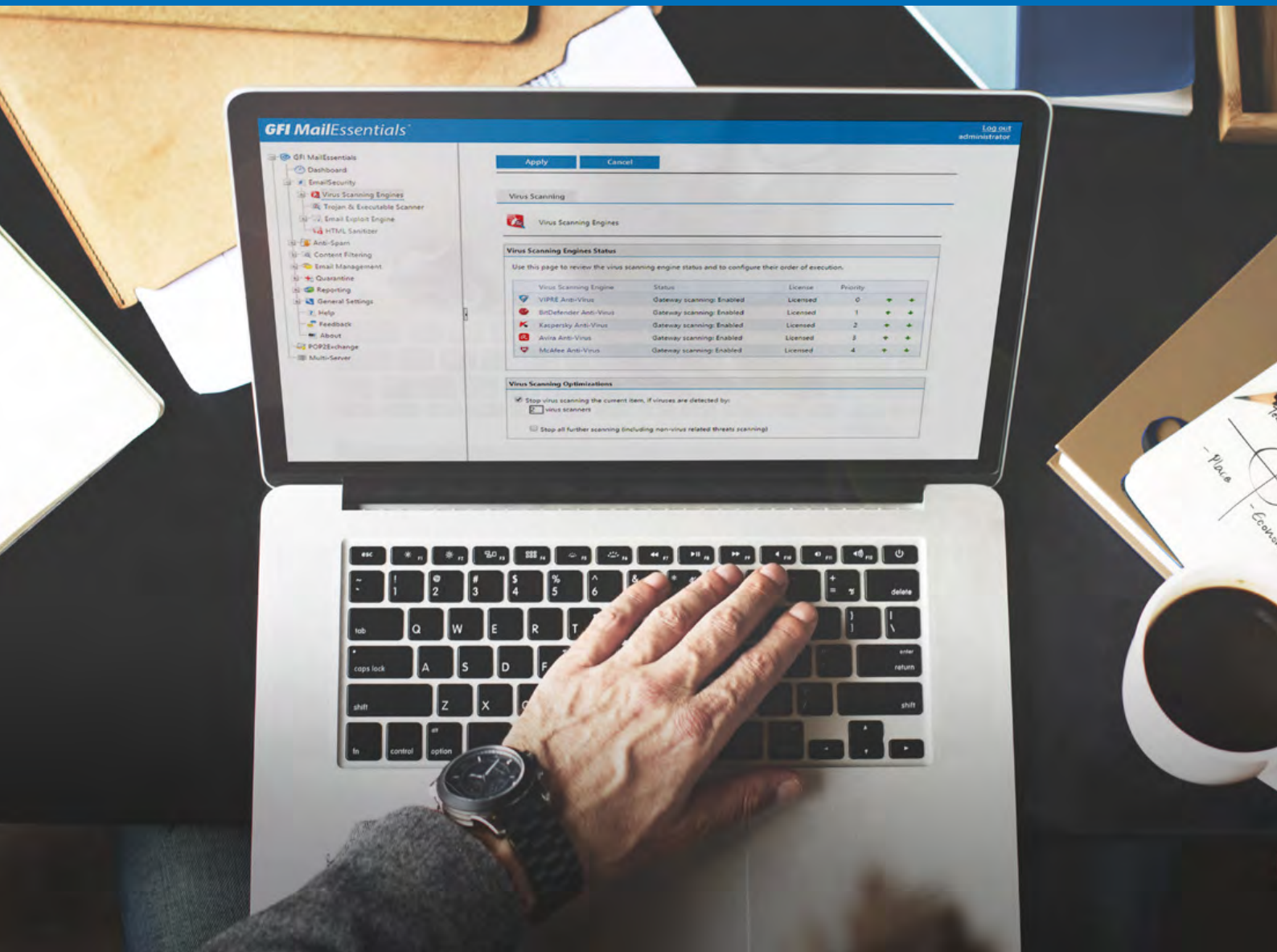






# The benefits of integrating GFI MailEssentials with Microsoft Exchange Server



## Table of Contents

	Introduction	3
	Current Challenges	4
	Choosing GFI MailEssentials	5
	Easy to Install	5
	Easy to Use	5
	Completely on-premises	6
	Multiple Anti-Malware Scanning Engines	6
	Powerful Anti-Spam	7
	Suitable for large environments	7
	Conclusion	10



## Introduction

Unless you have just started to work with Exchange, it is almost certain you still remember Forefront Protection for Exchange Server (FPE). FPE, now discontinued, was a message hygiene software that detected viruses, spyware, and spam by integrating multiple scanning engines from security partners in a single solution to protect on-premises Exchange messaging environments. It provided an administration console with customisable configuration settings, filtering options, monitoring features and reports, and, at a later stage, integration with the Forefront Online Protection for Exchange (FOPE) product. After installation, managing FPE on multiple Exchange servers could be done with the Protection Server Management Console.

Back in September 2012, Microsoft stopped offering FPE (and other security solutions offered under the Forefront brand), but committed to supporting FPE subscriptions through December 31, 2015 to allow customers to find an alternative solution. This decision, criticised by many, left a gap in the market as not everyone was ready to move to a cloud solution such as FOPE.

Exchange 2013 only offered basic anti-malware protection, so an alternative solution was necessary. Some companies started their journey to the cloud by migrating their Exchange environment to Office 365, which offered Exchange Online Protection (EOP), introduced as the replacement for FPE; other companies remained on-premises and routed their inbound and outbound emails through EOP for message hygiene; and for others, cloud solutions like EOP were still not an option (and today are still not), so a fully on-premises alternative was required.

One of these alternatives was, and is, GFI Mail Essentials.



## Current Challenges

Consensus says that Exchange's built-in malware engine does not provide enough protection, enabling malware to potentially make it through to users' Inboxes. This is obviously a huge security risk for companies, especially in a time where ransomware is becoming an increasingly common form of attack.

Traditional Windows antivirus programs don't replace email-based antimalware solutions because Windows antivirus programs that run on Windows servers can't usually detect viruses, malware, and spam that are distributed only through email. There are a few exceptions, as some solutions use transport agents to intercept emails on the Exchange servers themselves and analyse them. However, it is not uncommon for these to cause problems, especially when it is time to upgrade Exchange.

In terms of anti-spam, Exchange does provide good protection. It uses transport agents to provide anti-spam protection such as connection filtering, sender/recipient filtering, content filtering, and more. However, the built-in agents that are available in Exchange 2016 and 2019 are relatively unchanged from Exchange 2010. This means that the level of protection offered by on-premises Exchange is miles away from Exchange Online Protection (EOP).

With Microsoft's strategy of "cloud first", companies need to subscribe to EOP in order to get the latest features and the greatest level of protection. Microsoft promotes the cloud service as secure, reliable and easy to deploy and manage. At the same time, organisations benefit from the well-known cloud advantages including increased flexibility, reduced costs and hardware requirements. All in all, EOP is a good fit for many companies.

The problem is that there are many organisations that prefer an on-premises security solution for Exchange. This could be due to objections to using cloud in general, or because of regulatory or legal requirements that prevent them from using such solutions. Organisations with on-prem Exchange often prefer an on-prem security solution. It allows them to stay in full control of corporate data and knowledge. Third-party security solutions are usually more customisable as well. The ability to tweak different security settings to meet an organisation's particular needs can be a big reason to choose third-party security software for Exchange.

GFI Mail Essentials helps organisations address all of these challenges.



## Choosing GFI MailEssentials

### 1 Easy to Install

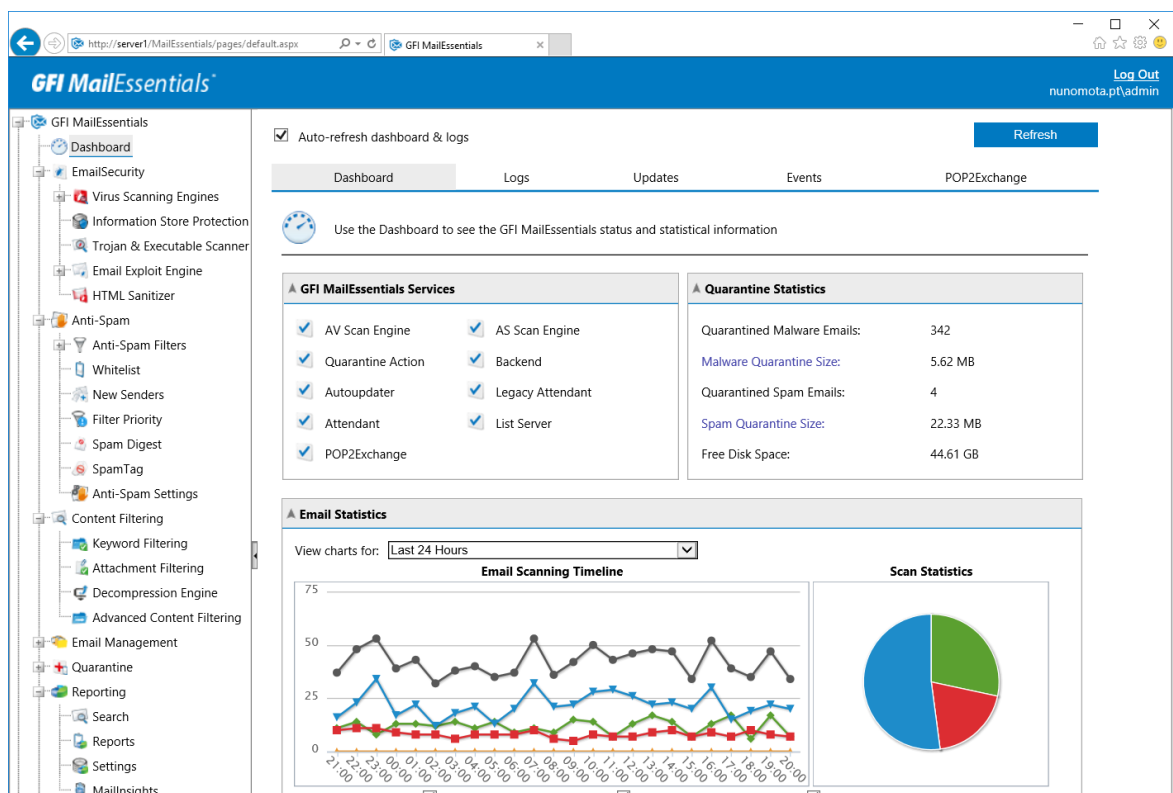
GFI MailEssentials can be deployed on its own server(s), or it can be installed directly in the same server(s) as Exchange. Independently of the chosen method, it should be installed and configured in a way that makes it the email gateway for the organisation, both for inbound and outbound emails.

Installing MailEssentials on a mail gateway/relay server is commonly used for larger organisations, or those that wish to keep MailEssentials and Exchange (or any other mail server being used) separate for any reason, like patching, high availability, and so on. This way, spam and viruses are filtered before these emails are received on the mail server, thus reducing unnecessary email traffic. It also provides additional fault tolerance: if the mail server is down, organisations can still receive email since these are queued on the MailEssentials server(s).

Installing MailEssentials directly on Microsoft Exchange server is the easiest method and it does not require any additional configuration. This makes it extremely easy to set up and get up and running.

### 2 Easy to Use

Thanks to a modern and fresh interface, GFI MailEssentials is easier than ever to use. Administrators will of course need to be familiar with anti-malware and anti-spam terms and technologies, but as long as they are, they will not have problems finding out where each feature is, how to configure it, and how to troubleshoot it should the need arise.



Everything is grouped per technology or feature and properly labelled, making the interface navigation simple and intuitive.

### 3 Completely on-premises

As already mentioned, many organisations prefer an on-premises security solution for their messaging environment. This is typically due to regulatory or legal requirements they must adhere to. No matter the reason, GFI MailEssentials is the perfect solution to address this issue since it is fully on-premises. Having such a powerful and complete solution fully on-premises without having to route emails through cloud solutions hosted by 3<sup>rd</sup>-party companies, is a big win for many companies. It guarantees that organisations retain full control over the solution and its upgrades, as well as the data itself.

### 4 Multiple Anti-Malware Scanning Engines

GFI MailEssentials provides multi-scanning techniques in order to achieve “Zero-Hour” malware protection, drastically reducing the time required to obtain the latest virus definitions against the latest threats. Organisations gain maximum protection for their email environment via five engines’ heuristic and polymorphic malware detection methods, enabling them to take advantage of the strengths of each engine. The five anti-malware scanning engines are: Avira, BitDefender, Kaspersky, Cyren, and Sophos. Antivirus engine vendors have different response times to new viruses and malware, so this capability ensures MailEssentials can always detect new threats in the shortest possible time.

**GFI MailEssentials**

The settings on this page will be synced to all MailEssentials servers

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	Evaluation license	0	↑	↓
BitDefender Anti-Virus	Gateway scanning: Enabled	Evaluation license	1	↑	↓
Kaspersky Anti-Virus	Gateway scanning: Enabled	Evaluation license	2	↑	↓
Cyren Anti-Virus	Gateway scanning: Enabled	Evaluation license	3	↑	↓
Sophos Anti-Virus	Gateway scanning: Enabled	Evaluation license	4	↑	↓

**Virus Scanning Optimizations**

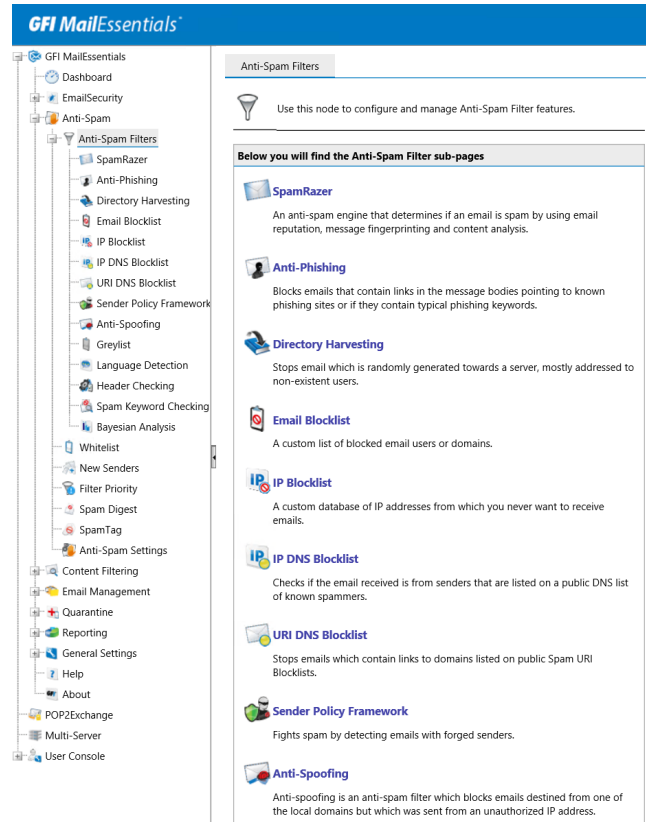
Stop virus scanning the current item, if viruses are detected by:  
 virus scanners

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

This also provides more control for the sysadmin over the malware scanning process (after all, different admins and organisations have their own preferences and requirements), and significantly lowers the business security risk.

## 5 Powerful Anti-Spam

Another major feature of MailEssentials is its powerful anti-spam capability. This VBSpam-certified solution uses multiple anti-spam filters that combine SpamRazer technology, greylisting, IP reputation filtering, Bayesian filtering, and other advanced technologies to provide a spam capture rate of more than 99% and minimal false-positives, ensuring the safe delivery of important emails. The Bayesian Analysis, for example, is an anti-spam adaptive technique based on artificial intelligence algorithms, designed to withstand the widest range of spamming techniques available today. Organisations will have everything they could expect from a solid anti-spam solution, with 14 anti-spam technologies at their disposal.



## 6 Suitable for large environments

GFI MailEssentials provides a feature called multi-server, which makes it suitable for large and dispersed environments. Two common issues when managing a large messaging environment are:

- Ensuring that all servers are configured identically. When deploying multiple servers, how do you ensure they are all configured the way they should be? For example, a typical solution is to use a script to reduce the possibility of human error. But even then, how do you guarantee they remain identical going forward?
- Troubleshooting. How many times have you had to search the logs on individual servers, one by one, hoping to find what you were looking for?

The multi-server feature is designed to help with these issues. It enables communication between different GFI MailEssentials servers so that configuration data can be shared across them all. This is great for organisations with multiple email gateways and email servers, where managing individual servers can be a tedious task without a unified console, not to mention being prone to errors and misconfiguration. Once multi-server is configured, this problem is solved and day-to-day configuration tasks can be done using a single unified console.

**GFI MailEssentials**

Apply Cancel

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:

Password:

Port used to synchronize data

Port:

Centralize Quarantine and Reporting data within the Multi-Install network

Host:

Port:

Test

**Multi-Install Network**

Multi-Install network status: Online

<input type="checkbox"/>	Server	Type	Member Status
<input type="checkbox"/>	SERVER1	Master & Reporting/Quarantine Host	
<input type="checkbox"/>	SERVER2	Slave	

Detach

Synchronised data include the attachment, keyword and advanced filtering rules, and black/white lists. Quarantined emails from different GFI MailEssentials scanning servers are stored in a central server of your choice. This gives you a central quarantine to maintain for your entire organisation.



**GFI MailEssentials**

Apply Cancel

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 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

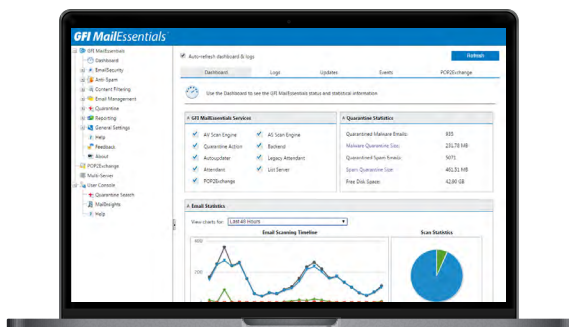
GFI MailEssentials logs all email flow activity to a central reporting database so you can consolidate all your email flow reports and easily detect any mail flow trends or issues. These unified settings are highly customisable, giving you total flexibility in how you deploy GFI MailEssentials on your network.



## Conclusion

Cloud solutions like Exchange Online Protection are great for many organisations. However, they are not suitable for everyone. Some organisations cannot use cloud services due to regulatory or legal requirements. Some simply prefer to keep everything on-premises as much as possible; others might just not be able to afford it.

GFI MailEssentials is on-premises email protection software that will meet the anti-spam and anti-malware requirements for most, if not all, organisations. It is simple to configure and manage, yet extremely powerful and effective.



**Get your FREE MailEssentials trial!**



All product names and companies mentioned may be trademarks or registered trademarks of their respective owners.

All information in this document was valid to the best of our knowledge at the time

of its publication. The information contained in this document may be changed without prior notice.