PRODUCT REVIEW

GFI MailEssentials

Reviewed by Nuno Mota

TechGenix

Introduction

GFI Software is an American developer of IT solutions founded in 1992. Its products range from network performance to patch management, from auditing to security scanning, and more.

One of these solutions is **GFI MailEssentials**, which provides anti-spam and email security for on-premises mail servers. Having reviewed in the past GFI Archiver, and being pleasantly surprised by it, I was eager to have a look at MailEssentials. And here we are! In this product review, I took an in-depth look at GFI MailEssentials v21.5 (build 20190321). However, being such a powerful and complete product means that I can only cover its main features briefly in this review.

01 Requirements

It shouldn't come as a surprise that MailEssentials can be installed in a VMware or Hyper-V virtual environment, which is exactly what I did for this review.

In terms of hardware, the requirements obviously depend on a range of factors, such as email volume and the number of anti-virus engines enabled, but as a minimum:

- Processor: 2GHz with multiple cores;
- Memory (RAM): 2GB dedicated to MailEssentials;
- Disk space: 10GB dedicated to MailEssentials.

As to software, MailEssentials supports:

- Any version of Microsoft Windows Server (64-bit) from 2008 R2 onwards;
- Microsoft IIS SMTP service or Microsoft Exchange Server 2010/2013/2016/2019;
- Microsoft Messaging Queuing Service (MSMQ);
- Microsoft .NET Framework 4/4.5;
- ASP.NET & Windows Authentication role services when installing on Windows Server 2008 R2 onwards;
- Microsoft SQL Server/Express is suggested for the Reporting engine database for installs with more than 100 mailboxes.

02 Installation

GFI MailEssentials can be deployed in a variety of ways. Ideally, it should be installed and configured in a way that makes it the email gateway for the organization, both for inbound and outbound emails. However, it can be installed on its own server(s), or it can be installed directly in the same server(s) as Exchange. In Exchange 2010 environments, MailEssentials can be installed on the servers with the Edge Server Role, Hub Transport Role, or Hub Transport and Mailbox Roles. With Exchange 2013 and above, it can be installed on the Edge Transport role, or Mailbox role servers.

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. In this scenario, MailEssentials is usually hosted in the DMZ and relays inbound emails to the mail server. 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, where if the mail server is down, we can still receive email since these are queued on the MailEssentials server(s).

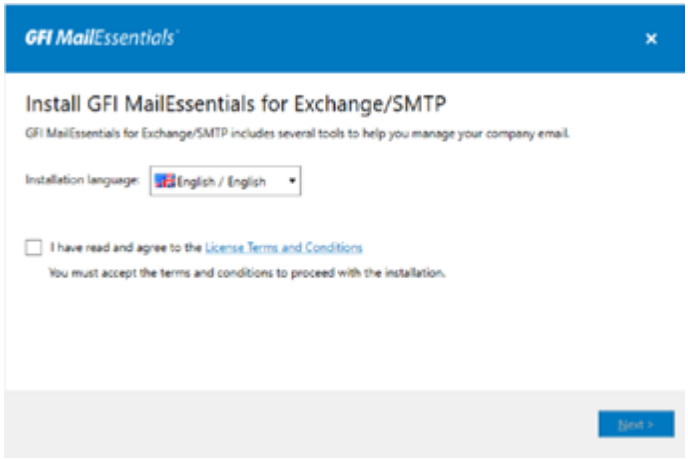
For this review, I deployed two GFI MailEssentials servers in my DMZ, and configured them to relay emails to the internal Exchange 2016 environment. Outbound emails were also being relayed through MailEssentials.

Pre-Requisites

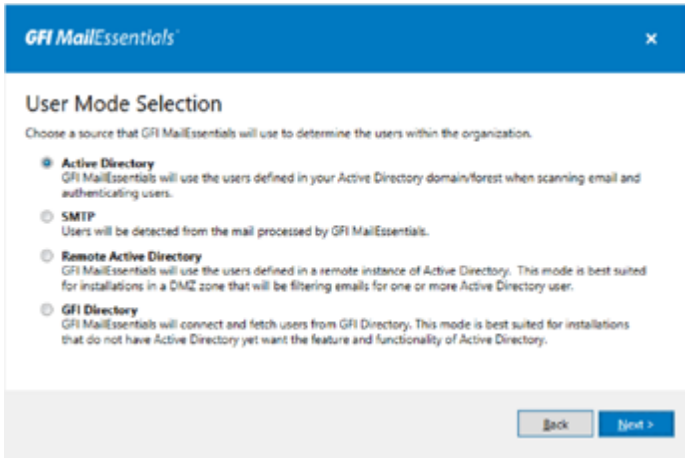
When installing GFI MailEssentials on the same server as Exchange, no pre-install actions or configurations are required. When installed on its own, MailEssentials uses the IIS SMTP service as its SMTP Server and, therefore, the IIS SMTP service is configured to act as a mail relay server. The admin guide provides clear instructions on how to do this, so administrators will not have a problem whatsoever. In a high-level, these are the steps involved:

1. Enable IIS SMTP Service;
2. Create SMTP domain(s) for email relaying;
3. Enable email relaying to the internal mail server(s);
4. Secure the SMTP email-relay server;
5. Enable mail server to route emails via MailEssentials;
6. Update MX record(s) to point to MailEssentials;
7. Test new mail relay server.

The installation itself is as straightforward as possible using the intuitive installation wizard:



The only important decision during this wizard, is the User Mode Selection screen:

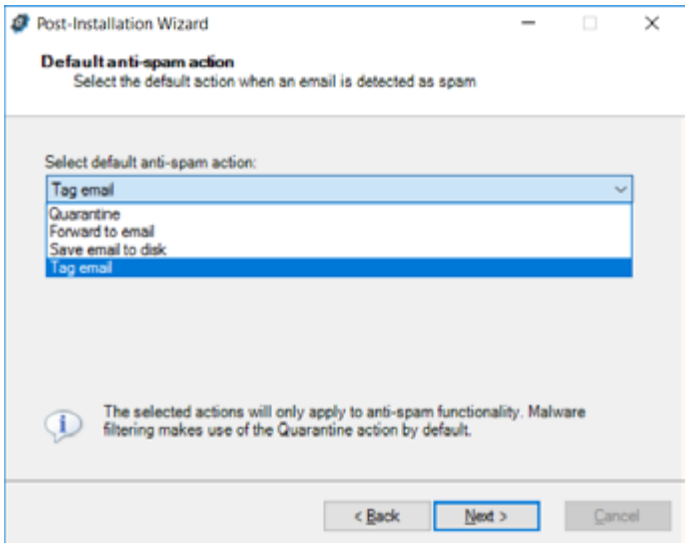


In this screen, we must choose the mode that MailEssentials will use to retrieve the list of email users. Please note that the selected user mode cannot be changed after installation. The list of modes available depends on the environment where GFI MailEssentials is installed.

- **Active Directory:** this option, which is only available when installing MailEssentials on an Active Directory (AD) domain-joined server, allows MailEssentials to retrieve a list of mail-enabled users from AD, which can be used for filtering;
- **SMTP:** this mode is for when an AD domain is not available or if we want to manually manage the list of users. In this mode, 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 MailEssentials' admin console;
- **Remote Active Directory:** this option is only available when installing MailEssentials on a machine that is not AD-joined. In this mode, MailEssentials retrieves the list of users from a remote AD domain (using LDAP), even though the MailEssentials server is not joined to a domain. This mode can be used, for example, when installing MailEssentials in a DMZ;
- **GFI Directory:** only available when installing MailEssentials on a server that is not AD-joined. In this mode, MailEssentials connects and fetches users from GFI Directory (a directory of users and groups that integrates with GFI products). This mode is best suited for installations that do not have AD, yet want the features and functionalities that a user directory offers.

Following the installation of MailEssentials, we are presented with a post-installation wizard, which allows us to configure the basic settings to get MailEssentials routing and processing emails:

In this wizard, there is another important screen named Default anti-spam action where we select the default action to be taken when emails are detected as spam. This action applies to anti-spam filters only. Emails found with malware are automatically quarantined by default. When installing MailEssentials on Exchange, we have the option to Move to Outlook junk email folder. However, when installing it on its own, only the following options are available:

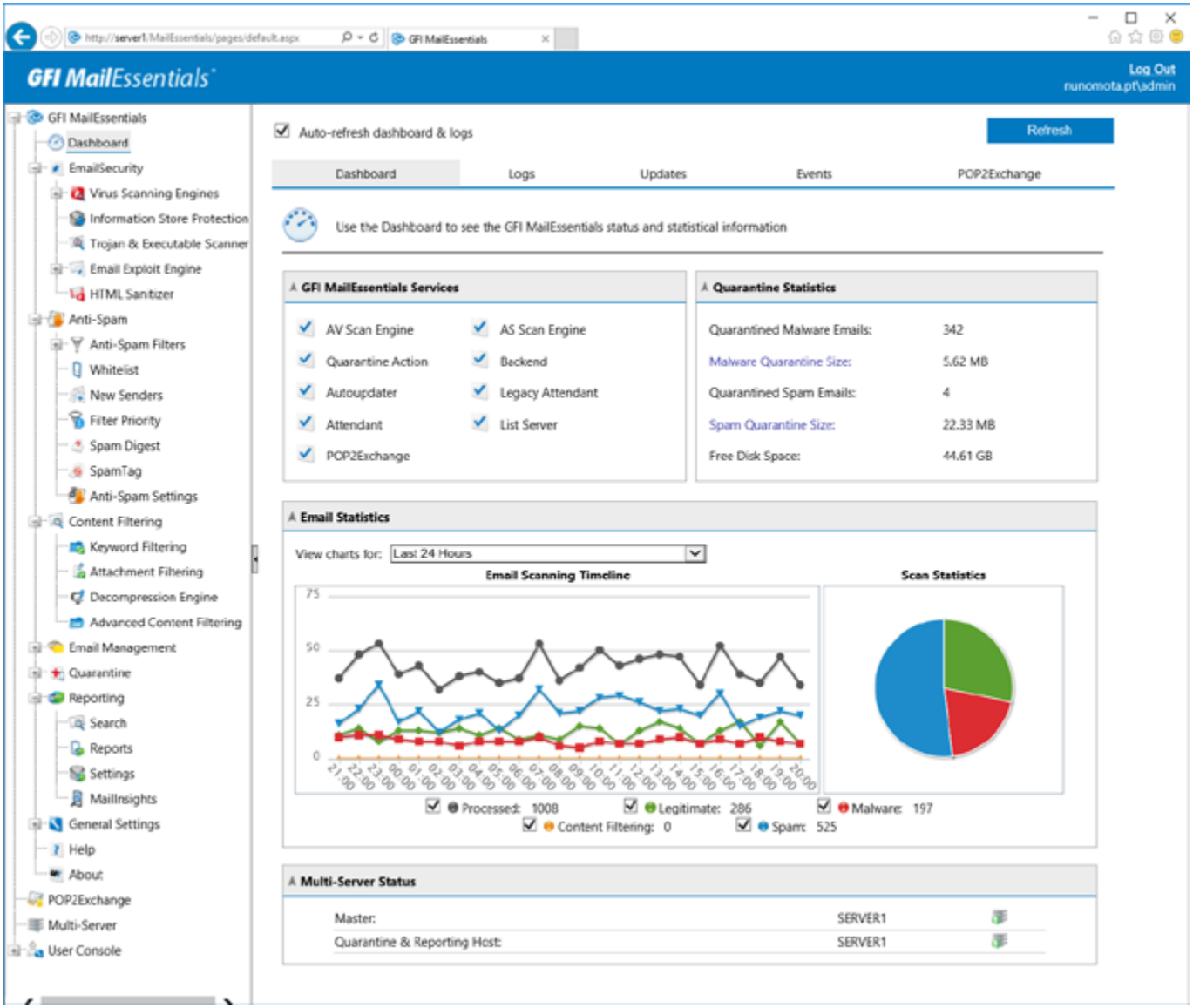


Since many organizations prefer their spam email to be delivered to users' Junk Email folder, we can achieve this by creating a mail flow rule in Exchange that looks for the X-GFIME-MASPAM and/or X-GFIME-BLOCK-REASON message headers and sets the Spam Confidence Leve (SCL) for that message. This way, those emails will be delivered to the users' junk email folder.

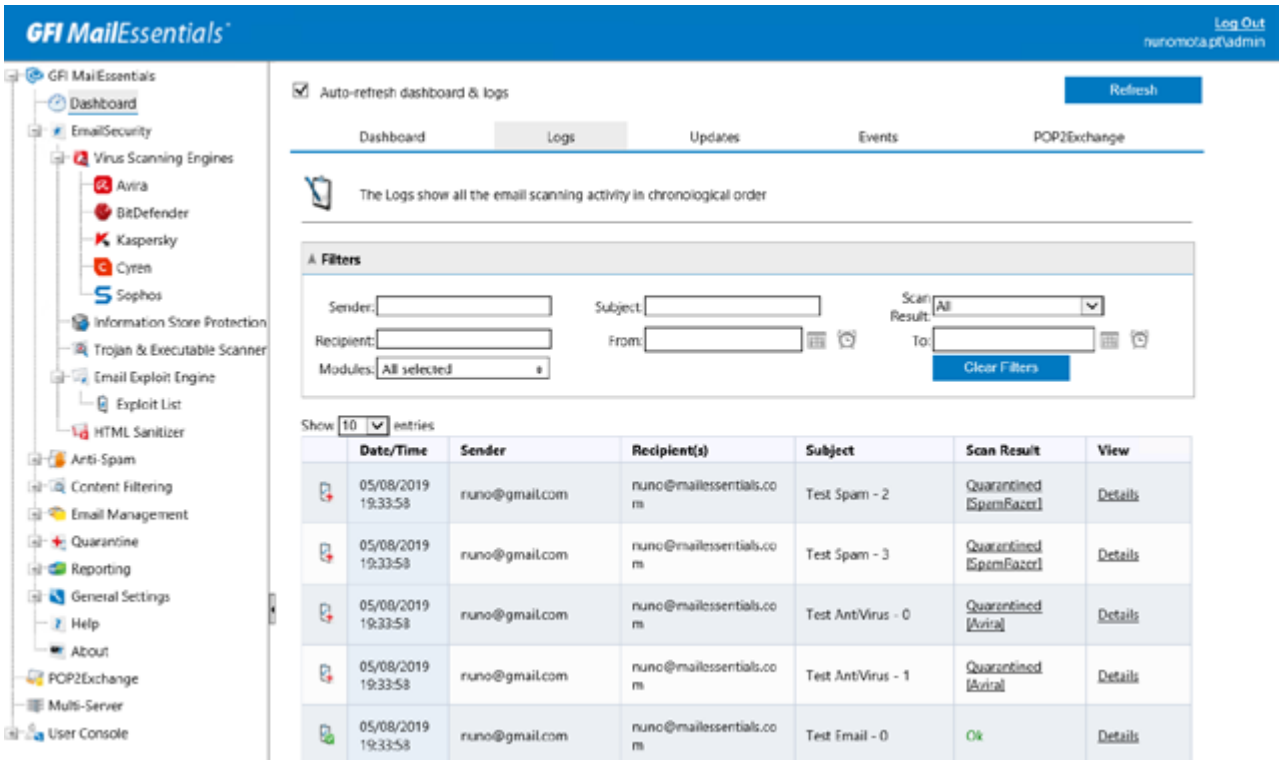
Let's now have a look at MailEssentials' dashboard and main features.

03 Main Features

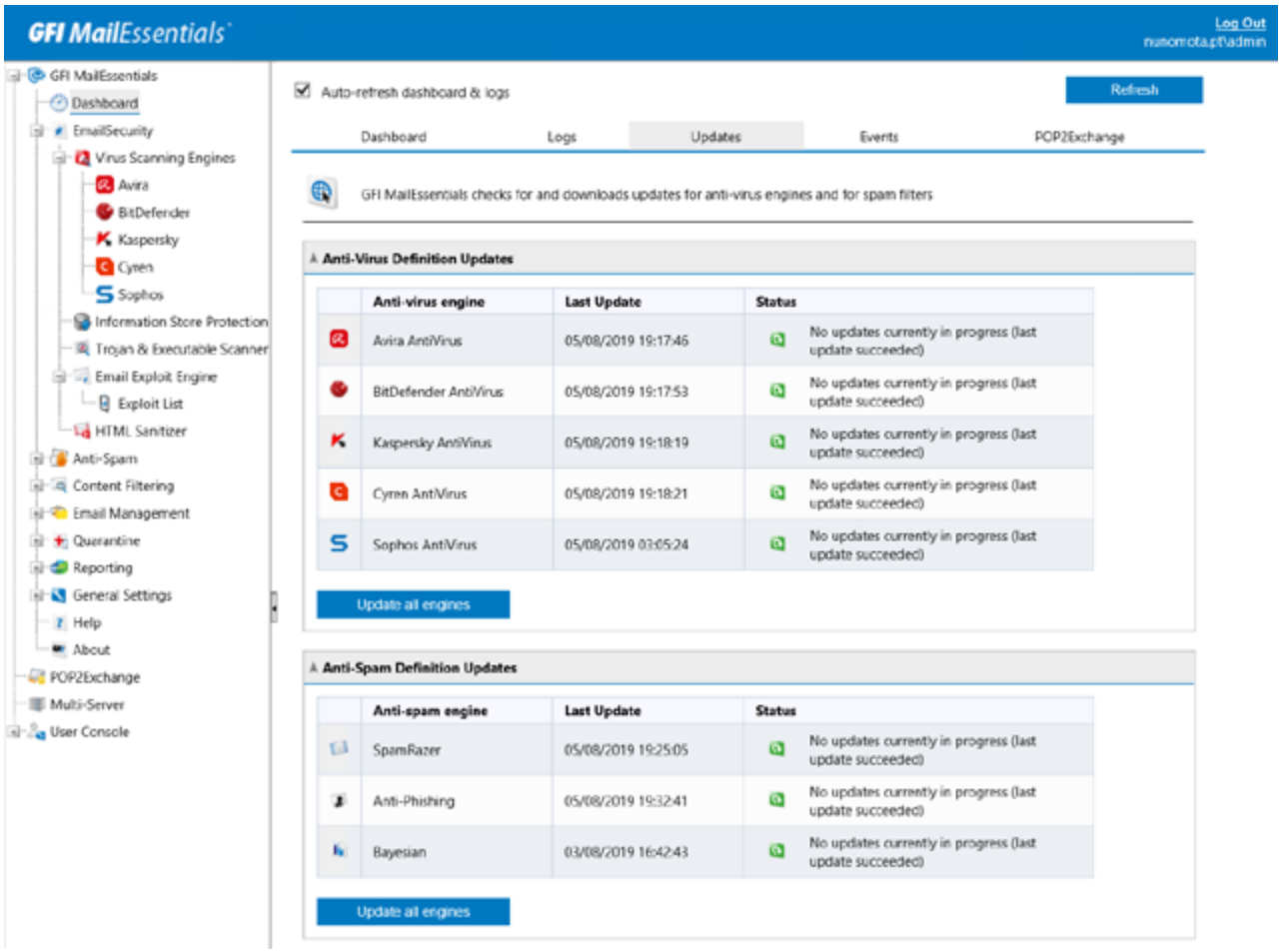
When we open MailEssentials, we are presented with the **Dashboard**. This gives us a quick overview of all the enabled or disabled services, how many emails have been quarantined, how many emails were detected with malware or spam, and more. Straightaway, we can see from the left-hand pane, some of the great number of features available in MailEssentials.



Under the **Logs** tab, we can see a list of all the processed emails, or we can easily perform a search for any email received in the past:



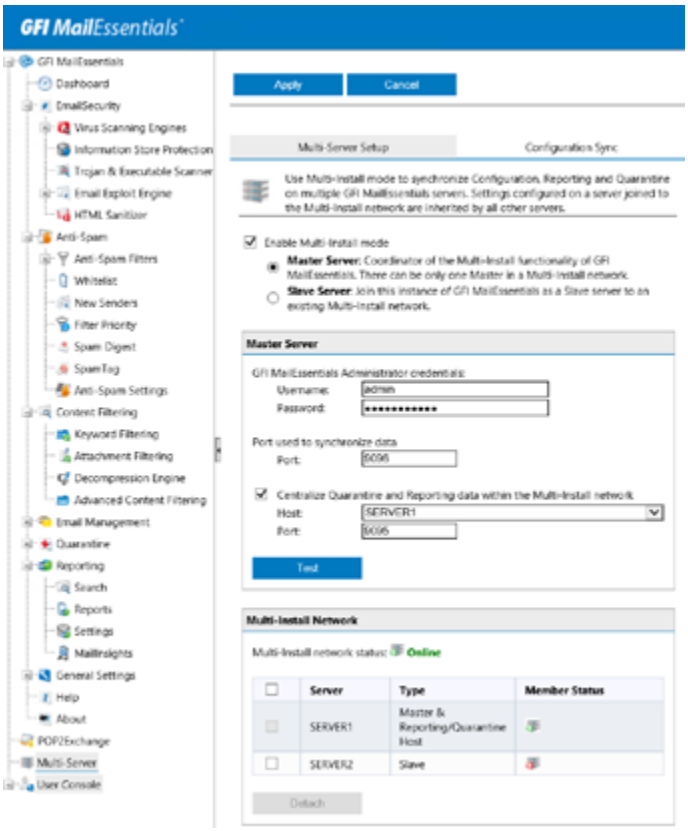
Updates gives us a quick overview of the anti-virus and anti-spam definition updates:



04 Multi-Server

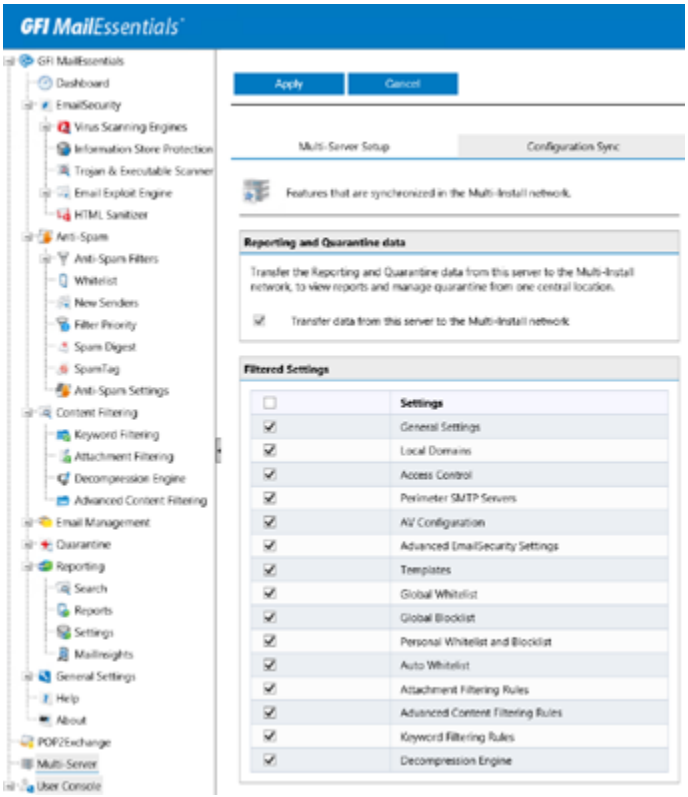
The reason why I am starting with the multi-server feature is because it is both an important one as well as new. It enables communication between different GFI MailEssentials servers so that configuration data can be shared across the servers. This is great for organizations with multiple email gateways and email servers, where managing individual servers can be a tedious task without a unified console, not to mention prone to errors and misconfiguration. Once multi-server is configured, this problem is resolved, and day-to-day configuration tasks can be done using a single console.

Configuring the multi-server feature is straightforward. We promote one of the servers as the master server while all the other servers are configured to connect to it as slaves.



We can also define what we want to be synchronized between servers, and choose to have a centralized quarantine and reporting.

When everything is set up, each server will scan emails flowing through it, but their configuration, such as anti-spam policies for example, are synchronized from the master server. If the master goes down, the slave server(s) will continue to work normally. For reporting and quarantine data, all this data is queued on the slave server(s) until the master is back online.



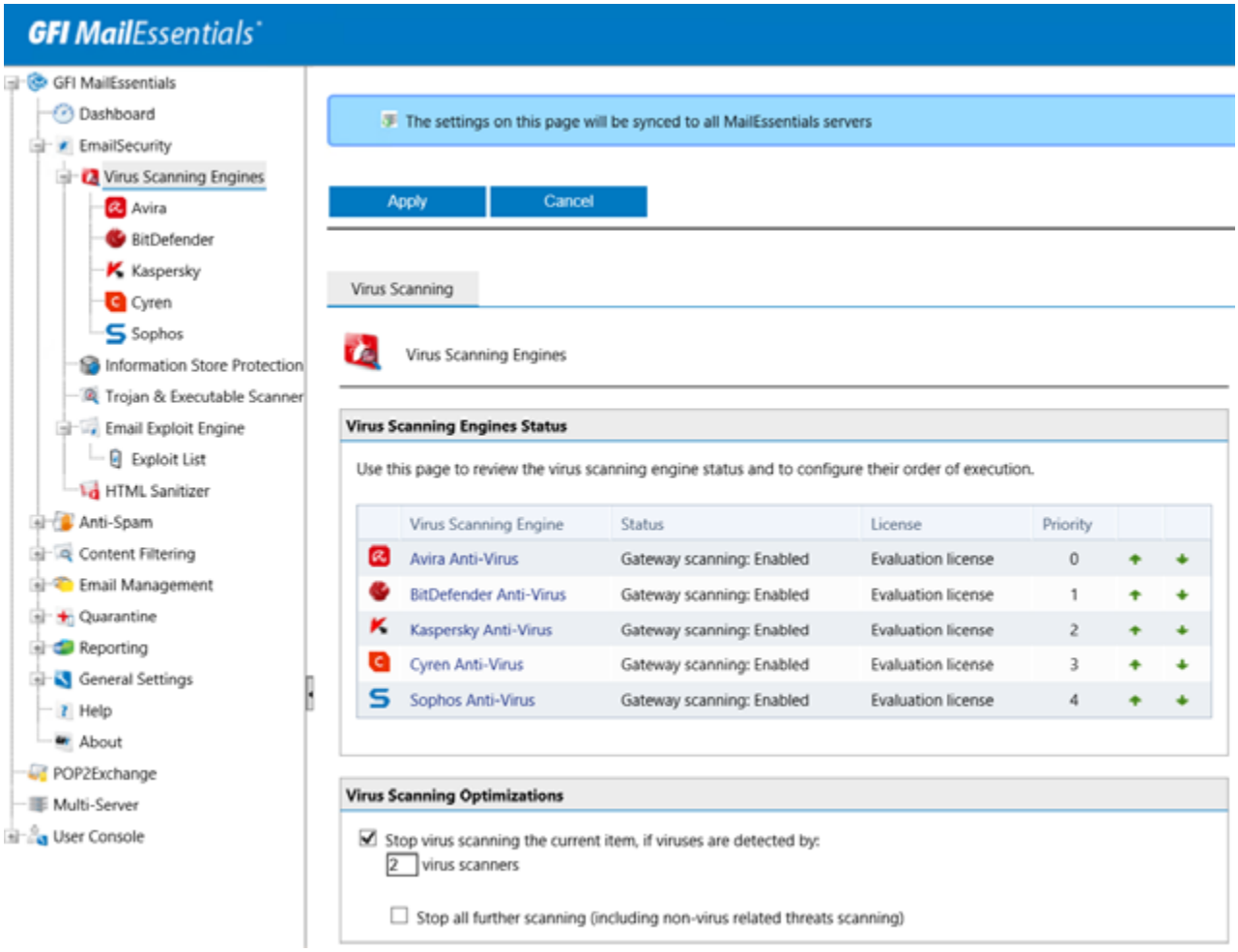
05 E-mail Filtering

GFI MailEssentials enables administrators to filter and detect viruses, spam and other malicious content in emails. After all, this is its main purpose! The following are the three main nodes in MailEssentials:

- **Email Security** configures virus scanning and other malware related filters;
- **Anti-Spam** configures spam filters, as well as the Whitelist for email that bypass spam filtering;
- **Content Filtering** configures rule-based filters that identify and block specific email content.

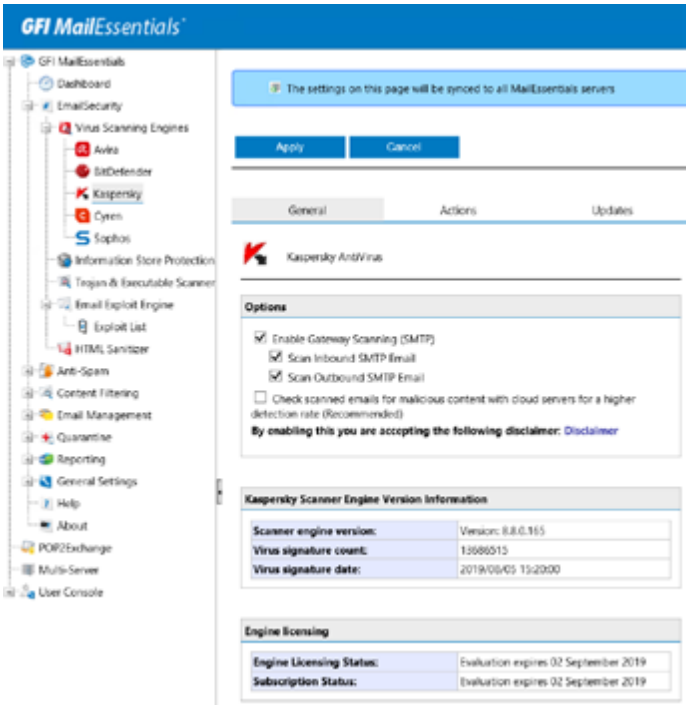
06 E-mail Security

One of the strong points of GFI MailEssentials is that it provides five different anti-malware scanning engines: Avira, BitDefender, Kaspersky, Cyren, and Sophos:

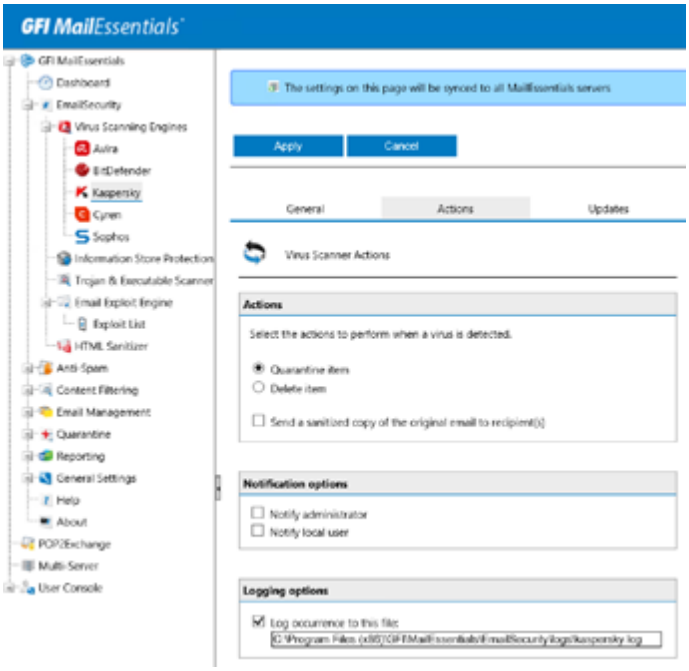


Notice the message at the top stating that “the settings on this page will be synced to all MailEssentials servers”. This is because of the multi-server feature we just discussed.

As expected, we can configure the priority of each scanning engine, as well as disable any we might not want to use:

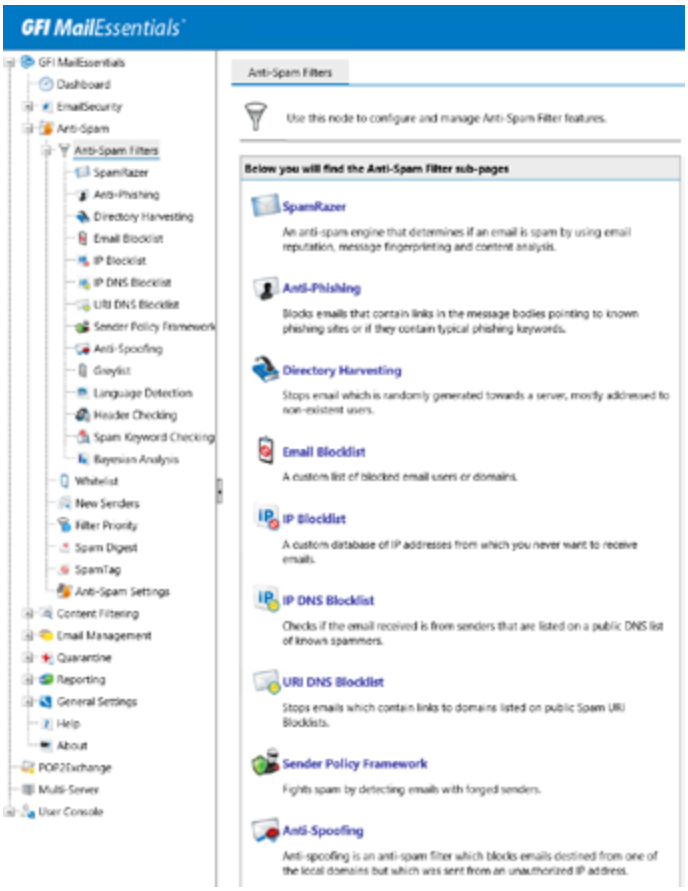


There are also additional options, such as **Information Store Protection** which enables scanning the Exchange Information Store for viruses; **Trojan and Executable Scanner** which blocks emails with executable files; **Email Exploit Engine** checks for known email exploits; and **HTML Sanitizer** removes scripts from emails and HTM\HTML attachments within them. By default, all features are enabled, and blocked emails get quarantined. This can be changed by updating the properties of each virus scanners\filters individually.

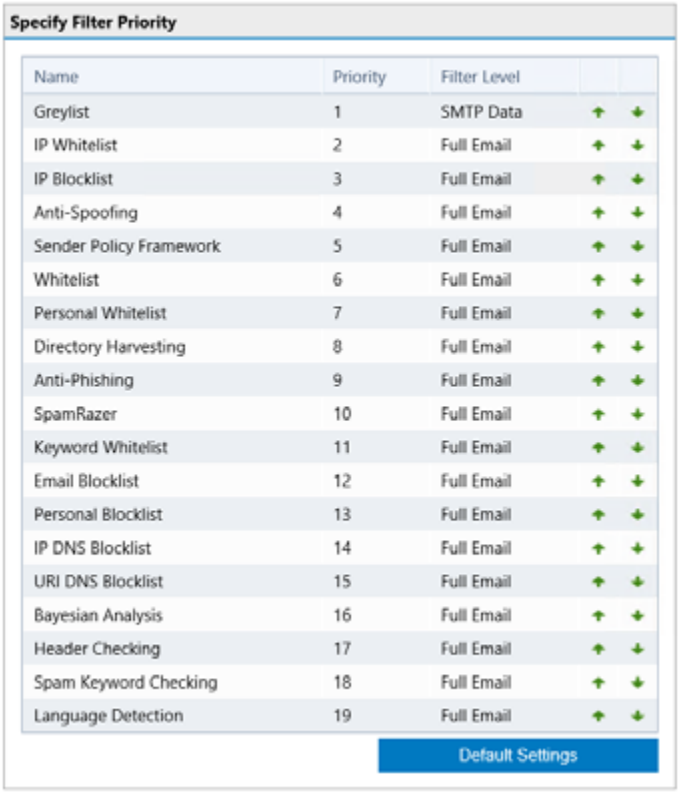


07 Anti-Spam

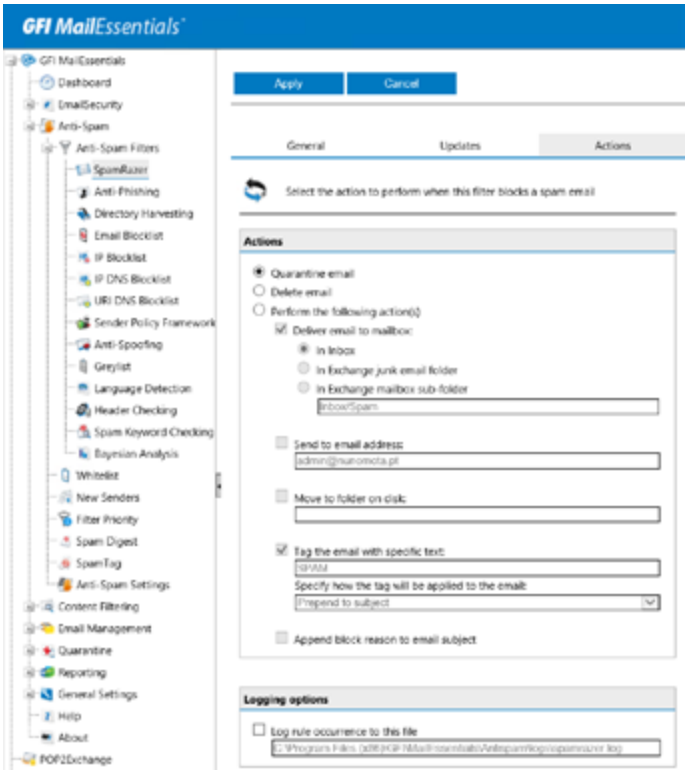
Another major feature of MailEssentials is, obviously, its powerful anti-spam capabilities. Here, we have everything we could expect from a solid anti-spam solution, with the following spam filters enabled by default: SpamRazer, Anti-Phishing, Directory Harvesting (if installed on an AD-joined server), Email Blocklist, IP DNS Blocklist, and URI DNS Blocklist.



Similar to the anti-virus scanning engines, we can configure the filter priority for every anti-spam feature or agent, giving us great control over what takes precedence over what.



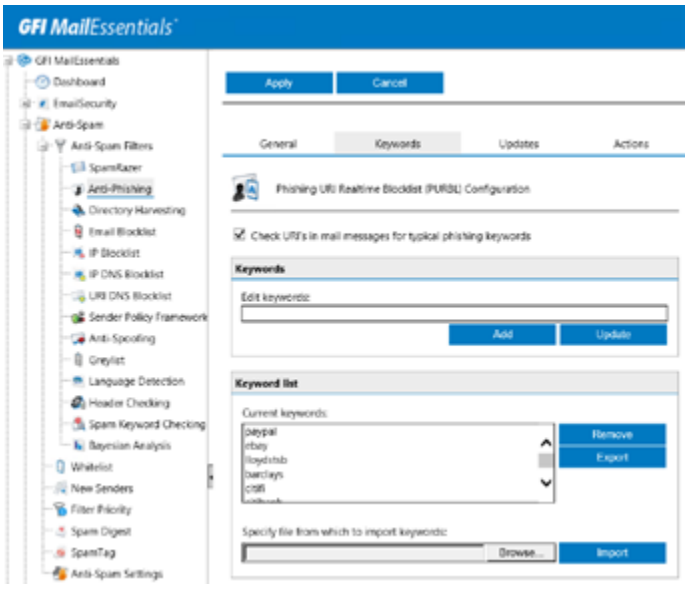
There are just so many features that it is simply impossible to cover them all, so I will just focus on a few important ones. **SpamRazer** is the anti-spam engine that determines if an email is spam or not by using email fingerprints, email reputation and content analysis. SpamRazer is the primary anti-spam engine and is enabled by default. It also includes Sender Policy Framework (SPF) filtering which detects forged senders.



As mentioned earlier, when MailEssentials processes an email and determines it is spam, it adds two message headers to the email. These can be used to create an Exchange mail flow rule to act on them, for example, or to troubleshoot the reasons why a particular email was deemed spam. In the following screenshot, we can see these headers and all the findings from SpamRazer that lead to the decision to mark this particular email as Spam:

21	X-GFIME-MASPAM	SPAM
22	X-GFIME-BLOCK-REASON	Message was found to be spam: (30%) BODY: contains "viagra",(23%) Sender has spammy reputation, (15%) BODY: contains custom phrases,(11%) BODY: contains text similar to "million united states dolla r",(11%) BODY: contains text similar to "million united states dollar",(8%) Body:Likely_Adult_Phrases,

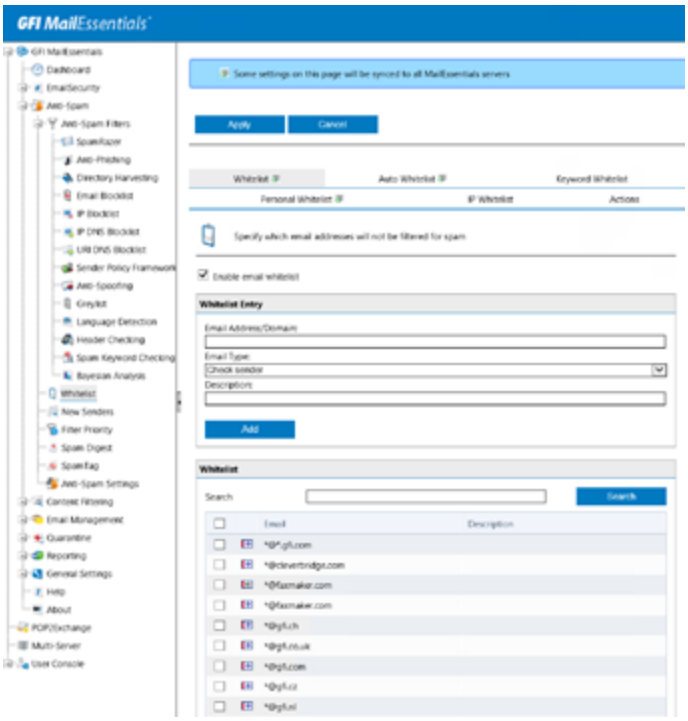
With **Anti-Phishing**, we can configure MailEssentials to Quarantine, Delete, or Tag emails that attempt to fraudulently acquire sensitive information by trying to convince the recipient to visit a malicious website by clicking on the URI in the message. We can even configure our own keyword list to adapt MailEssentials to our environment. Afterall, a financial organization typically has different requirements than an educational institution.



Another great feature is the **Bayesian Analysis**, an anti-spam adaptive technique based on artificial intelligence algorithms, hardened to withstand the widest range of spamming techniques available today. It is disabled by default as it is highly recommended that administrators "train" the Bayesian filter before enabling it. GFI recommends operating MailEssentials 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 once it adapts to an organization's email patterns.

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. The mathematical basis of Bayesian filtering 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.

The **Email Blocklist** and **Whitelist** nodes enable administrators to enable or disable Personal Whitelist/Blocklist for end users, block/allow specific domains at a global level, configure trusted IPs that are ignored by the GFI MailEssentials spam filtering, and much more.

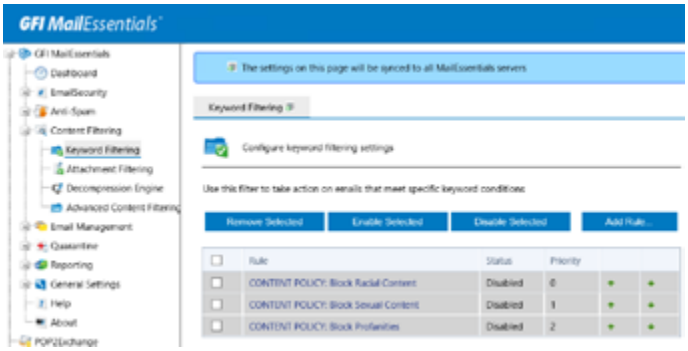


08 Content Filtering

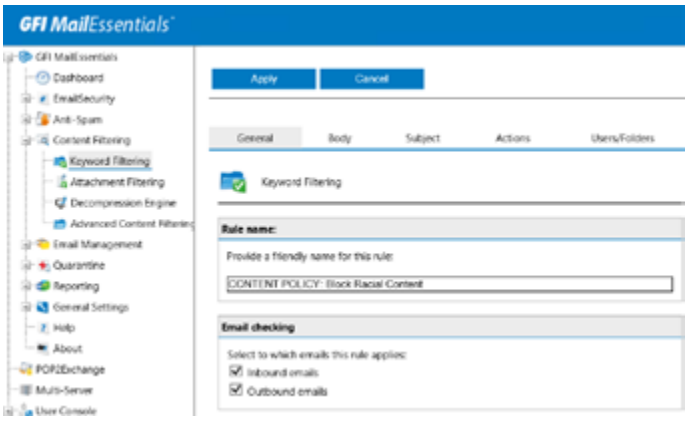
Content Filtering is another crucial feature of any anti-spam/malware solution. Its engines allow MailEssentials to scan the content of emails and attachments, and block emails containing content matching any configured content filtering rules. Here we have all the filters we could expect, such as:

- **Keyword Filtering** blocks emails based on keywords in the body, subject and/or attachments;
- **Attachment Filtering** blocks emails based on type or size of its attachment(s);
- **Decompression Engine** blocks emails with specific types of compressed files within the email, such as password protected archives, recursive archives, and so on;
- **Advanced Content Filtering** blocks emails based on text in header, subject or body of the email, using text search or regular expressions. This allows administrators to, for example, prevent users from sending outbound emails with credit card numbers.

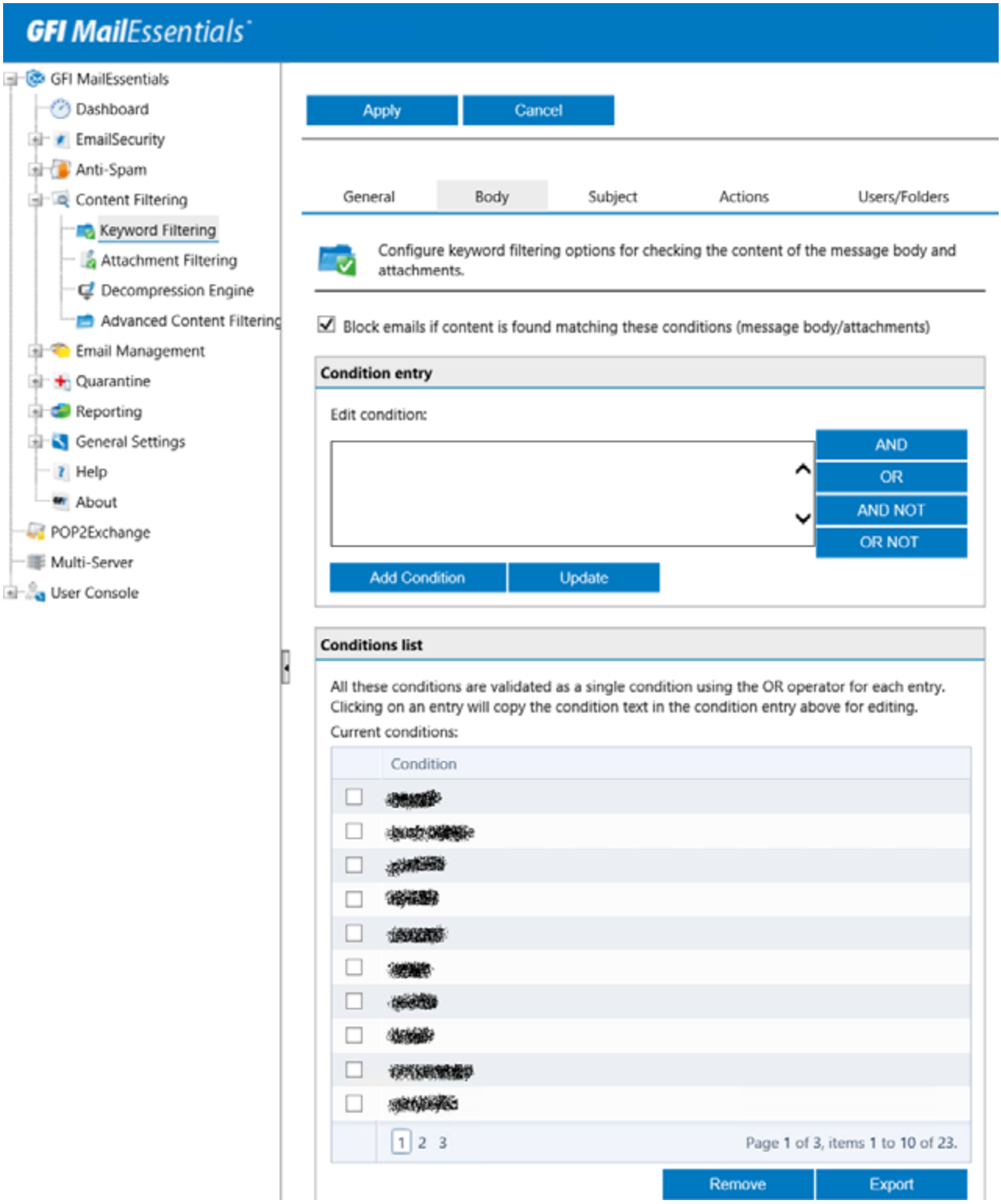
Under Keyword Filtering, we have three out-of-the-box policies that allows us to block emails with racial, sexual, or profanity content.



We can apply each policy to inbound and/or outbound emails.

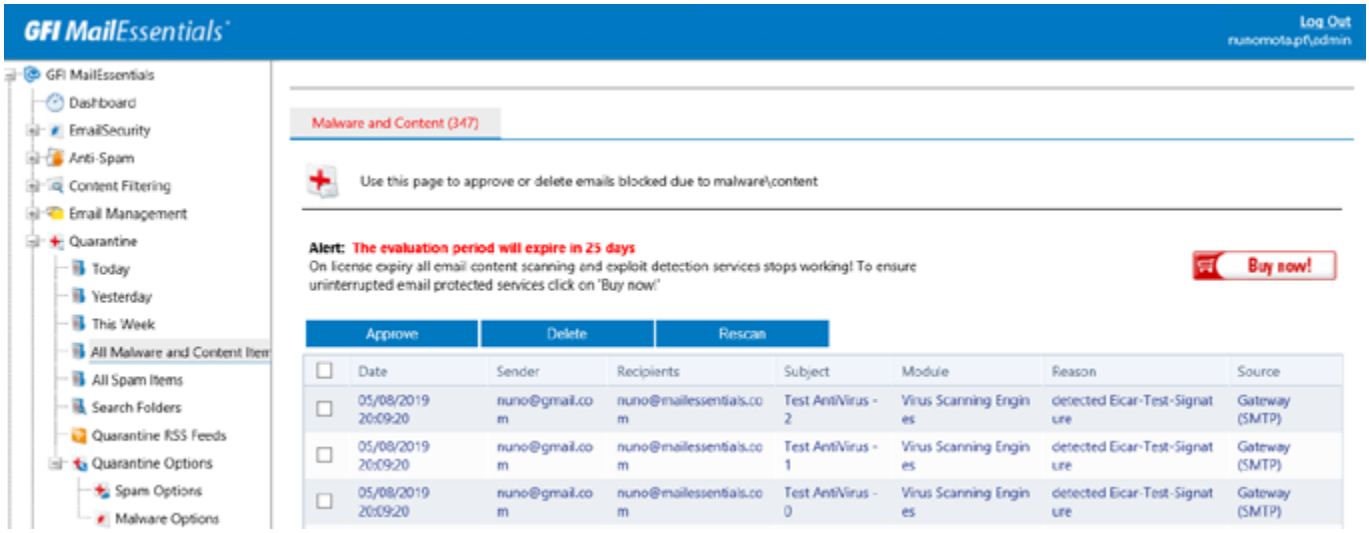


We can also specify what to do when an email triggers the policy, which users to apply the policy to, as well as edit the list of words that will be searched for:



09 Quarantine

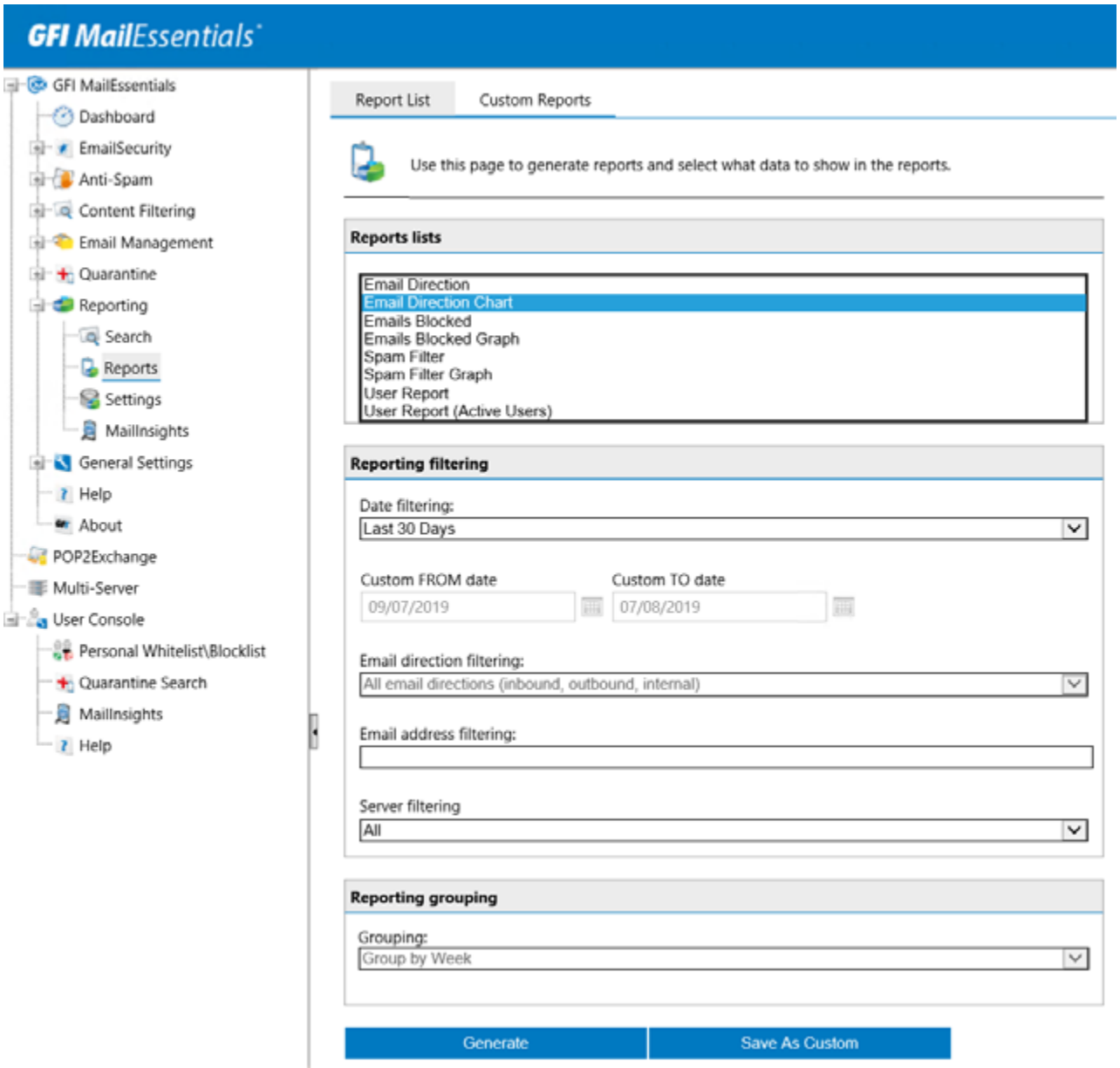
Administrators can use the **Quarantine** to analyze, and act, on blocked/quarantined emails. It provides a central store where all emails detected as spam or malware are retained. This ensures that users do not receive spam and malware in their mailbox and processing on the mail server is reduced. Administrators and mail users can review quarantined emails by accessing the quarantine interface from a web browser. MailEssentials can also send regular email reports to users so they can review their blocked emails.



There is also a handy RSS (Really Simple Syndication) feed to notify administrators of newly quarantined items.

10 Reporting

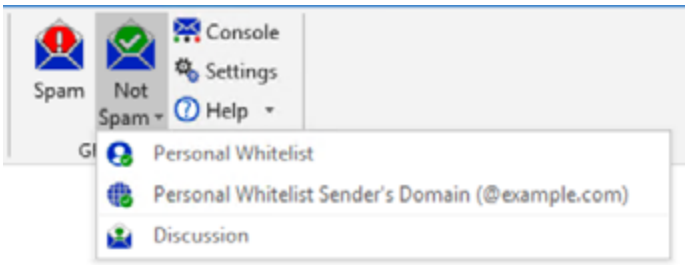
MailEssentials offers some basic **Reporting** out-of-the-box, which provide some useful information. These reports can be scheduled to run at a specific date/time, or generated on-the-fly.



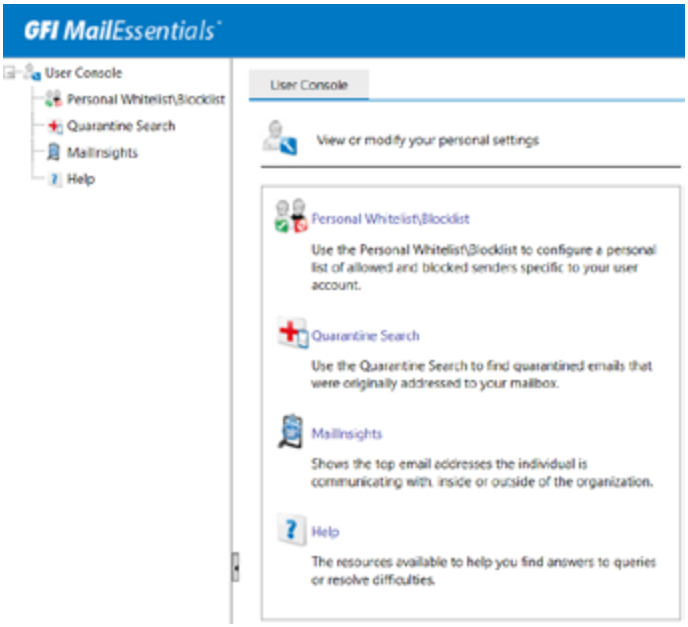
For more advanced reports, administrators need to resort to MailInsights, a reporting facility that uses the data in the reporting database to deliver information related to email usage and trends. However, MailInsights reports can only be generated using another tool from GFI called MailArchiver.

11 SpamTag for Microsoft Outlook

The last feature we will cover in this review is the SpamTag Outlook plugin, which gives users some control over the management of spam emails. Using this plugin, users can mark emails as spam or not spam, and whitelist/blocklist the sender or sender's domain for example. The plugin also synchronizes Outlook's Junk settings with MailEssentials.

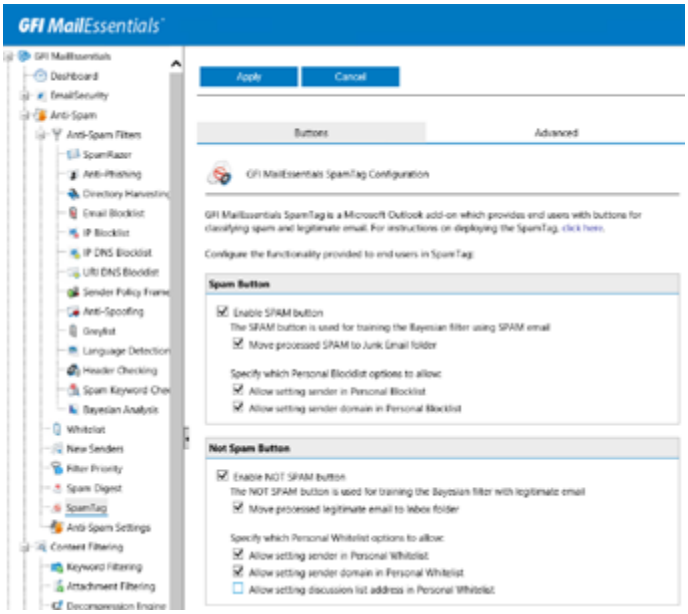


Users can also navigate to their personal MailEssentials console to manage their whitelist and blocklist, or search emails that were addressed to them but quarantined:



Using the SpamTag panel, Administrators can choose which of the following features and functions to enable/disable for end users:

- Import Outlook Junk Settings to Personal Blocklist and Personal Whitelist;
- Import Outlook contacts to Personal Whitelist;
- Allow users to access their console;
- Add the email's sender or domain to either the Personal Blocklist or Personal Whitelist;
- Automatically synchronize allowed and blocked senders in Outlook with the GFI MailEssentials Personal Whitelist and Personal Blocklist respectively;
- Automatically add users' contacts to the Personal Whitelist.



12 Shortfalls

From my short experience of using MailEssentials, there are three things I would like to see improved. The first one is monitoring. It would be great if MailEssentials monitored and alerted admins when its mail queue goes over a certain threshold, when its next hop becomes unavailable, or when the IIS SMTP service goes down, just to mention a few examples. If MailEssentials is to be the mail gateway for an organization, it needs to provide not only a great level of highly-availability, but also in-depth monitoring to avoid any downtime, mail queuing, and so on.

Secondly, it would be great if we could have different actions for different Spam Confident Levels. It is common for organizations to send emails with a SCL of 5 or 6 to users' Junk Email folder, and quarantine emails with a SCL of 7 or above. With MailEssentials we are limited to one action.

Finally, I find it hard to understand why we need MailArchiver just to access all the MailInsights reports, since this data is already captured by MailEssentials and stored in its own database. It would be great if GFI made all these reports available as part of MailEssentials, all in one package.

13 Conclusion

GFI Mail Essentials is, without a doubt, a powerful and very capable anti-spam and anti-malware solution. With its new multi-server feature, it became suitable for large organizations as it provides a central management portal. Even with the shortfalls mentioned above, I would have no problem recommending it!

TechGenix