	Select/Unselect to enable/disable email blocklist.
Add	<p>Add email addresses, email domains or an entire domain suffix to the blocklist.</p> <ol style="list-style-type: none"> 1. Key in an email address, domain (for example, *@spammer.com); or an entire domain suffix (for example *@*.tv) to add to the blocklist. 2. Specify the email type to match for the emails to be blocklisted. <p>NOTE For more information about the difference between SMTP and MIME refer to: http://go.gfi.com/?pageid=ME_DifferenceSMTPMIME</p> <ol style="list-style-type: none"> 3. (Optional) You can also add a description to the entry in the Description field. 4. Click Add.
Remove	Select a blocklist entry and click Remove to delete.
Import	<p>Import a list of blocklist entries from a file in XML format.</p> <p>NOTE A list of entries can be imported from a file in XML format in the same structure that GFI MailEssentials would export the list of entries.</p>
Export	Export the list of blocklist entries to a file in XML format.
Search	Key in an entry to search for. Matching entries are filtered in the list of blocklist entries.

3. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

4. Click **Apply**.

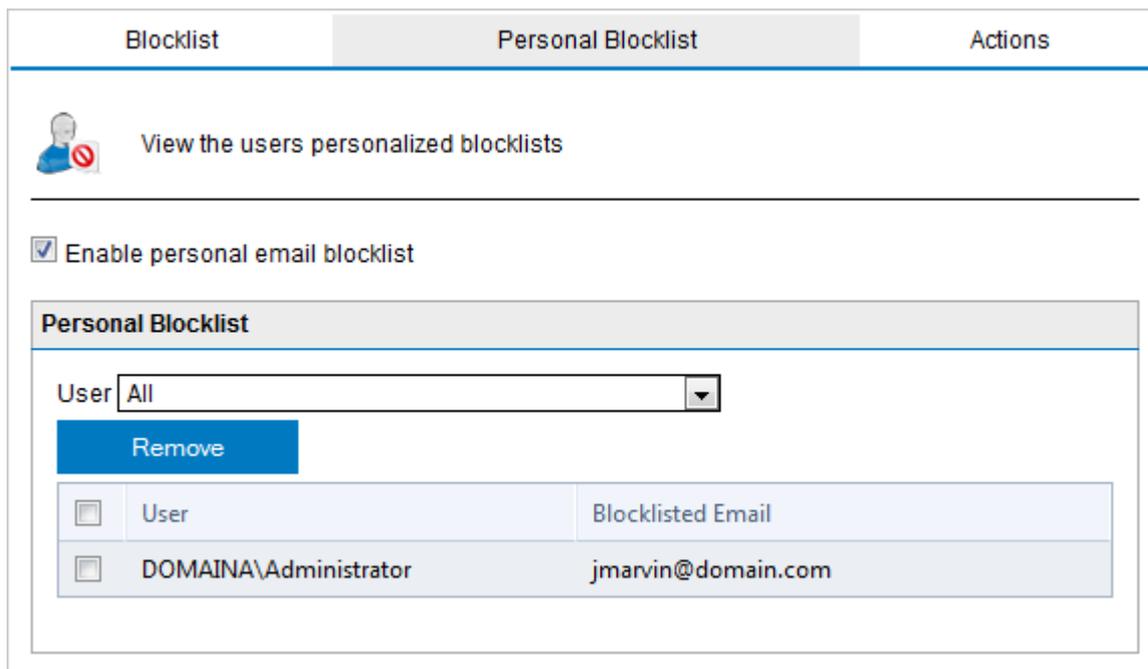
Personal Blocklist

The personal blocklist is an additional blocklist that compliments global blocklist. Disabled by default, the personal blocklist can be enabled for users to enable them to add specific email addresses to a personal blocklist that they can manage. For more information, refer to [End User Actions](#) (page 15).

For management purposes, administrators can also remove specific email addresses that the users have added to their personal blocklist.

Enabling/Disabling Personal Blocklist

1. Go to **Anti-Spam > Email Blocklist**.



Screenshot 73: Personal blacklist

2. Select **Personal Blocklist** tab and select or unselect **Enable personal email blacklist** to enable or disable personal blacklist feature.
3. Click **Apply**.

Removing emails from users' personal blacklist

1. Go to **Anti-Spam > Email Blocklist** and select **Personal Blocklist** tab.
2. From the **User** drop down list, select the user for whom to delete an email address.
3. Select an email address from the list of email addresses. Click **Remove**.
4. Click **Apply**.

5.1.5 IP Blocklist

The IP Blocklist is a custom database of IP addresses from which you never want to receive emails.

This filter can be configured to execute when the full email is received or at SMTP level, that is, emails are filtered while they are being received. SMTP level filtering terminates the email's connection and therefore stops the download of the full email, economizing on bandwidth and processing resources. In this case the connection is terminated immediately and emails are not required to go through any other anti-spam filters. For more information, refer to [SMTP Transmission Filtering](#) (page 148).

The IP Blocklist is NOT enabled by default.

Configuring Whitelist

1. Go to **Anti-Spam > Anti-Spam Filters > IP Blocklist**.

General	Actions								
 A custom database of IP addresses from which you never want to receive emails.									
<input checked="" type="checkbox"/> Enable IP Blocklist									
IP Blocklist Entry									
<input checked="" type="radio"/> Single computer/CIDR IP Address: <input type="text"/>									
<input type="radio"/> Group of computers Subnet Address: <input type="text"/>									
Subnet Mask <input type="text"/>									
Description <input type="text"/>									
<input type="button" value="Add"/>									
IP Blocklist									
<table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Address</th> <th>Mask</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td colspan="4">No records to display.</td> </tr> </tbody> </table>		<input type="checkbox"/>	Address	Mask	Description	No records to display.			
<input type="checkbox"/>	Address	Mask	Description						
No records to display.									
<input type="button" value="Remove"/>									
<p>If perimeter servers are configured, the verified IP address is the one sending to the perimeter. If no perimeters are configured, the verified IP address is the IP of the server sending to GFI MailEssentials.</p>									

Screenshot 74: IP Blocklist

- From the **General** tab, select **Enable IP Blocklist** to block all emails received from specific IP addresses.
- In the **IP Blocklist Entry** box, specify the IP addresses to block:

Option	Description
Single computer / CIDR	Key in a single IP address or a range of IP addresses using CIDR notation.
Group of computers	Specify the Subnet Address and Subnet Mask of the group of IPs to whitelist. 2. (Optional) Add a Description . 3 Click Add .
Description	Optionally, add a description to help identify the specified IPs.

- Click **Add** to add the specified IP addresses to the **IP Blocklist** box.
- To delete IP addresses from the IP Blocklist, select the addresses to remove and click **Remove**.

6. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

NOTE

If IP Blocklist is set to run at SMTP level, only the **Log rule occurrence to this file** option will be available in the **Actions** tab.

7. Click **Apply**.

5.1.6 IP DNS Blocklist

IP DNS Blocklist checks the IP address of the sending mail server against a public list of mail servers known to send spam. GFI MailEssentials supports a number of IP DNS Blocklists. There are a number of third party IP DNS Blocklists available, ranging from reliable lists that have clearly outlined procedures for getting on or off the IP DNS Blocklist to less reliable lists.

GFI MailEssentials maintains a cache with the results of queries to the IP DNS Blocklist to avoid querying the IP DNS Blocklists multiple times for the same IP addresses. Items remain in the cache for 4 days and are cleared on GFI MailEssentials AS Scan Engine service restart.

This filter can be configured to execute when the full email is received or at SMTP level, that is, emails are filtered while they are being received. SMTP level filtering terminates the email's connection and therefore stops the download of the full email, economizing on bandwidth and processing resources. In this case the connection is terminated immediately and emails are not required to go through any other anti-spam filters. For more information, refer to [SMTP Transmission Filtering](#) (page 148).

This filter is enabled by default on installing GFI MailEssentials.

Important notes

1. The DNS server must be properly configured for this feature to work. If this is not the case, time outs will occur and email traffic will be slowed down. For more information refer to: http://go.gfi.com/?pageid=ME_ProcessingSlow
2. Querying an IP DNS Blocklist can be slow (depending on your connection), so email can be slowed down a little bit.
3. Ensure that all perimeter SMTP servers are configured in the Perimeter SMTP servers dialog so that GFI MailEssentials can check the IP address that is connecting to the perimeter servers. For more information, refer to [Perimeter SMTP Server Settings](#) (page 224).

Configuring IP DNS Blocklist

1. Go to **Anti-Spam > Anti-Spam Filters > IP DNS Blocklist**.

General
Actions

IP DNS Blocklist Configuration

Check whether the sending mail server is on one of the following IP DNS Blocklist.

IP DNS

Domain:

IP DNS list

<input type="checkbox"/>	Name	Status	Priority		
<input type="checkbox"/>	bl.spamcop.net	Enabled	1	↑	↓
<input type="checkbox"/>	dul.dnsbl.sorbs.net	Disabled	2	↑	↓

Screenshot 75: IP DNS Blocklist

2. Configure the following options:

Option	Description
Check whether the sending mail server is on one of the following IP DNS Blocklists:	Select to enable the IP DNS Blocklist filter.
Add IP DNS Blocklist	If required, add more IP DNS Blocklists to the ones already listed. Key in the IP DNS Blocklist domain and click Add IP DNS Blocklist .
Enable Selected	Select an IP DNS Blocklist and click Enable Selected to enable it.
Disable Selected	Select an IP DNS Blocklist and click Disable Selected to disable it.
Remove Selected	Select an IP DNS Blocklist and click Remove Selected to remove it.

3. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

4. Click **Apply**.

NOTE

To enable IP DNS Blocklist at SMTP Transmission Filtering level, select **Anti-Spam > Filter Priority > SMTP Transmission Filtering** tab and click **Switch** next to IP DNS Blocklist to enable/disable filtering at SMTP level or on receipt of full email.

5.1.7 URI DNS Blocklist

Stops emails that contain links to domains listed on public Spam URI Blocklists.

A Universal Resource Identifier (URI) is a standard means of addressing resources on the Web. Realtime Blocklists (RBL) detect spam based on hyperlinks in the email known to be used by spammers. This filter is enabled by default on installing GFI MailEssentials.

Configuring URI DNS Blocklist

1. Go to **Anti-Spam > Anti-Spam Filters > URI DNS Blocklist**.

Screenshot 76: URI DNS Blocklist

2. From the **URI DNS Blocklist** tab:

Option	Description
Check if mail message contains URIs with domains that are in these blocklists:	Select this option to enable the URI DNS Blocklist filter.
Add URI DNS Blocklist	If required, add more URI DNS Blocklists to the ones already listed. Key in the full name of the URI DNS Blocklist domain and click Add URI DNS Blocklist .
Order of preference	The order of preference for enabled URI DNS Blocklists can be changed by selecting a blocklist and clicking on the Up or Down buttons.
Enable Selected	Select a URI DNS Blocklist and click Enable Selected to enable it.
	NOTE It is recommended to disable all other URI DNS Blocklists when enabling multi.surbl.org as this might increase email processing time.
Disable Selected	Select a URI DNS Blocklist and click Disable Selected to disable it.
Remove Selected	Select a URI DNS Blocklist and click Remove Selected to remove it.

3. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).
4. Click **Apply**.

5.1.8 Sender Policy Framework

This filter uses SPF records to stop email sent from forged IP addresses by identifying if the sender IP address is authorized. The Sender Policy Framework filter is based on a community-based effort, which requires that the senders publish the IP addresses of their mail servers in an SPF record.

Example: If an email is sent from xyz@CompanyABC.com then companyABC.com must publish an SPF record in order for SPF to be able to determine if the email was really sent from the companyABC.com network or whether it was forged. If an SPF record is not published by CompanyABC.com, the SPF result will be 'unknown'.

For more information on SPF and how it works, visit the Sender Policy Framework website at:

<http://www.openspf.org>

NOTE

GFI MailEssentials does not make it a requirement to publish an SPF record.

The SPF filter is NOT enabled by default and it is recommended to enable this option and to have this filter running prior to the Email Whitelist so to block forged senders before these are whitelisted.

Prerequisites

Before enabling the Sender Policy Framework filter on a non-gateway server installation:

1. Go to **General Settings > Perimeter SMTP Servers**.
2. Click **Detect** in the **SMTP Server list** area to perform a DNS MX lookup and automatically define the IP address of your perimeter SMTP server.

Enabling the Sender Policy Framework

1. Select **Anti-Spam > Anti-Spam Filters > Sender Policy Framework**.

General IP Exceptions Email Exceptions Actions

 The Sender Policy Framework (SPF) fights spam by detecting emails with forged senders.

Block Level

The Sender Policy Framework (SPF) filter identifies and blocks spam with forged senders. It is recommended to run the SPF filter before Whitelist. This can be configured in the Filter Priority node.

Disabled
 Enabled (Recommended)
 Blocks emails identified as having a forged sender if SPF check result is 'FAIL'. This denotes that the sender is definitely not authorized to use the sender domain.
 For more information, refer to: http://go.gfi.com/?pageid=ME_SPFfilter

Advanced

Advanced SPF filter settings enables blocking of other SPF check results (SOFT FAIL, Neutral, Unknown and NONE). Enabling advanced filtering is only recommended for advanced users since it may trigger false positives. For more information on SPF filters refer to: http://go.gfi.com/?pageid=ME_SPFfilter

Enable Advanced SPF filtering
 Block SOFT FAIL result
 Block SOFT FAIL, Neutral, Unknown and NONE results

Screenshot 77: Enable and configure the Sender Policy Framework

- Click **Enabled** to enable the Sender Policy Framework filter. If the email sender IP address is definitely not authorized to send emails from the sender domain, emails are blocked.
- Optionally, select **Enable Advanced SPF filtering** and select one of the advanced option from:

Option	Description
Block SOFT FAIL result	Blocks all emails which: <ul style="list-style-type: none"> » Sender IP address is definitely not allowed to send emails from the sender domain » Sender IP address is probably not allowed to send emails from the sender domain. For more information on Advanced SPF filtering, refer to: http://go.gfi.com/?pageid=ME_SPFfilter

Option	Description
Block SOFT FAIL, Neutral, Unknown and NONE results	<p>Blocks all emails which:</p> <ul style="list-style-type: none"> » Sender IP address is definitely not allowed to send emails from the sender domain » Sender IP address is probably not allowed to send emails from the sender domain. » Sender IP address is explicitly inconclusive, unknown or for which there is no published data. <p>For more information on Advanced SPF filtering, refer to: http://go.gfi.com/?pageid=ME_SPFfilter</p>

4. Select **IP Exceptions** or **Email Exceptions** tab to configure IP addresses and/or recipients to exclude from SPF checks:

» **IP exception list:** Entries in this list automatically pass SPF checks. Select **IP Exception List** checkbox, add a new IP address and description and click **Add**. To remove entries, select entries from the list and click **Remove Selected**. To disable the IP exception list unselect **IP Exception List** checkbox.

NOTE

When adding IP addresses to the IP exception list, you can also add a range of IP addresses using the CIDR notation.

» **Email exception list:** This option ensures that certain email senders or recipients are excluded from SPF checking, even if the messages are rejected. Select **Email Exception List** checkbox, add a new email address and description and click **Add**. To remove entries, select entries from the list and click **Remove Selected**. To disable the Email exception list unselect **Email Exception List** checkbox. An email address can be entered in any of the following three ways:

- local part - 'abuse' (matches 'abuse@abc.com', 'abuse@xyz.com', etc...)
- domain - '@abc.com' (matches 'john@abc.com', 'jill@abc.com', etc...)
- complete - 'joe@abc.com' (only matches 'joe@abc.com')

5. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

6. Click **Apply** to save settings.

5.1.9 Anti-Spoofing

Checks emails received with a sender email address claiming to originate from your own domain against a list of IP addresses by GFI MailEssentials. If the sender IP address is not on the list of own-domain server IP addresses, email is blocked.

This filter is NOT enabled by default.

WARNING

If enabling this feature do not whitelist internal users since this defeats Anti-Spoofing check.

Enabling and configuring Anti-Spoofing

1. Go to **Anti-Spam > Anti-Spam Filters > Anti-Spoofing**.

General
Actions

Anti-Spoofing Configuration

Anti-spoofing is an anti-spam filter which blocks emails from one of the local domains but which were sent from an unauthorized IP address.

Options

Enable Anti-Spoofing

Authorized IP / CIDR

SMTP Server:

Description:

[Add SMTP Server](#)

Authorized IP address list

<input type="checkbox"/>	Server	Description
No records to display.		

[Remove Selected](#)

Use authorized IP addresses from perimeter servers list (Recommended)

Do not block authenticated connections

Screenshot 78: GFI MailEssentials Anti-Spoofing filter

2. Select **Enable Anti-Spoofing** to enable Anti-Spoofing filter.
3. In the **SMTP Server:** field, provide the SMTP server where GFI MailEssentials checks for email recipient addresses. Also provide a description for the server in the **Description:** field.

NOTE

The SMTP Server field supports the following types of entry:

- » A single IP Address
- » A CIDR range (for example, 192.0.2.1/24)

4. Click **Add SMTP Server** to save SMTP server details.

NOTE

To remove previously added SMTP Servers, select an SMTP Server from the Authorized IP Address list and click **Remove Selected**.

By default, **Use authorized IP addresses from perimeter servers list** and **Do not block authenticated connections** are enabled. It is not recommended that these options are disabled.

5.1.10 Greylist

The Greylist filter temporarily blocks incoming emails received from unknown senders. Legitimate mail systems typically try to send the email after a few minutes; spammers simply ignore such error messages. If an email is received again after a predefined period, Greylist will:

1. Store the details of the sender in a database so that when the sender sends another email, the email will not be greylisted
2. Receive the email and proceed with anti-spam scanning

Greylist is **NOT** enabled by default.

Important Notes

1. To enable Greylist, GFI MailEssentials must be installed on the perimeter SMTP server. For more information refer to http://go.gfi.com/?pageid=ME_GreylistSMTP
2. Greylist contains exclusion lists so that specific email addresses, domains and IP addresses are not greylisted. Exclusions must be configured when:
 - » Emails originating from particular email addresses, domains or IP addresses cannot be delayed
 - » Emails addressed to a particular local user cannot be delayed

Configuring Greylist

1. Go to **Anti-Spam > Anti-Spam Filters > Greylist**.
2. From the **General** tab select/unselect **Enable Greylist** to enable/disable Greylist.

General
Email Exclusions
IP Exclusions
Actions

Configure email addresses which Greylist would not process

Email Addresses/Domains

Select email/domain address type:

From
 To

Specify email/domain address:

Email list

<input type="checkbox"/>		Email
<input type="checkbox"/>	<input type="button" value="↔"/>	jm@domain.com

Options

Exclude email addresses and domains specified in Whitelist and Personal Whitelist

Screenshot 79: Email Exclusions

3. Select **Email exclusions** tab to specify any email addresses or domains that you do not want to greylist. In the **Edit Addresses** area specify:

- » full email address; or
- » emails from an entire domain (for example: `trusteddomain.com`)

Also specify if the exclusion applies to senders (select **From**) or to the local recipients (select **To**)

» **Example 1:** Do not greylist emails if the recipient is `administrator@mydomain.com`, so that any emails *sent to* `administrator@mydomain.com` are never delayed.

» **Example 2:** Do not greylist emails if the sender's domain is `trusteddomain.com` (`trusted-domain.com`), so that emails *received from* domain `trusteddomain.com` are never delayed.

Click **Add emails** to add the exclusion.

NOTE

To exclude whitelisted and auto-whitelisted email addresses and domains from being greylisted and delayed, select **Exclude email addresses and domains specified in Whitelist and Personal Whitelist**.

4. Select the **IP exclusions** tab to specify any IP addresses to exclude from being greylisted. Click **Add IPs** and specify an IP to exclude.
5. To exclude whitelisted IP addresses from being greylisted and delayed, select **Exclude IP addresses specified in Whitelist**.
6. To log Greylist occurrences to a log file, click **Actions** tab and select **Log rule occurrence to this file**.

NOTE

Log files may become very large. GFI MailEssentials supports log rotation, where new log files are created periodically or when the log file reaches a specific size. To enable log file rotation navigate to **Anti-Spam > Anti-Spam Settings**. Select **Anti-spam logging** tab, check **Enable log file rotation** and specify the rotation condition.

7. Click **Apply**.

5.1.11 Language Detection

Determines the language of the email body text and configurable to block certain languages. GFI MailEssentials takes a portion of the email body message and compares it to an in-built language engine.

Configure the Language Detection filter to block certain languages or allow only some language.

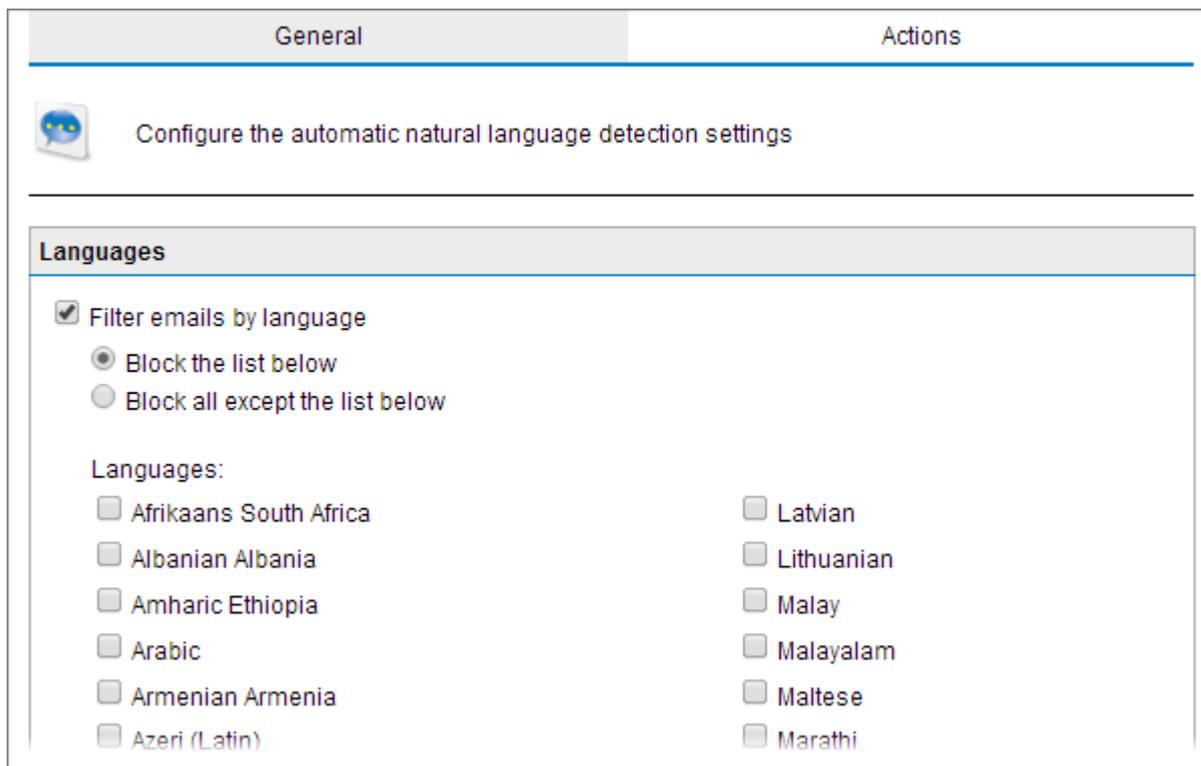
NOTE

The Language Detection filter is different than the [Header Checking - Language](#) filter since it analyzes the language of the email body text. The Header Checking analyzes the encoding (character set) of the email header. Results of the Language Detection filtering engine are generally more reliable.

The Language Detection filter is **NOT** enabled by default on installation.

Configuring Language Detection

1. Go to **Anti-Spam > Anti-Spam Filters > Language Detection**.



Screenshot 80: Language Detection options

2. From the **General** tab, select/unselect **Filter emails by language** option to enable/disable Language Detection.
3. Select **Block the list below** to select the languages to block or **Block all except the list below** to block all languages except the ones selected.
4. Select the languages to block/allow from the **Languages** area.
5. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).
6. Click **Apply**.

5.1.12 Header Checking

The Header Checking filter analyses the email header to identify spam emails.

Configuring Header Checking

1. Go to **Anti-Spam > Anti-Spam Filters > Header Checking**.

General	Languages	Actions				
 Specify which checks to perform on email headers						
Email and IP Addresses <ul style="list-style-type: none"> <input type="checkbox"/> Check if the email header contains an empty MIME FROM: field. <input type="checkbox"/> Check if the email header contains a malformed MIME FROM: field. <input type="checkbox"/> Maximum number of recipients allowed in email: <input type="text" value="20"/> <input type="checkbox"/> Check if the email headers contain different SMTP TO: and MIME TO: fields. <input type="checkbox"/> Verify if sender domain is valid (performs DNS lookup on MIME FROM:) <input type="checkbox"/> Maximum numbers allowed in the first part of the MIME FROM: field (eg. joe31516u9@domain.com): <input type="text" value="4"/> <input type="checkbox"/> Check if email contains encoded IP addresses. <p>'SMTP' fields are specified by the SMTP server, whereas 'MIME' fields are specified by the client.</p>						
Content Related <ul style="list-style-type: none"> <input type="checkbox"/> Check if email contains remote images only. Minimum HTML body size: <input type="text" value="512"/> bytes <input type="checkbox"/> Check if email contains GIF images. <input type="checkbox"/> Check if email contains attachment spam. 						
Subject <ul style="list-style-type: none"> <input type="checkbox"/> Check if the email subject contains the first part of the recipient email address. <p>Email exception list:</p> <table border="0" style="width: 100%;"> <tr> <td style="border: 1px solid black; width: 80%; height: 20px;"></td> <td style="text-align: center; width: 20%;"><input type="button" value="Add"/></td> </tr> <tr> <td style="border: 1px solid black; width: 80%; height: 20px; vertical-align: bottom;"> <div style="text-align: right;"> <input type="button" value="Remove"/> </div> </td> <td style="text-align: center;"><input type="button" value="Remove"/></td> </tr> </table>				<input type="button" value="Add"/>	<div style="text-align: right;"> <input type="button" value="Remove"/> </div>	<input type="button" value="Remove"/>
	<input type="button" value="Add"/>					
<div style="text-align: right;"> <input type="button" value="Remove"/> </div>	<input type="button" value="Remove"/>					

Screenshot 81: Header checking options

2. Enable, disable or configure the following parameters:

Option	Description
Check if the email header contains an empty MIME FROM: field.	Checks if the sender has identified himself in the From: field. If this field is empty, the message is marked as spam.

Option	Description
Check if the email header contains a malformed MIME FROM: field.	Checks if the MIME from field is a correct notation as defined in the RFCs.
Maximum number of recipients allowed in email	Identifies emails with large amounts of recipients and flags them as SPAM.
Check if the email headers contain different SMTP TO: and MIME TO: fields.	Checks whether the SMTP to: and MIME to: fields are the same. The spammers email server always has to include an SMTP to: address. However, the MIME to: email address is often not included or is different. NOTE: This feature identifies a lot of spam, however some list servers do not include the MIME to: either. It is therefore recommended to whitelist newsletter sender address to use this feature.
Verify if sender domain is valid (performs DNS lookup on MIME FROM:)	Performs a DNS lookup on the domain in the MIME from field and verifies the domain validity. NOTE: Ensure that the DNS server is properly configured to avoid timeouts and slow email flow.
Maximum numbers allowed in the first part of the MIME FROM: field:	Identifies the presence of numbers in the MIME from field. Spammers often use tools that automatically create unique reply-to: addresses by using numbers in the address.
Check if email contains encoded IP addresses.	Checks the message header and body for URLs which have a hex/octal encoded IP (http://0072389472/hello.com) or which have a username/password combination (for example www.citibank.com@scammer.com). The following examples are flagged as spam: » http://12312 » www.microsoft.com:hello%01@123123
Check if email contains remote images only. Minimum HTML body size	Flag emails that only have remote images and a minimal amount of text as spam. Assists in identifying 'image only email' spam.
Check if email contains GIF images.	Checks if the email contains one or more embedded GIF images. Embedded GIF images are often used to circumvent spam filters. IMPORTANT: Since some legitimate emails contain embedded GIF images, this option is prone to false positives.
Check if email contains attachment spam.	Checks email attachments for properties that are common to attachments sent in spam email. This helps in keeping up with the latest techniques used by spammers in using attachments to send spam.
Check if the email subject contains the first part of the recipient email address.	Identifies the personalized spam email, where spammers frequently include the first part of the recipient email address in the subject.

3. From the **Languages** tab, select **Block mail that use these languages (character sets)** to enable language detection.

NOTE

The Header Checking - Language filter is different than the [Language Detection](#) filter since it analyzes the encoding (character set) of the email header. The Language Detection analyzes the language of the email body text. Results of the Language Detection filtering engine are generally more reliable.

General	Languages	Actions																		
 Configures the Language Settings																				
<div style="border: 1px solid gray; padding: 5px;"> <p>Languages</p> <p><input checked="" type="checkbox"/> Block mail that use these languages (character sets)</p> <p> <input checked="" type="radio"/> Block the list below <input type="radio"/> Block all except the list below </p> <p>Languages:</p> <table border="0"> <tr> <td><input type="checkbox"/> Arabic</td> <td><input type="checkbox"/> Japanese</td> </tr> <tr> <td><input type="checkbox"/> Armenian</td> <td><input type="checkbox"/> Korean</td> </tr> <tr> <td><input type="checkbox"/> Baltic</td> <td><input type="checkbox"/> Simplified Chinese</td> </tr> <tr> <td><input type="checkbox"/> Central Europe</td> <td><input type="checkbox"/> Thai</td> </tr> <tr> <td><input type="checkbox"/> Cyrillic</td> <td><input type="checkbox"/> Traditional Chinese</td> </tr> <tr> <td><input type="checkbox"/> Georgian</td> <td><input type="checkbox"/> Turkic</td> </tr> <tr> <td><input type="checkbox"/> Greek</td> <td><input type="checkbox"/> Vietnamese</td> </tr> <tr> <td><input type="checkbox"/> Hebrew</td> <td><input type="checkbox"/> Western Europe and United States</td> </tr> <tr> <td><input type="checkbox"/> Indic</td> <td></td> </tr> </table> </div>			<input type="checkbox"/> Arabic	<input type="checkbox"/> Japanese	<input type="checkbox"/> Armenian	<input type="checkbox"/> Korean	<input type="checkbox"/> Baltic	<input type="checkbox"/> Simplified Chinese	<input type="checkbox"/> Central Europe	<input type="checkbox"/> Thai	<input type="checkbox"/> Cyrillic	<input type="checkbox"/> Traditional Chinese	<input type="checkbox"/> Georgian	<input type="checkbox"/> Turkic	<input type="checkbox"/> Greek	<input type="checkbox"/> Vietnamese	<input type="checkbox"/> Hebrew	<input type="checkbox"/> Western Europe and United States	<input type="checkbox"/> Indic	
<input type="checkbox"/> Arabic	<input type="checkbox"/> Japanese																			
<input type="checkbox"/> Armenian	<input type="checkbox"/> Korean																			
<input type="checkbox"/> Baltic	<input type="checkbox"/> Simplified Chinese																			
<input type="checkbox"/> Central Europe	<input type="checkbox"/> Thai																			
<input type="checkbox"/> Cyrillic	<input type="checkbox"/> Traditional Chinese																			
<input type="checkbox"/> Georgian	<input type="checkbox"/> Turkic																			
<input type="checkbox"/> Greek	<input type="checkbox"/> Vietnamese																			
<input type="checkbox"/> Hebrew	<input type="checkbox"/> Western Europe and United States																			
<input type="checkbox"/> Indic																				

Screenshot 82: Language Detection

4. Select **Block the list below** to select the languages to block or **Block all except the list below** to block all languages except the ones selected.
5. Select the languages to block/allow from the **Languages** area.
6. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).
7. Click **Apply**.

5.1.13 Spam Keyword Checking

This filter enables the identification of Spam based on keywords in the email being received.

This filter is **NOT** enabled by default on installing GFI MailEssentials.

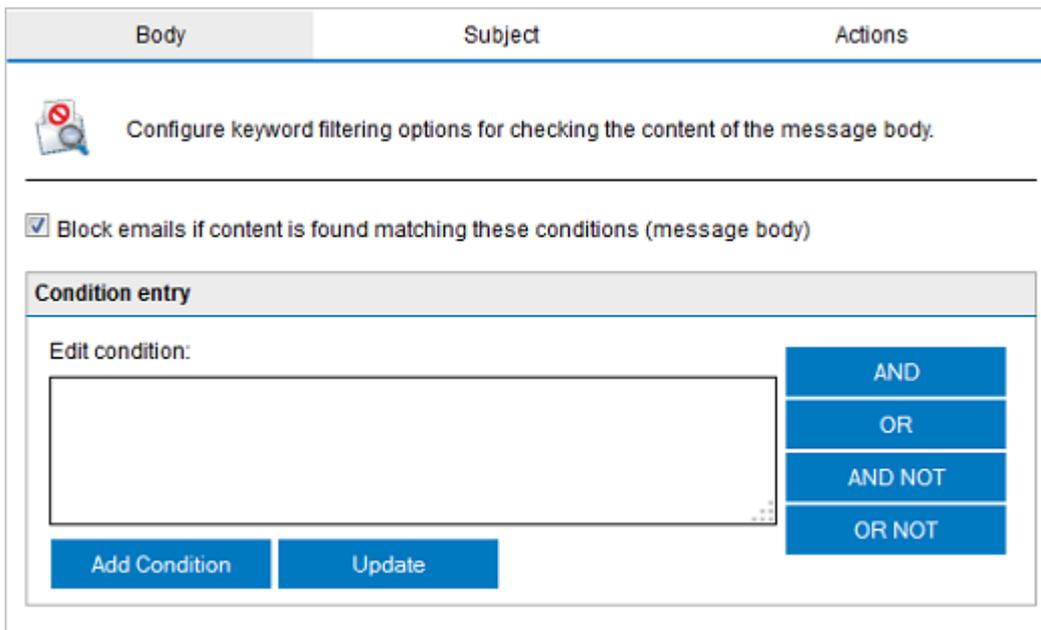
NOTE

This filter only checks the content of the email for text that identifies the email as Spam. For comprehensive content filtering of email (for example to block Racial content or Profanities), use the Keyword filtering option within the Content Filtering node.

Add Spam Keyword Check

1. Go to **Anti-Spam > Anti-Spam Filters > Spam Keyword Checking**.

2. From the **Body** tab, select **Block emails if content is found matching these conditions (message body)** to enable Spam Keyword checking on email body.



Screenshot 83: Spam Keyword checking properties

3. In the **Condition Entry** area, key in a keyword or a combination of keywords for this filter to block. Use the 'AND', 'OR', 'AND NOT' and 'OR NOT' operators to configure specific conditions.

For example:

- `Basketball sports` - GFI MailEssentials blocks emails with the phrase `Basketball sports`. Only this phrase would activate the rule, not the word `basketball` OR the word `sports` separated by some other words.
- `Basketball AND Baseball` - GFI MailEssentials blocks emails that have both words in the email. Emails with only `Basketball` or only `baseball` will not be blocked.

4. Select **Match whole words only** to search specifically for whole words and avoid blocking words that are part of other words. For example, enabling this option would not block the word 'MSEExchange', notwithstanding the fact that the word 'sex' is part of 'MSEExchange'.

5. Select **Subject** tab, select **Block emails if content is found matching these conditions (message subject)** to enable Spam Keyword checking on email subject.

6. In the **Condition Entry** area, key in a keyword or a combination of keywords for this filter to block. Use the 'AND', 'OR', 'AND NOT' and 'OR NOT' operators to configure specific conditions.

7. Select **Apply the keywords list to also scan senders' display names** to check the display name of the sender email, which can contain spam keywords. For example, Viagra spam, which often has forged senders and the word Viagra in the senders' display name.

8. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

9. Click **Apply**.

Removing conditions

To remove a Spam Keyword Checking condition:

1. From the **Conditions list** area within the **Body** or **Subject** tab, select one or more conditions to remove.

NOTE

To find the condition to remove, use the controls under the list of conditions to move between the pages listing the conditions.

2. Click **Remove** and **Apply**.

Importing and Exporting conditions

To export more conditions:

1. From the **Conditions list** area within the **Body** or **Subject** tab, select one or more conditions to export.

NOTE

To find the conditions to export, use the controls under the list of conditions to move between the pages listing the conditions.

2. In the **File Download** screen, click **Save** and select a folder where to save the export file.

To import conditions:

1. From the **Conditions list** area within the **Body** or **Subject** tab, key in the folder and filename of the file to import.
2. Click **Import**.

5.1.14 Bayesian Analysis

An anti-spam filter that can be trained to accurately determine if an email is spam based on past experience.

This manual also contains information how the Bayesian filter works and how it can be trained. For more information, refer to [How Bayesian Analysis works](#) (page 136).

The Bayesian Analysis filter is **NOT** enabled by default.

IMPORTANT

Enable learning from outbound emails and allow at least a week for before enabling filter. This is required because the Bayesian filter acquires its highest detection rate when it adapts to your email patterns.

Configuring the Bayesian filter

Configuring the Bayesian filter requires 2 stages:

Stage 1: Training the Bayesian filter

Stage 2: Enabling the Bayesian filter

Stage 1: Training the Bayesian filter

The Bayesian filter can be trained in two ways:

Method 1: Automatically, through outbound emails.

GFI MailEssentials processes legitimate email (ham) by scanning outbound emails. The Bayesian filter can be enabled after it has collected at least 500 outbound emails (If you send out mainly English email) or 1000 outbound mails (If you send out non-English email).

To do this:

1. Go to **Anti-Spam > Anti-Spam Filters > Bayesian Analysis**.
2. Select **Automatically learn from outbound e-mails**.
3. Click **Apply**.

Method 2: Manually, through existing email.

Copying between 500-1000 mails from your sent items to the **This is legitimate email** sub folder in the **GFI AntiSpam Folders** public folders trains the Bayesian filter in the same way as live outbound email sending.

NOTE

To use this option, Public Folder Scanning must be enabled. For more information, refer to [Public Folder Scanning](#) (page 164).

Stage 2: Enabling the Bayesian filter

After the Bayesian filter is trained, it must be enabled.

1. From GFI MailEssentials configuration console, go to **Anti-Spam > Anti-Spam Filters > Bayesian Analysis**.
2. From the **General** tab select **Enable Bayesian Analysis**.

General	Updates	Actions
 Configure the Bayesian Analysis settings		
Bayesian options		
<input checked="" type="checkbox"/> Enable Bayesian Analysis Allow GFI MailEssentials to learn for a minimum of one week (depending on your mail volume) from your outbound mail before enabling. Alternatively, run Bayesian Wizard (see Administrator Guide for more information).		
<input checked="" type="checkbox"/> Automatically learn from outbound e-mails		
Amount of emails in Bayesian database:		
Legitimate emails (HAM):	46247	
Spam emails:	78367	
If you rarely send and receive English emails then it is recommended to have a minimum of 3000 HAM and spam emails to ensure effective filtering.		
If, however, you send and receive mostly English emails then a minimum recommendation of 2500 HAM and spam emails should be enough to ensure effective filtering.		

Screenshot 84: Bayesian analysis properties

3. In the **Updates** tab, configure the frequency of updates to the spam database by enabling **Automatically check for updates** and configuring an hourly interval.

NOTE

Click **Download updates now...** to immediately download any updates.

NOTE

You can download updates using a proxy server. For more information, refer to [Proxy settings](#) (page 227).

4. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

5. Click **Apply**.

NOTE

GFI MailEssentials also provides a Bayesian Analysis wizard that enables you to train the Bayesian Analysis filter from a machine other than where GFI MailEssentials is installed. For more information, refer to [Training the Bayesian Analysis filter](#) (page 137).

How Bayesian Analysis works

The Bayesian filter is an anti-spam technology used within GFI MailEssentials. It is an adaptive technique based on artificial intelligence algorithms, hardened to withstand the widest range of spamming techniques available today.

This chapter explains how the Bayesian filter works, how it can be configured and how it can be trained.

NOTE

1. The Bayesian anti-spam filter is disabled by default. It is highly recommended that you train the Bayesian filter before enabling it.
2. GFI MailEssentials must operate for at least one week for the Bayesian filter to achieve its optimal performance. This is required because the Bayesian filter acquires its highest detection rate when it adapts to your email patterns.

How does the Bayesian spam filter work?

Bayesian filtering is based on the principle that most events are dependent and that the probability of an event occurring in the future can be inferred from the previous occurrences of that event.

NOTE

Refer to the links below for more information on the mathematical basis of Bayesian filtering:

http://go.gfi.com/?pageid=ME_BayesianParameterEstimation

This same technique has been adapted by GFI MailEssentials to identify and classify spam. If a snippet of text frequently occurs in spam emails but not in legitimate emails, it would be reasonable to assume that this email is probably spam.

Creating a tailor-made Bayesian word database

Before Bayesian filtering is used, a database with words and tokens (for example \$ sign, IP addresses and domains, etc.) must be created. This can be collected from a sample of spam email and valid email (referred to as 'ham').

A probability value is then assigned to each word or token; this is based on calculations that account for how often such word occurs in spam as opposed to ham. This is done by analyzing the users' outbound email

and known spam: All the words and tokens in both pools of email are analyzed to generate the probability that a particular word points to the email being spam.

This probability is calculated as per following example:

If the word 'mortgage' occurs in 400 out of 3,000 spam emails and in 5 out of 300 legitimate emails then its spam probability would be 0.8889 (i.e. $[400/3000] / [5/300 + 400/3000]$).

Creating a custom ham email database

The analysis of ham email is performed on the company's email and therefore is tailored to that particular company.

» **Example:** A financial institution might use the word 'mortgage' many times and would get many false positives if using a general anti-spam rule set. On the other hand, the Bayesian filter, if tailored to your company through an initial training period, takes note of the company's valid outbound email (and recognizes 'mortgage' as being frequently used in legitimate messages), it will have a much better spam detection rate and a far lower false positive rate.

Creating the Bayesian spam database

Besides ham email, the Bayesian filter also relies on a spam data file. This spam data file must include a large sample of known spam. In addition it must also constantly be updated with the latest spam by the anti-spam software. This will ensure that the Bayesian filter is aware of the latest spam trends, resulting in a high spam detection rate.

How is Bayesian filtering done?

Once the ham and spam databases have been created, the word probabilities can be calculated and the filter is ready for use.

On arrival, the new email is broken down into words and the most relevant words (those that are most significant in identifying whether the email is spam or not) are identified. Using these words, the Bayesian filter calculates the probability of the new message being spam. If the probability is greater than a threshold, the message is classified as spam.

NOTE

For more information on Bayesian Filtering and its advantages refer to:

http://go.gfi.com/?pageid=ME_Bayesian

Training the Bayesian Analysis filter

NOTE

The Bayesian Analysis filter can also be trained using Public folders. For more information, refer to [Configuring the Bayesian filter](#) (page 134).

It is recommended that the Bayesian Analysis filter is trained through the organization's mail flow over a period of time. It is also possible for Bayesian Analysis to be trained from emails sent or received before GFI MailEssentials is installed by using the Bayesian Analysis wizard. This allows Bayesian Analysis to be enabled immediately.

This wizard analyzes sources of:

- » legitimate mail - for example a mailbox' sent items folder
- » spam mail - for example a mailbox folder dedicated to spam emails.

Step 1: Install the Bayesian Analysis wizard

The Bayesian Analysis wizard can be installed on:

- » A machine that communicates with Microsoft® Exchange - to analyze emails in a mailbox
- » A machine with Microsoft Outlook installed - to analyze emails in Microsoft Outlook

To install the Bayesian Analysis wizard:

1. Copy the setup file **Bayesian Analysis Wizard.exe** to the chosen machine. This is located in: GFI MailEssentials *installation path*\AntiSpam\BSW
2. Launch **Bayesian Analysis Wizard.exe**.
3. In the initial screen, choose the language and review the End-User License Agreement. Click **Next**.
4. Select the installation folder and click **Next**.
5. Click **Install** to start installation.
6. Click **Finish** when installation is complete.

Step 2: Analyze legitimate and spam emails

To start analyzing emails using the Bayesian Analysis wizard:

1. Load the Bayesian Analysis wizard from **Start > Programs > GFI MailEssentials > GFI MailEssentials Bayesian Analysis Wizard**.
2. Click **Next** in the welcome screen.
3. Choose whether to:
 - » Create a new Bayesian Spam Profile (.bsp) file or update an existing one. Specify the path where to store the file and the filename.
 - » Update the Bayesian Spam profile used by the Bayesian Analysis filter directly when installing on the same machine as GFI MailEssentials.

Click **Next** to proceed.

4. Select how the wizard will access legitimate emails. Select:
 - » **Use Microsoft Outlook profile configured on this machine** - Retrieves emails from a Microsoft Outlook mail folder. Microsoft Outlook must be running to use this option.
 - » **Connect to a Microsoft® Exchange Server mailbox store** - Retrieves emails from a Microsoft® Exchange mailbox. Specify the logon credentials in the next screen.
 - » **Do not update legitimate mail (ham) in the Bayesian Spam profile** - skip retrieval of legitimate emails. Skip to step 6.

Click **Next** to continue.

5. After the wizard connects to the source, select the folder containing the list of legitimate emails (e.g. the Sent items folder) and click **Next**.

6. Select how the wizard will access the source of spam emails. Select:

- » **Download latest Spam profile from GFI website** - Downloads a spam profile file that is regularly updated by collecting mail from leading spam archive sites. An Internet connection is required.
- » **Use Microsoft Outlook profile configured on this machine** - Retrieves spam from a Microsoft Outlook mail folder. Microsoft Outlook must be running to use this option.
- » **Connect to a Microsoft® Exchange Server mailbox store** - Retrieves spam from a Microsoft® Exchange mailbox. Specify the logon credentials in the next screen.
- » **Do not update Spam in the Bayesian Spam profile** - skip retrieval of spam emails. Skip to step 8.

Click **Next** to continue.

7. After the wizard connects to the source, select the folder containing the list of spam emails and click **Next**.

8. Click **Next** to start retrieving the sources specified. This process may take several minutes to complete.
9. Click **Finish** to close the wizard.

Step 3: Import the Bayesian Spam profile

When the wizard is not run on the GFI MailEssentials server, import the Bayesian Spam Profile (.bsp) file to GFI MailEssentials.

1. Move the file to the **Data** folder in the GFI MailEssentials installation path.
2. Restart the **GFI MailEssentials AS Scan Engine** and the **GFI MailEssentials Legacy Attendant** services.

5.1.15 Whitelist

NOTE

Whitelist affects only Anti-Spam filters and not email security and content filtering

The Whitelist contains lists of criteria that identify legitimate email. Emails that match these criteria are not scanned by anti-spam filters and are always delivered to the recipient. Emails can be whitelisted using the following criteria:

- » Sender's email address, email domain or IP address
- » Senders to whom an email was previously sent (Auto-whitelist)
- » Recipient (exclude local email addresses from having emails filtered)
- » Keywords in email body or subject

The whitelist and Auto Whitelist features are enabled by default.

Important notes

Using the Auto Whitelist feature is highly recommended since this eliminates a high percentage of false positives.

In Keyword Whitelist it is recommended to add terms that spammers do not use and terms that relate to your nature of business, for example your product names. Entering too many keywords increases the possibility of emails not filtered by GFI MailEssentials and delivered to users' mailboxes.

Whitelisting an internal user defeats the purpose of the Anti-Spoofing filter. For more information, refer to [Anti-Spoofing](#) (page 124).

Configuring Whitelist

1. Go to **Anti-Spam > Whitelist**.

Whitelist
Auto Whitelist
Keyword Whitelist

Personal Whitelist
IP Whitelist
Actions

Specify which email addresses will not be filtered for spam

Enable email whitelist

Whitelist Entry

Email Address/Domain:

Email Type:

Description:

[Add](#)

Whitelist

Search [Search](#)

<input type="checkbox"/>	Email	Description
<input type="checkbox"/>	*@*.gfi.com	
<input type="checkbox"/>	*@cleverbridge.com	
<input type="checkbox"/>	*@faxmaker.com	
<input type="checkbox"/>	*@faxmaker.com	
<input type="checkbox"/>	*@gfi.ch	
<input type="checkbox"/>	*@gfi.co.uk	
<input type="checkbox"/>	*@gfi.com	
<input type="checkbox"/>	*@gficom.at	
<input type="checkbox"/>	*@gfihispana.com	
<input type="checkbox"/>	*@gfisoftware.com	
<input type="checkbox"/>	*@gfisoftware.de	

Page 1 of 2, items 1 to 15 of 20.

[Show Statistics](#)
[Remove](#)
[Export](#)

Specify the full path and filename of the file to use for importing:

[Import](#)

Note: Import of list data cannot be performed unless the import list is on the server where GFI MailEssentials is installed.

Screenshot 85: Whitelist tab

2. From the **Whitelist** tab, configure the email addresses and domains to whitelist. Select/Unselect **Enable email whitelist** to enable/disable whitelist. Perform the following actions:

Action	Description
Add a whitelist entry	<ol style="list-style-type: none"> In Email Address/Domain, provide the email address/domain to whitelist. For example: . *@companysupport.com or. *@*.edu. In Email Type specify the email header field to match for the emails to be whitelisted. <div style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"> <p>NOTE For more information about the difference between SMTP and MIME refer to: http://go.gfi.com/?pageid=ME_DifferenceSMTPMIME</p> </div> <ol style="list-style-type: none"> (Optional) In Description add a description to the entry. Click Add.
Remove whitelist entries	<ol style="list-style-type: none"> Select one or more whitelist entries from the Whitelist list. Click Remove.
Search for a whitelist entry	<ol style="list-style-type: none"> In Search, key in the details of the whitelist entry to search for. Click Search to display list of matching terms.
Show Statistics	Use the Show Statistics button to view the total number of emails blocked per whitelist entry.
Import whitelist entries	<ol style="list-style-type: none"> Specify the full path and filename of the file to use for importing the previously exported data. Click Import to import entries.
Export whitelist entries	Click Export to export current list of whitelist entry to an XML file.

3. Select the **Auto Whitelist** tab to configure the following options:

Option	Description
Populate Auto Whitelist automatically:	If selected, destination email addresses of outbound emails are automatically added to the auto-whitelist.
Enable Email Auto Whitelist	Select this option to enable auto-whitelist. Senders of incoming emails are matched against the auto-whitelist. If the sender is present in the list, the email is forwarded directly to the recipient's Inbox.
Maximum entries allowed in the Auto Whitelist:	Specify the number entries allowed in Auto-Whitelist. When the limit specified is exceeded, the oldest and least used entries are automatically replaced by the new entries.
	<div style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"> <p>NOTE Entering a value larger than the default value of 30,000 can negatively affect the performance of GFI MailEssentials.</p> </div>

4. From the **Keyword Whitelist** tab, specify keywords that flag emails as valid emails:

Option	Description
Enable email body keyword whitelist	Select this option to check for keywords in the email body which qualify an email as valid. Add keywords to the Body Keywords list. You can also import or export lists of keywords from/to an XML file.
Enable email subject keyword whitelist	Select this option to check for keywords in the email subject which qualify an email as valid. Add keywords to the Subject Keywords list. You can also import or export lists of keywords from/to an XML file.
Match whole words only (word-s/phrases in subject/body)	When selecting this option, only whole words from the keyword whitelist are matched that qualify an email as valid.

5. From the **IP Whitelist** tab, configure:

Option	Description
Enable IP Whitelist	Select to allow emails received from specific IP addresses to be whitelisted.
Add IP Whitelist entries	1. Specify: <ul style="list-style-type: none"> » Single computer / CIDR: Key in a single IP address or a range of IP addresses using CIDR notation. » Group of computers: Specify the Subnet Address and Subnet Mask of the group of IPs to whitelist. 2. (Optional) Add a Description . 3 Click Add .
Remove IP Whitelist entries	Select the IPs to remove and click Remove .

6. Click **Actions** tab to enable / disable logging of whitelist occurrences to a file. Provide a path/folder where to store the generated log file.

7. Click **Apply**.

Personal Whitelist

The personal whitelist is an additional whitelist that compliments global whitelist. Disabled by default, the personal whitelist can be enabled for users allowing them to add specific email addresses to a personal whitelist that they can manage. For more information, refer to [End User Actions](#) (page 15).

For management purposes, administrators can also remove specific email addresses that the users have added to their personal whitelist.

Enabling/Disabling Personal Whitelists

1. Go to **Anti-Spam > Whitelist**.

Whitelist	Auto Whitelist	Keyword Whitelist
Personal Whitelist	IP Whitelist	Actions

View the users personalized whitelists

Enable personal email whitelist

Personal Whitelist

User: All

Remove

<input type="checkbox"/>	User	Whitelisted Email
<input type="checkbox"/>	DOMAINA\Administrator	janedoe@domain.com
<input type="checkbox"/>	DOMAINA\Administrator	johnsmith@domain.com

Screenshot 86: Personal whitelist

2. Select **Personal Whitelist** tab and select or unselect **Enable personal email whitelist** to enable or disable personal whitelist feature.
3. Click **Apply**.

Removing emails from users' personal whitelist

1. Go to **Anti-Spam > Whitelist** and select **Personal Whitelist** tab.
2. From the **User** drop down list, select the user for whom to delete an email address.
3. Select an email address from the list of email addresses. Click **Remove**.
4. Click **Apply**.

5.1.16 New Senders

The New Senders filter identifies emails that have been received from senders to whom emails have never been sent before. Such senders are identified by referencing the data collected in the Whitelist.

Only emails in which no spam is detected and where the sender is not present in any Whitelist are triggered by the New Senders filter.

This filter is **NOT** enabled by default.

Important

Enable at least one of the available Whitelists to use the New Senders function. In the absence of the Whitelist functions (should no spam be detected by the other filters) received messages will be delivered to the recipient's Inbox. **ONLY** emails in which no spam was detected and whose senders are not present in the Whitelist are delivered in the New Senders folder.

Configuring New Senders Filter

1. Go to **Anti-Spam > New Senders**.

General	Exceptions	Actions
 Configure New Senders		
<p>The New Senders module automatically identifies emails which have been sent from senders to whom you have never sent emails. These emails could be legitimate senders or else spam which were not detected by the GFI MailEssentials spam filters.</p>		
<p>Options</p> <p><input checked="" type="checkbox"/> Enable New Senders</p>		
<p>Note</p> <p>For the New Senders to work, there has to be at least one whitelist enabled from the Whitelist configuration node.</p>		

Screenshot 87: New Senders General tab

2. In the **General** tab, select **Enable New Senders** to enable check for new senders on all inbound messages.

Screenshot 88: New Senders Exceptions

3. From **Exceptions** tab, configure recipients whose emails are excluded from the New Senders check.

Option	Description
Enable New Senders exception list	Select this option to enable the exceptions list.
Add exception	Key in an email address to exclude and click Add . Repeat for each address to add.
Edit exception	<ol style="list-style-type: none"> 1. Select an exception from the Email list. 2. Edit the email address. 3. Click Update.
Delete exception	Select an exception from the Email list and click Remove .

4. Click **Actions** tab to select the actions to perform on messages identified as spam. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

5. Click **Apply**.

5.2 Spam Actions - What to do with spam emails

The **Actions** tab in the Anti-Spam filters properties define what should be done with emails marked as spam. Different actions can be defined for each of the spam filters.

» **For Example:** Delete emails detected by SpamRazer filter, but do not delete emails marked as spam by the Email Blocklist filter.

5.2.1 Configuring Spam Actions

In the **Actions** tab, select an option that defines which action to take on emails marked as spam.

General Updates **Actions**

Select the action to perform when this filter blocks a spam email

Actions

- Quarantine email
- Delete email
- Perform the following action(s)
 - Deliver email to mailbox:
 - In Inbox
 - In Exchange junk email folder
 - In Exchange mailbox sub-folder
Inbox/Spam
 - Send to email address:

 - Move to folder on disk:

 - Tag the email with specific text:
SPAM
Specify how the tag will be applied to the email:
Prepend to subject
 - Append block reason to email subject

Screenshot 89: Anti-spam actions

Action	Description
Quarantine Email	Emails detected as spam are stored in the Quarantine Store. Other spam actions are disabled if the email is quarantined. For more information, refer to Quarantine (page 191).
Delete Email	Delete an email blocked by that particular spam filter. Other spam actions are disabled if the email is deleted.

Action	Description
Deliver email to mailbox - In Inbox	Routes spam to user's inbox
Deliver email to mailbox - In Exchange junk email folder	Routes spam to users' Junk email folder. This option only works when GFI MailEssentials is installed on Microsoft Exchange. It is not available for the New Senders filter. If GFI MailEssentials is not installed on the Microsoft® Exchange Server, refer to Moving spam to user's mailbox folders .
Deliver email to mailbox - In Exchange mailbox sub-folder	Route all spam to a specific folder in the user's mailbox. Type the folder where to move spam email. » Example 1: Type <code>Suspected Spam</code> for a custom folder to be created in the same level of the Inbox folder. » Example 2: Type <code>Inbox\Suspected Spam</code> for a custom folder to be created in the Inbox folder. This option requires that GFI MailEssentials is installed on the Microsoft® Exchange Server machine. In Microsoft® Exchange 2010 onwards, the Mailbox Server Role is required. For Microsoft® Exchange 2010 or newer versions, a dedicated user is also required to enable this option. For more information, refer to Set a Microsoft® Exchange account (page 260). If GFI MailEssentials is not installed on the Microsoft® Exchange Server, refer to Moving spam email to user's mailbox folders .
Send to email address	Send email identified as spam to a specific email address. Example: Forward all spam to an email address checked by someone who checks email that might have been wrongly marked as spam. The subject of the email will be in the format: <code>[recipient] [subject]</code>
Move to folder on disk	Saves email detected as spam to the path specified, Example: <code>C:\Spam\</code> File names of saved emails are in the following format: <code>[Sender_recipient_subject_number_.eml]</code> Example: <code>C:\Spam\jim@ad.com_bob@ad.com_Offers_1_.eml</code>
Tag the email with specific text	Select this option to add a tag to the email subject. Key in the text to use for tagging and specify where to place the tag: » Prepend to subject - insert the specified tag at the start (i.e. as a prefix) of the email subject text. Example: <code>[SPAM]Free Web Mail</code> » Append to subject - insert the specified tag at the end (i.e. as a suffix) of the email subject text. Example: <code>Free Web Mail[SPAM]</code> » Add tag in an X-header... - Add the specified tag as a new X-header to the email. In this case, the X-Header will have the following format : <ul style="list-style-type: none"> • X-GFIME-SPAM: [TAG TEXT] • X-GFIME-SPAM-REASON: [REASON] Example: <ul style="list-style-type: none"> • X-GFIME-SPAM: [This is SPAM] • X-GFIME-SPAM-REASON: [IP DNS Blocklist Check failed - Sent from Blocklisted Domain]
	NOTE Rules manager can be used to move emails when this feature is used.
Append block reason to email subject	If this option is enabled, the name of the filter which blocked the email and the reason for blocking are appended to the subject of the blocked email.

Action	Description
Log rule occurrence to this file	<p>Log the spam email occurrence to a log file of your choice. By default, log files are stored in: <i><GFI MailEssentials installation path>\GFI\MailEssentials\AntiSpam\Logs\<filtername>.log</i></p> <p>NOTE Log files may become very large. GFI MailEssentials enables log rotation, where new log files are created periodically or when the log file reaches a specific size. To enable log file rotation navigate to Anti-Spam > Anti-Spam Settings. Select Anti-spam logging tab and check Enable log file rotation. Specify the rotation condition by time or file size.</p>

5.3 Sorting anti-spam filters by priority

In GFI MailEssentials, the order in which the anti-spam checks are applied to inbound messages can be customized.

NOTE

The order of all available filters can be customized except for the **New Senders** filter, which is always automatically set to the lowest priority. This is due to its dependency on the results of the Whitelist checks and the other anti-spam filters.

Default priority is recommended in most situations.

1. Go to **Anti-Spam > Filter Priority**.

Filter Priority
SMTP Transmission Filtering

Configure the priority of spam filter execution

Specify Filter Priority

Name	Priority	Filter Level		
Greylist	1	SMTP Data	↑	↓
IP Whitelist	2	Full Email	↑	↓
IP Blocklist	3	Full Email	↑	↓
Anti-Spoofing	4	Full Email	↑	↓
Sender Policy Framework	5	Full Email	↑	↓
Whitelist	6	Full Email	↑	↓
Personal Whitelist	7	Full Email	↑	↓
Directory Harvesting	8	Full Email	↑	↓
Anti-Phishing	9	Full Email	↑	↓
SpamRazer	10	Full Email	↑	↓
Keyword Whitelist	11	Full Email	↑	↓
Email Blocklist	12	Full Email	↑	↓
Personal Blocklist	13	Full Email	↑	↓
IP DNS Blocklist	14	Full Email	↑	↓
URI DNS Blocklist	15	Full Email	↑	↓
Bayesian Analysis	16	Full Email	↑	↓
Header Checking	17	Full Email	↑	↓
Spam Keyword Checking	18	Full Email	↑	↓

Default Settings

Screenshot 90: Assigning filter priorities

2. Select a filter and click **↑** (up) button to assign a higher priority or click **↓** (down) button to assign a lower priority.

NOTE

Click **Default Settings** to restore the filters' order to default.

3. Click **Apply**.

5.4 SMTP Transmission Filtering

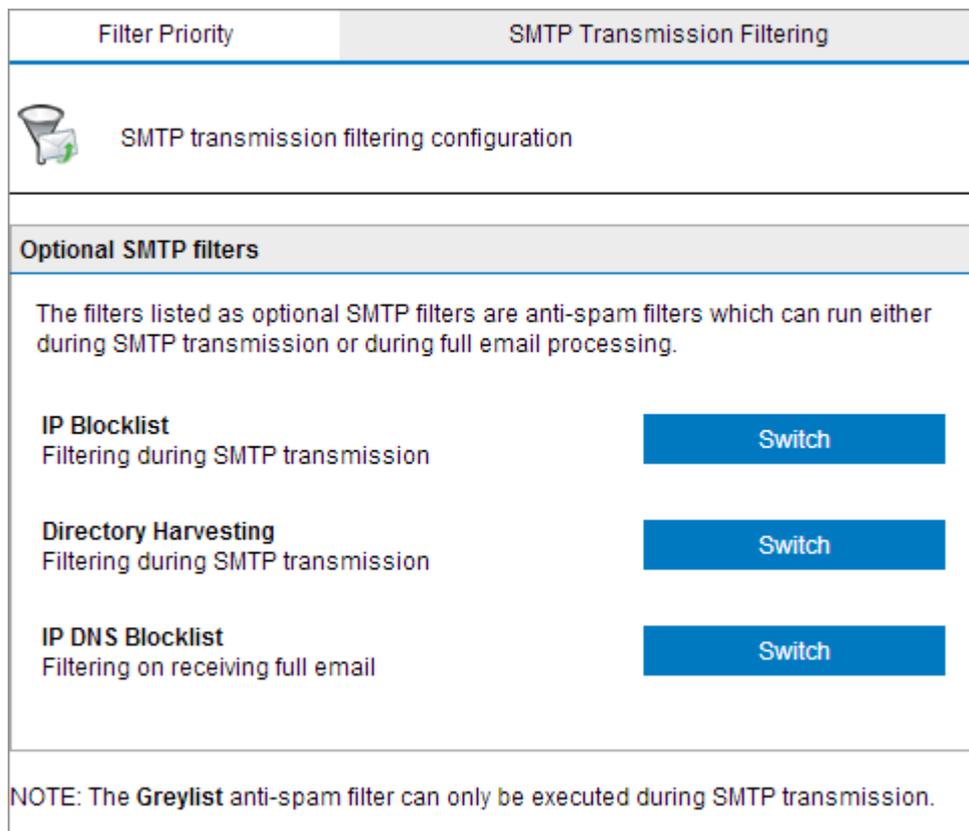
In GFI MailEssentials, some anti-spam filters can be configured to execute when the full email is received or at SMTP Transmission level. In SMTP Transmission filtering, emails are scanned whilst they are being received.

SMTP level filtering terminates the email's connection and therefore stops the download of the full email, economizing on bandwidth and processing resources. In this case the connection is terminated immediately and emails are not required to go through any other anti-spam filters.

IMPORTANT

To make the best of SMTP Transmission filtering, use it when GFI MailEssentials is installed on an Internet gateway or when it is the first server to receive emails from the Internet.

1. Go to **Anti-Spam > Filter Priority** and select the **SMTP Transmission Filtering** tab.



Screenshot 91: SMTP Transmission Filtering properties

2. Click **Switch** to toggle the Directory Harvesting filtering between:

Option	Description
Filtering on receiving full email	Filtering is done when the whole email is received.
Filtering during SMTP transmission	Filtering is done during SMTP transmission. If this option is chosen, the filter is always run before the other spam filters.

NOTE

The Greylist filter runs at SMTP Transmission level only.

3. Click **Apply**.

5.5 Spam Digest

The spam digest is a short report sent to an administrator or user via email. This report lists the total number of emails processed by GFI MailEssentials and the number of spam emails blocked over a specific period of time (since the last spam digest).

5.5.1 Administrator spam digest

1. Go to **Anti-Spam > Spam Digest**.

Administrator Digest Recipient Digest Recipient List

Enable and configure the administrator's spam email digest

The administrator's spam digest is an email sent to the administrator containing the total email processed and the total spam blocked per spam filter.

Send administrator spam digest

Options

Frequency Day Time

Daily 07:00

Digest Contents

Total count of processed email and spam

Total spam captured per spam filter

Screenshot 92: Spam digest properties/Administrator spam digest

2. From the **Administrator Digest** tab, click **Send administrator spam digest** to enable spam digest.
3. Configure the desired sending frequency (Daily, Weekly, Monthly) and specify a date and a time when email is sent.
4. Specify the digest content that will be sent in the email, either a **Total count of processed email and spam** or **Total spam captured per spam filter** or both.
5. Finalize settings by selecting **Apply**.

5.5.2 Recipient spam digest

1. Go to **Anti-Spam > Spam Digest**.

Administrator Digest	Recipient Digest	Recipient List
 Enable and configure the recipients' spam email digest		
<p>The recipient spam digest is an email sent to inbound domain recipients which contains, for the recipient's email, the total email processed, the total spam blocked per spam filter and the details of each spam email.</p>		
<input checked="" type="checkbox"/> Send recipient spam digest		
Options		
Frequency	Day	Time
Daily		07:00
Digest Contents		
<input checked="" type="checkbox"/> Total count of processed email and spam		
<input checked="" type="checkbox"/> Total spam captured per spam filter type		
<input type="checkbox"/> List of blocked spam (date/time, sender, subject)		

Screenshot 93: Recipient spam digest

2. From the **Recipient Digest** tab, select **Send recipient spam digest** to enable spam digest.
3. Configure the desired sending frequency (Daily, Weekly, Monthly) and specify a date and a time when email is sent.
4. Specify the digest content that will be sent in the email:
 - Total count of processed email and spam
 - Total spam captured per spam filter type
 - List of blocked spam or any combination of options as required.

Administrator Digest	Recipient Digest	Recipient List								
 <p>Specify which recipients should or should not receive the spam digest via email</p>										
<p>For the recipient digest, specify the inbound domain recipients that should or should not receive the spam digest</p> <p> <input checked="" type="radio"/> Only users listed below should receive the recipient spam digest <input type="radio"/> All users except the ones listed below will receive the recipient spam digest </p>										
<p>Email Address List</p> <table border="1"> <tr> <td><input type="text"/></td> <td><input type="button" value="Add"/></td> </tr> <tr> <td><input type="text"/></td> <td><input type="button" value="Delete"/></td> </tr> <tr> <td> <input type="button" value="Browse..."/> No file selected. </td> <td><input type="button" value="Import"/></td> </tr> <tr> <td colspan="2"><input type="button" value="Export"/></td> </tr> </table>			<input type="text"/>	<input type="button" value="Add"/>	<input type="text"/>	<input type="button" value="Delete"/>	<input type="button" value="Browse..."/> No file selected.	<input type="button" value="Import"/>	<input type="button" value="Export"/>	
<input type="text"/>	<input type="button" value="Add"/>									
<input type="text"/>	<input type="button" value="Delete"/>									
<input type="button" value="Browse..."/> No file selected.	<input type="button" value="Import"/>									
<input type="button" value="Export"/>										

Screenshot 94: Spam digest recipient list

5. Click on the **Recipients list** tab, add the users to receive the spam digest and select the method used to determine who should receive the spam digest. Available options are:

- Only users listed below should receive the recipient spam digest.
- All users except the ones listed below will receive the recipient spam digest.

NOTE

The required list of users can also be imported from a file in XML format in the same structure that GFI MailEssentials would export files.

6. Select **Apply** to finalize settings.

5.6 Anti-Spam settings

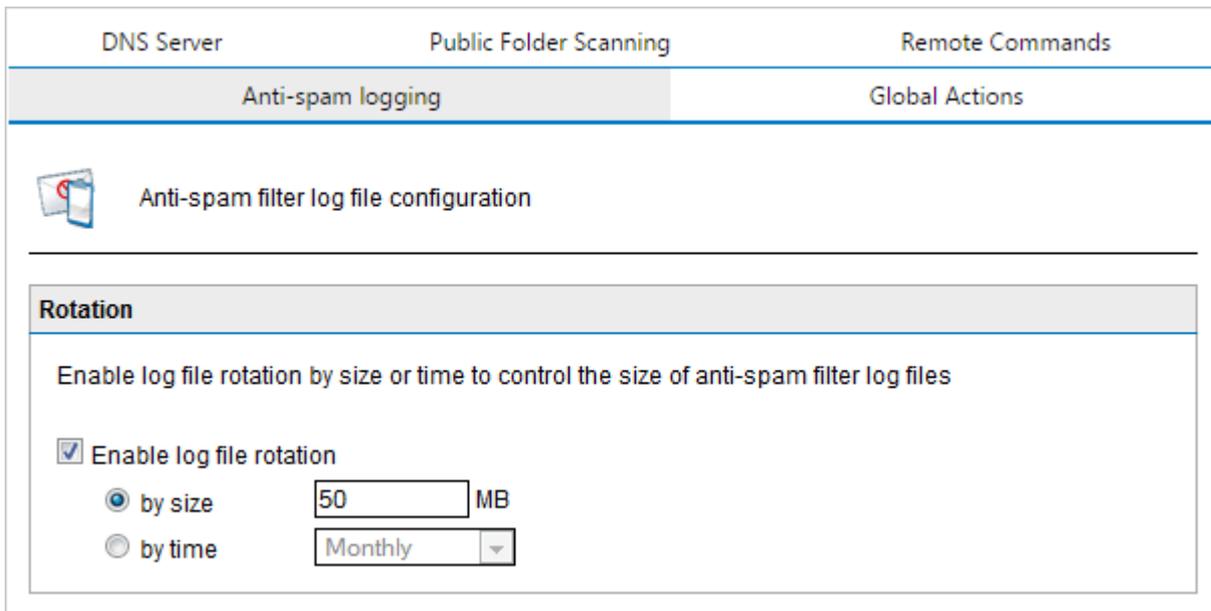
The following settings are configurable for anti-spam filters and emails blocked by anti-spam filters only.

5.6.1 Log file rotation

Over time, log files may become very large. GFI MailEssentials enables log rotation, where new log files are created periodically or when the log file reaches a specific size.

To enable log file rotation:

1. Go to **Anti-Spam > Anti-Spam Settings**.



Screenshot 95: Log file rotation

2. From the **Anti-spam logging** tab, select **Enable log file rotation** and specify the rotation condition (**by size** or **by time**).
3. Provide the size or time values and click **Apply**.

5.6.2 Anti-Spam Global Actions

A lot of spam is sent to email addresses that no longer exist. Generally, these emails are simply deleted however for troubleshooting or evaluation purposes, you might want to move these emails to a folder or forward them to a particular email address.

NOTE

This section only applies for installations on Microsoft® Exchange Server that have spam action **Move to subfolder of user's mailbox** enabled. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

On other mail servers, the anti-spam global actions tab will not appear.

Configuring Anti-spam global actions

1. Go to **Anti-Spam > Anti-Spam Settings**.

DNS Server	Public Folder Scanning	Remote Commands
Anti-spam logging	Global Actions	
 Specify global actions to be performed		
Actions Configures the actions that will be performed when spam cannot be moved to a user's Exchange folder because the user does not exist on the Exchange server		
<input type="radio"/> Delete		
<input type="radio"/> Forward to email address: <input type="text" value="Administrator@domaina.tcv"/>		
<input checked="" type="radio"/> Move to specified folder: <input type="text" value="C:\Program Files (x86)\GFI\MailEssentials\Antispam\globalactions"/>		
<input checked="" type="checkbox"/> Log occurrence to this file: <input type="text" value="C:\Program Files (x86)\GFI\MailEssentials\Antispam\logs\antispamglobal.log"/>		

Screenshot 96: Global actions

2. Select **Global Actions** tab and choose whether to:
 - » Delete the email
 - » Forward it to an email address
 - » Move it to a specified folder.
3. Select **Log occurrence to this file** to log these occurrences to a log file.
4. Click **Apply**.

5.6.3 DNS Server Settings

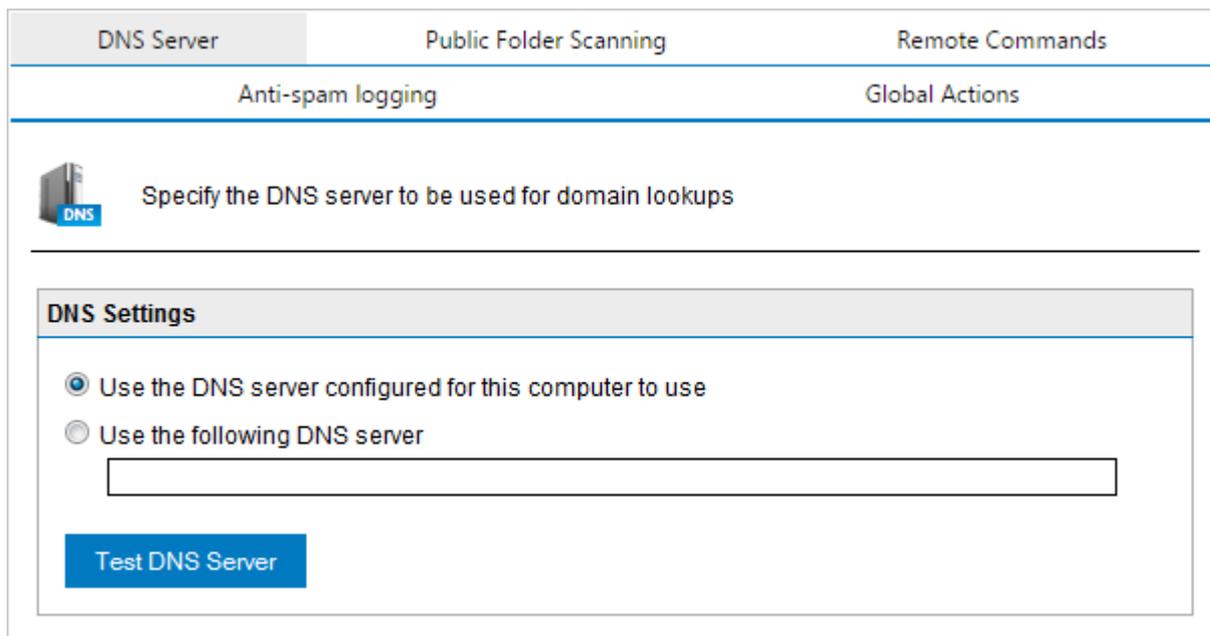
DNS Server settings are very important in GFI MailEssentials since a number of anti-spam filters, such as IP DNS Blocklist, URI DNS Blocklist and SpamRazer, perform domain lookups when filtering spam. It is critical for the performance of GFI MailEssentials to have quick and reliable DNS lookups. DNS problems can cause slow processing of emails and a decreased spam catching rate.

NOTE

Usage of Google DNS is known to cause slow processing of emails and a decreased spam catching rate. It is recommended to NOT use Google DNS (IPv4 8.8.8.8 or 8.8.4.4 or IPv6 2001:4860:4860::8888 or 2001:4860:4860::8844).

To configure DNS:

1. From the GFI MailEssentials Configuration, go to **Anti-Spam > Anti-Spam Settings**.



Screenshot 97: DNS server settings

1. From the **DNS Server** tab configure:

Option	Description
Use the DNS server configured for this computer to use	Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
Use the following DNS server	Select this option to specify a DNS server that is different than the one used by the local machine.

2. Click **Test DNS Server** to test connectivity with the specified DNS server. If unsuccessful, specify another DNS server.

3. Click **Apply**.

5.6.4 Remote Commands

Remote commands facilitate adding domains or email addresses to the Email Blocklist/Whitelist, as well as update the Bayesian filter with spam or ham (valid emails).

Remote commands work by sending an email to GFI MailEssentials. Addressing an email to **rcommands@mailessentials.com** (configurable) will have GFI MailEssentials recognize the email as containing remote commands and processes them as described below.

With remote commands, the following tasks can be achieved:

1. Add Spam or ham to the Bayesian Analysis database.
2. Add keywords either to the subject keyword checking feature or to the body keyword checking feature.
3. Add email addresses to the Email Blocklist filter and Whitelist.

Configuring remote commands

1. Click **Anti-Spam > Anti-Spam Settings**, go to **Remote Commands** tab and select **Enable remote commands**.
2. Edit the email address to which remote commands should be sent to.

NOTE

The email address should **NOT** be a local domain. The default address is **rcommands@mailessentials.com**. A mailbox for the configured address does not need to exist, but the domain-part of the address must consist of a real email address domain that returns a positive result to an MX-record lookup via DNS. This can also be a public email account that you can manage (for example Gmail or Yahoo mail)

3. Optionally, configure some basic security for remote commands:

- » A shared password to include in the email. For more information, refer to [Using remote commands](#) (page 156).
- » Which users are allowed to send emails with remote commands.

4. Click **Apply**.

Using remote commands

Remote commands can be sent via email to GFI MailEssentials from an email client within the domain. Conditions for sending remote commands:

- » The email must be in Plain Text format
- » The subject of the email is ignored
- » The following syntax must be used for all commands:

```
<command name>: <parameter1>, <parameter2>, <parameter3>, ... ;
```

For example: ADDBLIST: spammer@spam.com;

- » There can be more than one command in the body of an email with each command separated by a semi-colon (;).
- » If a password is configured for remote commands, enter the password in the first line using the following syntax:

```
PASSWORD: <shared password>;
```

- » Command names are case-sensitive and should be written in UPPERCASE only.
- » Conditions such as IF, AND, OR are not supported.
- » Remote commands can only be used to add entries and not delete or modify existing entries.

Keyword commands

Use keyword commands to add keywords or combination of keywords in the body or subject lists in Keyword Checking filter.

Available commands are:

- » ADDSUBJECT - Adds keywords specified to the subject keyword checking database.
 - Example: ADDSUBJECT: sex, porn, spam;
- » ADDBODY - Adds keywords specified to the body keyword checking database.
 - Example: ADDBODY: free, "100% free", "absolutely free";

NOTE

When configuring phrases other than a single words, enclose them in double quotes (" ").

Blocklist commands

Use blocklist commands to add a single email address or an entire domain to the email blocklist.

Available commands are:

» `ADDBLIST: <email>;`

- **Example:** `ADDBLIST: user@somewhere.com;`

NOTES

1. Add an entire domain to the blocklist by specifying a wildcard before the domain

Example: `ADDBLIST: *@domain.com;`

2. Wildcards cannot be used in domain names.

Example: `ADDBLIST: *@*.domain.com;` is invalid and will be rejected.

3. For security reasons, there can be only one `ADDBLIST` command in an email, and only one address can be specified as the command parameter. The parameter is either a user email or a domain:

Example: `ADDBLIST: spammer@spam.com;` or `ADDBLIST: *@spammers.org;`

Bayesian filter commands

Add spam email or valid email (ham) to the Bayesian filter database. Available commands are:

Command	Description
<code>ADDASSPAM</code>	Instructs Bayesian filter to classify email as spam.
<code>ADDASGOODMAIL</code>	Instructs Bayesian filter to classify email as HAM.

NOTE

These commands do not have parameters - the content of the email is the parameter.

Remote command logging

To keep track of changes made to the configuration database via remote commands, each email with remote commands (even if the email with remote commands was invalid) is saved in:

```
<GFI MailEssentials installation
path>\GFI\MailEssentials\AntiSpam\ADBRProcessed\
```

The file name of each email is formatted according to the following format:

- » `<sender_email_address>_SUCCESS_<timestamp>.eml` - in case of successful processing.
- » `<sender_email_address>_FAILED_<timestamp>.eml` - in case of failure.

NOTE

Timestamp is formatted as `yyyymmddhhmmss`.

5.6.5 Adding blocking reason to headers

GFI MailEssentials allows administrator to append the reason for blocking an email to its headers. The header of a blocked email will contain email blocked by one of the GFI MailEssentials spam filters.

For example:

```
X-GFIME-BLOCK-REASON: Found word(s) spammer in the subject
```

In the above example, the entry added to the email header indicates that the email was blocked by the [Spam Keyword Checking](#) filter because the subject contained the word `spammer`.

This option can be useful to troubleshoot false positives, whereby legitimate emails have been incorrectly classified as spam.

To add blocking reason to headers:

1. Go to **Anti-Spam > Anti-Spam Settings**.
2. From the **General** tab, check the option **Append an XHeader to the headers with the blocked reason**.
3. Click **Apply**.

5.7 SpamTag for Microsoft Outlook

The GFI MailEssentials SpamTag Plugin is an add-on for Microsoft Outlook that installs a toolbar on end users' machines, giving some control to users in management of spam emails. The plugin also synchronizes Microsoft Outlook Junk settings with GFI MailEssentials.

Whereas the Microsoft Outlook Junk functionality enables users to manage spam emails at client side, with the SpamTag plugin users can manage their spam emails at server level.

The GFI MailEssentials administrator can choose which of the following features and functions to enable:

- » Train the Bayesian Analysis filter
- » Add senders and/or domains to Personal Blocklist or Personal Whitelist
- » Automatically synchronize allowed and blocked senders in Microsoft Outlook with the GFI MailEssentials Personal Whitelist and Personal Blocklist respectively.
- » Automatically add users' contacts to the Personal Whitelist.

NOTE

Users assigned [full access](#) to GFI MailEssentials are also allowed to add senders/domains to the GFI MailEssentials Email Global Blocklist & Global Whitelist.

NOTE

When using SpamTag, install WCF HTTP Activation on the GFI MailEssentials server. To do this go to **Server Manager > Features > Add Feature > .NET Framework > WCF Activation > HTTP Activation**.

5.7.1 Choosing SpamTag features

The GFI MailEssentials administrator can configure which features SpamTag users can make use of. For example, the administrator can enable users to add senders to personal whitelist, but disable adding of domains to the personal whitelist. SpamTag can also be configured to override the Microsoft Outlook Junk features.

To configure SpamTag features:

1. Go to **Anti-Spam > SpamTag**.

Buttons	Advanced
 GFI MailEssentials SpamTag Configuration	
<p>GFI MailEssentials SpamTag is a Microsoft Outlook add-on which provides end users with buttons for classifying spam and legitimate email. For instructions on deploying the SpamTag, click here.</p> <p>Configure the functionality provided to end users in SpamTag:</p>	
Spam Button	
<p><input checked="" type="checkbox"/> Enable SPAM button The SPAM button is used for training the Bayesian filter using SPAM email</p> <p><input checked="" type="checkbox"/> Move processed SPAM to Junk Email folder</p> <p>Specify which Personal Blocklist options to allow:</p> <p><input type="checkbox"/> Allow setting sender in Personal Blocklist</p> <p><input type="checkbox"/> Allow setting sender domain in Personal Blocklist</p>	
Not Spam Button	
<p><input checked="" type="checkbox"/> Enable NOT SPAM button The NOT SPAM button is used for training the Bayesian filter with legitimate email</p> <p><input checked="" type="checkbox"/> Move processed legitimate email to Inbox folder</p> <p>Specify which Personal Whitelist options to allow:</p> <p><input checked="" type="checkbox"/> Allow setting sender in Personal Whitelist</p> <p><input checked="" type="checkbox"/> Allow setting sender domain in Personal Whitelist</p> <p><input checked="" type="checkbox"/> Allow setting discussion list address in Personal Whitelist</p>	

2. From the **Spam Button** area configure the features related to false-negatives, that is, when spam emails are not detected as spam:

Option	Description
Enable SPAM button	The Spam button is shown in SpamTag and when clicked, the selected email trains the Bayesian Analysis filter.
Move processed SPAM to Junk Email folder	When clicking Spam , the selected email is automatically moved to the Microsoft Outlook Junk E-mail folder.
Allow setting sender in Personal Blocklist	A sub-option is shown under Spam button that enables users to add the sender's email address to their Personal Blocklist. To use this option, the Personal Blocklist must be enabled.
Allow setting sender domain in Personal Blocklist	A sub-option is shown under Spam button that enables users to add the sender's domain to their Personal Blocklist. To use this option, the Personal Blocklist must be enabled.

3. From the **Not Spam Button** area configure the features related to false-positives, that is, when legitimate emails are incorrectly identified as spam.:

Option	Description
Enable NOT SPAM button	The Not Spam button is shown in SpamTag and when clicked, the selected email trains the Bayesian Analysis filter.
Move processed legitimate email to Inbox folder	When clicking Not Spam , the selected email is automatically moved to the Inbox folder.
Allow setting sender in Personal Whitelist	A sub-option is shown under Not Spam button that enables users to add the sender's email address to their Personal Whitelist. To enable this option, the Personal Whitelist must be enabled.
Allow setting sender domain in Personal Whitelist	A sub-option is shown under Not Spam button that enables users to add the sender's domain to their Personal Whitelist. To enable this option, the Personal Whitelist must be enabled.
Allow setting discussion list address in Personal Whitelist	A sub-option is shown under Not Spam button that enables users to whitelist newsletters/discussion lists. To enable this option, the Personal Whitelist must be enabled.

4. From the **Advanced** tab, configure the following advanced options.

Option	Description
Import Outlook Junk Settings to Personal Blocklist and Personal Whitelist	Imports the addresses listed in Microsoft Outlook Safe Senders and Blocked Senders into the GFI MailEssentials Personal Whitelist and Personal Blocklist. The list of Safe Senders and Blocked Senders in Microsoft Outlook is available from Junk > Junk e-mail options . NOTE: Imports are done automatically in the background by SpamTag every 2 hours and the user does not configure or see any options on screen. NOTE: When the user uses Microsoft Outlook that is installed on a battery-powered device, such as a laptop or tablet, automatic synchronization is not done to economize on battery life.
Import Outlook contacts to Personal Whitelist	Imports the list of Microsoft Outlook contacts to the Personal Whitelist. NOTE: Imports are done automatically in the background by SpamTag every 2 hours and the user does not configure or see any options on screen. NOTE: When the user uses Microsoft Outlook that is installed on a battery-powered device, such as a laptop or tablet, automatic synchronization is not done to economize on battery life.
Override Microsoft Outlook Junk	When selecting this option, the options that are enabled in SpamTag override the equivalent settings in Microsoft Outlook Junk, to ensure that only one anti-spam management system is utilized on client-side. When users use a Microsoft Outlook Junk option, a SpamTag function is run instead. For example if users click Never Block Sender in Outlook Junk, the Not Spam function of SpamTag is run instead. NOTE: If a particular option is not enabled in SpamTag and user utilizes the equivalent function in Outlook, no action is taken when the Outlook Junk function is used. For example, if Not Spam button is not enabled, nothing will happen when users click Never Block Sender .
Hide the Console button	Hides the Console button from the SpamTag toolbar. No direct access to the GFI MailEssentials console is provided but users can still log in by manually typing the URL in a browser. The settings provided to the user in the GFI MailEssentials console depend on Active Directory permissions or other custom Access Control settings. For more information, refer to Access Control (page 236).

5. Click **Apply**.

IMPORTANT

SpamTag checks which features are enabled or disabled in GFI MailEssentials when Microsoft Outlook starts. After changing any of the above settings, Microsoft Outlook needs to be restarted to apply changes.

5.7.2 SpamTag requirements

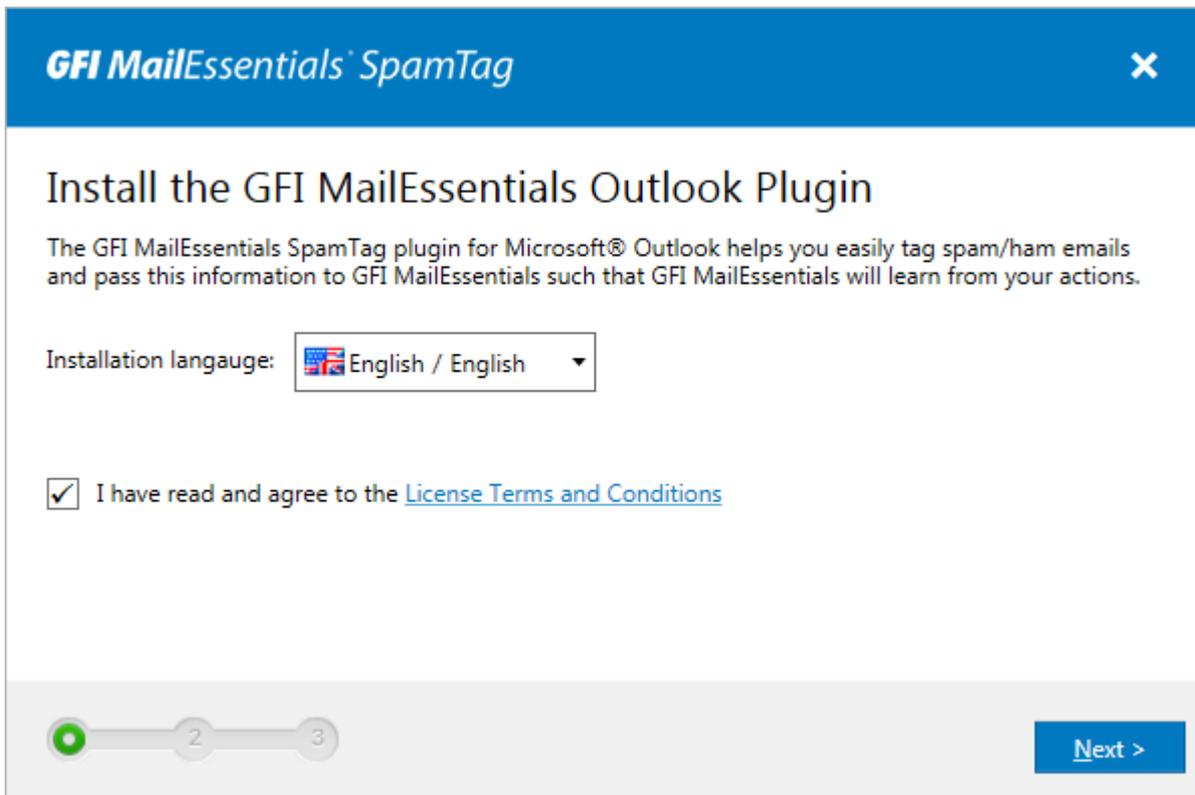
The machines where to install SpamTag must meet or exceed the following specifications:

Hardware	<ul style="list-style-type: none">» Processor - 1Ghz or more» Memory - Minimum 512MB, Recommended 2GB» Physical Storage - 50MB physical storage dedicated for SpamTag
Supported operating systems	<ul style="list-style-type: none">» Windows® 10» Windows® 8.1» Windows® 7» Windows® Server 2016» Windows® Server 2012 R2» Windows® Server 2012» Windows® Server 2008 R2
Supported Microsoft Outlook® Versions	<ul style="list-style-type: none">» Microsoft Outlook® 2016» Microsoft Outlook® 2013» Microsoft Outlook® 2010
Connection with GFI MailEssentials	SpamTag connects with GFI MailEssentials on port 80 over HTTP. To confirm connection, from the client's browser ensure that you can open the GFI MailEssentials URL.
Other software	Microsoft .Net Framework 4 - this is downloaded and installed automatically if not found.

5.7.3 Installing SpamTag manually

Run the SpamTag installer on client's machines to manually install SpamTag.

1. Get the installer from <GFI MailEssentials installation folder>/Outlook.
2. Copy **GFIMailEssentialsSpamTag.exe** to the machine where to install SpamTag.
3. Close Microsoft Outlook.
4. Right-click the installer and select **Run as administrator**.
5. In the first screen, select the language for the installation.



Screenshot 98: SpamTag installation language and license terms

6. Read the **License Terms and Conditions** and if you agree, select **I have read and agree to the License Terms and Conditions**. Click **Next**.
 7. Key in the URL used to connect to GFI MailEssentials. For example: `http://192.168.1.2/MailEssentials` or `http://mygfiserver.mydomain.com/MailEssentials`. Wait for the installer to verify connection with GFI MailEssentials via the specified URL and click **Next**.
 8. Specify the location where to install SpamTag and click **Install**.
 9. On completion click **Finish**.
 10. Start Microsoft Outlook and key in the user's credentials.
- SpamTag is now available in the Microsoft Outlook Home ribbon.
- For more information, click **Help** from SpamTag.

5.7.4 Installing SpamTag via GPO

Use Group Policy (GPO) to install GFI MailEssentials SpamTag on numerous machines at one go. The following procedure is supported on Microsoft Server Windows 2008 R2 or later:

Step 1: Prepare MSI and ADM files

1. From the GFI MailEssentials server, go to the GFI MailEssentials installation folder and open the **Outlook** sub-folder.
2. Copy the MSI and the ADM files to a shared folder that is accessible by all users that will have SpamTag installed. Ensure that users have at least Read permissions to the folder.

Step 2: Deploy SpamTag

1. On the domain controller, open **Server Manager**.
2. Expand **Server Manager > Features > Group Policy Management > Forest > Domains > domain name**. Right-click the domain name or an organizational unit and select **Create a GPO in this domain, and Link it here...**
3. Enter a name for the new Group Policy Object (GPO). For example: `GFI MailEssentials SpamTag`. Click **OK**.
4. Right-click the newly created GPO and click **Edit**.
5. In the **Group Policy Management Editor** window, expand **Computer Configuration > Policies > Software settings > Software Installation**. Right click **Software Installation > New > Package** to configure the GPO to install on log in.
6. Enter the network path of the shared folder that contains the SpamTag MSI package. Click **OK**.

NOTE

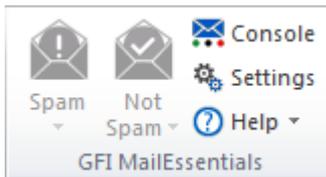
When selecting the location of the MSI file ensure that this is done through 'My network locations' so that the share name in GFI MailEssentials includes the full network share location rather than the local path.

7. In the **Deploy Software** pop-up, select **Assigned** and click **OK**.
8. The new package is now added under **Software Installation**.
9. Right-click **Computer Configuration > Policies > Administrative Templates** and select **All Tasks > Add/Remove Templates**.
10. Click **Add**, browse to the shared folder containing `spamtag.adm`.
11. Click **Close**.
12. Go to **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates (ADM) > GFI MailEssentials SpamTag**.
13. From the right pane, double click `DefaultWebServiceUrl` policy and select **Enabled**. In **GFI MailEssentials Portal Website Address** key in the public URL of GFI MailEssentials. Machines that deploys SpamTag must be able to connect to this URL via their web browser, otherwise SpamTag cannot connect with GFI MailEssentials.
14. Optionally, click **Previous Setting** to change the SpamTag default language. Click **Enabled** and modify the **Default Language** value.
15. Click **OK**.

Step 3: Verify installation

The set up should now be complete. SpamTag will be installed the next time each client machine is started. To check installation, verify that the SpamTag toolbar is visible in Microsoft Outlook® and that it connects successfully to GFI MailEssentials.

5.7.5 Using SpamTag



Screenshot 99: SpamTag in Microsoft Outlook 2010

For information on how to use SpamTag refer to the built-in help by clicking **Help** in SpamTag.

The help automatically shows information related to the features that are enabled by the administrator in SpamTag settings page.

5.8 Public Folder Scanning

Spamming techniques are continuously evolving and consequently you might encounter instances when spam still makes it through anti-spam filters to the recipient's Inbox. Through public folder scanning, users can manually classify email as spam and 'teach' GFI MailEssentials spam patterns to classify similar email as spam. Emails can also be added to the whitelist.

IMPORTANT

It is highly recommended to use GFI MailEssentials SpamTag instead of Public Folder Scanning when network clients use Microsoft Outlook as their email client. For more information, refer to [SpamTag for Microsoft Outlook](#) (page 158).

How it works:

1. When an incorrectly classified email (false positive or false negative) is identified, users drag and drop the email to the appropriate GFI AntiSpam public folder. For more information, refer to [Using Public folder scanning](#) (page 166).
2. Public folder scanning retrieves emails from the GFI AntiSpam public folders and adds them to the HAM/SPAM databases.

The GFI Antispam public folders must be created and configured on the mail server. For more information, refer to [Enabling Public folder Scanning](#) (page 164).

5.8.1 Enabling Public folder Scanning

This topic describes how to enable Public Folder Scanning in GFI MailEssentials and configure a dedicated public folder in Microsoft Exchange with the required permissions.

- » [Step 1: Enabling Public folder scanning in GFI MailEssentials](#)
- » [Step 2: Configure a dedicated user account for Microsoft® Exchange](#)
- » [Step 3: Hiding user posts in GFI AntiSpam folders](#)

Step 1: Enabling Public folder scanning in GFI MailEssentials

1. From the GFI MailEssentials configuration console go to **Anti-spam > Anti-Spam > Anti-Spam Settings**. Select **Public folder Scanning** tab.
2. Select **Enable Public folder Scanning** and from **Poll public folder via** list select:

- » **Exchange Server 2003** - Choose IMAP or WebDAV.
- » **Exchange Server 2007** - Choose WebDAV or Web Services.
- » **Exchange Server 2010/2013/2016** - Choose Web Services.

Options are described in the table below.

Option	Description
IMAP	Requires Microsoft® Exchange IMAP service. IMAP enables remote scanning of public folders and works well in environments running firewalls. In addition, IMAP can be used with other mail servers that support IMAP. Parameters required are: <ul style="list-style-type: none"> » Mail server name » Port number (default IMAP port is 143) » Username/password. Use an administrative account with permission to create Public folders. » Select the Use SSL option to use a secure connection
WebDAV	Specify mail server name, port (default WebDAV port is 80), username/password and domain. To use a secure connection select the Use SSL checkbox. By default, public folders are accessible under the 'public' virtual directory. If this has been changed, specify the correct virtual directory name to access the public folders by editing the text in the URL box.
Web Services	Specify the following details: <ul style="list-style-type: none"> » Server - mail server name » Domain - use the local domain. If both a local and a public domain exist, always use the local domain. » Port - default Web Services port (80, or 443 if using SSL). » Username/password - use credentials with administrative privileges or create a dedicated user from Microsoft® Exchange Management Shell by entering the following command to add the appropriate permissions: <pre>Add-ADPermission -identity "Mailbox Store" -User NewUser -AccessRights GenericALL</pre> Replace <i>Mailbox Store</i> with the name of the mailbox store that contains the user mailboxes and <i>NewUser</i> with the username of the created user. » Use SSL - Select this option if Exchange Web Services requires a secure connection. By default, Web Services requires SSL. » URL - By default, public folders are accessible under the 'EWS/exchange.asmx' virtual directory. If this has been changed, specify the correct virtual directory name to access the public folders by editing the text in the URL box. It is recommended to test the settings manually, by loading the URL in a web browser. This should load an XML formatted file, named services.wsdl.

3. Click **Apply**.

4. Click **Test** if you are setting up IMAP, WebDAV or Web Services. On screen notification will confirm success/failure. If the test fails, verify/update credentials and re-test.

5. Click **Scan Now** to automatically create the Public folders.

Step 2: Configure a dedicated user account for Microsoft® Exchange Public folders

For security reasons, it is recommended that when GFI MailEssentials is installed in a DMZ, a dedicated user account is created to retrieve or scan emails from public folders.

Microsoft® Exchange Server 2007 or later

1. Create a new Active Directory user.
2. Login to the Microsoft® Exchange Server using administrative privileges.
3. Open **Microsoft® Exchange Management Shell** and key in following command:

```
Get-PublicFolder -Identity "\GFI AntiSpam Folders" -Recurse | ForEach-Object
{Add-PublicFolderClientPermission -Identity $_.Identity -User "USERNAME" -
AccessRights owner}
```

Replace USERNAME with the username of a dedicated Active Directory user that has 'owner' access rights on the GFI AntiSpam Public folders. For example:

```
Get-PublicFolder -Identity "\GFI AntiSpam Folders" -Recurse | ForEach-Object
{Add-PublicFolderClientPermission -Identity $_.Identity -User "mesuser" -
AccessRights owner}
```

Step 3: Hiding user posts in GFI AntiSpam folders

For privacy and security purposes, it is highly recommended that you hide user posts made on GFI AntiSpam folders. This way, email users will only be able to post to the folders without viewing existing posts (not even the ones they posted themselves).

For more information on how to do this refer to http://go.gfi.com/?pageid=me_phideposts

5.8.2 Using Public folder scanning

Reviewing spam email

1. When spam emails are delivered to the user's mailbox (in Inbox, Junk E-mail folder or a custom folder) instruct the individual email users to periodically review spam emails.
2. There may be cases where legitimate emails are incorrectly identified as spam (false positives). For more information, refer to [Managing legitimate email](#) (page 166).
3. There may also be cases where spam emails are not detected (false negatives). For more information, refer to [Managing spam](#) (page 167).

Managing legitimate email

As with any anti-spam solution, GFI MailEssentials might require some time until the optimal anti-spam filtering conditions are achieved. In cases where this is not yet achieved, there might be instances where legitimate email is identified as spam.

In such cases users should add emails incorrectly identified as spam to **Add to whitelist** and **This is legitimate email** folders to 'teach' GFI MailEssentials that the email in question is not spam.

NOTES

1. In Microsoft® Outlook, dragging and dropping email moves the email to the selected folder. To retain a copy of the email, hold down the CTRL key to copy the email rather than moving it.
2. Detailed information how to create the GFI AntiSpam folders is included in this manual. For more information, refer to [Enabling Public folder Scanning](#) (page 164).

Adding senders to the whitelist

1. In the public folders list of the mail client (example, Microsoft® Outlook), locate the **GFI AntiSpam Folders > Add to whitelist** public folder.
2. Drag and drop emails or newsletters to **Add to whitelist** public folder.

Adding discussion lists to the whitelist

Emails sent to discussions lists have the discussion list's email address as the recipient of the message. To

receive emails from specific discussion lists, the list's email address needs to be whitelisted.

1. Using your email client, (example, Microsoft® Outlook), locate the **GFI AntiSpam Folders > I want this Discussion list** public folder.
2. Drag and drop discussion lists to the **I want this Discussion list** public folder.

Using legitimate emails to train the Bayesian filter

1. In the public folders of the mail client (example, Microsoft® Outlook), locate the **GFI AntiSpam Folders > This is legitimate email** public folder.
2. Drag and drop emails to the **This is legitimate email** folder.

Managing spam

While GFI MailEssentials starts identifying spam emails right out of the box, there may be instances where spam makes it through undetected to the users mailbox. Typically this might be either due to configuration settings that have not yet been performed or to new forms of email spam to which GFI MailEssentials has not yet adapted itself. In both cases, these situations are resolved when GFI MailEssentials is configured to capture such spam.

In these cases users should add such emails to **Add to blacklist** and **This is spam email** folders to 'teach' GFI MailEssentials that the email in question is spam.

NOTES

1. In Microsoft® Outlook, dragging and dropping email moves the email to the selected folder. To retain a copy of the email, hold down the CTRL key to copy the email rather than moving it.
2. Detailed information how to create the GFI AntiSpam folders is included in this manual. For more information, refer to [Enabling Public folder Scanning](#) (page 164).

Adding senders to the Email Blocklist

1. In the public folders of the mail client (example, Microsoft® Outlook), locate the **GFI AntiSpam Folders > Add to blacklist** public folder.
2. Drag and drop emails to the **Add to blacklist** public folder.

Use spam emails to 'teach' the Bayesian filter

1. In the public folders of the mail client (example, Microsoft® Outlook), locate the **GFI AntiSpam Folders > This is spam email** public folder.
2. Drag and drop the spam email to the **This is spam email** folder.

6 Content Filtering

Content Filtering engines enable administrators to control the content of emails. These engines scan the content of emails and attachments, and block emails containing content matching the content filtering rules.

Topics in this chapter:

6.1 Keyword Filtering	168
6.2 Attachment Filtering	174
6.3 Advanced Content Filtering	180
6.4 Decompression Engine	185

6.1 Keyword Filtering

Keyword Filtering enables you to set up rules that filter emails with particular keywords or a combination of keywords in the body or subject of the email. A rule is composed of:

- » Keywords to block in the email body, subject or attachment
- » Actions to take when a keyword is found
- » The users to which a rule applies.

To configure content rules, navigate to **Content Filtering > Keyword Filtering**. This page allows you to view, create, enable, disable or delete rules.

6.1.1 Creating a Keyword Filtering rule

To create a Keyword filtering rule follow the steps listed below:

- » [Step 1: Configuring basic rule setting](#)
- » [Step 2: Configuring terms to block](#)
- » [Step 3: Configuring the actions to take on detected emails](#)
- » [Step 4: Specifying the users to whom to apply this rule](#)

Step 1: Configuring basic rule settings

1. Go to **Content Filtering > Keyword Filtering** and select **Add Rule...**
2. Specify a name for the rule in the **Rule name** text box.
3. Select whether to scan inbound, outbound and/or internal emails.

Option	Description
Scan Inbound SMTP Email	Select this option to scan incoming emails
Scan Outbound SMTP Email	Select this option to scan outgoing emails

Option	Description
Check Internal emails	Select this option to scan internal emails. NOTE This option is only available when GFI MailEssentials is installed on the Microsoft® Exchange server

4. To block emails encrypted using PGP technology, select **Block PGP encrypted emails**.

NOTE

PGP encryption is a public-key cryptosystem often used to encrypt emails.

Step 2: Configuring terms to block

1. Select the **Body** tab to specify the keywords in the email body to block.
2. Select **Block emails if content is found matching these conditions (message body/attachments)** checkbox to enable scanning of body for keywords.

General	Body	Subject	Actions	Users/Folders				
 Configure keyword filtering options for checking the content of the message body and attachments.								
<input checked="" type="checkbox"/> Block emails if content is found matching these conditions (message body/attachments)								
Condition entry								
Edit condition: <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="flex: 1; border: 1px solid #ccc; height: 60px; margin-right: 10px;"></div> <div style="display: flex; flex-direction: column; gap: 5px;"> <div style="background-color: #0070c0; color: white; padding: 5px; text-align: center;">AND</div> <div style="background-color: #0070c0; color: white; padding: 5px; text-align: center;">OR</div> <div style="background-color: #0070c0; color: white; padding: 5px; text-align: center;">AND NOT</div> <div style="background-color: #0070c0; color: white; padding: 5px; text-align: center;">OR NOT</div> </div> </div> <div style="display: flex; margin-top: 10px; gap: 10px;"> <div style="background-color: #0070c0; color: white; padding: 5px 15px; border-radius: 3px;">Add Condition</div> <div style="background-color: #0070c0; color: white; padding: 5px 15px; border-radius: 3px;">Update</div> </div>								
Conditions list								
<p>All these conditions are validated as a single condition using the OR operator for each entry. Clicking on an entry will copy the condition text in the condition entry above for editing.</p> <p>Current conditions:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30px;"></th> <th>Condition</th> </tr> </thead> <tbody> <tr style="background-color: #e6f2ff;"> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>TEST</td> </tr> </tbody> </table> <div style="display: flex; justify-content: flex-end; margin-top: 10px; gap: 10px;"> <div style="background-color: #0070c0; color: white; padding: 5px 15px; border-radius: 3px;">Remove</div> <div style="background-color: #0070c0; color: white; padding: 5px 15px; border-radius: 3px;">Export</div> </div> <p>Specify the full path and filename of the file to use for importing:</p> <div style="border: 1px solid #ccc; height: 20px; width: 100%; margin-bottom: 5px;"></div> <div style="display: flex; justify-content: flex-end; margin-top: 5px;"> <div style="background-color: #0070c0; color: white; padding: 5px 15px; border-radius: 3px;">Import</div> </div> <p><small>Note: Import of list data cannot be performed unless the import list is on the server where GFI MailEssentials is installed.</small></p>						Condition	<input checked="" type="checkbox"/>	TEST
	Condition							
<input checked="" type="checkbox"/>	TEST							

Screenshot 100: Content Filtering: Body Tab - setting conditions

3. From the **Condition entry** area, key in keywords to block in the **Edit condition** box. You can also use conditions **AND**, **OR**, **AND NOT** and **OR NOT** to use a combinations of keywords.

4. To add the keyword or combination of keywords keyed in, click **Add Condition**.

To modify an entry in the **Conditions** list, select it and make the required changes in the **Condition entry** box. To remove an entry from the **Conditions** list, select it and click **Remove**.

Click **Update** to apply changes.

Screenshot 101: Content Filtering: Body Tab- configuring other options

5. (Optional) From the **Options** area, configure the following settings:

Option	Description
Match whole words only	Block emails when the keywords specified match whole words.
Apply above conditions to attachments	Select this option to apply this rule also to text in attachments. In the Attachment filtering area specify the attachments' file extension (for example, .doc) to apply or exclude from this rule.

6. Select the **Subject** tab to specify keywords to block in the email subject.

7. From the **Condition entry** area, key in keywords to block in the **Edit condition** box. You can also use conditions **AND**, **OR**, **AND NOT** and **OR NOT** to use a combinations of keywords.

8. To add the keyword or combination of keywords keyed in, click **Add Condition**.

To modify an entry in the **Conditions** list, select it and make the required changes in the **Condition entry** box. To remove an entry from the **Conditions** list, select it and click **Remove**.

Click **Update** to apply changes.

9. From the **Options** area, configure how keywords are matched. Select **Match whole words only** to block emails where the keywords specified match whole words in the subject

Step 3: Configuring the actions to take on detected emails

1. Click the **Actions** tab to configure what should be done when this rule is triggered.

2. To block an email that matches the rule conditions, select **Block email and perform this action** and select one of the following options:

Option	Description
Quarantine email	Stores blocked emails in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 191).
Delete email	Deletes blocked emails.
Move to folder on disk	Moves the email to a folder on disk. Key in the full folder path where to store blocked emails.

IMPORTANT

Actions always affect the whole email containing the blocked content, even if there is other content (such as attachments) that do not trigger this rule.

3. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients but with the malicious content removed.

4. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

5. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation
path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

Step 4: Specifying users to whom this rule applies

1. By default, the rule is applied to all email users. GFI MailEssentials, however, allows you to apply this rule to a custom list of email users specified in the Users / Folders tab.

2. Specify the users to apply this rule to.

Option	Description
Only this list	Apply this rule to a custom list of email users, groups or public folders.
All except this list	Apply this rule to all email users except for the users, groups or public folders specified in the list.

3. To add email users, user groups and/or public folders to the list, click **Add**.

User Lookups

 **Select User/Group**

	Name	Email Address	Email Aliases
<input checked="" type="checkbox"/>	 John Smith	jsmith@domaina.tcv	No other aliases

Screenshot 102: Add users to a Content Filtering rule

4. In the **User Lookups** window, specify the name of the email user/user group or public folder that you wish to add to the list and click **Check Names**. Matching users, groups or public folders are listed underneath.

NOTE

You do not need to input the full name of the users, groups or public folder. It is enough to enter part of the name. GFI MailEssentials will list all the names that contain the specified characters. For example, if you input `sco`, GFI MailEssentials will return names such as `Scott Adams` and `Freeman Prescott`, if they are available.

5. Select the check box next to the name(s) that you want to add to the list and click **OK**.

NOTE

To remove entries from the list, select the user/user group/public folder you want to remove and click **Remove**.

6. Repeat steps 3 to 5 to add all the required users to the list.

7. Click **Apply**.

6.1.2 Enabling/disabling Rules

To enable/disable content filtering rules:

1. Go to **Content Filtering > Keyword Filtering**.
2. From the **Content Filtering** page, select the checkbox of the rule(s) to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly

6.1.3 Removing content filtering rules

WARNING

Deleted rules are not recoverable. If in doubt, it is recommended to disable a rule.

1. Go to **Content Filtering > Keyword Filtering**.
2. From the Content Filtering page, select the checkbox of the rule(s) that you want to remove.

3. Click **Remove Selected**.

6.1.4 Modifying an existing rule

1. Go to **Content Filtering > Keyword Filtering**.
2. From the **Content Filtering** page, click the name of the rule to modify.
3. Perform the required changes in the rule properties and click **Apply**.

6.1.5 Changing rule priority

Content Filtering rules are applied in the same order, from top to bottom as they are listed in the Content Filtering page (that is, rule with priority value 1 is checked first). To change the sequence/priority of rules:

1. Go to **Content Filtering > Keyword Filtering**.
2. From the **Content Filtering** page, click the **↑** (up) or **↓** (down) arrows to respectively increase or decrease the priority of the selected rule.
3. Repeat step 2 until rules are placed in the desired sequence.

6.2 Attachment Filtering

Attachment Filtering allows you to set up rules to filter what types of email attachments to allow and block on the mail server. A rule is composed of:

- » Attachment types to block
- » Actions to take when a matching attachment is found
- » The users to which a rule applies.

To configure attachment rules, navigate to **Content Filtering > Attachment Filtering**. This page allows you to view, create, enable, disable or delete rules.

6.2.1 Creating an Attachment Filtering rule

To create an Attachment filtering rule follow the steps listed below:

- » **Step 1: Configuring basic rule settings and the terms to block**
- » **Step 2: Configuring the actions to take on detected emails**
- » **Step 3: Specifying the users to whom to apply this rule**

Step 1: Configuring basic rule settings and the terms to block

1. Navigate to **Content Filtering > Attachment Filtering** node.
2. Click **Add Rule...**

General	Actions	Users/Folders
 Attachment Filtering		
Rule display name		
Rule name: <input type="text" value="New Attachment Checking Rule"/>		
Email checking		
<input checked="" type="checkbox"/> Check inbound emails <input checked="" type="checkbox"/> Check outbound emails <input checked="" type="checkbox"/> Check internal emails		
Attachment blocking		
<input type="radio"/> Block all <input checked="" type="radio"/> Block this list <input type="checkbox"/> Do not block attachments smaller than the following size: <input type="text" value="0"/> KB <input type="radio"/> Block all except this list		
Enter filenames with optional wildcards: (eg. *.vbs) (eg. *letter.vbs) (eg. happy*.exe) (eg. orders.mdb)		
<input type="text"/>	<input type="button" value="Add"/>	
<input type="text"/>	<input type="button" value="Remove Selected"/>	
<input type="text"/>	<input type="button" value="Export"/>	
Specify the full path and filename of the file to use for importing:		
<input type="button" value="Browse..."/>	<input type="text" value="No file selected."/>	<input type="button" value="Import"/>

Screenshot 103: Attachment Filtering: General Tab

- Specify a name for the rule in the **Rule name** text box.
- Select whether to scan inbound, outbound and/or internal emails.

Option	Description
Scan Inbound SMTP Email	Select this option to scan incoming emails

Option	Description
Scan Outbound SMTP Email	Select this option to scan outgoing emails
Check Internal emails	Select this option to scan internal emails.
	<p>NOTE This option is only available when GFI MailEssentials is installed on the Microsoft® Exchange server</p>

5. In the **Attachment Blocking** area, specify the types of attachments to block:

Option	Description
Block all	Block all email attachments of any type.
Block this list	Block a custom list of attachment types. Key in a filename and/or attachment type to block in the Enter filename with optional wildcards text box and click Add . Repeat this step for all filenames and/or attachment types to block.
Do not block attachments smaller than the following size:	Select this option to allow attachment types in the list that are smaller than a particular size. Specify the size (in KB) in the text box provided.
Block all except this list	Block all attachments except the ones specified in the list. Key in a filename and/or attachment type to allow in the Enter filename with optional wildcards text box and click Add . Repeat this step for all filenames and/or attachment types to exclude.

NOTE

When specifying filenames and/or attachment types, you can use asterisk (*) wildcards. For example, specifying `*orders*.mdb` refers to all files of type `mdb` that contain the string `orders` in the file name. Specifying `*.jpg` will block all images of type `jpg`.

NOTE

To remove an entry from the list, select it and click **Remove Selected**.

6. You can also block attachments that have a size bigger than a particular size. To enable this option, from the **Options** area select **Block all attachments greater than the following size** and specify the maximum attachment size (in KB).

NOTE

This feature blocks all attachments with a file size bigger than the one specified irrespective if the attachment matches an entry in the **Attachment blocking** list.

Step 2: Configuring the actions to take on detected emails

1. Click the **Actions** tab to configure what happens when this rule is triggered.

General	Actions	Users/Folders
 Attachment Filtering Actions		
Actions <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Block attachment and perform this action: <ul style="list-style-type: none"> <input checked="" type="radio"/> Quarantine email <input type="radio"/> Delete email <input type="radio"/> Move to folder on disk: <input type="text"/> <input type="checkbox"/> Send a sanitized copy of the original email to recipient(s) 		
Notification options <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Notify administrator <input checked="" type="checkbox"/> Notify local user 		
Logging options <ul style="list-style-type: none"> <input type="checkbox"/> Log rule occurrence to this file: <input type="text"/> 		

Screenshot 104: Attachment Filtering: Actions Tab

2. To block an email that matches the rule conditions, select **Block attachment and perform this action** and select one of the following options:

Option	Description
Quarantine email	Stores blocked emails in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 191).
Delete email	Deletes blocked emails.
Move to folder on disk	Moves the email to a folder on disk. Key in the full folder path where to store blocked emails.

IMPORTANT

Actions always affect the whole email containing the blocked content, even if there is other content (such as attachments) that do not trigger this rule.

3. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients but with the malicious content removed.

4. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

5. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

Step 3: Specifying users to whom this rule applies

1. By default, the rule is applied to all email users. GFI MailEssentials, however, allows you to apply this rule to a custom list of email users specified in the Users / Folders tab.

2. Specify the users to apply this rule to.

Option	Description
Only this list	Apply this rule to a custom list of email users, groups or public folders.
All except this list	Apply this rule to all email users except for the users, groups or public folders specified in the list.

3. To add email users, user groups and/or public folders to the list, click **Add**.

User Lookups		
Select User/Group		
<input type="text"/>	<input type="button" value="Check Names"/>	<input type="button" value="Submit"/>
<input type="checkbox"/>	Name	Email Address
<input checked="" type="checkbox"/>	John Smith	jsmith@domaina.tcv
		Email Aliases
		No other aliases

Screenshot 105: Add users to a Content Filtering rule

4. In the **User Lookups** window, specify the name of the email user/user group or public folder that you wish to add to the list and click **Check Names**. Matching users, groups or public folders are listed underneath.

NOTE

You do not need to input the full name of the users, groups or public folder. It is enough to enter part of the name. GFI MailEssentials will list all the names that contain the specified characters. For example, if you input `sco`, GFI MailEssentials will return names such as `Scott Adams` and `Freeman Prescott`, if they are available.

5. Select the check box next to the name(s) that you want to add to the list and click **OK**.

NOTE

To remove entries from the list, select the user/user group/public folder you want to remove and click **Remove**.

6. Repeat steps 3 to 5 to add all the required users to the list.
7. Click **Apply**.

6.2.2 Enabling/disabling rules

To enable or disable attachment filtering rules:

1. Go to **Content Filtering > Attachment Filtering**.
2. From the **Attachment Filtering** page, select the checkbox of the rule(s) to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly.

6.2.3 Removing attachment rules

Warning

Deleted rules are not recoverable. If in doubt, it is recommended to disable a rule.

1. Go to **Content Filtering > Attachment Filtering**.
2. From **Attachment Filtering** page, select the rule(s) that you want to remove.
3. Click **Remove Selected**.

6.2.4 Modifying an existing rule

1. Go to **Content Filtering > Attachment Filtering**.
2. From **Attachment Filtering** page, click the name of the rule to modify.
3. Perform the required changes in the rule properties and click **Apply**.

6.2.5 Changing the rule priority

Attachment Filtering rules are applied in the same order, from top to bottom as they are listed in the Attachment Filtering page (that is, rule with priority value 1 is checked first). To change the sequence/priority of rules:

1. Go to **Content Filtering > Attachment Filtering**.
2. From the Attachment Filtering page, click the **↑** (up) or **↓** (down) arrows to respectively increase or

decrease the priority of the selected rule.

3. Repeat step 2 until rules are placed in the desired sequence.

6.3 Advanced Content Filtering

Advanced Content filtering enables scanning of email header data and content using advanced configurable search conditions and regular expressions (regex).

To configure advanced content rules, go to **Content Filtering > Advanced Content Filtering**. This page allows you to view, create, enable, disable or delete rules.

6.3.1 Creating Advanced Content Filtering rules

To create an Advanced Content Filtering rule follow the steps listed below:

- » [Step 1: Configuring basic rule settings and conditions to block](#)
- » [Step 2: Configuring the actions to take on detected emails](#)
- » [Step 3: Specifying the users to whom to apply this rule](#)

Step 1: Configuring basic rule settings and conditions to block

1. Go to **Content Filtering > Advanced Content Filtering** and click **Add Rule...**

General	Actions	Users/Folders
 Advanced Content Filtering		
Rule name Please specify a friendly name for this rule: <input type="text" value="New Advanced Checking Rule"/>		
Condition Choose the condition for this rule: <input type="text" value="Headers"/> <input type="text" value="Starts With"/> <input type="text"/>		
Email checking This rule can be applied to inbound, outbound and internal emails. Select below: <input checked="" type="checkbox"/> Check inbound emails <input checked="" type="checkbox"/> Check outbound emails <input checked="" type="checkbox"/> Check internal emails		

Screenshot 106: Adding a new Advanced Content Filtering rule

- In **Rule Name** area, provide a name for the new rule.
- In **Condition** area, provide the condition that the email has to meet to match this rule. From the drop down select the email part (**Headers, Subject, Body, Attachment Name** or **Attachment Content**) and choose a condition (**Start with, Ends with, Contains, Matches Exactly, Matches Regex**). In the text box, key in the keyword or regular expression that the email should match.

For example: To match emails having `swiss` in subject - Select **Subject** and **Contains** and key in `swiss` in textbox.

- Select whether to scan inbound, outbound and/or internal emails.

Option	Description
Scan Inbound SMTP Email	Select this option to scan incoming emails
Scan Outbound SMTP Email	Select this option to scan outgoing emails

Option	Description
Check Internal emails	Select this option to scan internal emails.
	<p>NOTE</p> <p>This option is only available when GFI MailEssentials is installed on the Microsoft® Exchange server</p>

Step 2: Configuring the actions to take on detected emails

1. From the **Actions** tab, configure what happens when this rule is triggered.

The screenshot shows the 'Actions' tab of the configuration interface. It is titled 'Attachment Filtering Actions'. The 'Actions' section includes a checked checkbox for 'Block attachment and perform this action:' with three radio button options: 'Quarantine email' (selected), 'Delete email', and 'Move to folder on disk:'. The 'Notification options' section has checked checkboxes for 'Notify administrator' and 'Notify local user'. The 'Logging options' section has an unchecked checkbox for 'Log rule occurrence to this file:'.

Screenshot 107: Actions Tab

2. To block an email that matches the rule conditions, select **Block email and perform this action** and select one of the following options:

Option	Description
Quarantine email	Stores blocked emails in the Quarantine Store. You can subsequently review (approve/delete) all the quarantined emails. For more information, refer to Quarantine (page 191).

Option	Description
Delete email	Deletes blocked emails.
Move to folder on disk	Moves the email to a folder on disk. Key in the full folder path where to store blocked emails.

IMPORTANT

Actions always affect the whole email containing the blocked content, even if there is other content (such as attachments) that do not trigger this rule.

3. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients but with the malicious content removed.

4. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

5. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation
path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

Step 3: Specifying users to whom this rule applies

1. By default, the rule is applied to all email users. GFI MailEssentials, however, allows you to apply this rule to a custom list of email users specified in the Users / Folders tab.

2. Specify the users to apply this rule to.

Option	Description
Only this list	Apply this rule to a custom list of email users, groups or public folders.
All except this list	Apply this rule to all email users except for the users, groups or public folders specified in the list.

3. To add email users, user groups and/or public folders to the list, click **Add**.

User Lookups

Select User/Group

	Name	Email Address	Email Aliases
<input checked="" type="checkbox"/>	John Smith	jsmith@domaina.tcv	No other aliases

Screenshot 108: Add users to a Content Filtering rule

4. In the **User Lookups** window, specify the name of the email user/user group or public folder that you wish to add to the list and click **Check Names**. Matching users, groups or public folders are listed underneath.

NOTE

You do not need to input the full name of the users, groups or public folder. It is enough to enter part of the name. GFI MailEssentials will list all the names that contain the specified characters. For example, if you input `sco`, GFI MailEssentials will return names such as `Scott Adams` and `Freeman Prescott`, if they are available.

5. Select the check box next to the name(s) that you want to add to the list and click **OK**.

NOTE

To remove entries from the list, select the user/user group/public folder you want to remove and click **Remove**.

6. Repeat steps 3 to 5 to add all the required users to the list.

7. Click **Apply**.

6.3.2 Removing Rules

1. From **Content Filtering > Advanced Content Filtering**, select rule to remove.

2. Click **Remove Selected**.

6.3.3 Enabling/Disabling Rules

1. From **Content Filtering > Advanced Content Filtering**, select rule to enable/disable.

2. Click **Disable Selected** to disable rule or **Enable Selected** to enable.

6.3.4 Sorting Rules

Advanced Content Filtering rules are applied in the same order, from top to bottom as they are listed in the Advanced Content Filtering page (that is, rule with priority value 1 is checked first). To change the sequence/priority of rules:

1. Navigate to the **Content Filtering > Advanced Content Filtering** node.
2. Click the  (up) or  (down) arrows to respectively increase or decrease the priority of the rule.
3. Repeat step 2 until rules are placed in the desired sequence.

6.4 Decompression Engine

The Decompression engine extracts and analyzes archives (compressed files) attached to an email.

The following is a list of checks performed by the decompression engine:

- » Password protected archives
- » Corrupted archives
- » Recursive archives
- » Size of decompressed files in archives
- » Amount of files in archives
- » Scan within archives

6.4.1 Configuring the decompression engine filters

Decompression

 **Decompression Engine**

Configure how compressed attachments (.rar, .zip files) are processed.

Disable Selected
Enable Selected

<input type="checkbox"/>	Description	Status
<input type="checkbox"/>	Check password protected archives	Enabled
<input type="checkbox"/>	Check corrupted archives	Enabled
<input type="checkbox"/>	Check for recursive archives	Enabled
<input type="checkbox"/>	Check size of uncompressed files in archives	Enabled
<input type="checkbox"/>	Check for amount of files in archives	Enabled
<input type="checkbox"/>	Scan within archives	Enabled

Screenshot 109: Decompression engine checks

To configure decompression engine filters:

- » [Check password protected archives](#)
- » [Check corrupted archives](#)
- » [Check for recursive archives](#)
- » [Check size of uncompressed files in archives](#)

- » Check for amount of files in archives
- » Scan within archives

Check password protected archives

1. Navigate to **Content Filtering > Decompression Engine** node.
2. From the list of available filters, click **Check password protected archives**.
3. To enable this filter, select **Check password protected archives**.
4. Specify what to do when an email contains an archive that triggers this filter:

Option	Description
Quarantine	Quarantines blocked emails
Automatically Delete	Deletes blocked emails

5. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients.
6. Click the **Actions** tab to configure further actions.
7. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation
path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

9. Click **Apply**.

NOTE

To create exception for password protected files see: <https://www.gfi.com/support/products/gfi-mailessentials/How-to-whitelist-users-for-a-Block-password-protected-files-policy>

Check corrupted archives

1. Navigate to **Content Filtering > Decompression Engine** node.
2. From the list of available filters, click **Check corrupted archives**.
3. To enable this filter select **Check corrupted archives**.
4. Specify what to do when an email contains an archive that triggers this filter:

Option	Description
Quarantine	Quarantines blocked emails
Automatically Delete	Deletes blocked emails

5. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients.

6. Click the **Actions** tab to configure further actions.

7. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation
path>\GFI\MailEssentials\EmailSecurity\Logs\

```

9. Click **Apply**

Check for recursive archives

This filter allows you to quarantine or delete emails that contain recursive archives. Recursive archives, also known as nested archives, are archives that contain multiple levels of sub-archives (that is, archives within archives). A high number of archive levels can indicate a malicious archive. Recursive archives can be used in a DoS (Denial of Service) attack, since recursive archives consume machine resources when they are being analyzed. To configure this filter:

1. Navigate to **Content Filtering > Decompression Engine** node.

2. From the list of available filters, click **Check for recursive archives**.

3. To enable this filter select **Check for recursive archives**.

4. Specify the maximum number of recurring archives in the **Maximum number of recurring archives** text box. If an archive contains more recurring archives than the specified number, the email is triggered as malicious.

5. Specify what to do when an email contains an archive that triggers this filter:

Option	Description
Quarantine	Quarantines blocked emails
Automatically Delete	Deletes blocked emails

6. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to forward a copy of the blocked email to the recipients but with the malicious content removed.

7. Click the **Actions** tab to configure further actions.

8. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

9. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

10. Click **Apply**.

Check size of uncompressed files in archives

This filter allows you to block or delete emails with archives that exceed the specified physical size when uncompressed. Hackers sometimes use this method in a DoS (Denial of Service) attack by sending an archive that can be uncompressed to a very large file that consumes hard disk space and takes a long time to analyze by content security or antivirus software.

To configure this filter:

1. Navigate to **Content Filtering > Decompression Engine** node.
2. From the list of available filters, click **Check size of uncompressed files in archives**.
3. To enable this filter select **Check size of uncompressed files in archives**.
4. Specify the maximum size of uncompressed archives in the Maximum **size of uncompressed files in archive in MB** text box. If an uncompressed archive's size is bigger than the specified value, the email is triggered as malicious.
5. Specify what to do when an email contains an archive that triggers this filter:

Option	Description
Quarantine	Quarantines blocked emails
Automatically Delete	Deletes blocked emails

6. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients but with the malicious content removed.

7. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

8. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

9. Click **Apply**.

Check for amount of files in archives

This filter allows you to quarantine or delete emails that contain an excessive amount of compressed files within an attached archive. You can specify the number of files allowed in archive attachments from the configuration options included in this filter. To configure this filter:

1. Navigate to **Content Filtering > Decompression Engine** node.
2. From the list of available filters, click **Check for amount of files in archives**.
3. To enable this filter select **Check for amount of files in archives**.
4. Specify the maximum number of files in archives in the **If the number of files within archive exceeds** text box. If the archive contains more files than the specified value, the email is triggered as malicious.
5. Specify what to do when an email contains an archive that triggers this filter:

Option	Description
Quarantine	Quarantines blocked emails
Automatically Delete	Deletes blocked emails

6. Select **Send a sanitized copy of the original email to recipient(s)** to choose whether to send a copy of the blocked email to the recipients.

7. Click the **Actions** tab to configure further actions.

8. To send email notifications whenever an email gets blocked, check any of the following options:

Option	Description
Notify administrator	To notify the administrator whenever this engine blocks an email. For more information, refer to Administrator email address (page 225). For more information, refer to Administrator email address (page 225).
Notify local user	To notify the email local recipients about the blocked email.

9. To log the activity of this engine to a log file, check **Log rule occurrence to this file** and specify the path and file name to a custom location on the disk to store the log file. By default, log files are stored in:

```
<GFI MailEssentials installation  
path>\GFI\MailEssentials\EmailSecurity\Logs\<EngineName>.log
```

10. Click **Apply**.

Scan within archives

You can configure GFI MailEssentials to apply Keyword and Attachment Filtering of files within archives.

1. Navigate to **Content Filtering > Decompression Engine** node.
2. From the list of available filters, click **Scan within archives**.
3. To enable scanning within archives select **Apply Attachment and Content Filtering rules within archives**. For more information, refer to [Content Filtering](#) (page 168).
4. Click **Apply**.

6.4.2 Enable/disable decompression filters

To enable or disable decompression filters:

1. Navigate to **Content Filtering > Decompression Engine** node.
2. From the **Decompression engine** page, select the checkbox of the filters to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly.

7 Quarantine

The GFI MailEssentials Quarantine feature provides a central store where all emails detected as spam or malware are retained. This ensures that users do not receive spam and malware in their mailbox and processing on the mail server is reduced.

Administrators and mail users can review quarantined emails by accessing the quarantine interface from a web browser. GFI MailEssentials can also send regular email reports to email users to review their blocked emails.

Refer to the following sections for more information on configuring the GFI MailEssentials Quarantine.

7.1 Important Notes	191
7.2 Searching the quarantine	191
7.3 Search Folders	196
7.4 Working with Quarantined emails	198
7.5 Quarantine RSS Feeds	202
7.6 Quarantine Options	203
7.7 Quarantine Store Location and Public URL	209

7.1 Important Notes

1. To quarantine spam or malicious emails, change the filters' and engines' actions to **Quarantine email**.
2. The Quarantine Store requires disk space to retain the organization's spam email or malware for a number of days. The amount of disk space required depends on:
 - » The quantity received
 - » How long it is retained.
3. On average, 100,000 spam or malware emails of 5 KB each will require approximately 600 MB of disk space to store the email and its metadata.
4. If the free disk space where the Quarantine Store is saved is 512 MB or less, GFI MailEssentials stops quarantining spam and malware; it is instead tagged and delivered to recipients' mailboxes until free disk space increases to more than 512 MB. This ensures that the disk will not run out of space.

7.2 Searching the quarantine

The Quarantine Store is accessible from the GFI MailEssentials interface and allows management of quarantined emails.

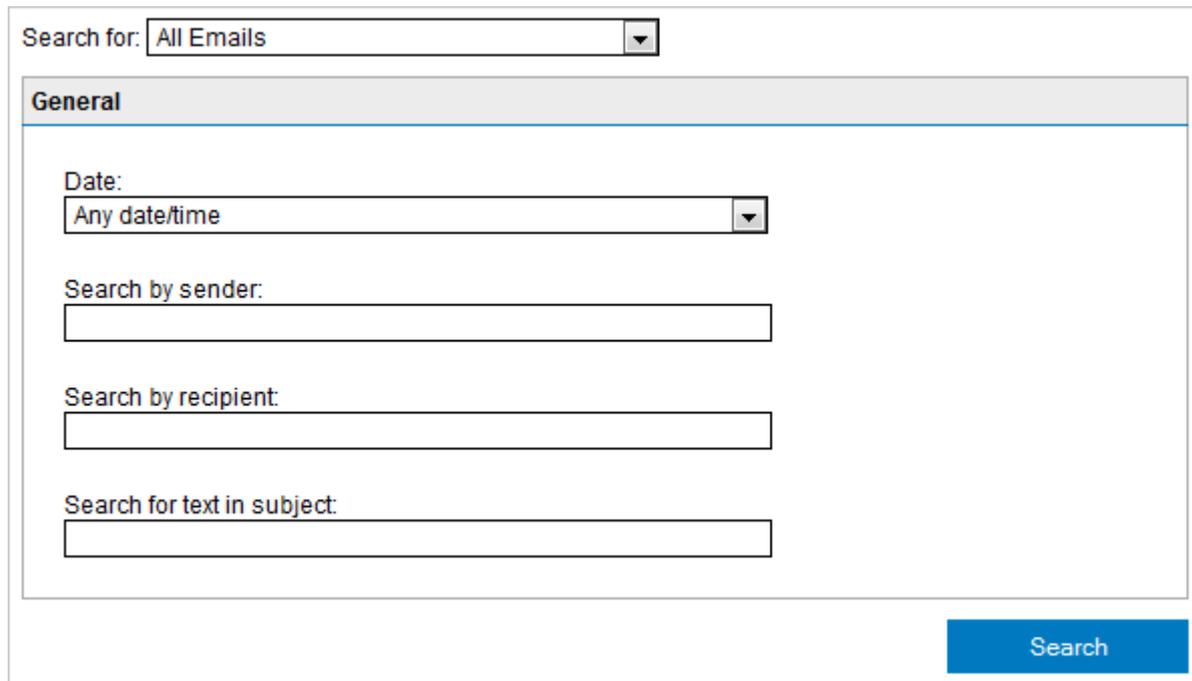
To access the GFI MailEssentials Quarantine Store, go to **GFI MailEssentials > Quarantine**.

There are various ways how to search for content in the GFI MailEssentials Quarantine:

- » [Searching though quarantined Malware and Spam](#)
- » [Searching through Malware emails only](#)
- » [Search through Spam emails only](#)

Search through both Malware and Spam

1. Go to **GFI MailEssentials > Quarantine**.



Search for: All Emails

General

Date: Any date/time

Search by sender:

Search by recipient:

Search for text in subject:

Search

Screenshot 110: Malware and Spam Search Area

2. From the **Quarantine** page, select **All Emails** from **Search for** dropdown.

3. Specify the required search criteria.

SEARCH CRITERIA	DESCRIPTION
Date:	Select the date range when the email was quarantined. Available date ranges are: <ul style="list-style-type: none">» Any date/time» Since yesterday» Last 7 days» Last 30 days» Custom date range
Search by sender	Specify a sender who sent the email that was quarantined.
Search by recipient	Specify a recipient for whom an email was quarantined.
Search for text in subject	Specify the text to search for within quarantined email subject.

4. Click **Search**.

NOTE

Use the search results to review quarantined emails. You can approve false positives for delivery to recipients. For more information, refer to [Working with Quarantined emails](#) (page 198).

Search for Malware and Content only

1. Go to **GFI MailEssentials > Quarantine**.

Search for:

General

Date:

Search by sender:

Search by recipient:

Search for text in subject:

Malware and Content

Quarantine Reason:

Item Source:

Item Direction:

Quarantined By: Only

Screenshot 111: Malware and Spam Search Area

2. From the **Quarantine** page, select **Malware and Content Only** from **Search for** dropdown.
3. Specify the required search criteria.

SEARCH CRITERIA	DESCRIPTION
Date:	Select the date range when the email was quarantined. Available date ranges are: <ul style="list-style-type: none"> » Any date/time » Since yesterday » Last 7 days » Last 30 days » Custom date range
Search by sender	Specify a sender who sent the email that was quarantined.
Search by recipient	Specify a recipient for whom an email was quarantined.

SEARCH CRITERIA	DESCRIPTION
Search for text in subject	Specify the text to search for within quarantined email subject.
Quarantine Reason	Key in the reason for which the email to search for was quarantined.
Item Source	Select the source from where email was identified as Malware and quarantined. Available options are: <ul style="list-style-type: none"> » Information Store (VSAPI) » Gateway (SMTP) » Information Store (Transport)
Item Direction	Select the direction of the quarantined email to search for, <ul style="list-style-type: none"> » Any » Inbound » Outbound
	<p>NOTE</p> <p>This option is available only if Gateway (SMTP) is selected in Item Source.</p>
Quarantined by	Select one of the GFI MailEssentials filters that quarantined the email. Select Only checkbox to search for emails quarantined only by a specific filter.

4. Click **Search**.

NOTE

Use the search results to review quarantined emails. You can approve false positives for delivery to recipients. For more information, refer to [Working with Quarantined emails](#) (page 198).

Search for Spam Only

1. Go to **GFI MailEssentials > Quarantine**.

Search for:

General

Date:

Search by sender:

Search by recipient:

Search for text in subject:

Spam

Search by anti-spam filter:

Screenshot 112: Spam Only search area

2. From the **Quarantine** page, select **Spam Only** from **Search for** dropdown.
3. Specify the required search criteria. Available options are:

SEARCH CRITERIA	DESCRIPTION
Date:	Select the date range when the email was quarantined. Available date ranges are: <ul style="list-style-type: none"> » Any date/time » Since yesterday » Last 7 days » Last 30 days » Custom date range
Search by sender	Specify a sender who sent the email that was quarantined.
Search by recipient	Specify a recipient for whom an email was quarantined.
Search for text in subject	Specify the text to search for within quarantined email subject.
Search by anti-spam filter	Select the anti-spam filter that identified the email to search for as Spam.

4. Click **Search**.

NOTE

Use the search results to review quarantined emails. You can approve false positives for delivery to recipients. For more information, refer to [Working with Quarantined emails](#) (page 198).

7.3 Search Folders

A Search Folder is a folder that has a custom search query associated to it and displays all quarantined emails that match the search query.

Examples of search folders:

- » A search folder that displays only outbound emails quarantined by the Virus Scanning Engines.
- » A search folder that displays inbound emails quarantined in a particular date range and addressed to a particular user.
- » A search folder that displays emails that meet specific search criteria
- » A search folder that displays the results of a previously defined search query.

To display emails in a particular search folder:

1. Go to **Quarantine** node.

Default Search Folders			
Search Folder Name	Malware and Content	Spam	
Today	0	130	
Yesterday	0	0	
This Week	0	130	
All Malware and Content Items	381	N/A	
All Spam Items	N/A	365	

Custom Search Folders			
Search Folder Name	Malware and Content	Spam	Auto-purging
Spam Deletion	381	365	Disabled

Screenshot 113: Default and custom search folders

2. Click a search folder displayed in the **Default Search Folders** or **Custom Search Folders** areas. Alternatively, select one of the search folder nodes under the **Quarantine** and **Quarantine > Search Folders** node.

NOTE

Use the search results to review quarantined emails. You can approve false positives for delivery to recipients. For more information, refer to [Working with Quarantined emails](#) (page 198).

7.3.1 Default Search Folders

Default Search Folders are preconfigured search folders that enable you to access quarantined emails according to specific time periods or by a specific quarantined email type. To use the default search folders:

1. Go to **Quarantine** node.



Use this page to search for quarantined emails.

Search for:

General

Date:

Search by sender:

Search by recipient:

Search for text in subject:

Search

Default Search Folders

Search Folder Name	Malware and Content	Spam
Today	0	130
Yesterday	0	0
This Week	0	130
All Malware and Content Items	381	N/A
All Spam Items	N/A	365

Custom Search Folders

Search Folder Name	Malware and Content	Spam	Auto-purging
Spam Deletion	381	365	Disabled

Screenshot 114: Default search folders

2. Select a search folder from the **Default Search Folders** area or from a node beneath **Quarantine** node to access the search folder. GFI MailEssentials will automatically search for and display all quarantined emails that satisfy the default search folder search criteria.

Available default search folders are:

» **Time based:**

- Today
- Yesterday

- This week

» **Category based:**

- All Malware and Content Items
- All Spam Items

NOTE

Use the search results to review quarantined emails. You can approve false positives for delivery to recipients. For more information, refer to [Working with Quarantined emails](#) (page 198).

7.3.2 Creating, editing and removing Custom Search Folders from Searches

1. Go to **Quarantine** node.
2. Create a new search for quarantined emails. For more information, refer to [Searching the quarantine](#) (page 191).
3. In the results page, click **Save as Search Folder** and key in an easily identifiable name for the new Search Folder.

The newly created search folder is listed in **Quarantine > Search Folders** node.

NOTE

To edit or delete a previously created search folder, access the search folder and click **Edit Search Folder** or **Delete Search folder**.

7.3.3 Using the Search Folders node to auto-purge quarantined emails

The **Search Folders** node enables you to create Search folders and set an auto-purge value (in days). When a quarantined email exceeds the specified number of days in the quarantine, the email is deleted.

1. Select **Quarantine > Search Folders** node.
2. Configure a new search folder for the emails to purge on a regular basis using the instructions in this chapter.
3. Select **Enable Auto-purging** and provide the number of days to keep emails for.
4. Click **Save Folder**.

7.4 Working with Quarantined emails

Within GFI MailEssentials there are a number of actions you can take on quarantined emails.

The Quarantine Store is accessible from the GFI MailEssentials interface and the administrator can manage quarantined emails.

To access the GFI MailEssentials Quarantine Store, go to **GFI MailEssentials > Quarantine**.

7.4.1 Viewing quarantined emails

Searching within the Quarantine or using default or customized search folders yields a list of quarantined emails.

New Search
Save as Search Folder

Malware and Content (381)
Spam (365)

Use this page to approve or delete emails blocked due to malware\content

Approve
Delete
Rescan

<input type="checkbox"/>	Date	Sender	Recipients	Subject	Module	Reason	Source
<input type="checkbox"/>	04/09/2013 11:24:50	spam@spam2do main.com	Administrator@dom aina.tcv	Energy Issu es	Keyword Filt ering	Triggered rule "threa t content"	Gateway (SMTP)
<input type="checkbox"/>	04/09/2013 11:24:45	spam@spam2do main.com	Administrator@dom aina.tcv	Energy Issu es	Keyword Filt ering	Triggered rule "threa t content"	Gateway (SMTP)
<input type="checkbox"/>	04/09/2013 11:24:42	spam@spam2do main.com	Administrator@dom aina.tcv	IEP News 5 /30	Keyword Filt ering	Triggered rule "threa t content"	Gateway (SMTP)
<input type="checkbox"/>	04/09/2013 11:24:41	spam@spam2do main.com	Administrator@dom aina.tcv	IEP News 5 /30	Keyword Filt ering	Triggered rule "threa t content"	Gateway (SMTP)
<input type="checkbox"/>	04/09/2013 11:24:39	spam@spam2do main.com	Administrator@dom aina.tcv	Energy Issu es	Keyword Filt ering	Triggered rule "threa t content"	Gateway (SMTP)
<input type="checkbox"/>	04/09/2013 11:24:40	spam@spam2do main.com	Administrator@dom aina.tcv	Energy Issu es	Keyword Filt ering	Triggered rule "threa t content"	Gateway (SMTP)

⏪ ⏩ ... 30 31 32 33 34 35 36 37 38 39 ⏪ ⏩

Page size: 10

381 items in 39 pages

Approve
Delete
Rescan

Screenshot 115: Search Results

NOTE

The results page may be split in two tabs:

- » **Malware and Content** - Emails blocked by anti-malware engines and content filtering rules.
- » **Spam** - Emails blocked by anti-spam filters.

1. Choose **Malware and Content** tab or **Spam** tab to view quarantined emails for the specific quarantined email type. The results page provides the following functions and details:

Option	Description
Back	Returns you to the previous screen.
Approve	Enables you to approve a single or multiple emails. For more information, refer to Approving Quarantined Emails (page 201).
Delete	Deletes a single or multiple emails. For more information, refer to Permanently Delete Quarantined Emails (page 201).
Rescan	Rescans emails using current antivirus signatures (which may be more up to date than the antivirus signatures that quarantined the email in the first place). Select one or more emails and click Rescan to rescan.
Module	The module that identified the email as to be quarantined.
Reason	The reason/rule that triggered the action to quarantine the email.

Option	Description
Sender	The email address of the sender
Recipients	The email address of the recipient
Subject	The email subject as sent by the sender.
Date	The date when email was quarantined
Source	The location from where the email was quarantined
Item Source	Enables selecting a source to filter the display with. Available options are: <ul style="list-style-type: none"> » View all » Information Store (VSAPI) » Gateway (SMTP) » Information Store (Transport)
Page size	Enables customizing how many emails per page are currently displayed. Choose a number to view a maximum number of items per page.

2. Click a row to access the individual email details.

Approve
Sanitize and Approve
Rescan
Delete
Delete and Notify
Download item

Item Information

From:	spam@spam2domain.com	Date:	07/09/2013 11:40:17
To:	Administrator@domaina.tcv	Module:	Keyword Filtering ⊞
Subject:	IEP news 4/9		
Source:	Gateway (SMTP)		

Attachments

Quarantined item has no attachments to display.

Message Text

Text Body

[Please click here to see quarantined content](#)

The message body might contain malicious content. Instead of displaying the message body, the threat description is being shown. The following table shows the threat details for this message body. To view the actual message body, please click the link above.

Plugin	Threat
Keyword Filtering	Words in body triggered rule "threat content" (Words found: energy)

Screenshot 116: Quarantined Items details

From the **Quarantined Items details** page, review the email details and perform the following actions

Action	Description
Approve	Approve email. For more information, refer to Approving Quarantined Emails (page 201).
Sanitize and Approve	Sanitize email and approve. For more information, refer to Approving Quarantined Emails (page 201).

Action	Description
Rescan	Rescans emails using current antivirus signatures (which may be more up to date than the antivirus signatures that quarantined the email in the first place).
Delete	Deletes email. For more information, refer to Permanently Delete Quarantined Emails (page 201).
Delete and Notify	Deletes email and notifies user. For more information, refer to Permanently Delete Quarantined Emails (page 201).
Download Item	Downloads quarantined email to a location you choose in .eml format.
	Warning: Emails in Quarantine Store may contain malicious content. Use this feature with caution.

7.4.2 Approving Quarantined Emails

There might be instances where you might want to approve an email blocked by GFI MailEssentials. GFI MailEssentials allows the administrator to approve a quarantined email so that it is released from the Quarantine Store and delivered to its intended recipients.

To approve emails:

1. Use the search features described in the previous sections to return a list of quarantined emails.
2. Select the checkbox next to the quarantined email(s) to approve and click **Approve**.

Sanitize and Approve Emails

GFI MailEssentials also enables you to remove the item that caused the email to be quarantined and send the email to recipient.

To sanitize and approve emails:

1. Use the search features described in the previous sections to return a list of quarantined emails.
2. Click on an email to view its details.
3. Click **Sanitize and Approve**.

NOTE

Emails quarantined by the Information Store (VSAPI) source cannot be sanitized.

7.4.3 Permanently Delete Quarantined Emails

1. Use the search features described in the previous sections to return a list of quarantined emails
2. Select the checkbox next to the quarantined email(s) and click **Delete**.

Delete Quarantined Emails and notify user

The Delete and Notify feature enables notifying recipients when deleting emails from quarantine.

To delete and notify recipients:

1. Use the search features described in the previous sections to return a list of quarantined emails.
2. Click on an email to view its details.
3. Click **Delete and Notify**.

7.5 Quarantine RSS Feeds

RSS (Really Simple Syndication) is a protocol used to distribute frequently updatable content or feeds (for example, news items) with its subscribers. An RSS Feed Reader is required by subscribers to view RSS feeds. RSS feeds usually include a summary of the content and a link to view the full article.

To facilitate the monitoring of quarantined emails, RSS feeds can be used. The GFI MailEssentials Quarantine RSS feed displays quarantined emails for review and enables users to approve or delete quarantined emails.

NOTE

GFI MailEssentials Quarantine RSS feeds can be used on most RSS Feed Readers. For a list of freely available RSS Feed Readers that were tested with GFI MailEssentials Quarantine RSS feeds refer to: <http://kbase.gfi.com/showarticle.asp?id=KBID002661>

7.5.1 Enabling Quarantine RSS Feeds

1. Navigate to **GFI MailEssentials > Quarantine > Quarantine RSS Feeds**.

Quarantine RSS Feeds

 Use this page to configure GFI MailEssentials RSS Feeds.

GFI MailEssentials uses RSS (Really Simple Syndication) feeds to notify you on newly quarantined items.

To receive RSS Feeds, use an RSS feed reader and subscribe to a feed. Copy the URL of orange RSS button to the left of the Quarantine folder to monitor and create a new subscription in the RSS feed reader.

NOTE: Only users with "Access" privileges are allowed to subscribe to the Quarantine RSS Feeds. For a list of free RSS Feed Readers that are known to work well with GFI MailEssentials Quarantine RSS Feeds, refer to: <http://www.gfi.com/link/entry.aspx?page=skynet&id=KBID002661>

Enable Quarantine RSS Feeds
If unselected, no feeds are generated regardless of any individual filter settings.

RSS Feeds

 To subscribe to all enabled feeds, copy the URL associated with the orange OPML button. [Edit...](#)

Default quarantine folder	RSS Feed Status	Interval	Maximum Items	
 Today	Disabled	10 minutes	100	Edit...
 Yesterday	Disabled	10 minutes	100	Edit...
 This Week	Disabled	10 minutes	100	Edit...
 All Items	Disabled	10 minutes	100	Edit...

Screenshot 117: Quarantine RSS feeds

2. Select the **Enable Quarantine RSS Feeds** checkbox.
3. From the **RSS Feeds** area, click **Edit** to the right of the quarantine search folder for which to enable RSS feeds.
4. Select **Enable Quarantine RSS feeds on this folder** checkbox.
5. Specify the refresh interval in minutes in the **Refresh feed content every** text box. The default value is 10 minutes.

6. Specify the maximum number of items you want the feed to include in the **Feed should contain at most** text box. The default value is 100 items.

NOTE

You can change the URL of an RSS feed by clicking **Reset Feed URL**. To change the URL of all enabled RSS feeds, click **Edit** to the right of the **OPML** entry and click **Reset all the URLs**. When changing URLs, ensure to update all present subscriptions accordingly.

Reset feed url should be done in case of unauthorized access

7. Click **Apply**.

7.5.2 Subscribing to Quarantine RSS feeds

Subscribing to all enabled Quarantine RSS feeds

1. Navigate to **GFI MailEssentials > Quarantine > Quarantine RSS Feeds**.
2. In the RSS Feeds area, right-click on **OPML** icon and choose to copy the link URL. (actual option depends on browser used)
3. Use the copied URL in your RSS Feed Reader application to create a new RSS feed subscription.

Subscribing to a search folder Quarantine RSS feed

To subscribe to an RSS feed of a default or custom search folder:

1. Navigate to **GFI MailEssentials > Quarantine > Quarantine RSS Feeds**.
2. In the RSS Feeds area, right-click on **RSS** icon next to the search folder to subscribe to and choose to copy the link URL. (option depends on browser used)
3. Use the copied URL in your RSS Feed Reader application to create a new RSS feed subscription.

7.5.3 Securing access to the GFI MailEssentials Quarantine RSS feeds

Configure who can subscribe to the quarantine RSS feeds from the Access Control node in GFI MailEssentials Configuration. For more information, refer to [Access Control](#) (page 236).

7.6 Quarantine Options

Use the Quarantine Options to configure spam retention, user quarantine reports, quarantined malware and emails sent to inexitent users.

7.6.1 Spam Options

1. Navigate to **Quarantine > Quarantine Options > Spam Options**.

General Options **User Settings**

 Use this tab to configure the general quarantine options for spam emails.

The quarantine store of spam emails can grow to several gigabytes of size depending on the quantity of quarantined emails and the retention period for emails.

Retention Period

The email retention period will delete ALL quarantined spam emails older than the configured number of days.

Spam quarantine store email retention:

days (recommended 21 days)

Screenshot 118: Spam Options - General Options tab

2. From the **General Options** tab change or confirm the **Spam quarantine store email retention** period.
3. Click **User Settings** tab.

General Options
User Settings


Use this tab to configure user-related settings for spam quarantine store access.

Users access quarantined emails using email reports sent at configurable intervals. Search and management of quarantined emails by users is done through a web browser.

User Quarantine Reports

Send user quarantine reports at regular intervals

Specify the days & time when the report will be sent to users:

Send every Monday at 0:00

Send every Weekday at 8:00

Send every Weekday at 15:00

Add rule
Delete

Specify which users will receive the spam quarantine report:

All Users except the ones listed below

Only users in the list below

Add...
Remove
Export

Specify the full path and filename of the file to use for importing:

Browse...
No file selected.

Import

Screenshot 119: Spam Options - User Settings tab

4. Select **Send user quarantine reports at regular intervals** to enable sending of User quarantine reports.

NOTE

User quarantine reports are emails sent to users on a regular basis with a list of blocked spam for that user. Using this list, users can check and approve any legitimate emails. Email blocked by the Malware and Content Filtering filters are not shown in these emails.

5. Configure the frequency at which report will be sent. To add to the preset schedule, select a date and time and click **Add rule**. Select an existing date and time and click **Delete** to delete selected date/time.

6. Configure the users that will receive the Quarantined Spam reports. Select **All Users except the ones listed below** or **Only users in the list below** and provide the email address of the users to include or exclude.

NOTE

Click **Browse** to select a file with a list of email addresses to import and click **Import**.

7. Click **Apply**.

7.6.2 Malware Options

GFI MailEssentials can also be configured to notify the administrator or authorized users via email (Quarantine Action Form) whenever an email is quarantined.

The Quarantine Approval Form contains details related to the quarantined email including the reason why it was blocked and any attachments that were included in the email. The administrator can then action the quarantined email (for example, approve the email) directly from the email client.

NOTE

To automatically purge emails older than a specific number of days, create a new search folder and set the Auto-purging feature to purge emails after a number of days. For more information, refer to [Using the Search Folders node to auto-purge quarantined emails](#) (page 198).

Enabling Quarantine Approval Forms

1. Navigate to **Quarantine > Quarantine Options > Malware Options**.

Quarantine Mode
Nonexistent recipients

Quarantine mode

Email options

Select where the quarantine approval forms are sent. These enable recipients to see the quarantine store and approve or discard quarantined email.

Send quarantine approval forms by email

Select recipient

Send to administrator

Send to the following email address

Audit options

Save quarantine audit to this file:

quarantineaudit.log

If no path is specified, the audit file will be saved to the 'EmailSecurity\Data' folder by default. Audit files are saved with the current year number appended to the specified filenames, e.g. quarantineaudit_2012.log.

Screenshot 120: Quarantine Mode

2. From **Quarantine Mode** tab, select **Send quarantine approval forms by email** checkbox to enable the sending of Quarantine Approval Forms.
3. From the **Select recipient** area, specify the recipient of the Quarantine Approval Forms:

Option	Description
Send to administrator	Sends Quarantine Approval Forms to the administrator as configured in General Settings node. For more information, refer to Administrator email address (page 225).
Send to the following email address	Sends Quarantine Approval Forms to another email address. Key in the recipient in the text box provided.

4. Optional - Select **Save quarantine audit to this file** and configure a filename where to save a copy of the quarantine log.
5. Click **Apply**.

Nonexistent Recipients

The GFI MailEssentials Nonexistent recipients feature scans emails for non-existing local email addresses before these are stored to the Quarantine Store. If an email contains non-existing local email addresses, it is permanently deleted. This reduces the number of emails for administrative reviewing.

Configuring Nonexistent Recipients

The Nonexistent Recipients filter requires access to the list of local addresses. This is done either via Active Directory or if communication with Active Directory is not possible, via an LDAP server.

1. Navigate to **Quarantine > Quarantine Options > Malware Options**.

Quarantine Mode Nonexistent recipients

 **Nonexistent recipients**

If enabled, this feature automatically deletes emails with nonexistent recipients instead of quarantining them.
Use this feature to automatically keep your quarantine store clean from malicious spam email.

Delete quarantined emails for nonexistent recipients

Lookup options

- Use native Active Directory lookups
- Use LDAP lookups

LDAP Settings

Server:

Port: Use SSL

Base DN:

Anonymous bind Update DN list

User:

Password:

* For security reasons, the length in the password box above does not necessarily reflect the true password length

Email address test

Email address: Test

Logging options

Log occurrence to this file:

Screenshot 121: Nonexistent Recipients

2. From **Nonexistent Recipients** tab, select **Delete quarantined emails for nonexistent recipients** checkbox.

3. Select the user lookups method to use:

Option	Description
Use native Active Directory look-ups	Select this option if GFI MailEssentials is installed in Active Directory mode and has access to ALL users on Active Directory. Skip to step 8. NOTE When GFI MailEssentials is installed in Active Directory user mode on a DMZ, the AD of a DMZ usually does not include all the network users (email recipients). In this case configure GFI MailEssentials to use LDAP lookups. NOTE When GFI MailEssentials is behind a firewall, this feature might not be able to connect directly to the internal Active Directory because of Firewall settings. Use LDAP lookups to connect to the internal Active Directory of your network and ensure to enable default port 389 on your Firewall.
Use LDAP lookups	Select this option when GFI MailEssentials is installed in SMTP mode and/or when GFI MailEssentials does not have direct access to the full list of users.

4. Specify the LDAP server name or IP address in the **Server** text box.

NOTE

In an Active Directory environment, the LDAP server is typically the Domain Controller or Global Catalog.

5. Specify the port number, default 389, in the **Port** text box. If connection to the LDAP server is via SSL, select **Use SSL** and the default port changes to 636.

NOTE

Ensure that the port is enabled from the Firewall.

6. Click **Update DN list** to populate the **Base DN** list and select the Base DN (that is, the top level in the Active Directory hierarchy).

7. If your LDAP server requires authentication specify the **User** and **Password**. Alternatively, if no authentication is required, select **Anonymous bind**.

8. Test your configuration settings by specifying a valid email address in the **Email address** box and click **Test**. If the email address is not found, review the configuration settings.

9. To log Nonexistent Recipient activity to a log file, select **Log occurrence to this file** and specify path and file name (including .txt extension) to a custom location on disk where to store the log file. Alternatively specify the file name only (including .txt extension) and the log file will be stored in the following default location

```
<GFI MailEssentials installation path>\GFI\MailEssentials\\EmailSecurity\Logs\<filename>.txt
```

10. Click **Apply**.

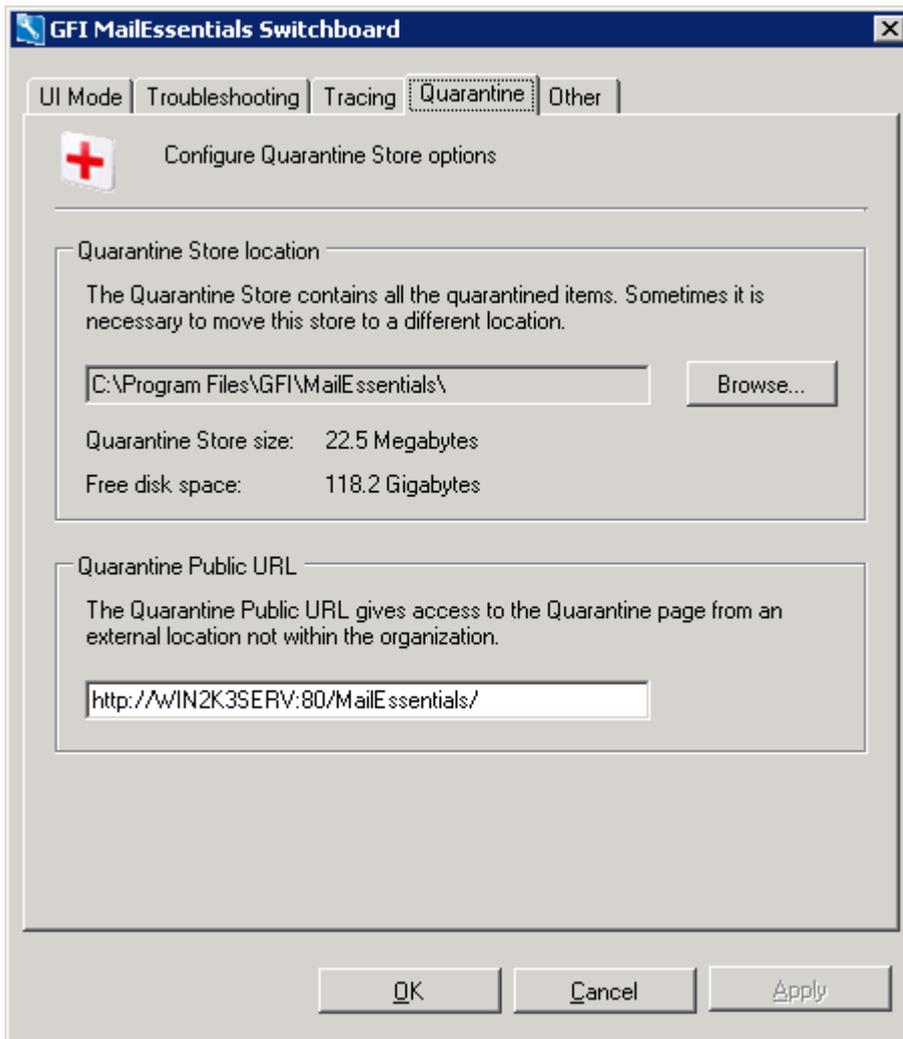
7.7 Quarantine Store Location and Public URL

Use the GFI MailEssentials Switchboard to configure the Quarantine Store location and the Quarantine Public URL.

The Quarantine Store location is the Quarantine Store location where quarantined emails are stored. By default, this is located in the GFI MailEssentials installation path. This might however need to be moved to an alternate location in cases where, for example, you might be running out of disk space.

The Quarantine Public URL provides access to the Quarantine Page from an external location. By default, this is based on the GFI MailEssentials IIS Virtual directory settings you provided during installation. This however might need to be changed if you are sending quarantine digest emails or notifications that are accessed outside of the internal network. When this is the case, the URL should be changed to be reached through Internet.

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard**.



Screenshot 122: Quarantine Store location and Public URL

2. From **Quarantine** tab, click **Browse** to select an alternate location for the Quarantine Store.

IMPORTANT

Ensure that the disk partition where the Quarantine Store is saved has sufficient disk space. Spam emails will not be quarantined if the free disk space is less than 512 MB. On reaching 512 MB, email quarantine operation will stop and spam will be tagged and delivered to recipients' mailboxes until free disk space increases to more than 512 MB

3. Provide an alternate URL as the URL to use to access the quarantine from an external location outside your organization,

4. Click **OK** to save setup.

8 Email Management

GFI MailEssentials includes a number of tools that facilitate management of incoming and outgoing emails.

Topics in this chapter:

8.1 Disclaimers	212
8.2 Auto-Replies	215
8.3 List Server	217
8.4 Mail Monitoring	221

8.1 Disclaimers

Disclaimers are standard content added to the bottom or top of outbound email for legal and/or marketing reasons. These assist companies in protecting themselves from potential legal threats resulting from the contents of an email and to add descriptions about the products/services offered.

- » [Configuring disclaimers](#)
- » [Disabling and enabling disclaimers](#)
- » [Sorting disclaimers by priority](#)

8.1.1 Configuring Disclaimers

To customize or create a new disclaimer:

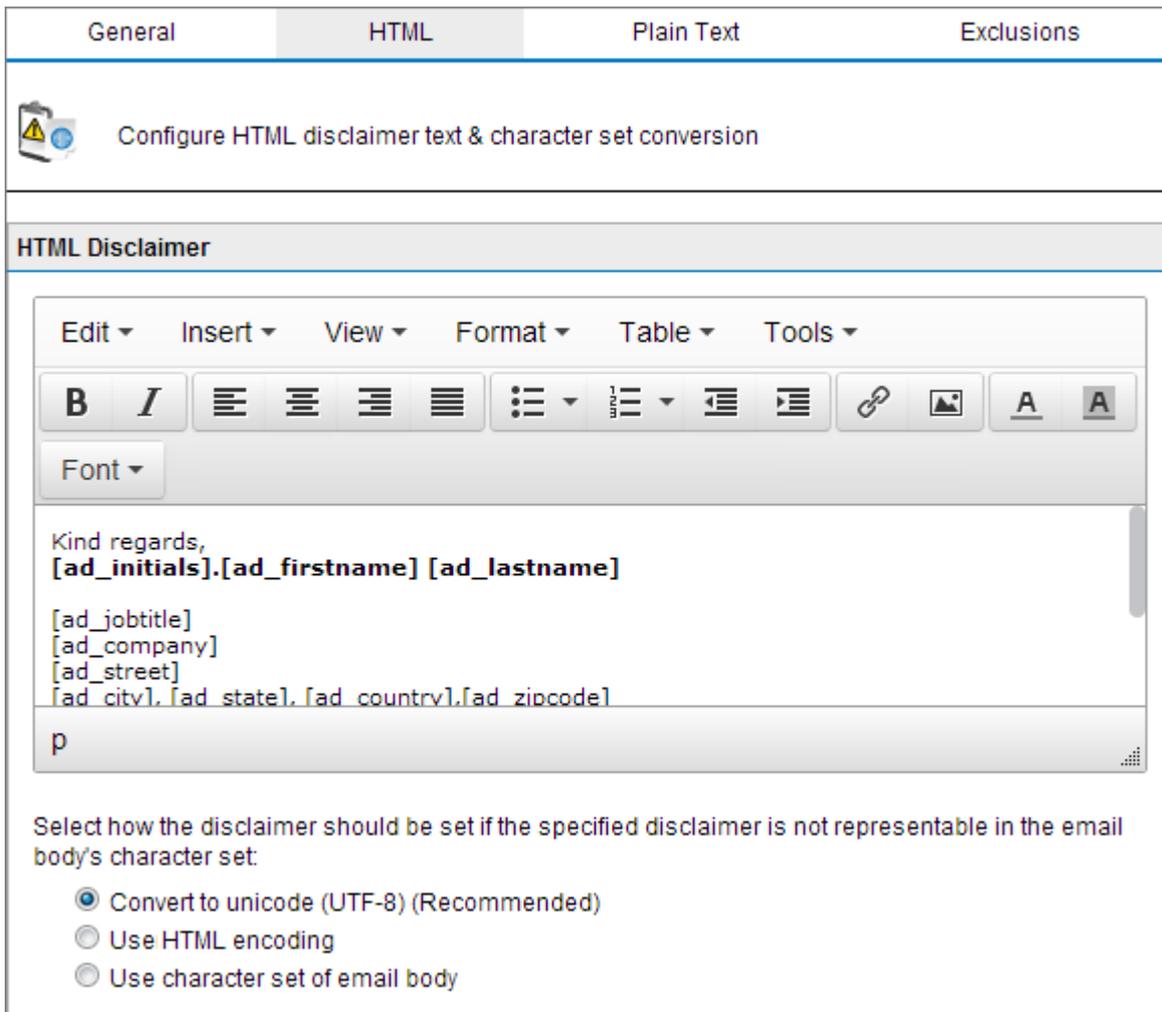
1. Go to **Email Management > Disclaimers**.
2. Click a disclaimer to edit its settings or click **Add Disclaimer** to create a new disclaimer.

General	HTML	Plain Text	Exclusions
 Configure disclaimer settings			
Disclaimer Name Provide a friendly name for this rule: <input type="text" value="New Disclaimer"/>			
Disclaimer Options Disclaimer Type: <input checked="" type="radio"/> Domain Disclaimer <input type="radio"/> User Disclaimer Domain: <input type="text" value="domaina.tcv"/>			
Specify position of disclaimer: <input type="text" value="Bottom"/>			

Screenshot 123: Adding a new disclaimer

3. In the **General** tab configure:

Option	Description
Disclaimer Name	Key in a unique and friendly name for the disclaimer.
Disclaimer Type	Choose to which user(s) to apply this disclaimer: » Domain disclaimer: All emails sent from a domain will have the disclaimer added. Select the domain from the Domain drop-down list. » User/Group disclaimer: Click Search User/Group to select a user or a group of users, to whom the disclaimer is added for outbound emails. If GFI MailEssentials is in Active Directory mode, pick users or groups directly from Active Directory; else specify the user's SMTP email address.
Disclaimer position	Select Top or Bottom option to configure if disclaimer should be located at the top or bottom of the email.



Screenshot 124: HTML Disclaimer

4. From the **HTML** tab, use the HTML editor to create a custom disclaimer in HTML format. To add email fields or Active Directory fields (variables) in disclaimer, navigate to **Insert > Variable...** Select the variable to add and click **Add**. The recipient display name and email address variables will only be included if the email is sent to a single recipient. If emails are sent to multiple recipients, the variables are replaced with 'recipients'.

NOTE

If you choose the Custom Attribute variable, you will need to specify a Microsoft Exchange custom attribute. For a full listing of attributes in your Active Directory configuration, install and use the ADSI Editor from Microsoft.

For more information, refer to: http://go.gfi.com/?pageid=ME_ADSI

5. Select the encoding for the HTML disclaimer if the email body's character set is not HTML:

Option	Description
Convert to Unicode	Convert both email body and disclaimers to Unicode so that both are properly displayed. (Recommended)
Use HTML encoding	Use to define character sets for email body and disclaimer.
Use character set of email body	Disclaimer is converted to the email body character set. NOTE: If selected, some disclaimer text might not display properly.

6. Select **Plain Text** tab and insert the text to include for use in plain text emails directly into the **Text Disclaimer** field. Optionally add variables in disclaimer by clicking **Variable...** The variables that can be added are email fields (sender name, recipient email address, etc...) or Active Directory fields (name, title, telephone numbers, etc..). Select the variable to add and click **Add**.

NOTE

The recipient display name and email address variables will only be included if the email is sent to a single recipient. If emails are sent to multiple recipients, the variables are replaced with 'recipients'.

7. Specify the encoding to be used for the plain text disclaimer if the email body's character set is not plain text:

Option	Description
Convert to Unicode	Converts both email body and disclaimers to Unicode so that both are properly displayed
Use character set of email body	Disclaimer is converted to the email body's character set NOTE: If this option is selected, some of the disclaimer text might not be displayed properly.

8. From the **Exclusions** tab, specify any senders or recipients for whom not to apply this disclaimer. Key in an email address or click **Search** to look-up email addresses from Active Directory. Click **Add** to add email address to the exclusion list.

NOTE

All recipients must be included in the exclusion list to not add a disclaimer in the email.

9. Click **Apply** to save settings.

8.1.2 Disabling and enabling disclaimers

By default, disclaimers are automatically enabled. To disable or enable a disclaimer:

1. Go to **Email Management > Disclaimers**.
2. Select the disclaimers to disable/enable and click **Disable selected** or **Enable selected** to perform the desired action.

8.1.3 Sorting disclaimers by priority

The order in which disclaimers are applied to outbound messages can be customized. If multiple disclaimers are enabled and applied to the same user, the disclaimer with the higher is applied to that user.

To customize the priority of disclaimers:

1. Go to **Email Management > Disclaimers**.
2. Next to the disclaimer to change priority, click **▲** (up) button to assign a higher priority or click **▼** (down) button to assign a lower priority.

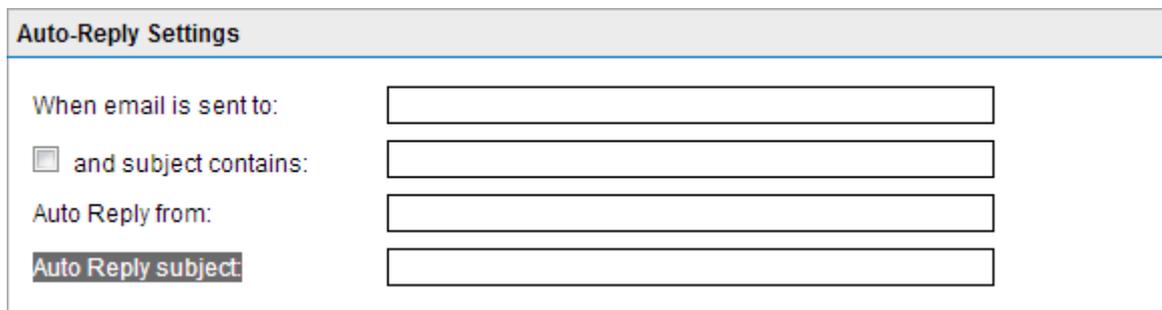
8.2 Auto-Replies

Auto-replies enable the sending of automated replies to specific inbound emails. A different auto-reply for each email address or subject can be specified. Variables can also be used in an auto-reply to personalize emails.

To enable auto-replies, go to **Email Management > Auto-Replies** and select **Enable Auto-Replies**.

8.2.1 Configuring auto-replies

1. Go to **Email Management > Auto-Replies**.
2. Click **Add Auto-Reply**.



Auto-Reply Settings

When email is sent to:

and subject contains:

Auto Reply from:

Auto Reply subject:

Screenshot 125: Auto-reply settings

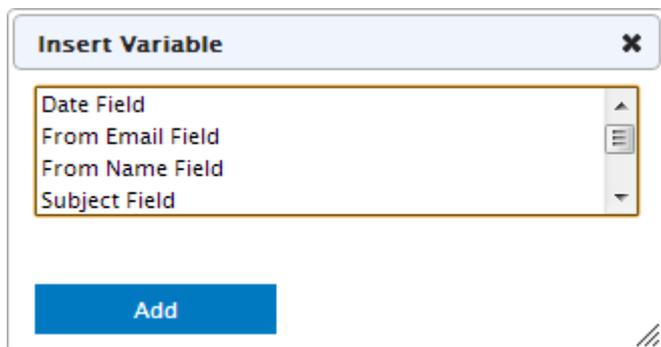
3. In **Auto-Reply Settings** configure the following options:

Option	Description
When email is sent to:	Key in the email address that sends auto-replies when receiving emails. Example - If 'sales@master-domain.com' is used, senders sending to this email address will receive an auto reply.
and subject contains:	This option enables auto replies only for emails containing specific text in the subject field.
Auto Reply from:	Specify an email address in case where an auto-reply is required from a different email address other than the email address to which the inbound email was addressed to.
Auto Reply subject:	Specify the subject of the auto reply email.

4. In **Auto Reply text**, specify the text to display in the auto reply email.

NOTE

Import auto reply text from a text file via the **Import** button. Click **Export** to download auto-reply text to a text file.



Insert Variable ✕

Date Field
From Email Field
From Name Field
Subject Field

Add

Screenshot 126: Variables dialog

5. Click **Variable...** to personalize auto-replies using variables. Select variable field to insert and click **Add**. Available variables are:

Option	Description
Date Field	Inserts the email sent date.
From Email Field	Insert sender email address.
From Name Field	Inserts the display name of the sender.
Subject Field	Inserts email subject.
To Email Field	Inserts the recipient's email address.
To Name Field	Inserts the recipient's display name.
Tracking Number	Inserts tracking number (if generated).

6. In **Attachments** area, select any attachments to send with the auto-reply email. Specify the location of the attachment and click **Add**. Remove attachments using **Remove**.

7. In **Other Settings** configure:

Option	Description
Generate tracking number in subject	Generates a unique tracking number in the auto reply. By default, tracking numbers are generated using the following format: ME_YYMMDD_nnnnnn Where: <ul style="list-style-type: none"> » ME - GFI MailEssentials tag. » YYMMDD - Date in year, month and date format. » nnnnnn - automatically generated tracking number.
Include email sent	Select to quote the inbound email in auto reply.

8. Click **Apply**.

8.3 List Server

List servers enable the creation of two types of distributions lists:

- » **Newsletter** - Used for creating subscription lists for company or product newsletters, to which users can either subscribe or unsubscribe.
- » **Discussion** - Enables groups of people to hold discussions via email, with each member of the list receiving the email that a user sends to it.

8.3.1 Creating a newsletter or discussion list

To create a new newsletter or discussion list:

1. Go to **Email Management > List Server** and click **Add List**.

General Database Footer Permissions Subscribers

 Configure the list name, domain and additional options for this list

Display Name

Provide a friendly name for this rule:

List Server Settings

List Type: Newsletter Discussion

List Name:

Which domain will the list use? (Only relevant if you have multiple domains.)

List email addresses:

List address: @
 Subscribe: -subscribe@
 Unsubscribe: -unsubscribe@

Other Options

Automatically unsubscribe NDRs and move NDR to the following folder:

Screenshot 127: Creating a new list

2. Configure the following options:

Option	Description
Display Name	Key in a friendly name for the new list.
List type	Select the type of discussion list to create: <ul style="list-style-type: none"> » Newsletter - Used for creating subscription lists for company or product newsletters, to which users can either subscribe or unsubscribe. » Discussion - Enables groups of people to hold discussions via email, with each member of the list receiving the email that a user sends to it.
List Name	The list name is used in the list email address fields. For example, if the list name is <code>MyNewsletter</code> , the list email address is <code>MyNewsLetter@mydomain.com</code>

Option	Description
List domain	The domain to use for the list. The list of domains is extracted from the Local Domains list. The list server utilizes this domain for the list addresses displayed in the List email addresses box.
Automatically unsubscribe NDRs and move NDR to the following folder:	When an NDR is received from a subscriber of the list, the subscriber is automatically unsubscribed and the NDR is moved to a custom folder.

3. From the **Database** tab, select **Microsoft Access** or **Microsoft SQL Server/MSDE** as database. Configure the database type selected to store the newsletter/discussion subscribers list. The available options are:

Option	Description
Microsoft Access	Specify a database name and location. GFI MailEssentials automatically creates a database.
Microsoft SQL Server	Specify SQL server name, database and logon credentials used to store newsletter/discussion subscribers list. Click Test to ensure that GFI MailEssentials can connect with the specified Microsoft SQL Server.

NOTE

You can use Microsoft Access for lists of up to a maximum of 5000 members.

4. Customize your distribution list. For more information, refer to [Configuring advanced newsletter/discussion list properties](#) (page 220).

5. Click **Apply**.

8.3.2 Using Newsletters/Discussions

After creating a newsletter/discussion list, users must subscribe to be part of the list.

Action	Description
Subscribing to list	Ask users to send an email to <newslettername>-subscribe@yourdomain.com
Completing subscription process	On receiving the request, list server sends a confirmation email back. Users must confirm their subscription via a reply email to be added as a subscriber. NOTE: The confirmation email is a requirement and cannot be turned off.
Sending a newsletter/discussion post	Members with permissions to send email to the list are required to send the email to the newsletter list mailing address: <newslettername>@yourdomain.com
Unsubscribing from list	To unsubscribe from the list, users must send an email to: <newslettername>-unsubscribe@yourdomain.com

NOTE

To enable users to easily subscribe to newsletters, add a web form asking for name and email address and automatically generate an email where the sender is the email address of the new user and the recipient is:

<newslettername>-subscribe@yourdomain.com

8.3.3 Configuring advanced newsletter/discussion list properties

After creating a new list, further options can be configured which enable the customization of elements and behavior of the list. These options include:

- » [Creating a custom footer for the list](#)
- » [Setting permissions to the list](#)
- » [Manually adding subscribers to the list](#)
- » [Importing subscribers to the list/database structure](#)

Creating a custom footer for the list

1. From the **Footer** tab configure a custom discussion list footer. A footer is added to each email sent to the list.
2. Use the HTML editor to add an HTML version of the footer. To add variable fields in the list footer, navigate to **Insert > Variables**. Select the variable to add and click **Add**.
3. You can also enter a plain text footer for plain text lists. Click **Variable...** to add variable fields.
4. Click **Apply**.

Tip

You can use footers to show how users can subscribe/unsubscribe from list and/or to promote your social media channels.

Setting permissions to newsletters

Specify the users who can submit newsletters.

NOTE

Permissions are not configurable for discussion lists.

1. Open an existing or create a new list and go to the **Permissions** tab.
2. Key in an email address that can send newsletters and click **Add**. The email address is added to the list.
3. A newsletter password secures access to newsletter in case someone else makes use of the email client or account details of a permitted user. Enable passwords by selecting the **Password required:** checkbox and providing a password.

NOTE

When sending emails to the newsletter, users must authenticate themselves by including the password in the email subject field. Password must be specified in the subject field as follows:

```
[PASSWORD:<password>] <Subject of the email>
```

Example: [PASSWORD:letmepost]Special Offer.

If password is correct, the list server automatically removes the password details from subject and relays email to newsletter subscribers.

4. Click **Apply**.

Manually adding subscribers to the list

Manually add users to newsletters/discussions without any action on their behalf.

NOTE

It is highly recommended that users subscribe themselves to the list by sending an email to the subscribe newsletter/discussion address. Ensure that you have users' authorization before manually adding them to the list.

1. Open an existing or create a new list and go to the **Subscribers** tab.
2. Key in the subscriber details in **Email Address** (required), **First name**, **Last name** and **Company** fields and click **Add**. The new subscriber email address is added to list.
3. To remove users from the subscription list table when unsubscribing from the list (and not just flag them as unsubscribed) select **Delete from database when user unsubscribes** checkbox.
4. Click **Apply**.

Importing subscribers to the list / database structure

When a new newsletter or discussion list is created, a table called 'listname_subscribers' with the following fields is created in the database.

To import data into the list, populate the database with data in the following fields.

Field Name	Type	Default Value	Flags	Description
Ls_id	Varchar(100)		PK	Subscriber ID
Ls_first	Varchar(250)			First name
Ls_last	Varchar(250)			Last name
Ls_email	Varchar(250)			Email
Ls_unsubscribed	Int	0	NOT NULL	Unsubscribe flag
Ls_company	Varchar(250)			Company name

8.4 Mail Monitoring

Mail monitoring enables copying emails sent to or from a particular local email address to another email address. This enables the creation of central store of email communications for particular persons or departments.

8.4.1 Adding new Mail Monitoring rules

1. Go to **Email management > Mail Monitoring**.
2. Click **Add Rule....**
3. From the **General** tab configure the following options:

Option	Description
Mail Monitor Name	Key in a friendly mail monitoring rule name.
Inbound or Outbound	Select whether to apply rule to inbound or outbound emails.
Copy monitored email to user or email address	The destination email address or mailbox where to copy the emails to. Select Email Address to manually key in an email address or select User to look-up

Option	Description
If sender is	Specify the email address of the sender to monitor. Click All Domains to monitor emails sent by all users.
and recipient is	Specify the email address of the recipient to monitor. Click All Domains to monitor emails received by all users.

- Click **Add** to add the configured rule.
- Repeat the above steps to specify multiple filters.
- From the **Exceptions** tab specify users and email addresses for whom the rule shall not apply. The available options are:

Option	Description
Except if sender is	Excludes the specified senders from mail monitoring. For inbound monitoring rules, key in non-local email addresses. For outbound monitoring rules, all addresses in this list are local. Click Search User to find local email addresses and click Add .
Except if recipient is	Excludes the specified recipients from the list. For inbound monitoring rules, all addresses in this list are local. Click Search User to find local email addresses and click Add . For outbound monitoring rules, key in non-local email addresses.

- Click **Apply**.

8.4.2 How to use Mail Monitoring

Refer to the below table for information on how to configure mail monitoring for different requirements and scenarios:

What to monitor	Description
All email sent by a particular user	Create an outbound rule and specify sender email or select user (if using AD) in the sender field. Click All Domains in the recipient's field.
All email sent to a particular user	Create an inbound rule and specify the recipient's email address or select user (if using AD) in the recipient field. Click All Domains in the sender's field.
Mail sent by a particular user to an external recipient	Create an outbound rule, specify sender or select user (if using AD) in the sender field. Key in external recipient email in the recipient field.
Mail sent to a particular user by an external sender	Create an inbound rule and specify external sender email address in the sender field. Key in email address or select user (if using AD) in the recipient field.
Mail sent by a particular user to a company or domain	Create an outbound rule and specify sender or select user (if using AD) in the sender field. Specify the domain of the company in the recipient field.
Mail sent to a particular user by a company or domain	Create an inbound rule and specify domain of the company in the sender field. Select domain when clicking on the sender button and enter username or user email address in the recipient field.

8.4.3 Enabling/Disabling email monitoring rules

- Go to **Email management > Mail Monitoring**.

2. Select the rule to enable/disable.
3. Click **Enable Selected** or **Disable Selected** to enable or disable the selected rule respectively.
4. Click **OK** to save changes.

9 General Settings

Topics in this chapter:

9.1 Perimeter SMTP Server Settings	224
9.2 Administrator email address	225
9.3 Enabling/Disabling scanning modules	226
9.4 Proxy settings	227
9.5 Local domains	229
9.6 Managing local users	230
9.7 Remote Active Directory mode	231
9.8 Licensing	232
9.9 SMTP Virtual Server bindings	233
9.10 Product Updates	234
9.11 Access Control	236
9.12 Notification Templates	238

9.1 Perimeter SMTP Server Settings

SMTP servers that relay emails to the GFI MailEssentials server must be specified.

1. From the GFI MailEssentials Configuration, go to **General Settings > Perimeter SMTP Servers**.

Perimeter SMTP Servers

 Specify which SMTP servers receive emails directly from the internet

This is the only SMTP server which receives emails from the internet
 The following SMTP servers receive email directly from the internet and forward them to this server:

SMTP Server (IP / CIDR)

SMTP Server:

Description:

SMTP Server list

<input type="checkbox"/>	Server	Description
No records to display.		

Detect button will automatically retrieve MX records of inbound domains.

Screenshot 128: Perimeter SMTP Server settings

2. Configure the following options:

Option	Description
This is the only SMTP server which receives emails from the Internet	Select this option when GFI MailEssentials is installed on the only SMTP server that receives external emails directly from the Internet.
The following SMTP servers receive emails directly from the Internet and forward them to this server	Emails are relayed to the GFI MailEssentials server from other SMTP servers. Add these SMTP Servers in the SMTP Server list: Automatic detection: To automatically detect SMTP servers by retrieving MX records of inbound domains, click Detect . Manual addition: To manually add the IP addresses of SMTP servers that relay emails to the GFI MailEssentials server, key in the IP address or a range of IP addresses (using CIDR notation) and click Add SMTP Server NOTE: This option is also required for installations in a Multi-Server environment. For more information, refer to GFI MailEssentials Multi-Server (page 272).

3. Click **Apply**.

9.2 Administrator email address

GFI MailEssentials sends important notifications to the administrator via email. To set up the administrator's email address:

1. From the GFI MailEssentials Configuration navigate to **General Settings > Settings** and select the **General** tab.

Administrator email

Enter the administrator's email address in the field below. Notifications sent to the administrator will be sent to this email address.

Administrator Email:

NOTE: GFI MailEssentials will communicate this email address to the GFI servers. GFI will only use this email address to send important GFI MailEssentials notices directly to the administrator.

Screenshot 129: Specifying the administrator's email address

2. Key in the administrator's email address in the **Administrator email** area.
3. Click **Apply**.

9.3 Enabling/Disabling scanning modules

From GFI MailEssentials you can enable or disable particular email scanning modules. This allows switching on and off scanning engines or filters in batch.

NOTE

This feature enables or disables particular scanning engines only. Disabled engines do not process inbound, outbound and/or internal emails. All other features of GFI MailEssentials, such as the quarantine store, is still functional.

1. From the GFI MailEssentials Configuration, navigate to **General Settings > Settings** and select the **General** tab.

Scanning Manager

Select which scanning modules will process emails:

- Enable Email Security
- Enable Anti-Spam
- Enable Content Filtering

Screenshot 130: Scanning Manager

2. Enable or disable scanning modules:

Option	Description
Enable Email Security	Enables/Disables the following scanning engines: <ul style="list-style-type: none"> » Virus Scanning Engines » Information Store Protection » Trojan & Executable Scanner » Email Exploit Engine » HTML Sanitizer

Option	Description
Enable Anti-Spam	Enables/Disables the following anti-spam filters: <ul style="list-style-type: none"> » SpamRazer » Anti-Phishing » Directory Harvesting » Email Blocklist » IP Blocklist » IP DNS Blocklist » URI DNS Blocklist » Sender Policy Framework » Anti-Spoofing » Greylist » Language Detection » Header Checking » Spam Keyword Checking » Bayesian Analysis » Whitelist » New Senders
Enable Content Filtering	Enables/Disables the following content filtering engines: <ul style="list-style-type: none"> » Keyword Filtering » Attachment Filtering » Decompression Engine » Advanced Content Filtering

3. Click **Apply**.

9.4 Proxy settings

GFI MailEssentials automatically checks for and downloads updates (for example, virus definitions updates and SpamRazer definitions) from the Internet. If the server on which GFI MailEssentials is installed, connects to the Internet through a proxy server, configure the proxy server settings as follows:

1. From GFI MailEssentials Configuration go to **General Settings > Settings** and select **Updates** tab.

General Updates Local Domains

 Automatic update checks

Proxy server settings

Enable proxy server

Proxy server: Port:

Proxy authentication settings

Configure proxy authentication settings

Enable proxy authentication

Username:

Password:

* For security reasons, the length in the password box above does not necessarily reflect the true password length

Screenshot 131: Updates server proxy settings

2. Select the **Enable proxy server** checkbox.
3. In the **Proxy server** field key in the name or IP address of the proxy server.
4. In the **Port** field, key in the port to connect on (default value is 8080).
5. If the proxy server requires authentication, select **Enable proxy authentication** and key in the **Username** and **Password**.
6. Click **Apply**.

9.5 Local domains

General Updates Local Domains

Local Domains

Local Domain

Domain:

Description:

Add

Local Domain List

<input type="checkbox"/>	Domain	Description
<input type="checkbox"/>	domaina.tcv	

Remove

Screenshot 132: Local Domains list

GFI MailEssentials requires the list of local domains to enable it to distinguish between inbound, outbound or internal emails. During installation or post install wizard, GFI MailEssentials automatically imports local domains from the IIS SMTP service or Microsoft® Exchange Server. In some cases, however, local domains may have to be added manually.

IMPORTANT

GFI MailEssentials only filters emails destined to local domains for spam. Some filters are also based on the direction. This is determined by the local domains

To add or remove local domains after installation, follow these steps:

1. Go to **General Settings > Settings** and select **Local Domains** tab.
2. Key in the name and description of the domain to add in the **Domain** and **Description** text boxes.
3. Click **Add** to include the stated domain in **Local Domains List**.

NOTE

To remove a listed domain, select it from the list and click **Remove**.

4. Click **Apply**.

9.6 Managing local users

GFI MailEssentials uses 4 ways to retrieve users depending on the installation environment. Choose the type of user mode during installation. The number of users retrieved is also used for licensing purposes.

9.6.1 GFI MailEssentials installed in Active Directory mode

When GFI MailEssentials is not installed on the same machine as your mail server and Active Directory is present, then GFI MailEssentials retrieves mail-enabled users from the Active Directory domain of which the GFI MailEssentials machine forms part.

9.6.2 GFI MailEssentials installed in Remote Active Directory mode

When GFI MailEssentials is installed on a machine that is not joined to a domain, it can be configured to retrieve mail-enabled users from a remote Active Directory domain using LDAP.

This mode can be used for example, when installing GFI MailEssentials in a DMZ, before the firewall that separates your internal and external networks. In this example, the GFI MailEssentials is typically not joined to the internal domain. In this mode, all other features of GFI MailEssentials function similarly to when GFI MailEssentials is joined to a domain.

Configure the Remote Active Directory server from the Switchboard. For more information, refer to [Remote Active Directory mode](#) (page 231).

9.6.3 GFI MailEssentials installed on the Microsoft® Exchange machine

When GFI MailEssentials is installed on the same machine as Microsoft® Exchange, GFI MailEssentials retrieves the Active Directory users that have a mailbox on the same Microsoft® Exchange Server.

9.6.4 GFI MailEssentials installed in SMTP mode

When you choose to install GFI MailEssentials in SMTP mode, the list of local users is stored in a database managed by GFI MailEssentials.

To populate and manage the user list when GFI MailEssentials is installed in SMTP mode, go to **General > Settings** and select the **User Manager** tab.

The **User Manager** tab displays the list of local users and allows you to add or remove local users. The list of local users is used when configuring user-based rules, such as **Attachment Filtering** rules and **Content Filtering** rules.

NOTE

GFI MailEssentials automatically populates the list of local users using the sender's email address in outbound emails.

To add a new local user:

1. Enter the email address in the **Email address** box.
2. Click **Add**.
3. Repeat to add more local users and click **Apply**.

To remove a local user:

1. Select the local user you want to remove from the **Local Users** list and click **Remove**.

2. Repeat to remove more local users and click **Apply**.

9.7 Remote Active Directory mode

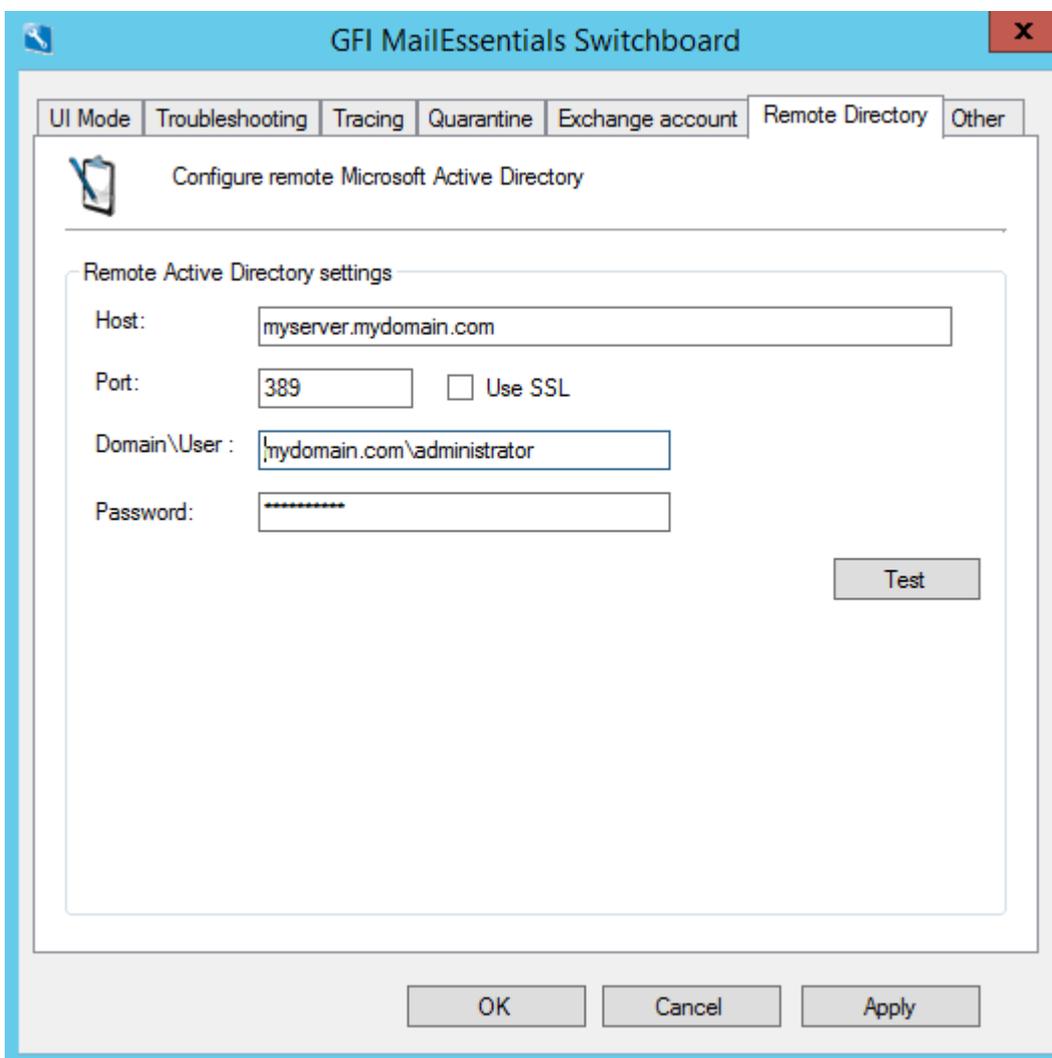
When GFI MailEssentials is installed in Remote Active Directory mode, configure the Remote Active Directory in use and connection settings from the Switchboard.

IMPORTANT

Use caution when changing Remote Active Directory settings. The newly retrieved user list may be different from existing user list (for example, when connecting to a different domain). In this case existing configurations may fail due to missing users.

To configure the Remote Active Directory connection:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard**.



Screenshot 133: GFI MailEssentials Switchboard - Remote Active Directory settings

2. Go to the **Remote Directory** tab and configure:

Option	Description
Host	Specify the host name of the remote Active Directory server.
Port	Key in the LDAP port to use to retrieve the list of users from Active Directory. By default LDAP uses port 389. To connect using a secure connection, select Use SSL , which by default uses port 636. An SSL certificate is required to use this setting. If there is a firewall between GFI MailEssentials and Active Directory, open the LDAP port to allow communication.
Domain\User & Password	Key in the credentials of a domain user which are used to connect to the directory service. Ensure that the password is not set to expire and does not change. If the password changes, this setting needs to be revised accordingly and you may experience some incorrect behavior by GFI MailEssentials since it will not be able to retrieve the list of users.

3. Click **Test** to ensure connection and retrieval of users from Active Directory.

4. Click **OK**.

9.8 Licensing

You should purchase a license that is equivalent to the number of mailboxes or users protected by GFI MailEssentials.

GFI MailEssentials 21 and later provides two licensing options:

- » Legacy licensing: Enter a valid license key in the product's user interface
- » Subscription licensing: Use a GFI Account that has a license for GFI MailEssentials. This method automatically synchronizes your license key with [GFI Accounts](#).

Screenshot 134: Licensing information

9.8.1 Editing License key

To modify your license information navigate to **General Settings > Licensing**. These are the available options:

Option	Description
GFI Account	Enter the username and password of an account that has a license for GFI MailEssentials assigned to it.
Available keys	Use the drop-down menu to select a key available for GFI MailEssentials.
Manually Enter license key	Type in manually the license for GFI MailEssentials
Reset GFI Account Credentials	Use this option if you have a GFI Account with a license assigned for GFI MailEssentials, but you cannot connect to GFI servers with the credentials entered.

9.8.2 License key information

To review your license information, including the subscription expiry date, go to **General Settings > Licensing** and review the details in the **License key information**.

Label	Description
Product Edition	The edition of GFI MailEssentials depending on the type of subscription purchased: <ul style="list-style-type: none">» Anti-spam - Enables the anti-spam filtering functionality. Security and anti-malware scanning engines are disabled.» EmailSecurity - Enables the security and anti-malware scanning engines. Anti-spam filters are disabled.» UnifiedProtection - Includes both the anti-spam and email security functionality.
Anti-spam	Indicates whether anti-spam functionality is licensed.
EmailSecurity	Indicates whether the security and anti-malware functionality is licensed.
Subscription status	Displays the date when the subscription expires. When the license expires, your email server will no longer be protected. GFI MailEssentials stops scanning emails and stops downloading updates.
Number of licensed users	The maximum number of users allowed, according to the purchased license.
Current number of users	The number of users protected by GFI MailEssentials.

9.8.3 How to determine license requirements

GFI MailEssentials counts the total mailboxes/email addresses, depending on the environment. For more information, refer to [Managing local users](#) (page 230).

Note that when the number of users in your environment exceeds the number of users allowed by the license key, GFI MailEssentials continues working for a 30 day grace period. Email scanning will stop if the license is not updated during this period or if the license user limit is not adjusted to reflect the increase in users.

9.9 SMTP Virtual Server bindings

GFI MailEssentials always binds to the first SMTP virtual server configured in IIS. In case of multiple SMTP virtual servers, GFI MailEssentials may be required to be bound to a new or a different SMTP Virtual Server.

NOTE

The SMTP Virtual Server Bindings tab is not displayed if you installed GFI MailEssentials on a Microsoft® Exchange Server 2010 or later machine.

9.9.1 Binding GFI MailEssentials to another other SMTP Virtual Server.

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

1. Go to **General Settings > Settings** and click **Bindings** tab.
2. Select the SMTP Virtual Server to bind GFI MailEssentials to.
3. Click **Apply**.
4. GFI MailEssentials will ask to restart services for the new settings to take effect.

9.10 Product Updates

The Product Updates feature verifies if there are any software patches available for your version of GFI MailEssentials by directly connecting to the GFI Update Servers.

By default, GFI MailEssentials downloads updates automatically on a preset schedule.

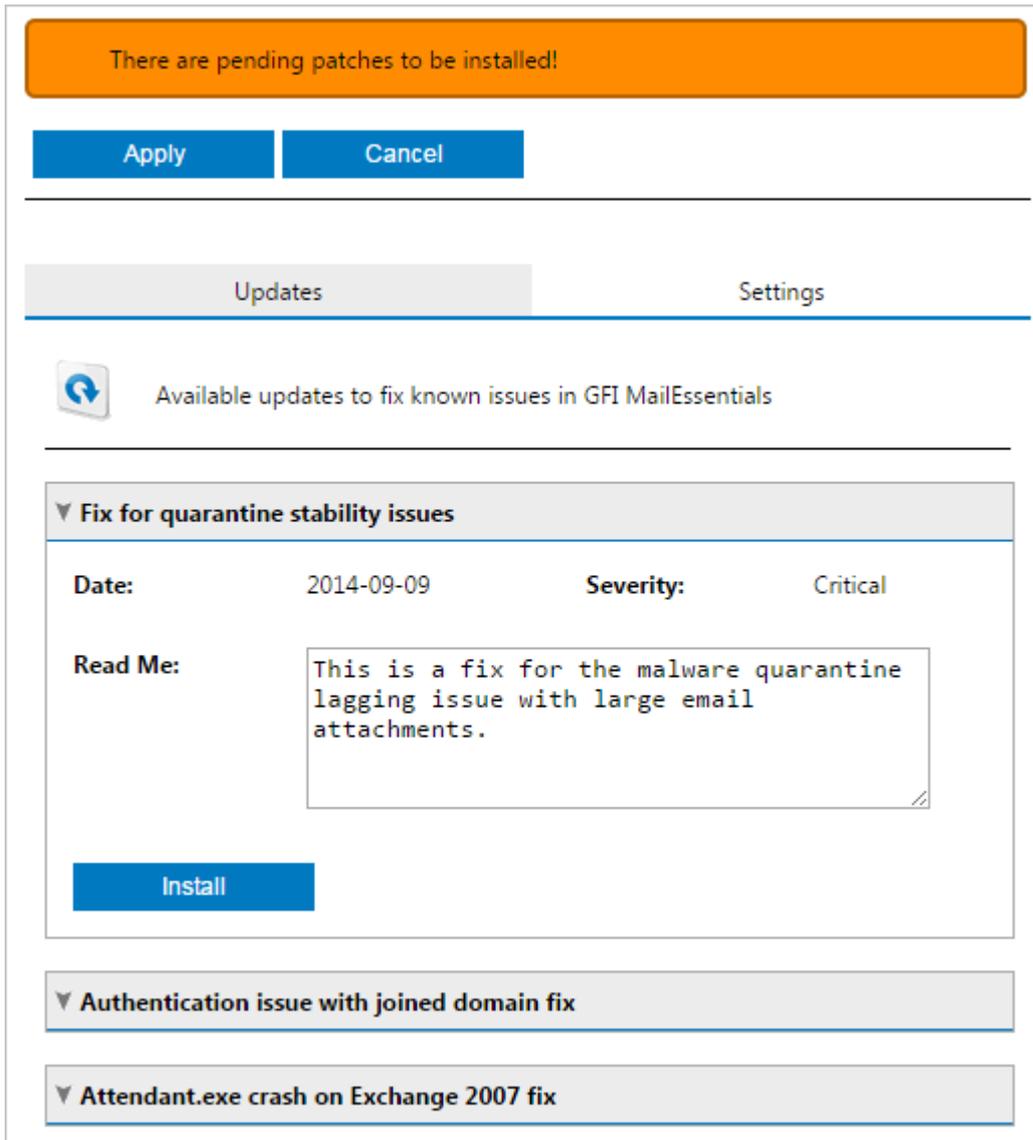
NOTE

It is highly recommended to check have this feature to download updates automatically to keep GFI MailEssentials updated.

9.10.1 Viewing and installing downloaded updates

To view or install downloaded updates:

1. Navigate to **General Settings > Product Updates** and select **Updates** tab.



Screenshot 135: View and install product updates

2. Expand any updates to see details about the downloaded updates. Click **Install** to install update.

9.10.2 Disabling or modifying schedules

To disable or modify this schedule:

1. Navigate to **General Settings > Product Updates** and select **Settings** tab.

Updates
Settings

Define the schedule when updates will be downloaded and installed

Settings

Manual
 Automatic

Daily at

Weekly on at

First of the month at

Last of the month at

Note

Updates are essential and keep your GFI MailEssentials server free from any known issues and security threats. GFI stresses that all updates are tested thoroughly prior release. Please note that certain updates require restart of GFI MailEssentials services and/or Microsoft Exchange / SMTP services, depending upon the update being installed.

Screenshot 136: Disable or modify product update schedule

2. Edit the following options:

Option	Description
Manual	Disables the schedule. Check for updates will only be triggered manually.
Automatic	Enables the schedule. Also configure the schedule that the update will follow: <ul style="list-style-type: none"> » Daily - Checks for updates daily at the set time. » Weekly - Checks for updates weekly at the set date and time. » First - Checks for updates on the first day of the month that is chosen and at the specified time. » Last - Checks for updates on the last day of the month that is chosen and at the specified time.

3. Click **Apply**.

9.11 Access Control

Allow or block access to various features of GFI MailEssentials for particular domain users or groups. Users can access the Web UI of GFI MailEssentials using their domain credentials. The features shown to logged in users depends on the Access Control configuration.

NOTE

Configuring access control from the web UI is only possible when GFI MailEssentials is running in IIS mode and can be accessed over the network. Access Control is configurable from the Switchboard when GFI MailEssentials is running in Local mode. For more information, refer to [Access Control List](#) (page 246).

The **Domain Admins** group (in an Active Directory environment only) and the server administrator account/group are automatically given full access privileges to all features of GFI MailEssentials.

Other users or groups can be given full or partial access to certain GFI MailEssentials features. To add users to the Access Control list:

1. From GFI MailEssentials Configuration, go to **General Settings > Access Control**. Add domain users or groups and select the product features to allow access to.

Access Control

 Configure who can access GFI MailEssentials and what features are available for which users.

	User/Group Name	Full Access	Quarantine Access	Reporting Access	RSS Access	Delete
	domaina\Administrators	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	domaina\Domain Admins	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	domaina\Administrator(Administrator@domaina.tcv)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

[Add User/Group](#)

Screenshot 137: Access control settings

2. Click **Add User/Group**.
3. In the **User Lookups** dialog, enter the name of the user or group to add and click **Check Names**.
4. GFI MailEssentials displays the list of users/groups found. Select the users/groups to add and click **Submit**.
5. For the newly added users/groups, select the features to allow access to.

Permission	Description
Full Access	User can access and configure all features of the product.
Quarantine	Allows access to quarantine search and search folders .
Reporting	Enables users to generate reports .
RSS	Allows users to subscribe to the quarantine RSS feeds .

6. Click **Apply**.

9.12 Notification Templates

GFI MailEssentials can send email notifications based on various events. Such emails are built from templates which are stored in the GFI MailEssentials installation directory. Users with experience in XSLT and XML can customize the design and the content of the templates.

IMPORTANT

Template modifications are for advanced users only. Preserve the structure of the template, special tags and the structure of the HTML syntax to avoid display issues in email notifications.

The **Templates** node lists the templates that are available in GFI MailEssentials. The templates are located in `\GFI\MailEssentials\Templates`. A template's name mirrors the folder name. Each template has a link to edit the template.

NOTE

The changes made in this page can be propagated to other GFI MailEssentials servers in the same network using the [Multi-server synchronization](#) feature.

The screenshot displays the 'Templates' configuration page. At the top, there is a 'Templates' tab. Below it, a blue banner states: 'The templates on this page will be synced to all MailEssentials servers'. A button with a folder icon and a checkmark is labeled 'Configure Notification Templates'. Below this is a section titled 'Configure Notification Templates' containing a table of notification templates.

Notification Templates
AUAPFAILEDDOWNLOAD
AUAPFAILEDUPDATE
AUAPSUCCESS
AUBFAILEDDOWNLOAD
AUBFAILEDUPDATE
AUBSUCCESS
auerrordownload
auerrorupdate
auerrorupdateerp
updatefailed
updateinstalled

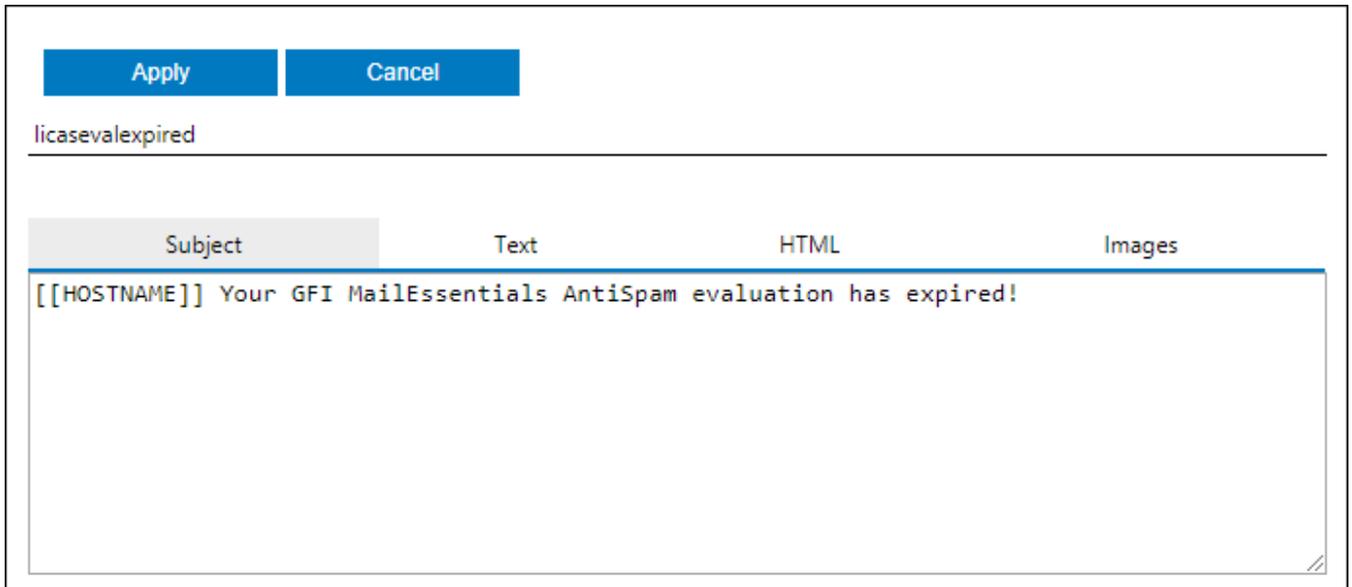
Screenshot 138: Templates note within the General Settings

9.12.1 Editing Templates

Administrators can edit templates to customize their design and their content.

To edit a template:

1. From the GFI MailEssentials Configuration, go to **General Settings > Templates**.
2. Click the template you want to edit.



Screenshot 139: Edit template options

3. The following options may be available:

Option	Content
Subject	Edit the email Subject
Text	Edit the plain text version of the email body.
HTML	Edit the HTML version of the email body.
Images	Change inline images for HTML emails. Click Edit and Choose File .

4. Click **Apply**.

List of Notification Templates

Here is a list of available templates:

Template	Component	Subject
AUAPFAILEDDOWNLOAD	Updates	Failed to check for Anti-Phishing updates.
AUAPFAILEDUPDATE	Updates	Failed to update local Anti-Phishing data.
AUAPSUCCESS	Updates	Anti-Phishing data updated.
AUBFAILEDDOWNLOAD	Updates	Failed to check for antispam updates.
AUBFAILEDUPDATE	Updates	Failed to update local antispam database.
AUBSUCCESS	Updates	Antispam database updated.

Template	Component	Subject
auerrordownload	Updates	Failed to download [ENGINE] update files.
auerrorupdate	Updates	Failed to update local [ENGINE] engine files.
auerrorupdateerp	Updates	Failed to update local [ENGINE] engines files (ERP).
aunewfilesavail	Updates	New [ENGINE] update files are available for download.
AUSRFAILEDDOWNLOAD	Updates	Failed to check for SpamRazer updates.
AUSRFAILEDUPDATE	Updates	Failed to update local SpamRazer data.
AUSRSUCCESS	Updates	SpamRazer data updated.
auupdated	Updates	New [ENGINE] update files downloaded and installed.
auupdatederp	Updates	New [ENGINE] update files downloaded and installed (ERP).
ConfigHostFailure	Multi Install Network	GFI MailEssentials failed to connect to the configuration master server!
ConfigHostRestored	Multi Install Network	Connection to the GFI MailEssentials Multi-Install configuration master server restored!
delnotifyuser	Malware Quarantine	Delete Notification: The administrator deleted an item from the GFI MailEssentials quarantine.
digest	Spam Quarantine	GFI MailEssentials Spam Digest.
EWSInfoStoreScanItemFail	Information Store Protection	GFI MailEssentials EWS Information Store did not scan an item.
EWSInfoStoreScanMailboxFail	Information Store Protection	GFI MailEssentials EWS Information Store did not scan a mailbox.
failedmails	License	Emails failed to be processed by GFI MailEssentials.
licasevalexpired	License	Your GFI MailEssentials AntiSpam evaluation has expired!
licasevalexpirednfr	License	Your GFI MailEssentials AntiSpam evaluation has expired! (NFR)
licasevalwillexpire	License	Your GFI MailEssentials AntiSpam evaluation will expire in [X] days!
licasevalwillexpirenfr	License	Your GFI MailEssentials AntiSpam evaluation will expire in [X] days! (NFR)
licavevalexpired	License	Your GFI MailEssentials EmailSecurity evaluation has expired!
licevalexpired	License	Your GFI MailEssentials evaluation has expired!
licevalexpirednfr	License	Your GFI MailEssentials evaluation has expired! (NFR)
licavevalwillexpire	License	Your GFI MailEssentials EmailSecurity evaluation will expire in [X] days!
licavevalwillexpirenfr	License	Your GFI MailEssentials EmailSecurity evaluation will expire in [X] days! (NFR)
licevalexpired	License	Your GFI MailEssentials evaluation has expired!
licevalexpirednfr	License	Your GFI MailEssentials evaluation has expired! (NFR)

Template	Component	Subject
licevalwillexpire	License	Your GFI MailEssentials evaluation will expire in [X] days!
licevalwillexpirenfr	License	Your GFI MailEssentials evaluation will expire in [X] days! (NFR)
licgpexpired	License	The number of users for which GFI MailEssentials is licensed has been exceeded. Please contact sales.
licgpstarted	License	The number of users for which GFI MailEssentials is licensed has been exceeded.
LowDiskSpace	Malware Quarantine	GFI MailEssentials free disk space for Quarantine stores is less than 1GB.
LowDiskSpace_ME	Spam Quarantine	GFI MailEssentials free disk space for Spam Quarantine is less than 1GB.
LowDiskSpace_MSEC	Malware Quarantine	GFI MailEssentials free disk space for Malware and Content quarantine store is less than 1GB.
MultiInstallVersionMismatch	Multi Server Network	GFI MailEssentials build is incompatible with master server.
notifymanager	Malware Quarantine	Administrative Notification: GFI MailEssentials detected a threat.
notifyuser	Malware Quarantine	Notification: GFI MailEssentials detected a threat.
oboundsnkcrit	Scan Engine	Critical failure occurred on the sender's messaging system
outofspace	Spam Quarantine	GFI MailEssentials stopped quarantining spam due to limited disk space.
LowDiskSpace_ME	Spam Quarantine	GFI MailEssentials free disk space for Spam quarantine store is less than 1GB.
LowDiskSpace_MSEC	Malware Quarantine	GFI MailEssentials free disk space for Malware and Content quarantine store is less than 1GB.
patchsvcnewpatch	Product Updates	New GFI MailEssentials patch(es) available for download.
quaractionform	Malware Quarantine	Quarantine Action Form
QuarantineHostFailure	Multi Server Network	GFI MailEssentials failed to connect to the quarantine master server!
QuarantineHostRestored	Multi Server Network	Connection to the GFI MailEssentials Multi-Install quarantine master server restored!
QuarDigest	Spam Quarantine	GFI MailEssentials Quarantine Digest.
reportingdblimit	Reporting	Reporting database size notification.
ReportingHostFailure	Multi Server Network	GFI MailEssentials failed to connect to the reporting master server!
ReportingHostRestored	Multi Server Network	GFI MailEssentials has restored the connection to the reporting master server!
ReportingNotWorking	Reporting	GFI MailEssentials reporting failed!

Template	Component	Subject
ReportsSQLConnDown	Reporting	GFI MailEssentials notification.
saproverereport	Scan Engine	GFI MailEssentials report.
scheduledreport	Reporting	GFI MailEssentials Schedule Report.
securityreport	Scan Engine	GFI MailEssentials Security Report.
securityreportvsapi	Information Store Protection	GFI MailEssentials Security VSAPI Report.
SubscriptionExpired	License	GFI MailEssentials subscription expired!
SubscriptionNoFiltering	License	GFI MailEssentials subscription expired - Final notice!
SubscriptionPreExpired	License	GFI MailEssentials subscription renewal!
tolevelthreat	Scan Engine	GFI MailEssentials has detected a threat and removed the message.
updateavailable	Product Updates	A GFI MailEssentials update is now available.
updatefailed	Product Updates	GFI MailEssentials update installation failed!
updateinstalled	Product Updates	GFI MailEssentials update installed successfully.

10 Miscellaneous topics

Topics in this chapter:

10.1 Installation information	244
10.2 Virtual directory names	244
10.3 User interface mode	245
10.4 GFI Directory mode	248
10.5 Failed emails	249
10.6 Tracing	251
10.7 POP2Exchange - Download emails from POP3 server	253
10.8 Moving spam to user's mailbox folders	257
10.9 Set a Microsoft® Exchange account	260
10.10 Exporting and importing settings manually	260
10.11 Disabling email processing	265
10.12 Email backup before and after processing	266
10.13 Remoting ports	268
10.14 Monitoring Virus Scanning API	269

10.1 Installation information

Current build version information	
Version:	2015
Build:	20150826

Screenshot 140: Version Information page

To view the GFI MailEssentials version information, navigate to **About** node. The **Version Information** tab displays the GFI MailEssentials installation version and build number.

To check whether you have the latest build of GFI MailEssentials installed on your machine, click **Check if newer build exists**.

NOTE

Always quote your GFI version and build information when contacting GFI support.

The **3rd Party Licenses** tab lists third party components in use by GFI MailEssentials.

10.2 Virtual directory names

The default virtual directory names of GFI MailEssentials and Quarantine RSS are **MailEssentials** and **MailEssentialsRSS** respectively. Virtual directory names are customizable; however it is recommended that these are not changed.

NOTE

If GFI MailEssentials is configured to be accessed only from the local machine, the GFI MailEssentials Configuration virtual directory is not configurable.

1. Launch GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard**.
2. From **IIS user interface mode options** area, specify custom virtual directory names for:

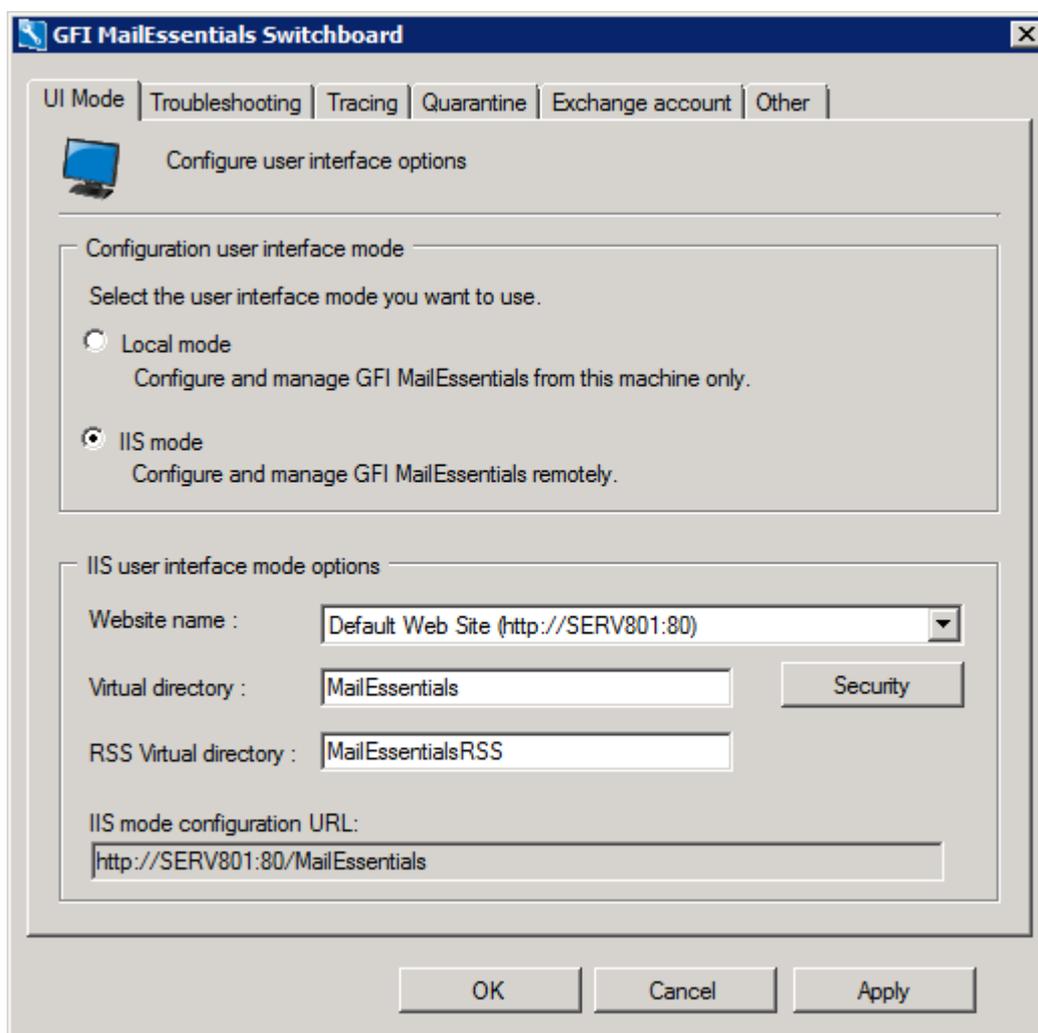
- » GFI MailEssentials Configuration - key in a custom name in the **Virtual directory** field.
 - » Quarantine RSS virtual directory - key in a custom name in the **RSS Virtual directory** field.
3. Click **Apply**.
 4. Click **OK** and wait while applying the new settings.
 5. When the process completes, click **OK**.

10.3 User interface mode

The GFI MailEssentials user interface can be loaded on the installation machine only (local mode) or accessible via http over the network (IIS mode).

To select the mode:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard**.



Screenshot 141: GFI MailEssentials Switchboard - UI Mode

2. From the **UI mode** area, select:

Option	Description
Local mode	<p>GFI MailEssentials loads in an html viewer application, accessible from the machine where GFI MailEssentials is installed only.</p> <p>NOTE If using Local mode:</p> <ul style="list-style-type: none"> » Spam digest links will not work » User portal will not be available - users will not be able to manage personal whitelists and blocklists and their personal quarantine. For more information, refer to End User Actions (page 15).
IIS mode (recommended)	<p>GFI MailEssentials loads in your default web browser using the IIS setup settings configured during installation. User interface is also accessible over the network via http.</p> <p>NOTE IIS setup settings can be altered using the Website name, Virtual directory and RSS virtual Directory fields. The Security options enable the configuration of an Access Control List and the IIS Authentication.</p>

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

3. Click **Yes** to restart the displayed services.
4. Click **OK**.

10.3.1 IIS Security Settings

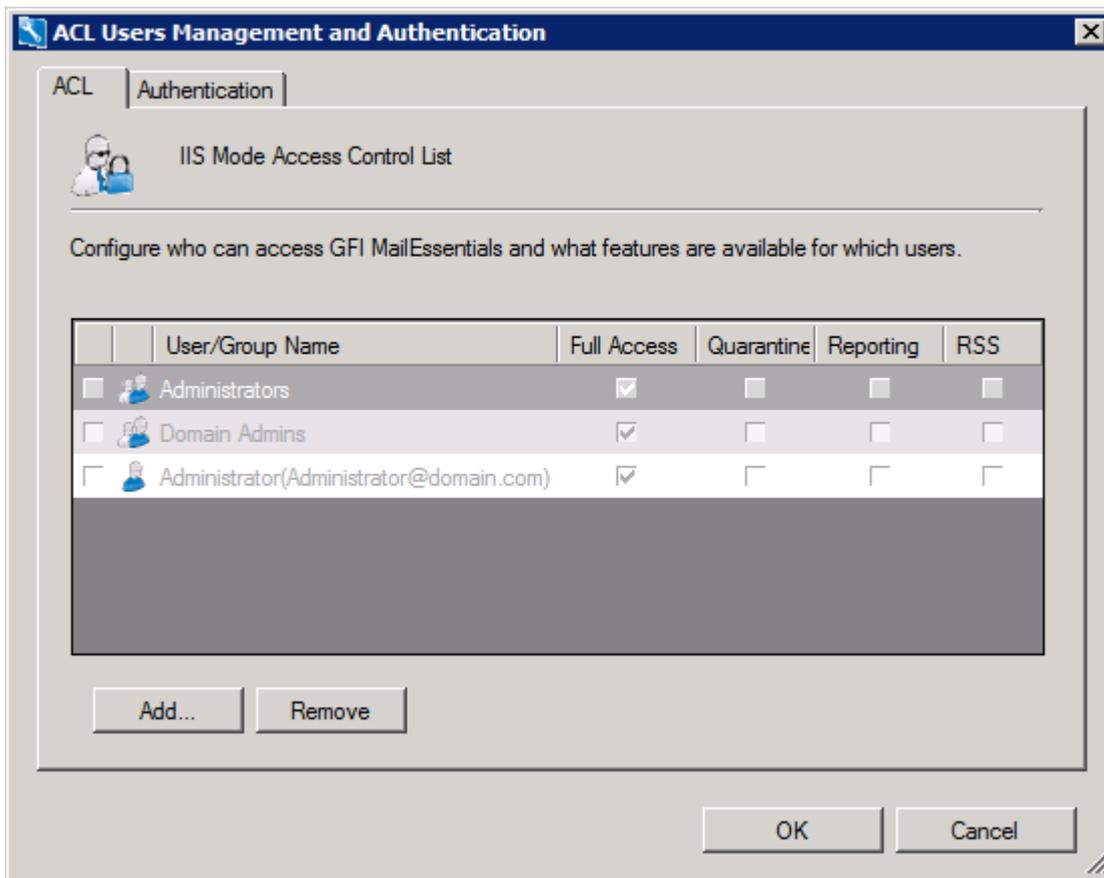
The **Security** button within the UI mode tab enables you to configure an Access Control List and Authentication method.

Access Control List

The Access control list specifies who can access GFI MailEssentials and what features are available for which users or groups. By default, Administrators are granted full access to GFI MailEssentials; you can however specify specific users or groups with different access types.

To add a user:

1. Load the Switchboard by navigating to **Start > Programs > GFI MailEssentials > Switchboard**.
2. Select **UI Mode** tab. Click **IIS Mode** and select **Security**.



Screenshot 142: IIS Security - ACL tab

3. Click **Add...** and provide the name of the user or group to add to the list.
4. Select the type of access to grant. Available options are:

Permission	Description
Full Access	User can access and configure all features of the product.
Quarantine	Allows access to quarantine search and search folders .
Reporting	Enables users to generate reports .
RSS	Allows users to subscribe to the quarantine RSS feeds .

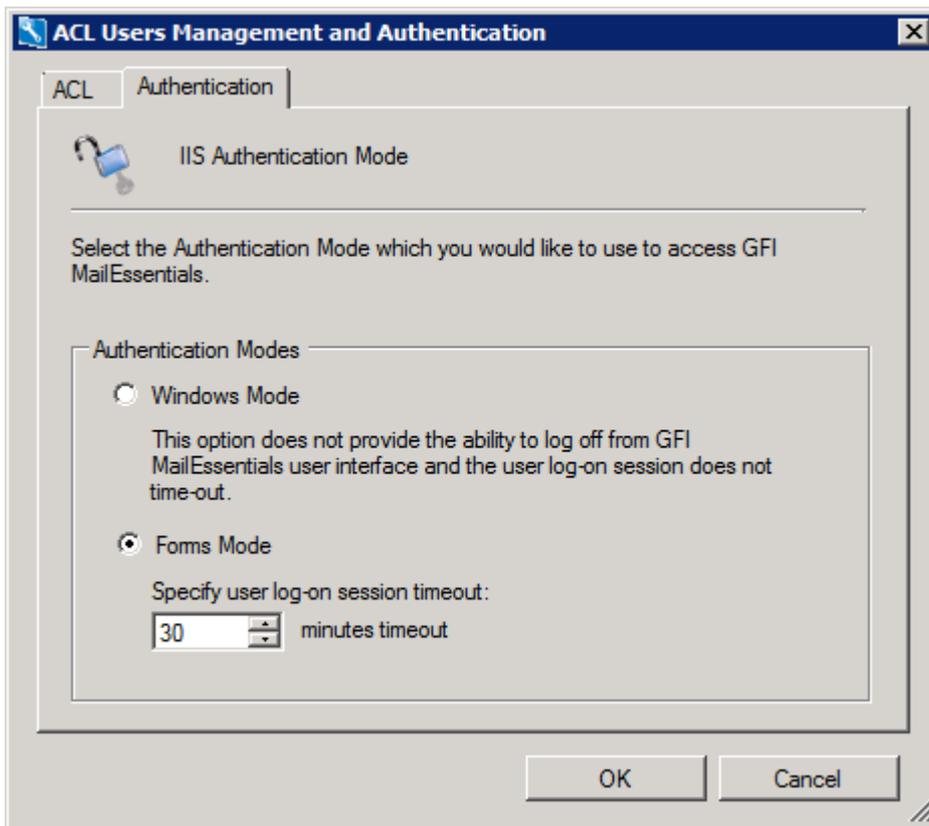
5. Click **OK** to finalize setup.

To remove access to a user or group, select the item to remove and click **Remove**.

IIS Authentication Mode

The IIS Authentication Mode enables you to choose the authentication method to use when accessing GFI MailEssentials.

1. Load the Switchboard by navigating to **Start > Programs > GFI MailEssentials > Switchboard**.
2. Select **UI Mode** tab. Click **IIS Mode** and select **Security**.
3. Select **Authentication** tab.



Screenshot 143: IIS Security - Authentication tab

4. Select one of the available options:

Option	Description
Windows Mode	Windows authentication enables GFI MailEssentials to make use of the credentials of the currently logged on user and does not provide log-off and automatic timeout of the user interface session.
Forms Mode	(Default) Forms authentication provides the ability for users to log off. It also enables you to configure an automatic timeout from the user interface session. This is recommended if end users are accessing their GFI MailEssentials user console, especially if used from public computers.

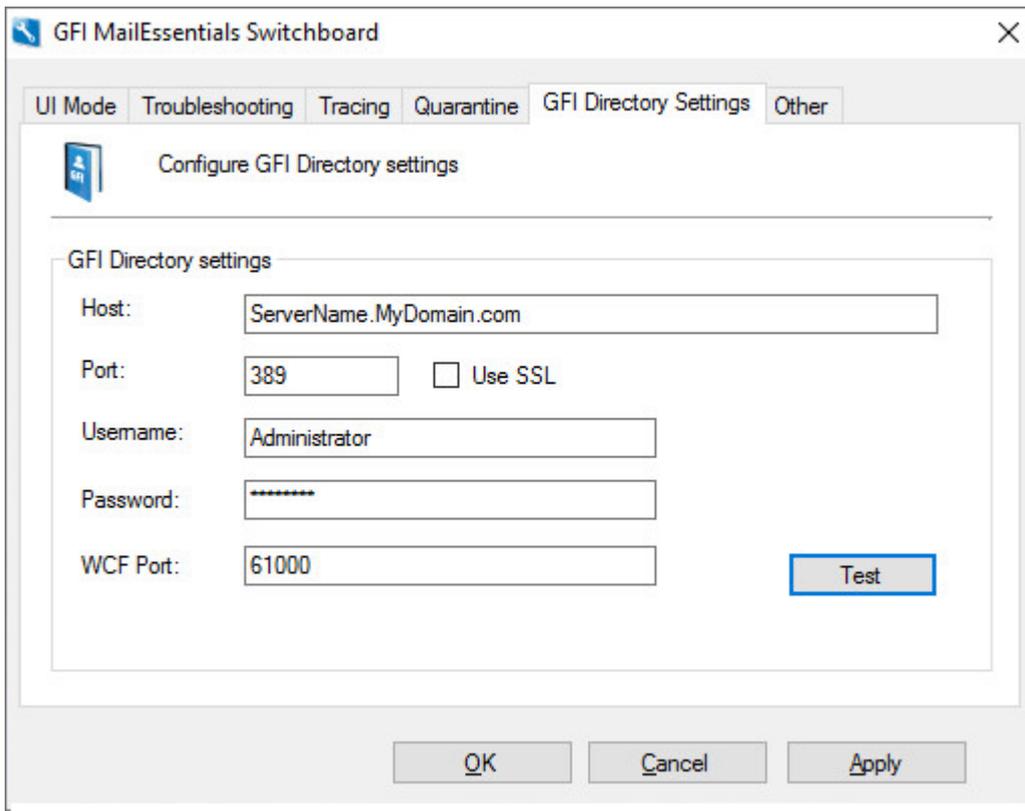
5. Click **OK** to save settings.

10.4 GFI Directory mode

When GFI MailEssentials is installed in GFI Directory mode, the connection settings are configured during the installation. At a later stage, the administrator can check or make changes to the settings from the Switchboard.

To revise the GFI Directory connection settings:

1. Launch the GFI MailEssentialsSwitchboard from **Start > Programs > GFI MailEssentials > Switchboard**.



Screenshot 144: GFI MailEssentials Switchboard - GFI Directory settings

2. Go to the **GFI Directory Settings** tab and configure:

Option	Description
Host	Specify the host name of the GFI Directory server. Use FQDN for the host name.
Port	Key in the LDAP port to use to retrieve the list of users from GFI Directory. By default, LDAP uses port 389. To connect using a secure connection, select Use SSL , which by default uses port 636. An SSL certificate is required to use this setting. If there is a firewall between GFI MailEssentials and GFI Directory, open the LDAP port to allow communication.
Username & Password	Key in the credentials of the user which are used to connect to GFI Directory. Ensure that the password is not set to expire and does not change. If the password changes, this setting needs to be revised accordingly, and you may experience some incorrect behavior by GFI MailEssentials since it will not be able to retrieve the list of users.
WCF Port	This port is used for communication between GFI MailEssentials and GFI Directory. The default port is 61000. This port must be open on the firewall.

3. Click **Test** to ensure connection and retrieval of users from GFI Directory.

4. Click **OK**.

For more information about GFI Directory refer to <http://go.gfi.com/?pageid=directory2.0UserHelp>

10.5 Failed emails

There may be instances where the GFI MailEssentials email security or content filters cannot scan an email, for example, emails containing corrupted header information. In this case, GFI MailEssentials blocks the email since it may contain malicious content. GFI MailEssentials moves these emails to the following folders, depending on the module that fails:

» **Email security module:** <GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\failedmails\

» **Spam filtering module:** <GFI MailEssentials installation path>\GFI\MailEssentials\Antispam\failedmails\

10.5.1 Reprocessing legitimate emails that fail

It is recommended to contact GFI Support when a number of emails are being moved to the **failedmails** folder. When the issue is resolved, emails can be re-scanned by GFI MailEssentials to determine if they are safe to be delivered.

NOTE

Files with extension .PROP in the **failedmails** folder are used for troubleshooting purposes. When reprocessing failed emails, these files can be deleted.

GFI MailEssentials installed on Microsoft® Exchange Server 2010 or newer

1. In the **failedmails** folder, change the extension of .TXT files to .EML.

NOTE

To automatically change the extension of all .TXT files in the **failedmails** folder to .EML files, from command prompt change the directory to the **failedmails** folder and run the following command:

```
ren *.txt *.eml
```

2. Move renamed files to the following folder:

<Microsoft Exchange installation path>\TransportRoles\Replay

GFI MailEssentials installed on Gateway server

1. In the **failedmails** folder, change the extension of .TXT files to .EML.

NOTE

To automatically change the extension of all .TXT files in the **failedmails** folder to .EML files, from command prompt change the directory to the **failedmails** folder and run the following command:

```
ren *.txt *.eml
```

2. Move renamed files to the following folder:

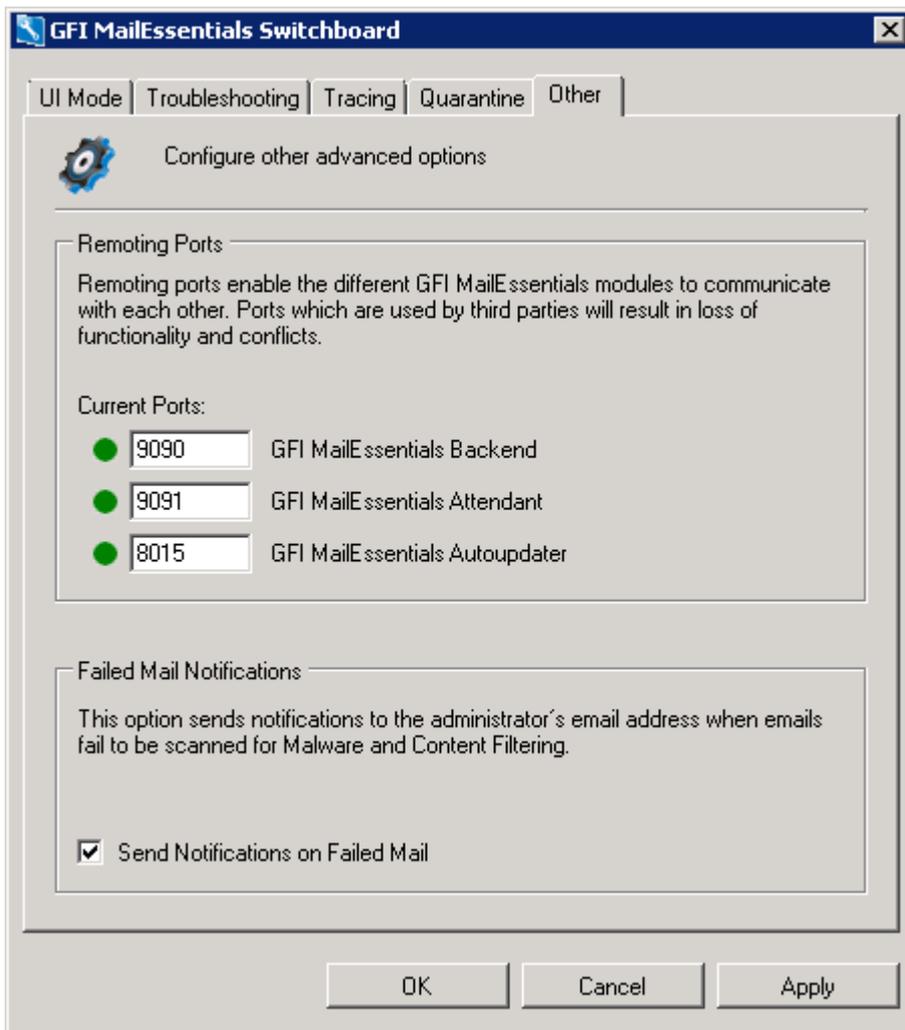
<drive>\Inetpub\mailroot\Pickup

10.5.2 Failed emails notifications

GFI MailEssentials can be configured to notify the administrator when an email fails to process.

The administrator's email address can be configured from GFI MailEssentials General Settings node. For more information, refer to [Administrator email address](#) (page 225).

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Other** tab.



Screenshot 145: Enabling Failed emails notification

2. Select **Send Notifications on Failed Mail**.
3. Click **Apply**.

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

4. Click **Yes** to restart the displayed services.
5. Click **OK**.

10.6 Tracing

GFI MailEssentials provides the facility of creating log files for debugging purposes. Use tracing for troubleshooting purposes or when contacting GFI Support. Disable tracing if there are performance issues with the GFI MailEssentials machine.

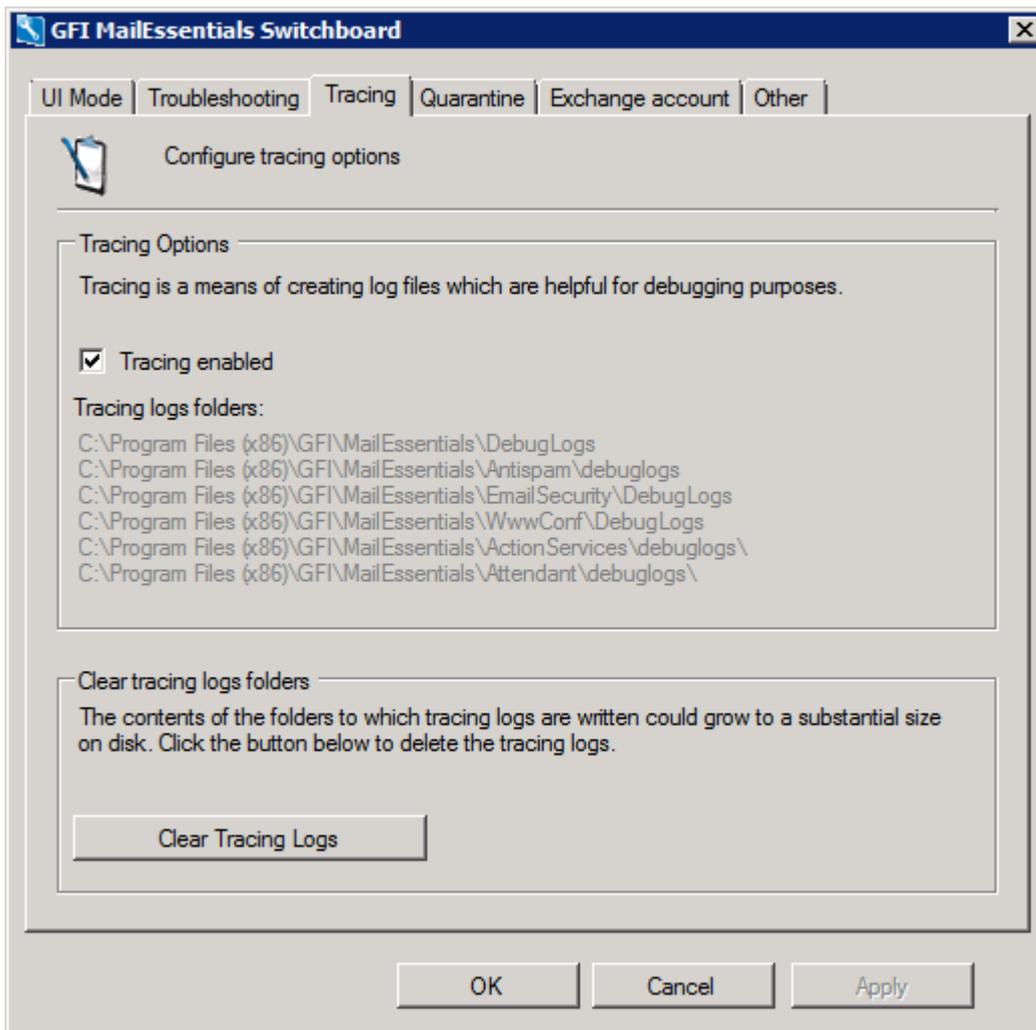
When enabled, GFI MailEssentials stores a number of log files in the following folders:

- » <GFI MailEssentials installation path>\GFI\MailEssentials\DebugLogs\
- » <GFI MailEssentials installation path>\GFI\MailEssentials\Antispam\DebugLogs\

- » <GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\DebugLogs\
- » <GFI MailEssentials installation path>\GFI\MailEssentials\WwwConf\DebugLogs\
- » <GFI MailEssentials installation path>\GFI\MailEssentials\ActionServices\DebugLogs\
- » <GFI MailEssentials installation path>\GFI\MailEssentials\Attendant\DebugLogs\
- » <GFI MailEssentials installation path>\GFI\MailEssentials\Backend\DebugLogs\

To enable or disable Tracing:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Tracing** tab.



Screenshot 146: Configuring Tracing options

2. Select or unselect **Tracing enabled** to enable or disable logging respectively.

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

3. Click **Yes** to restart the displayed services.
4. Click **OK**.

Clear Tracing Logs

To delete all Tracing logs:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Tracing** tab.

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

2. Click **Clear Tracing Logs** and click **Yes** to restart the displayed services.
3. Click **OK** when completed.

10.7 POP2Exchange - Download emails from POP3 server

POP2Exchange downloads emails from a POP3 server, processes them and sends them to the local mail server. The recommendation for GFI MailEssentials is to, if possible, avoid using POP3 and to use SMTP since POP3 is designed for email clients and not for mail servers. Notwithstanding this fact, and to cater for situations where a static IP address required by SMTP is not available, GFI MailEssentials can use POP3 to retrieve email.

10.7.1 Configuring POP3 downloader

1. Go to **POP2Exchange** node.

Enable POP2Exchange from POP3 server [Force Download](#)

POP3 Mailboxes

POP3 Server:

Port:

Use SSL Accept Invalid Certificate

Login:

Password:

Please provide an alternate address for this mailbox. If the recipient is not on a local domain, the email will be forwarded to this address.

Alternate address:

Send mail to:

POP3 Server	Login	Alternate address
No data available in table		

POP3 Options

Check every: (minutes)

Do not deliver mails larger than: (KBytes)
(emails will be sent to the post master instead)

If mail is larger, then:

Screenshot 147: The GFI MailEssentials POP3 downloader

2. In the **POP3** tab, select **Enable POP2Exchange from POP3 server** to enable POP3 downloader.
3. In the **POP3 Mailboxes** box, specify the details of the POP3 servers to download emails from:

Option	Description
POP3 Server	Key in the IP address of the POP3 server to download emails from.
Port	Key in the POP3 port. By default POP3 uses port 110, or port 995 when using a secure connection.
Use SSL	Select if the POP3 server requires a secure connection.
Accept Invalid Certificate	Select this option if you want to ignore unverified certificates from the POP3 server. It is recommended to unselect this option and ensure that all certificates are validated.
Login & Password	Specify the credentials to login to the POP3 mailbox.

Option	Description
Alternate address	If the emails in the mailbox are addressed to a recipient that is not on one of the GFI MailEssentials local domains, emails will be routed to this address. Ensure that this is a local address, configured on the mail server and protected by GFI MailEssentials.
Send mail to:	Choose: » Address stored in 'To' field: GFI MailEssentials analyzes the email header and routes the email accordingly. If email analyzing fails, email is sent to the email address specified in the Alternate address field. » Alternate address: GFI MailEssentials does not analyze the email headers and all emails from this mailbox are forwarded to email address configured in Alternate address .

4. Click **Add** to add the POP3 server details. Select an added POP3 Server and click **Update** to replace it with the newly entered settings.

5. Repeat the steps above to add multiple POP3 servers.

6. In **POP3 Options** configure:

Option	Description
Check every (minutes)	Specify the download interval in minutes.
Do not deliver mails larger than	Specify a maximum download size in KBytes. If email exceeds this size, it will not be downloaded.
If mail is larger, then:	Choose to delete email larger than the maximum allowed size, or send a message to the postmaster.

8. Click **Apply**.

10.7.2 Configure dial up connection options

1. Go to **POP2Exchange** node and select the **Dialup** tab.

2. Select **Receive mails by Dial-Up** or **Dial on Demand**.

POP3
Dialup

Configure connection for POP3 downloading

Receive mail by Dial-Up or Dial on Demand

Dialup Settings

Dial-Up Networking profile:

If not connected, dial
 Process only when already connected
 Dial on demand router

Username:

Password:

Process every (minutes):

Schedule

Send every

at

Everyday at 00:00
 Everyday at 01:00
 Everyday at 02:00
 Everyday at 03:00
 Everyday at 04:00
 Everyday at 05:00
 Everyday at 06:00
 Everyday at 07:00
 Everyday at 08:00
 Everyday at 09:00

Screenshot 148: Dialup options

3. Select a dial-up networking profile and configure a login name and password. The following options are available:

Option	Description
Dial-Up Networking profile	Choose the Dial-up Networking profile to use.
If not connected, dial	GFI MailEssentials will only dial-up if there is no connection.
Process only when already connected	GFI MailEssentials will only process email if a connection already exists.

Option	Description
Dial on demand router:	In case of an Internet connection that is automatically established (such as a dial on demand router) select this option. GFI MailEssentials will pick up email at the specified interval without triggering a dial-up connection.
Username & Password	Enter credentials used to logon to your ISP.
Process every (minutes)	Enter the interval in minutes.

- In the **Schedule** area, specify the hours when GFI MailEssentials should dial-up to pick up email.
- Click **Apply**.

10.8 Moving spam to user's mailbox folders

When GFI MailEssentials is installed on the Microsoft® Exchange Server, spam emails can be saved in a user's mailbox folder. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

If GFI MailEssentials is **NOT** installed on the Microsoft® Exchange Server, spam emails cannot be routed to a specific user's mailbox folder through the Spam Actions. Emails can still however be routed to the user's mailbox as described below. In the spam filter actions screen, use the **Tag the email with specific text** to add a tag to the email subject. This tag is then used to configure mail routing.

In Microsoft Exchange 2010 onwards, create a transport rule that forwards tagged emails to the user's Junk E-mail mailbox folder.

10.8.1 Microsoft® Exchange 2013/2016

Create a Microsoft® Exchange 2013/2016 Transport Rule that forwards tagged emails to the user's Junk E-mail mailbox folder.

IMPORTANT

In GFI MailEssentials Spam Actions select the **Tag the email with specific text** option only. If you select any other action, emails detected as spam will not reach the mailbox of the user, and therefore the configured transport rules will not be applicable.

To create a Transport Rule in Exchange 2013/2016:

- Launch the Microsoft® Exchange Administrative Center.
- Go to **Mail flow > Rules**.
- Click **Add +** and select **Create a new rule**.
- Type a name for the new rule, for example, `GFI MailEssentials SPAM`.
- Click **More options....**
- In **Apply this rule if...** select **The subject or body...** and choose **subject includes any of these words**.
- In **Specify words or phrases** key in the tag specified in the spam actions of each spam filter (example, `[SPAM]`) and click **Add +**. If using different tags for different spam filters, repeat until all tags are keyed in. Click **OK** on completion.

8. In **Do the following...** select **Modify the message properties** and choose **set the spam confidence level (SCL)**.
9. In **Specify SCL** choose **9** and click **OK**.
10. Specify additional properties for this rule. On completion click **Save**.

NOTE

Ensure that the Junk E-Mail folder is enabled for the users' mailboxes.

The transport rule created will now forward all emails which contain the GFI MailEssentials tag to the users' Junk E-mail folder.

10.8.2 Microsoft® Exchange 2010

To configure Microsoft® Exchange 2010 to forward tagged emails to the user's Junk E-mail mailbox folder, a Transport Rule needs to be created.

IMPORTANT

In GFI MailEssentials Spam Actions select the **Tag the email with specific text** option only. If you select any other action, emails detected as spam will not reach the mailbox of the user, and therefore the configured transport rules will not be applicable.

To create a Transport Rule in Exchange 2010:

1. Launch the Microsoft® Exchange Management Console.
2. Navigate to **Microsoft Exchange > Organization Configuration > Hub Transport** and select the **Transport Rules** node.
3. Click **New Transport Rule**.
4. Type a name for the new rule (example, `GFI MailEssentials SPAM`) and click **Next**.
5. In the **Conditions** area, select **When the Subject field contains specific words**.
6. In the **Edit rule** area, click **Specific Words** to enter the words used for tagging. Type the tag specified in the spam actions of each spam filter (example, `[SPAM]`) and click **Add**. Click **OK** when all words are added and click **Next**.
7. In the **Actions** area, select **Set the spam confidence level to value**.
8. In the **Edit rule** area, click **0** and set the confidence level to **9**. Click **OK** and click **Next**.
9. (Optional) Set any exceptions to this transport rule and click **Next**.
10. Click **New** to create the new Transport Rule.

NOTE

Ensure that the Junk E-Mail folder is enabled for the users' mailboxes.

The transport rule created will now forward all emails which contain the GFI MailEssentials tag to the users' Junk E-mail folder.

Install Rules Manager on the Microsoft® Exchange Server

1. From the GFI MailEssentials machine, go to:

`<GFI MailEssentials installation path>\GFI\MailEssentials\Antispam\`

2. Copy the following files to a folder on the Microsoft® Exchange Server:

- » rulemgmtres.dll
- » rulemgmt.exe
- » rule.dll
- » gfi_log.dll

3. From the Microsoft® Exchange Server, open command prompt and change the directory to the location where the Rules Manager files were copied.

4. In command prompt type: `regsvr32 rule.dll`

5. On confirmation, click **OK**.

Launch Rules Manager

1. From the Microsoft® Exchange Server, navigate to the location where Rules Manager files were copied and open **rulemgmt.exe**.

2. Select a Microsoft® Outlook profile (MAPI profile) or create a new profile to login (when using the Rules Manager the first time only).

3. Click **OK** to launch the Rules Manager.

4. The main window of the rules manager displays all the mailboxes enabled on the Microsoft® Exchange Server. The color of the mailboxes indicates the status of that mailbox:

- » **Blue** - mailbox has rules configured
- » **Black** - mailbox has no rules configured.

Setting new rules

1. Check the mailboxes to set a rule on and click **Configure...**

NOTES

1. New rules can be added to mailboxes which already contain rules.
2. Select multiple mailboxes to configure the same rule applicable to all mailboxes.

2. In the **Rule Condition** text box, type the tag given to the spam email in the GFI MailEssentials spam actions.

3. Specify the **Rule action**:

- » Select **Delete** to delete an email which has a subject that contains the rule condition
- » Select **Move to:** to move spam email to a folder in the mailbox. Key in the folder path where to save the spam email. If you specify `Inbox\Spam`, then a spam folder will be created in the Inbox folder. If you specify just `Spam`, then the folder will be created at the top level (same level as Inbox).

4. Click **Apply** to save the set rules.

Managing multiple rules

More than one rule can be set on the same mailbox.

Example: Delete emails tagged with `[Phishing]` and move emails tagged with `[SPAM]` to `Inbox\Spam` folder.

1. Double click on a mailbox to launch the Rules dialog.

2. A list of rules applicable to the selected mailbox is displayed.
 - » Click **Add rule** to add a new rule
 - » Select a rule and click **Edit rule** to change settings of the selected rule
 - » Select a rule and click **Delete rule** to delete the selected rule.
3. Click **Apply** to save settings.

10.9 Set a Microsoft® Exchange account

When GFI MailEssentials is installed on Microsoft® Exchange, a dedicated user must be created to use any one of these features:

- » Deliver spam email to an Exchange mailbox sub-folder (required when installing on Exchange 2010 or newer versions only)
- » Information Store Protection using EWS (not required when using VSAPI)

GFI MailEssentials can create this user and configure its permissions automatically or else create the user manually. For more information refer to http://go.gfi.com/?pageid=ME_SpamExch2010

This account's details (such as username and password) must not be changed from Microsoft® Exchange or Active Directory, else these features will not work.

Configure the dedicated user from the GFI MailEssentials Switchboard. To configure a dedicated user:

1. Launch GFI MailEssentialsSwitchboard from **Start > Programs > GFI MailEssentials > Switchboard**.
2. Select the **Exchange account** tab.
3. Click **Change...**
4. Select one of the following options:

Option	Description
Create a new account	Let GFI MailEssentials automatically create a user with all the required rights.
Use the following account	Use a manually created user. Specify the credentials (Domain\username and Password) of a dedicated user and click Set access rights to assign the required rights to the specified user.

5. Click **Finish** to apply settings.
6. Click **OK**.

10.10 Exporting and importing settings manually

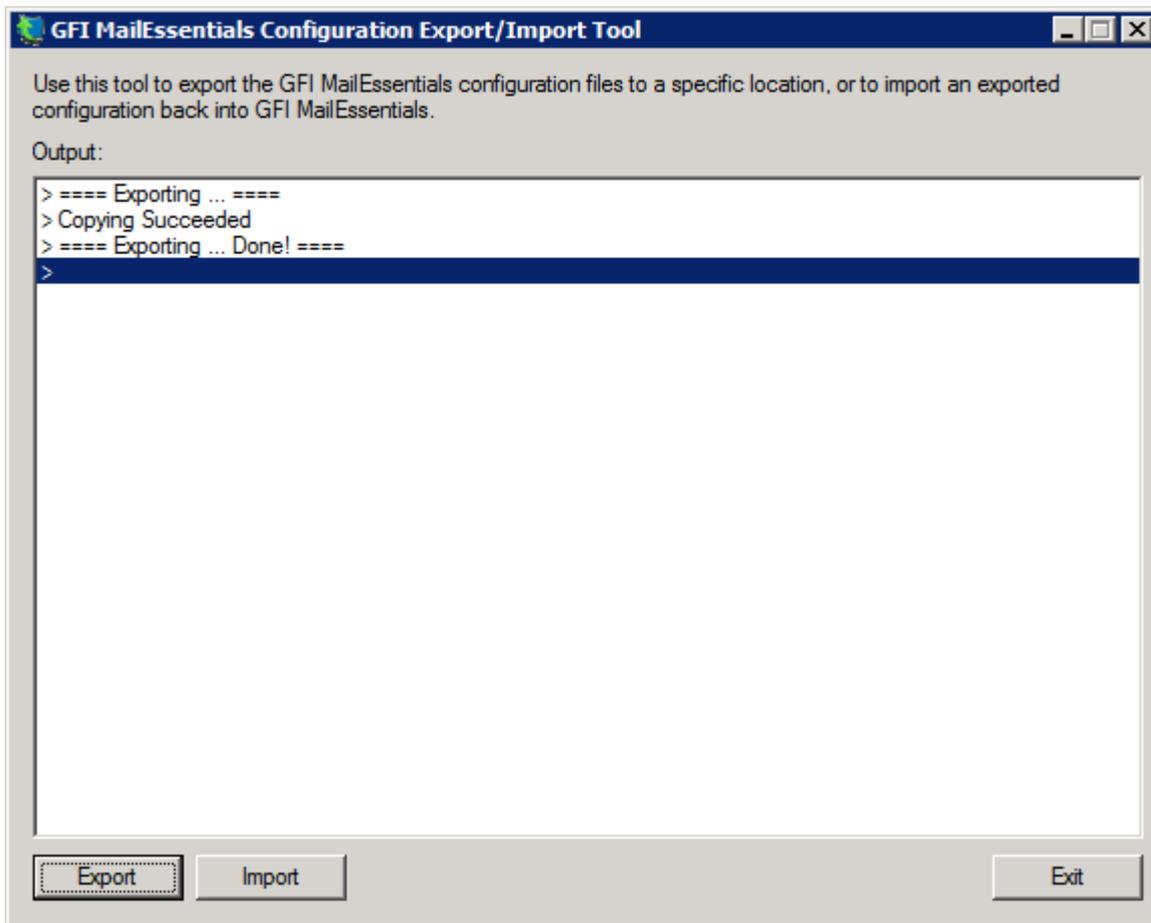
GFI MailEssentials includes a Configuration Export/Import tool to export settings from one installation and import them in another.

NOTE

Settings can also be imported and/or exported from command line. For more information, refer to [Export/Import settings via command line](#) (page 263).

Step 1: Export existing settings

1. Go to `<GFI MailEssentials installation path>\GFI\MailEssentials\` and launch `meconfigmgr.exe`.



Screenshot 149: Configuration Export/Import Tool

NOTE

Duration of the export process depends on the databases' sizes.

4. Click **Export**.
5. From **Browse for Folder** dialog, choose folder where to export configuration settings and click **OK**.
6. On completion, click **Exit**.

Step 2: Copy the exported settings

1. Manually copy the folder where the configuration settings were exported.
2. Paste the folder to the machines where to import the settings.

Step 3: Import settings to new installation

IMPORTANT

When importing settings, the imported files overwrite existing settings (for example, Source DNS settings) and may require reconfiguration of particular network settings and spam actions.

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

1. Stop the following services:

- » GFI List Server
- » GFI MailEssentials AS Scan Engine
- » GFI MailEssentials Attendant
- » GFI MailEssentials Autoupdater
- » GFI MailEssentials AV Scan Engine
- » GFI MailEssentials Backend
- » GFI MailEssentials Enterprise Transfer
- » GFI MailEssentials Legacy Attendant
- » GFI MailEssentials Quarantine Action Services
- » GFI POP2Exchange
- » IIS Admin service

2. Go to `<GFI MailEssentials installation path>\GFI\MailEssentials\` and launch **meconfigmgr.exe**.

NOTE

Duration of the import process depends on size of the databases to be imported.

4. Click **Import**, choose folder containing import data and click **OK**.

WARNING

The import process replaces the configuration files with the files found in this folder.

NOTE

Some imported settings may not be appropriate for the installation of GFI MailEssentials may need to be re-configured. This is possible for example, DNS settings, domains list and perimeter servers are different from the server from which settings were exported. Click **Yes** to launch the GFI MailEssentials Post-Installation wizard to reconfigure important settings.

For more information, refer to [Post-Installation Wizard](#) (page 37).

It is also recommended to verify the following settings that are not configured during the Post-Installation wizard.

- » **Directory Harvesting** - This must be verified when importing to a server that connects to a different Active Directory or with an Active Directory which is located on a different server. For more information, refer to [Directory Harvesting](#) (page 112).
- » **Spam Actions** - Some spam actions are only available for Microsoft® Exchange environments. If importing settings to a different environment (for example, on an IIS Server), these actions will not work. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

NOTE

For more information about settings to verify after import refer to:
http://go.gfi.com/?pageid=ME_CheckImportSettings

6. On completion, click **Exit**.
7. GFI MailEssentials automatically attempts to start the services that were stopped in step 1.

IMPORTANT

There may be other services that are stopped when stopping the **IIS Admin service**, such as the **Simple Mail Transfer Protocol (SMTP)** service. Restart these services manually from the Services applet.

10.10.1 Export/Import settings via command line

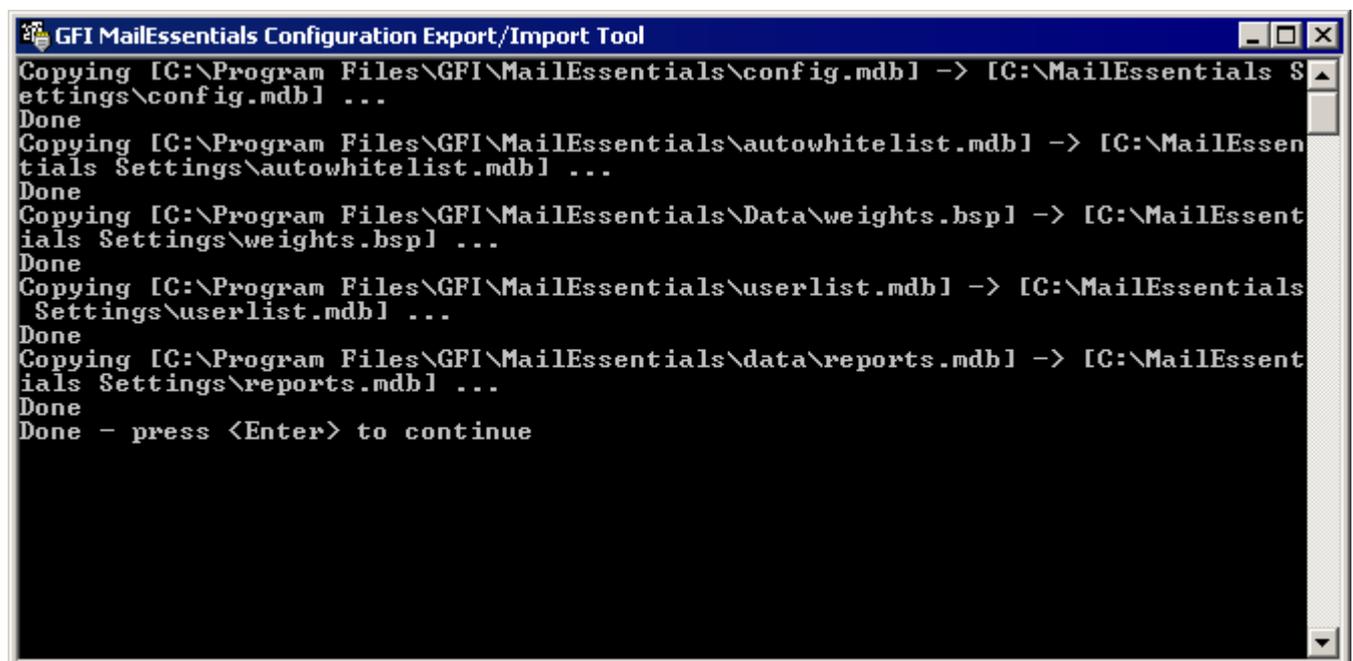
Exporting settings via command line

1. From command prompt, change directory to the GFI MailEssentials installation root folder.
2. Key in:

```
meconfigmgr /export:"c:\MailEssentials Settings" /verbose /replace
```

Where:

- » "C:\MailEssentials Settings" - location where to export files. Replace with the desired destination path.
- » /verbose - instructs the tool to display progress while copying the files.
- » /replace - instructs the tool to overwrite existing files in the destination folder.



```
GFI MailEssentials Configuration Export/Import Tool
Copying [C:\Program Files\GFI\MailEssentials\config.mdb] -> [C:\MailEssentials Settings\config.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\autowhitelist.mdb] -> [C:\MailEssentials Settings\autowhitelist.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\Data\weights.bsp] -> [C:\MailEssentials Settings\weights.bsp] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\userlist.mdb] -> [C:\MailEssentials Settings\userlist.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\data\reports.mdb] -> [C:\MailEssentials Settings\reports.mdb] ...
Done
Done - press <Enter> to continue
```

Screenshot 150: Exporting settings via command line

3. Restart the services stopped in step 1.

Importing settings via command line

1. Stop the following services:

- » GFI List Server
- » GFI MailEssentials AS Scan Engine
- » GFI MailEssentials Attendant
- » GFI MailEssentials Autoupdater
- » GFI MailEssentials AV Scan Engine
- » GFI MailEssentials Backend
- » GFI MailEssentials Enterprise Transfer
- » GFI MailEssentials Legacy Attendant
- » GFI MailEssentials Quarantine Action Services
- » GFI POP2Exchange
- » IIS Admin service

2. From command prompt, change directory to the GFI MailEssentials installation root folder.

3. Key in:

```
meconfigmgr /import:"c:\MailEssentials Settings" /verbose /replace
```

Where:

- » "C:\MailEssentials Settings" - location where the files to import are located. Replace with the path where files to be imported are located.
- » /verbose - instructs the tool to display progress while copying the files.
- » /replace - instructs the tool to overwrite existing files in the destination folder.

WARNING

The import process replaces the configuration files with the files found in this folder.

```
GFI MailEssentials Configuration Export/Import Tool
Copying [C:\MailEssentials Settings\config.mdb] -> [C:\Program Files\GFI\MailEssentials\config.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\autowhitelist.mdb] -> [C:\Program Files\GFI\MailEssentials\autowhitelist.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\weights.bsp] -> [C:\Program Files\GFI\MailEssentials\Data\weights.bsp] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\userlist.mdb] -> [C:\Program Files\GFI\MailEssentials\userlist.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\reports.mdb] -> [C:\Program Files\GFI\MailEssentials\data\reports.mdb] ...
File exists, overwritten
==== Importing ... Done! ====

==== Validating ... ====
Validating Anti-spam Action paths...
Validating Anti-spam Action paths...Done!
==== Validating ... Done! ====
Done - press <Enter> to continue
```

Screenshot 151: Importing settings via command line

4. Restart the services stopped in step 1.

NOTE

Some imported settings may not be appropriate for the installation of GFI MailEssentials may need to be re-configured. This is possible for example, DNS settings, domains list and perimeter servers are different from the server from which settings were exported. Click **Yes** to launch the GFI MailEssentials Post-Installation wizard to reconfigure important settings.

For more information, refer to [Post-Installation Wizard](#) (page 37).

It is also recommended to verify the following settings that are not configured during the Post-Installation wizard.

- » **Directory Harvesting** - This must be verified when importing to a server that connects to a different Active Directory or with an Active Directory which is located on a different server. For more information, refer to [Directory Harvesting](#) (page 112).
- » **Spam Actions** - Some spam actions are only available for Microsoft® Exchange environments. If importing settings to a different environment (for example, on an IIS Server), these actions will not work. For more information, refer to [Spam Actions - What to do with spam emails](#) (page 145).

NOTE

For more information on the settings to verify after import, refer to:

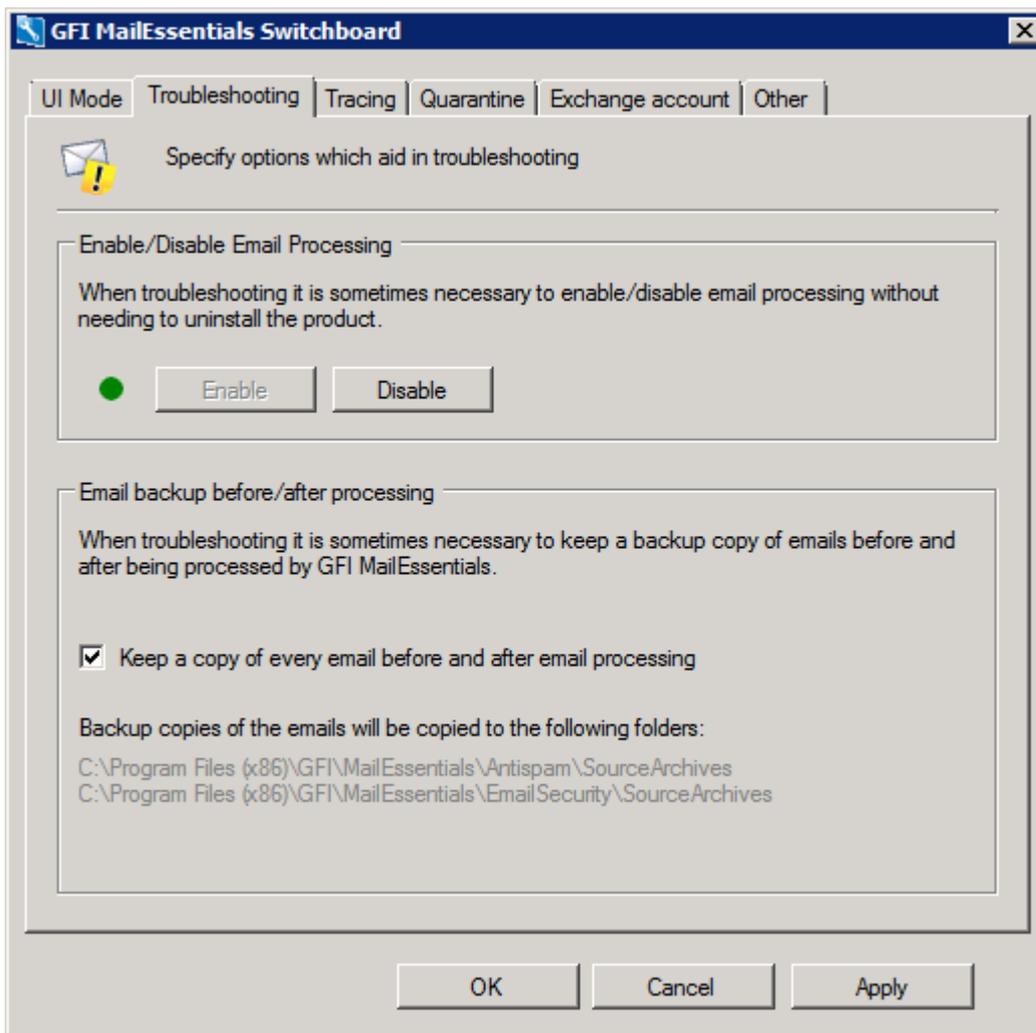
http://go.gfi.com/?pageid=ME_CheckImportSettings

10.11 Disabling email processing

Disabling email processing disables all protection offered by GFI MailEssentials and enables all emails (including spam and malicious emails) to get to your user's mailboxes. Email processing is typically disabled only for troubleshooting purposes.

To enable/disable GFI MailEssentials from processing emails:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Troubleshooting** tab.



Screenshot 152: The GFI MailEssentials Switchboard: Troubleshooting

2. Click **Enable** or **Disabled** to enable or disable email processing

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

3. In the **Service Restart Required** dialog, click **Yes** to restart services.

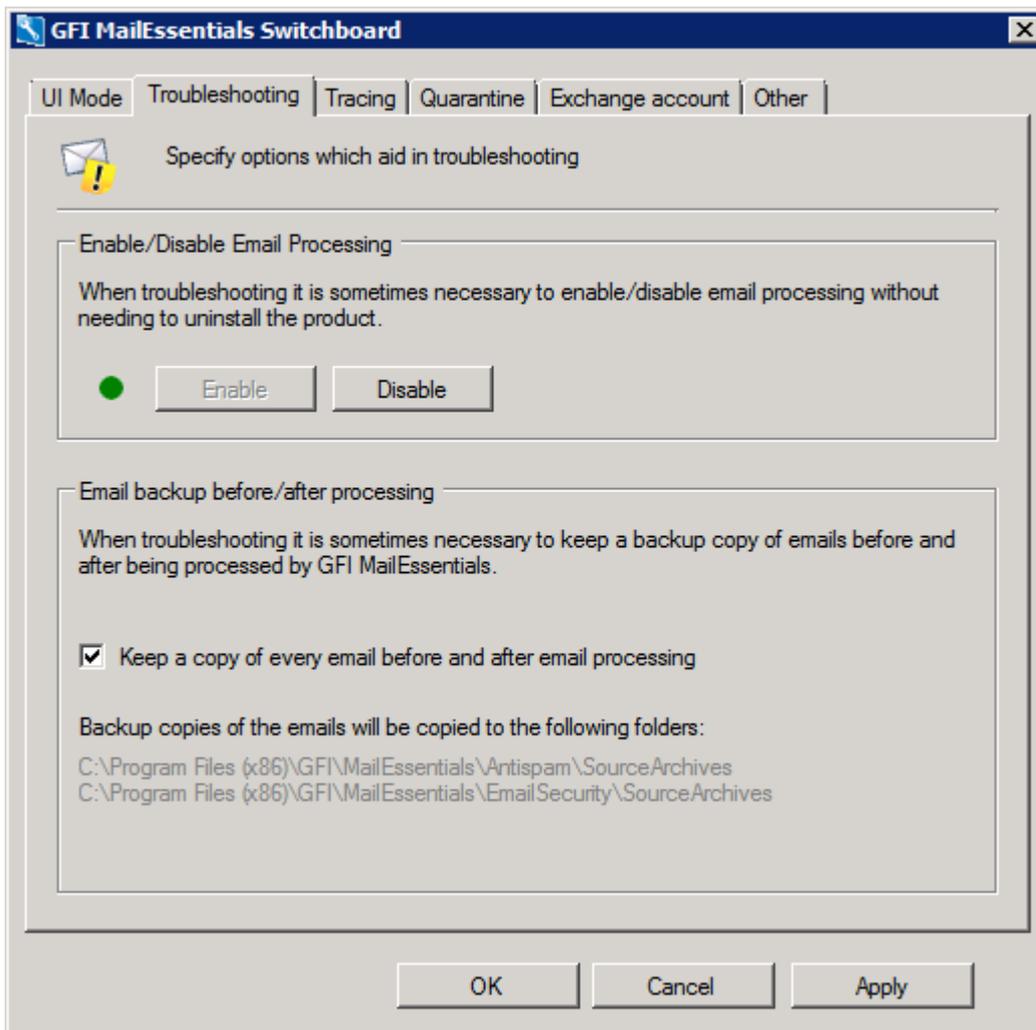
4. Click **OK**.

10.12 Email backup before and after processing

IMPORTANT

Use this option for troubleshooting purposes only.

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Troubleshooting** tab.



Screenshot 153: The GFI MailEssentials Switchboard: Troubleshooting

2. Select/unselect **Keep a copy of every email before and after email processing** checkbox to store a copy of each email processed.

All emails are stored in the following locations:

- » `<GFI MailEssentials installation path>\GFI\MailEssentials\AntiSpam\SourceArchives\`
- » `<GFI MailEssentials installation path>\GFI\MailEssentials\EmailSecurity\SourceArchives\`

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

3. Click **OK**.

4. In the **Service Restart Required** dialog, click **Yes** to restart services.

5. Click **OK**.

10.13 Remoting ports

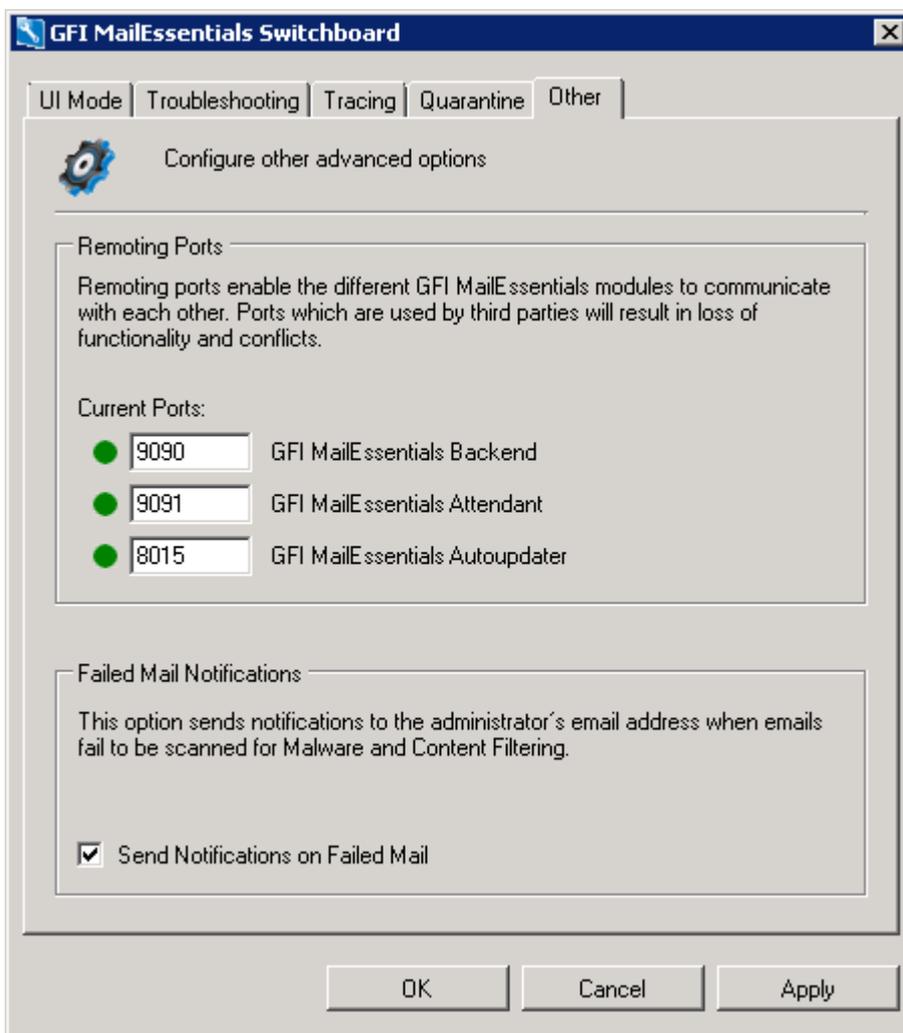
Remoting ports enable modules in GFI MailEssentials to communicate with each other. By default, GFI MailEssentials uses ports:

- » **9090** - used by the GFI MailEssentials Backend service
- » **9091** - used by the GFI MailEssentials Attendant service
- » **8015** - used by the GFI MailEssentials AutoUpdater service

Ensure that no other applications (except GFI MailEssentials) are listening on these ports. If these ports are used by some other application, change these port numbers to ports that are not used by other applications.

To change the Remoting ports:

1. Launch the GFI MailEssentials Switchboard from **Start > Programs > GFI MailEssentials > Switchboard** and select **Other** tab.



Screenshot 154: Changing Remoting ports

2. In the **Remoting Ports** area, change the number of the Remoting port to a one that is not utilized by other applications.
3. Click **Apply**.

NOTE

Some services are temporarily stopped while performing this operation. This may affect mail flow and/or email scanning.

4. Click **Yes** to restart the displayed services.
5. Click **OK**.

10.14 Monitoring Virus Scanning API

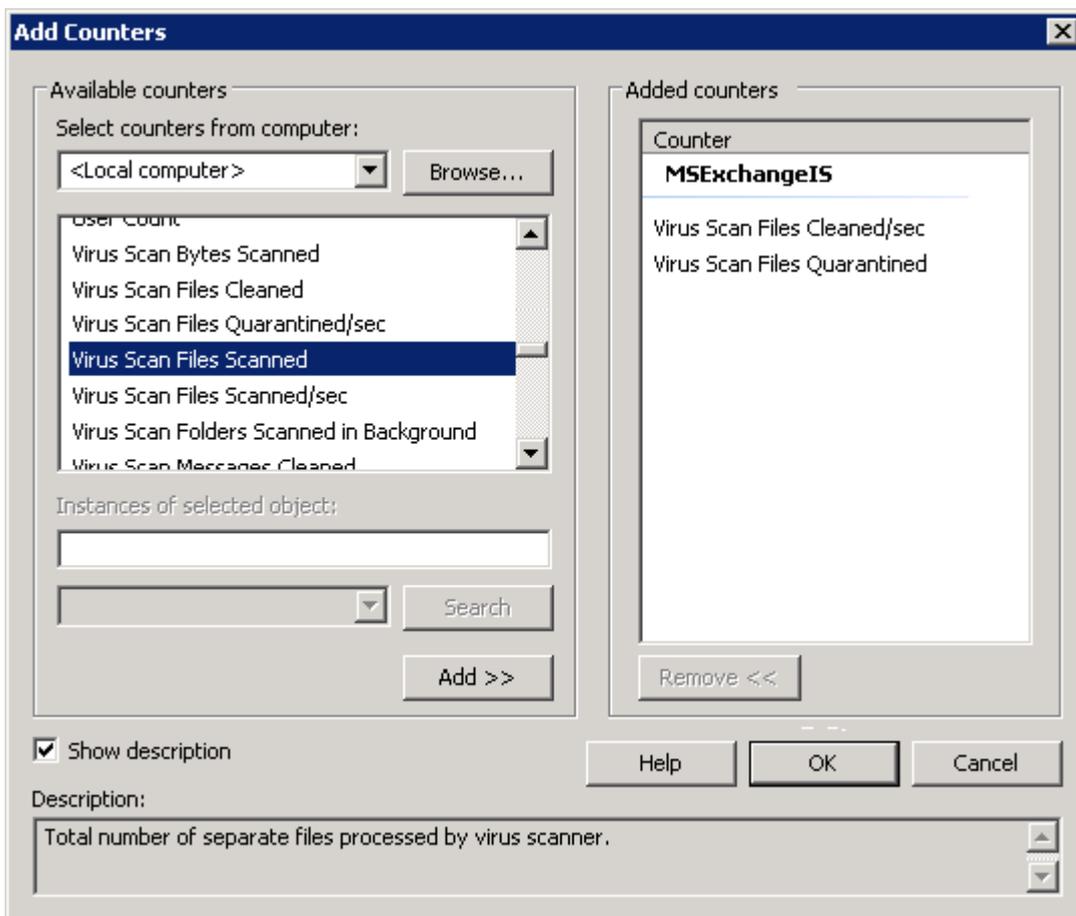
When using Virus Scanning API (VSAPI) to scan the Microsoft® Exchange Information Store, you can monitor Virus Scanning API performance using the Performance Monitor MMC.

NOTE

In a Microsoft® Exchange Server environment, the VSAPI performance monitor counters are only available on machines with the Mailbox Server Role installed.

To add and view, the performance monitor counter in Windows 2008 R2 Server or newer, follow these steps:

1. Go to **Start > Control Panel > Administrative Tools > Reliability and Performance Monitor**.
2. In the monitor dialog, expand **Monitoring Tools** and select **Performance Monitor**.
3. From the viewing pane, click **Add** to load the **Add Counters** dialog.

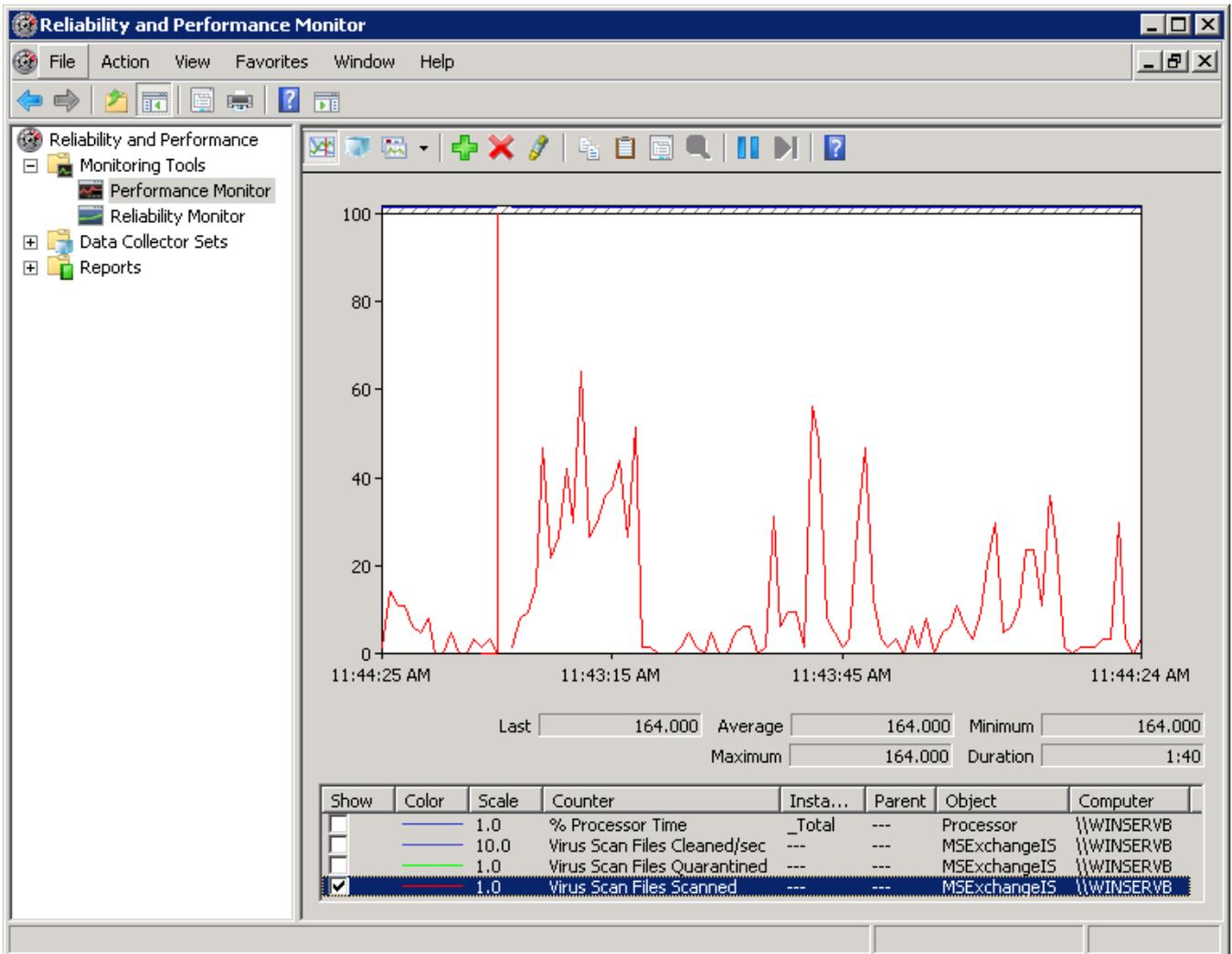


Screenshot 155: Adding VSAPI performance monitor counters in Windows 2008 R2 Server or newer

4. From the **Select counters from computer** dropdown list, select the computer to monitor.

5. From the list of available counters, expand **MSExchangeIS**.
6. Select any **Virus Scan** counter you need to add. For more information, refer to [Performance monitor counters](#) (page 270).
7. Click **Add**.
8. Repeat steps 6 and 7 for each process to monitor.
9. Click **Ok** to apply changes.

The counters of added processes are now displayed in the Performance Monitor.



Screenshot 156: Monitoring Virus Scan Files Scanned in Windows Server 2008 R2 Performance Monitor

10.14.1 Performance monitor counters

The following VSAPI Performance Monitor counters are available:

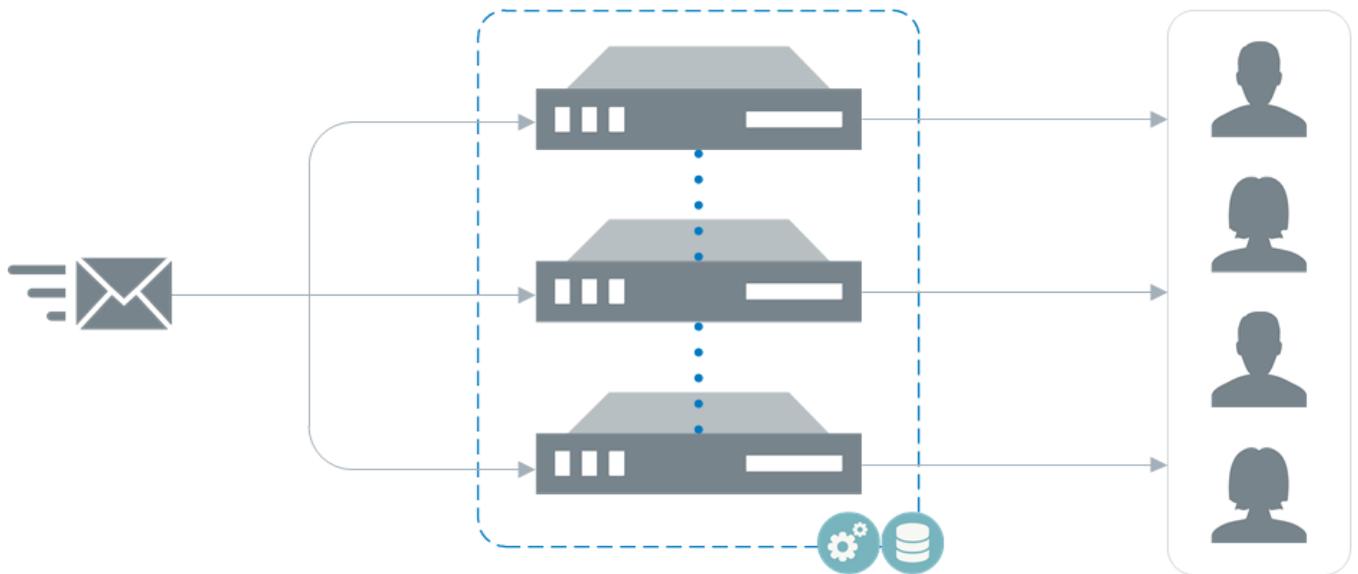
Performance Counter	Description
Virus Scan Messages Processed	A cumulative value of the total number of top-level messages that are processed by the virus scanner.
Virus Scan Messages Processed/sec	Represents the rate at which top-level messages are processed by the virus scanner.
Virus Scan Messages Cleaned	Total number of top-level messages that are cleaned by the virus scanner.

Performance Counter	Description
Virus Scan Messages Cleaned/sec	Rate at which top-level messages are cleaned by the virus scanner.
Virus Scan Messages Quarantined	Total number of top-level messages that are put into quarantine by the virus scanner.
Virus Scan Messages Quarantined/sec	Rate at which top-level messages are put into quarantine by the virus scanner.
Virus Scan Files Scanned	Total number of separate files that are processed by the virus scanner.
Virus Scan Files Scanned/sec	Rate at which separate files are processed by the virus scanner.
Virus Scan Files Cleaned	Total number of separate files that are cleaned by the virus scanner.
Virus Scan Files Cleaned/sec	Rate at which separate files are cleaned by the virus scanner.
Virus Scan Files Quarantined	Total number of separate files that are put into quarantine by the virus scanner.
Virus Scan Files Quarantined/sec	Rate at which separate files are put into quarantine by the virus scanner.
Virus Scan Bytes Scanned	Total number of bytes in all of the files that are processed by the virus scanner.
Virus Scan Queue Length	Current number of outstanding requests that are queued for virus scanning.
Virus Scan Folders Scanned in Background	Total number of folders that are processed by background scanning.
Virus Scan Messages Scanned in Background	Total number of messages that are processed by background scanning.

11 GFI MailEssentials Multi-Server

In environments where there are large email volumes, multiple email gateways and mail servers are usually used to process mail flow efficiently. The physical servers may be on the same site or at different locations. In such instances, GFI MailEssentials is also deployed on multiple gateway servers.

Without Multi-Install feature implemented, every instance of GFI MailEssentials has its own set of settings, a reporting database and a quarantine store. Configuration of the server, administration of quarantined items and generation of reports need to be done separately on each and every server.



With Multi-Install, all GFI MailEssentials installations are joined together. With this setup settings are synchronized between servers and reporting/quarantine databases are centralized. Configuration and management of GFI MailEssentials is done on one server for all GFI MailEssentials installations.

When certain features are configured on one GFI MailEssentials instance, these settings are automatically implemented on the other servers within the Multi-Install network. This enables the administrator to apply settings only once.

All reporting and quarantine data is transferred to one server within the network - the Reporting & Quarantine Host. The administrator can manage all quarantined items and generate reports from the Reporting & Quarantine Host.

One server within a GFI MailEssentials Multi-Install network must be set as a Master Server. The Master Server coordinates the operations of the Multi-Install network. It ensures that changes applied on any server within the network are automatically implemented on all servers.

The other servers that are joined to the Master server are the Slave servers. Together, these form the Multi-Install network.

11.1 Features synchronized by Multi-Server

With Multi-Install, all GFI MailEssentials installations are joined together. With this setup settings are synchronized between servers and reporting/quarantine databases are centralized.

Configuration and management of GFI MailEssentials are done on one server for all GFI MailEssentials installations.

Important

All GFI MailEssentials machines in a multi-server environment must have their IP address listed in the Perimeter SMTP Server Settings. This ensures that emails processed by a GFI MailEssentials server are not reprocessed by another server. For more information, refer to [Perimeter SMTP Server Settings](#) (page 224).

The GFI MailEssentials multi-install feature performs the following actions:

Configuration synchronization

All configuration settings that are set to be synchronized are retrieved from each server and merged together into a single list.

So, for example, if a whitelist on one machine has 10 whitelist entries, while another machine has 20 whitelist entries with 5 of these entries being common to both machines, the end result is a single merged whitelist list with 25 email addresses on both machines. (5 unique from the first machine, 15 unique from the second machine and 5 common from both machines).

This applies to the following features:

- » General Settings
- » Local Domains
- » Access Control
- » Perimeter SMTP Servers
- » AV Configuration
- » Advanced EmailSecurity Configuration
- » Templates
- » Global Whitelist
- » Global Blocklist
- » Personal Whitelist and Blocklist
- » Auto Whitelist

Content filtering synchronization

In the case of content filtering, there is a difference from how whitelists and blocklists are merged.

The rules and settings of Content Filtering engines from every server are gathered and merged into a single list. This applies to the following engines:

This applies to the following Rules and engines:

- » Keyword Filtering Rules
- » Attachment Filtering Rules
- » Advanced Content Filtering Rules
- » Decompression Engine

NOTE

Each rule and filter has an internal "last modified time" which is then used to determine whose rule\setting is the latest. If there are 2 rules with the same name on 2 different servers, only the latest one is merged.

Every update done on one server is immediately applied onto all the other servers. This effectively means that changes are immediately available on all servers.

Quarantine\Reporting synchronization

All slave machines upload all the local reporting/quarantine database data to the machine hosting Quarantine and Reporting. This server requires ample disk space, since it needs to store the quarantine of spam & malware engines, together with reporting data.

If there is no connection to the server (for example, a network outage), slave servers save records locally until the connection is re-established. When a machine is set to send all reporting/quarantine data, all current data in the local databases is transferred. This may take some time, given that a large volume of data may be required to be transferred.

11.2 Setting up Multi-Server

Configuring the GFI MailEssentials Multi-Server feature is a multi-stage process:

- 1. Plan your Multi-Server installation** - See which GFI MailEssentials servers will form part to the GFI MailEssentials Multi-Server setup and which one will be designated as the master server. If synchronizing the reporting and quarantine data, also decide which computer will be the Reporting and Quarantine host.
- 2. Install GFI MailEssentials on all the computers** - All computers within the GFI MailEssentials multi server installation must have the same version and build of GFI MailEssentials installed on them. We recommend upgrading to the latest version of GFI MailEssentials. For more information, refer to [Getting Started with GFI MailEssentials](#) (page 16).

Important

All GFI MailEssentials machines in a multi-server environment must have their IP address listed in the Perimeter SMTP Server Settings. This ensures that emails processed by a GFI MailEssentials server are not reprocessed by another server. For more information, refer to [Perimeter SMTP Server Settings](#) (page 224).

- 3. Open firewall ports 9095 & 9096** - These TCP ports are used for communications between GFI MailEssentials servers that are joined to the Multi-Server network. Ensure that the master and all slave servers can communicate together via these ports.
- 4. Configure the Master Server** - The master server is tasked with synchronizing the data within the GFI MailEssentials Multi-Server environment. For more information, refer to [Configuring the master server](#) (page 275).
- 5. Configure Slave Servers** - Slave servers are members of the multi-server environment. Slave servers get the synchronized configuration settings from the master server and other peers in the multi-install network. A slave server may also be the Reporting and Quarantine host. For more information, refer to [Configuring a slave server](#) (page 276).
- 6. Configure which configuration settings to sync** - GFI MailEssentials provides you with the facility to sync either all the configuration settings or a set of configuration settings. For more information, refer to [Configuring the settings to synchronize](#) (page 278).
- 7. Configure Reporting and Quarantine sync** - Syncing the Reporting and Quarantine data enables you to centralize all your reporting to a single location as well as enables you to have a single location your quarantined emails are stored. For more information, refer to [Configuring Reporting and Quarantine data centralization](#) (page 280).

11.2.1 Configuring the master server

The master server is the server that will be in charge of synchronizing the data between all the GFI MailEssentials instances within the multi-server network. You can only have a single master server per multi-server network instance. If you have multiple instances of multi-server networks, then each instance must have its own master server.

Important

All GFI MailEssentials machines in a multi-server environment must have their IP address listed in the Perimeter SMTP Server Settings. This ensures that emails processed by a GFI MailEssentials server are not reprocessed by another server. For more information, refer to [Perimeter SMTP Server Settings](#) (page 224).

1. Locate and click the Multi-Server node on the GFI MailEssentials console of the computer to designate as the Master Server.

Multi-Server Setup Configuration Sync

Use Multi-Install mode to synchronize Configuration, Reporting and Quarantine on multiple GFI MailEssentials servers. Settings configured on a server joined to the Multi-Install network are inherited by all other servers.

Enable Multi-Install mode

Master Server: Coordinator of the Multi-Install functionality of GFI MailEssentials. There can be only one Master in a Multi-Install network.

Slave Server: Join this instance of GFI MailEssentials as a Slave server to an existing Multi-Install network.

Master Server

GFI MailEssentials Administrator credentials:

Username: administrator

Password:

Port used to synchronize data

Port: 9096

Centralize Quarantine and Reporting data within the Multi-Install network

Host: SERV801

Port: 9095

Test

Screenshot 157: Setting a Master server

2. Select **Enable Multi-Install mode** option and choose **Master Server**.

3. Key in the GFI MailEssentials Administrator Credentials. If the default port used by GFI MailEssentials is used by another application, modify the **Port used to synchronize data** value to an unused port.

NOTE

The username and password provided must exist in the Access Control List for all the GFI MailEssentials installations (including Slave Servers) that are part of the multi-server network. The password should not expire.

It is recommended that this account is created solely for this purpose. For more information, refer to [Access Control List](#) (page 246).

4. Optionally, select **Centralize Quarantine and Reporting data within the Multi-Install network** option and select the computer that will host the quarantine and reporting data. The reporting and quarantine data host does not necessarily have to be the master server. Any GFI MailEssentials instance within the Multi-Server network can serve as the reporting and quarantine data host. To review and manage data in quarantine and reporting databases, access the web console of the Quarantine and Reporting host.
5. Click **Test** to test your settings.
6. Click **Apply**.

11.2.2 Configuring a slave server

A slave server is a server that is part of the GFI MailEssentials multi-server environment. Slave servers get the synchronized configuration settings from the master server and other peers in the multi-install network. Slave servers also send reporting and quarantine data to the designated Reporting and Quarantine host. A slave server may also be the Reporting and Quarantine host.

Important

All GFI MailEssentials machines in a multi-server environment must have their IP address listed in the Perimeter SMTP Server Settings. This ensures that emails processed by a GFI MailEssentials server are not reprocessed by another server. For more information, refer to [Perimeter SMTP Server Settings](#) (page 224).

1. Locate and click the Multi-Server node on the GFI MailEssentials console of the computer to designate as a slave server.



Use Multi-Install mode to synchronize Configuration, Reporting and Quarantine on multiple GFI MailEssentials servers. Settings configured on a server joined to the Multi-Install network are inherited by all other servers.

Enable Multi-Install mode

- Master Server:** Coordinator of the Multi-Install functionality of GFI MailEssentials. There can be only one Master in a Multi-Install network.
- Slave Server:** Join this instance of GFI MailEssentials as a Slave server to an existing Multi-Install network.

Slave Server

Master Server URL:
http://servername/MailEssentials

GFI MailEssentials Administrator credentials:

Username:

Password:

▼ **Advanced**

Multi-Install Network

Multi-Install network status:

Server	Type
S805	Slave

Screenshot 158: Setting server as a slave server

2. Select **Enable Multi-Install mode** option and choose **Slave Server**.
3. Key in the Master Server URL and the GFI MailEssentials Administrator credentials.

NOTE

The username and password provided must exist in the Access Control List for all the GFI MailEssentials installations (including Slave Servers) that are part of the multi-server network. The password should not expire.

It is recommended that this account is created solely for this purpose. For more information, refer to [Access Control List](#) (page 246).

4. Click **Advanced** and ensure that both the port used to synchronize data and the port used for quarantine and reporting data are correct.
5. Click **Test** to test setup.
6. Click **Apply**.

11.2.3 Configuring the settings to synchronize

GFI MailEssentials provides you with the facility to configure which settings to synchronize between all the servers in the Multi-Server network.

NOTE

The information in this topic applies only to the synchronization of configuration settings. For information on synchronizing Reporting and quarantine data, refer to [Configuring Reporting and Quarantine data sync](#).

To configure the settings to synchronize:

1. On the machine configured as the [Master Server](#), locate and click the **Multi-Server** node.
2. Click the **Configuration Sync** tab.

Multi-Server Setup
Configuration Sync

Features that are synchronized in the Multi-Install network.

Reporting and Quarantine data

Transfer the Reporting and Quarantine data from this server to the Multi-Install network, to view reports and manage quarantine from one central location.

Transfer data from this server to the Multi-Install network

Filtered Settings

<input checked="" type="checkbox"/>	Settings
<input checked="" type="checkbox"/>	General Settings
<input checked="" type="checkbox"/>	Local Domains
<input checked="" type="checkbox"/>	Access Control
<input checked="" type="checkbox"/>	Perimeter SMTP Servers
<input checked="" type="checkbox"/>	AV Configuration
<input checked="" type="checkbox"/>	Advanced EmailSecurity Settings
<input checked="" type="checkbox"/>	Templates
<input checked="" type="checkbox"/>	Global Whitelist
<input checked="" type="checkbox"/>	Global Blocklist
<input checked="" type="checkbox"/>	Personal Whitelist and Blocklist
<input checked="" type="checkbox"/>	Auto Whitelist
<input checked="" type="checkbox"/>	Attachment Filtering Rules
<input checked="" type="checkbox"/>	Advanced Content Filtering Rules
<input checked="" type="checkbox"/>	Keyword Filtering Rules
<input checked="" type="checkbox"/>	Decompression Engine

Screenshot 159: Choosing the settings to synchronize

3. From the **Filtered Settings** area, select the settings to sync. Available settings are:

Settings	Description
General Settings	All settings under General Settings section except for Local Domains, Access Control and Perimeter SMTP Servers.
Local Domains	Synchronize the Local Domains lists.
Access Control	Synchronize the Access Control lists.

Settings	Description
Perimeter SMTP Server Settings	Synchronize the Perimeter SMTP Servers.
AV Configuration	Synchronize the Configuration of all AV Engines including their enabled status, action on infected content and AV update configuration. This includes also the AV scanning priorities. NOTE Information Store Protection is not synchronized.
Advanced Email Security Settings	Synchronize the settings of the following sections in full » Trojan & Executable Scanner » Email Exploit Engine » HTML Sanitizer
Notification Templates	Synchronize the email templates available under General Settings.
Global Whitelist	Synchronize the Global Whitelist.
Global Blocklist	Synchronize the Global Blocklist.
AutoWhitelist	Synchronize the AutoWhitelist.
Keyword Filtering Rules	Synchronize the Keyword Filtering Rules.
Attachment Filtering Rules	Synchronize Attachment Filtering Rules.
Advanced Content Filtering Rules	Synchronize the Advanced Content Filtering Rules.
Decompression Engine	Synchronize the Decompression Engine settings.

4. Click **Apply**.

11.2.4 Configuring Reporting and Quarantine data centralization

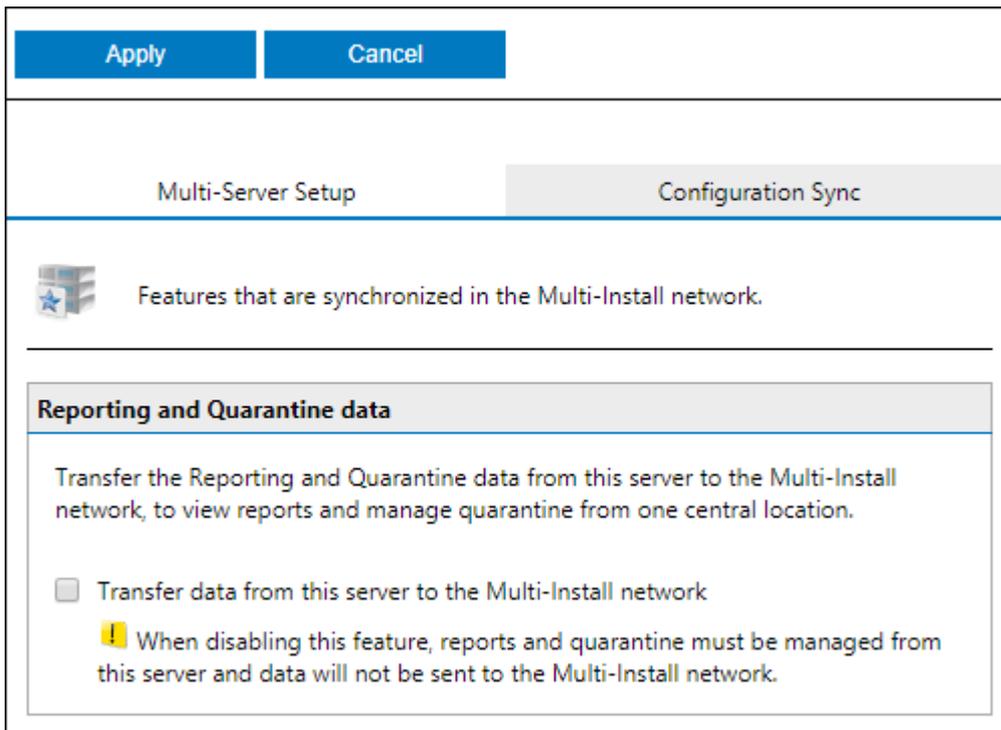
GFI MailEssentials provides you with the facility to centralize reporting and quarantine data recorded from all the GFI MailEssentials instances within a Multi-Server network. Through this feature, you will gain a better understanding of what your Multi-Server network is processing.

IMPORTANT

A computer must be designated as the Reporting and Quarantine data host. This computer does not necessarily have to be the master server. For more information, refer to [Configuring the master server](#) (page 275).

To synchronize Reporting and Quarantine data, perform the following procedure on each server in a Multi-Server network:

1. Navigate to the Multi-Server node.
2. Select the **Configuration Sync** tab.



Screenshot 160: Multi-Server synchronization features

3. From the Reporting and Quarantine data area, enable **Transfer data from this server to the Multi-Install network** option.
4. Click **Apply**.

NOTE

If the network connection between the computer sending the data and the Synchronize Quarantine and Reporting data host is lost, GFI MailEssentials stores reporting and quarantine data on the local server. When the connection is re-established, data automatically transfers to the Quarantine and Reporting data host.

12 Troubleshooting and support

For a list of common issues encountered when using GFI MailEssentials, go to <http://go.gfi.com/?pageid=MEdocs#cshid=troubleshooting>

Most issues can be solved through the information in this help system. If you cannot find a solution to your problem or if you think that our content can be improved in any way, let us know by sending an email to documentation@gfi.com

12.1 Other troubleshooting resources

12.1.1 Knowledge Base

GFI maintains a comprehensive Knowledge Base repository, which includes answers to the most common installation problems. In case that the information in this manual does not solve your installation problems, next refer to the Knowledge Base. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. Access the Knowledge Base by visiting: <http://www.gfi.com/support/products/gfi-mailessentials/>.

12.1.2 Web Forum

User to user technical support is available via the GFI web forum. Access the web forum by visiting: <http://forums.gfi.com/>.

12.1.3 Request technical support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

» **Online:** Fill out the support request form and follow the instructions on this page closely to submit your support request on: <http://www.gfi.com/support/technical-support-form>

» **Phone:** To obtain the correct technical support phone number for your region visit: <http://www.gfi.com/contact-us>

NOTE

Before contacting Technical Support, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: <http://customers.gfi.com>.

We will answer your query within 24 hours or less, depending on your time zone.

13 Glossary

A

Active Directory

A technology that provides a variety of network services, including LDAP directory services.

AD

Active Directory

Anti-virus software

Software that detects malware such as Trojan horses in emails, files and applications.

Auto-reply

An email reply that is sent automatically to incoming emails.

B

Background Intelligent Transfer Service

A component of Microsoft Windows operating systems that facilitates transfer of files between systems using idle network bandwidth.

Bayesian Filtering

An anti-spam technique where a statistical probability index based on training from users is used to identify spam.

BITS

Background Intelligent Transfer Service

Blocklist

A list of email addresses or domains from whom email is not to be received by users

Botnet

A network of infected computers that run autonomously and are controlled by a hacker/cracker.

C

CIDR

Classless Inter-Domain Routing

Classless Inter-Domain Routing

An IP addressing notation that defines a range of IP addresses.

D

Decompression engine

A scanning module that decompresses and analyzes archives (for example, .zip and .rar files) attached to an email.

Demilitarized Zone

An internet-facing section of a network that is not part of the internal network. Its purpose typically is to act as a gateway between internal networks and the internet.

Directory harvesting

Email attacks where known email addresses are used as a template to create other email addresses.

Disclaimer

A statement intended to identify or limit the range of rights and obligations for email recipients

DMZ

Demilitarized Zone

DNS

Domain Name System

DNS MX

Mail Exchange

Domain Name System

A database used by TCP/IP networks that enables the translation of hostnames to IP addresses and provides other domain related information.

E**Email headers**

Information that precedes the email text (body) within an email message. This includes the sender, recipient, subject, sending and receiving time stamps, etc.

Email monitoring rules

Rules which enable the replication of emails between email addresses.

Exploit

An attack method that uses known vulnerabilities in applications or operating systems to compromise the security of a system.

F**False negatives**

Spam emails that are not detected as spam.

False positives

Legitimate emails that are incorrectly identified as spam.

G**Gateway**

The computer (server) in a LAN that is directly connected to an external network. In GFI MailEssentials, gateway refers to the email servers within the company that first receive email from

external domains.

GFI Directory

A directory of users and groups that integrates with GFI products. It is meant to be used in environments where there is no Microsoft Active Directory available.

Greylist filter

An anti-spam filter that blocks emails sent from spammers that do not resend a message when a retry message is received.

H

Ham

Legitimate e-mail

HTML Sanitizer

A filtering module within GFI MailEssentials that scans and removes html scripting code from emails.

HTTP

Hypertext Transfer Protocol - A protocol used to transfer hypertext data between servers and internet browsers.

I

IIS

Internet Information Services

IMAP

Internet Message Access Protocol

Internet Information Services

A set of Internet-based services created by Microsoft Corporation for internet servers.

Internet Message Access Protocol

One of the two most commonly used Internet standard protocols for e-mail retrieval, the other being POP3.

L

LDAP

Lightweight Directory Access Protocol

Lightweight Directory Access Protocol

An application protocol used to query and modify directory services running over TCP/IP.

List server

A server that distributes emails sent to discussions lists and newsletter lists, and manages subscription requests.

M

Mail Exchange

The DNS record used to identify the IP addresses of the domain's mail servers.

Malware

All malicious types of software that are designed to compromise computer security and which usually spread through malicious methods.

MAPI

Messaging Application Programming Interface

MDAC

Microsoft Data Access Components

Messaging Application Programming Interface

A messaging architecture and a Component Object Model based API for Microsoft Exchange.

Microsoft Data Access Components

A Microsoft technology that gives developers a homogeneous and consistent way of developing software that can access almost any data store.

Microsoft Message Queuing Services

A message queue implementation for Windows Server operating systems.

MIME

Multipurpose Internet Mail Extensions

MSMQ

Microsoft Message Queuing Services

Multipurpose Internet Mail Extensions

A standard that extends the format of e-mail to support text other than ASCII, non-text attachments, message bodies with multiple parts and header information in non-ASCII character sets.

N

NDR

Non Delivery Report

Non Delivery Report

An automated electronic mail message sent to the sender on an email delivery problem.

P

Perimeter server/gateway

The host in a LAN that is directly connected to an external network. In GFI MailEssentials perimeter gateway refers to the email servers within the company that first receive email from external domains.

PGP encryption

A public-key cryptosystem often used to encrypt emails.

Phishing

The process of acquiring sensitive personal information with the aim of defrauding individuals, typically through the use of fake communications

POP2Exchange

A system that collects email messages from POP3 mailboxes and routes them to mail server.

POP3

Post Office Protocol ver.3

Post Office Protocol ver.3

A client/server protocol for storing emails so that clients can connect to the POP3 server at any time and read the email. A mail client makes a TCP/IP connection with the server and by exchanging a series of commands, enable users to read the email.

Public folder

A common folder that allows Microsoft Exchange user to share information.

Q**Quarantine**

A email database where emails detected as spam and/or malware are stored in a controlled environment. Quarantined emails are not a threat to the network environment.

Quarantine Store

A central repository within GFI MailEssentials where all blocked emails are retained until they are reviewed by an administrator.

R**RBL**

Realtime Blocklist

Realtime Blocklist

Online databases of spam IP addresses. Incoming emails are compared to these lists to determine if they are originating from blocked users.

Recursive archives

Archives that contain multiple levels of sub-archives (that is, archives within archives). Also known as nested archives.

Remote commands

Instructions that facilitate the possibility of executing tasks remotely.

RSS feeds

A protocol used by websites to distribute content (feeds) that frequently changes (for example news items) with its subscribers.

S

Secure Sockets Layer

A protocol to ensure an integral and secure communication between networks.

Simple Mail Transport Protocol

An internet standard used for email transmission across IP networks.

SMTP

Simple Mail Transport Protocol

Spam actions

Actions taken on spam emails received, e.g. delete email or send to Junk email folder.

SSL

Secure Sockets Layer

T

Trojan horse

Malicious software that compromises a computer by disguising itself as legitimate software.

V

Virus scanning engine

A virus detection technology implemented within antivirus software that is responsible for the actual detection of viruses.

W

WebDAV

An extension of HTTP that enables users to manage files remotely and interactively. Used for managing emails in the mailbox and in the public folder in Microsoft Exchange.

Whitelist

A list of email addresses and domains from which emails are always received

Z

Zombie

An infected computer that is made part of a Botnet through malware.

14 Index

A

Active Directory 11, 15, 19, 23, 32, 35, 46, 92, 106, 112, 160, 165, 208, 213, 230-231, 237, 260, 262, 265

Antispam 56, 164, 239, 250-251, 258

Antivirus 10, 18-19, 56, 70-71, 75, 79, 83, 87, 92, 188, 199

Attachment Filtering 11, 174, 189, 227, 230, 273, 280

Auto-replies 9, 215

B

Bayesian Analysis 12, 19, 107, 134, 136, 155, 158-159, 227

C

Cluster 68

D

Dashboard 50-51, 54, 56, 58-59

Database 25, 28, 50, 52, 58-59, 64, 66, 68, 94, 106, 110, 114, 117, 126, 135-136, 155, 219-220, 230, 239, 272

DEP 46

Directory harvesting 9, 11, 14, 46, 106, 112, 149, 227, 262, 265

Disclaimers 212, 215

DMZ 14, 19-20, 33, 165, 209, 230

DNS Server 22, 24, 38, 119, 131, 154

Domain 10, 14, 19, 23, 33, 46, 103, 106, 114, 120, 123-124, 131, 141, 146, 154, 165, 209, 213, 216, 230, 232, 237, 260

E

Edge Server 13, 20

Email Blocklist 11, 106, 114, 116, 145, 155, 167, 227

Email Direction 61, 63

Email monitoring 9-10, 222

F

firewall 14, 18, 31, 36, 57, 209, 230, 232, 249, 274

G

gateway 13, 16-20, 23, 31, 72, 76, 80, 84, 88, 122, 149, 194, 200, 250

Greylist 9, 12, 14, 46, 107, 126, 149, 227

H

Header checking 11, 107, 128, 130, 227

Hub Transport 13, 20, 92, 258

I

IIS 14-15, 17, 20, 24, 31, 210, 229, 233, 237, 244-245, 262, 264

IMAP 27, 165

Inbound mail filtering 9

Internal email 22, 48, 68, 71, 75, 79, 83, 87

Internet 10, 17, 21, 23, 39, 138, 149, 210, 225, 227, 257

IP 9, 11, 18, 21, 24, 36, 38, 67, 103, 106, 117, 119, 122, 124, 126, 131, 136, 139, 146, 154, 209, 225, 227-228, 253, 273-276

IP Blocklist 11, 106, 117

IP DNS Blocklist 9, 11, 18, 106, 146, 154

ISP 22, 24, 257

K

Kaspersky 10, 46, 70, 79

Keyword checking 12, 107, 133, 155, 158, 227

L

LDAP lookups 209

Legitimate email 12, 46, 107, 134, 139

Licensing 30, 72, 76, 80, 84, 88, 230, 232

Lotus Domino 13, 19, 22-23, 26

Lotus Notes 22, 26

M

MAPI 18, 259

Microsoft Exchange 16, 18-19, 91, 146, 164, 214, 250, 257

MSMQ 18

N

Net framework 161

New Senders 9, 12, 107, 143, 146-147, 227

Newsletter 131, 217-218, 220

O

Outbound mail filtering 10

P

Performance 2, 21, 46, 66, 91, 136, 141, 154, 251, 269

perimeter server 13, 16-17, 19-20, 31, 104

Phishing 11, 19, 106, 110, 227, 239, 259

POP2Exchange 50, 59, 253, 262, 264

POP3 22, 253

Post-Installation 34, 37, 262, 265

Q

Quarantine 9-10, 15, 34, 41, 48, 52, 58, 73, 77, 81, 85, 89, 94, 99, 145, 172, 177, 182, 186, 191, 196, 202-203, 209, 226, 237, 240, 244, 247, 262, 264, 272, 274, 276, 278, 280

R

Remote commands 10, 155

RSS Feeds 34, 202, 237, 247

S

Sender Policy Framework 11, 106-107, 122, 227

SMTP Server 19-20, 33, 37, 40, 125-126, 224, 273-276

SMTP Virtual Server 21, 33, 233

Spam actions 145, 257, 261, 265

SpamRazer 11, 18, 106-107, 145, 154, 227, 240

U

Updates 19, 50, 56, 58, 70, 74, 78, 82, 86, 90, 97, 100, 109, 111, 135, 227, 233-234, 239

Upgrade 30, 42-45, 49

URI DNS Blocklist 11, 106, 120, 154

V

Virtual directory 9, 34, 165, 210, 244, 246

W

WebDAV 165

Whitelist 10, 12, 15, 55, 103, 107-108, 117, 122, 124, 128, 131, 139, 142-143, 147, 155, 158, 160, 164, 166, 186, 227, 273, 280

Wizard 16, 20, 34, 37, 42-45, 49, 136, 138, 229