SPAMfighter Mail Gateway

User Manual

Revised 2009-05-19

Table of contents

1. Introduction

SPAMfighter Mail Gateway, often abbreviated as SMG, is an easy-to-use protection against spam e-mails. SPAMfighter Mail Gateway is intended for use as a SMTP gateway in front of an existing e-mail infrastructure. If enough SPAMfighters report the same e-mail as spam, it is instantly removed from all other SPAMfighters and SPAMfighter Mail Gateway users. In other words, SPAMfighter Mail Gateway provides instant protection against the growing threats from unwanted spam e-mails.

SPAMfighter Mail Gateway does not require any client-side software, no spam configuration or any daily maintenance for that matter after initial installation and configuration. This allows for an easy installation and administration, as well as a trouble-free integration into an existing e-mail infrastructure.

This document describes how to install and configure SPAMfighter Mail Gateway into an existing e-mail infrastructure – and how to configure SPAMfighter Mail Gateway to fit your particular e-mail filtering requirements.

2. Basic idea

SPAMfighter Mail Gateway is built upon the core notions "*detect-and-remove*" and "*power-through-simplicity*". These two notions are the very building blocks that SPAMfighter Mail Gateway has been developed upon, and is outlined in the following paragraphs.

2.1 Detect-and-remove

Once SPAMfighter Mail Gateway has been installed, it will instantly begin to listen for incoming e-mails. When an e-mail arrives, the following measures are taken:

- SPAMfighter Mail Gateway accepts the e-mail and look up the intended recipient / recipients
- For each recipient, their specific scanning policy is used to run the e-mail through SPAMfighter Mail Gateway's scanning engines
- If the e-mail is determined as unwanted, the users' policies dictate how the e-mail should be blocked (usually quarantined or deleted)
- If the e-mail is determined as legitimate, the users' policies dictate how the e-mail should be delivered (usually delivered to the users' mailboxes)

In addition to this effective detection and removal of spam, SPAMfighter Mail Gateway offers extensive reporting, advanced e-mail manipulation and extended e-mail capabilities through an open plug-in system.

With regards to the end-users, there are absolutely no causes for concern, as unwanted e-mails are automatically removed without the need for any user intervention. While SPAMfighter Mail Gateway simplifies administration and keeps software and configuration off the employee's desktop, it also provides the option for individual control for end-users at the administrator's request.

2.2 Power-through-simplicity

Extensive work has been done in the development of SPAMfighter Mail Gateway to make the application as simple as possible while still providing the end-users with powerful tools. Novice users as well as advanced users will be able to administer SPAMfighter Mail Gateway within minutes of installation.

This simplicity primarily shows itself in the Administration Module, as this is a dedicated web application. No need for logging onto the server or use an inappropriate Microsoft Management Console to administer the application – the Administration Module is available directly in a browser from any PC.

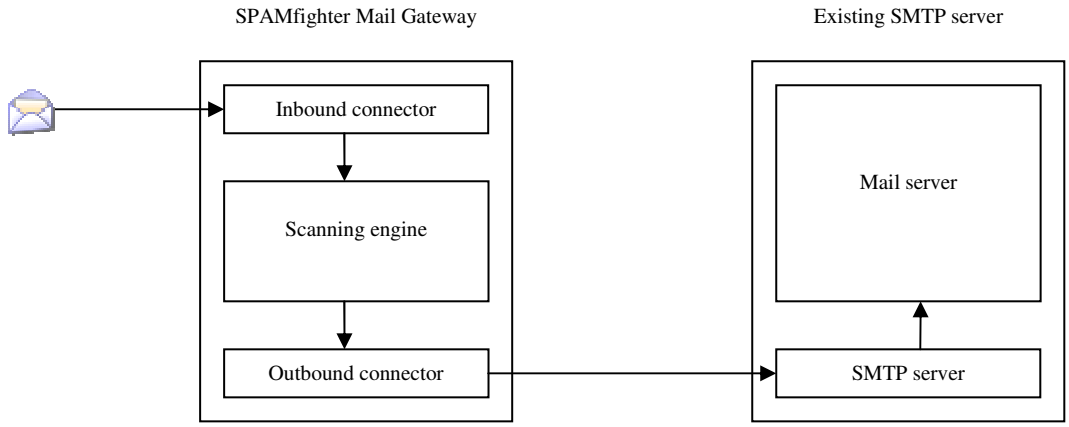
Simplicity also shows itself when configuration of the filters are made. SPAMfighter Mail Gateway don't use strange, technical terms and keeps the interfaces as simple as possible. SPAMfighter Mail Gateway is preconfigured to provide you with the best possible malware filtering right out of the box – but, if needed, users are able to tweak and bend SPAMfighter Mail Gateway practically in any way they may desire.

Finally, simplicity shows itself by providing users with extensive reporting capabilities. Use the Administration Module to browse statistical information – or get daily / weekly / monthly reports sent on e-mail.

3. How it works

SPAMfighter Mail Gateway works by running its own SMTP server – which will listen for incoming e-mails.

SPAMfighter Mail Gateway is a "store-and-forward" SMTP server – which means it will accept incoming e-mails instead of the existing SMTP server, scan the e-mail, and then route the e-mail on to another SMTP server if deemed legitimate. During the installation – or at any point in time afterwards – configuration of where to route e-mails can be configured. Due to this "store-and-forward" (i.e. gateway) concept – an existing SMTP server is required[1].



When a new e-mail arrives, SPAMfighter Mail Gateway will scan the e-mail and determine if the e-mail is a spam e-mail or a legitimate e-mail. If the e-mail is determined to be spam, SPAMfighter Mail Gateway will either:

- Quarantine the e-mail and notify the recipient(s) 1 time a day[2] of e-mails that have been quarantined for later retrieval if needed
- or Redirect the e-mail to a dedicated recipient (for example the Administrator's mailbox)
- or Prefix the subject with a text – for example "[SPAM]"
- or Add a header to the e-mail
- or Store the e-mail as a file on the disk
- or Delete the e-mail
- or any combination of the above

[1] If you already receive e-mails in your organisation, then you almost certainly already have a SMTP server
[2] This can of course be configured at the user's discretion

The way SPAMfighter Mail Gateway determines if an e-mail is spam or legitimate is by running the e-mail through a number of filters. The most significant filter is the “Community Filter” which will generate a unique signature of the e-mail and ask the global SPAMfighter Classification Network if this particular e-mail is a known spam e-mail or not. All of this takes only milliseconds to complete and users will not notice anything – except the massive decrease of spam received.

The SPAMfighter Classification Network is a global network of servers to which the millions of users in the SPAMfighter Community reports spam to. This means, to fully utilize the power of SPAMfighter Mail Gateway, the application needs to have access to the Internet.

4. Installation of SPAMfighter Mail Gateway

SPAMfighter Mail Gateway can be installed on virtually any type of Microsoft Windows operating system. Before installation please review the system requirements described in the following paragraph.

4.1 System requirements

Installation on Windows 2003 / 2008 is *recommended* in performance critical environments since SPAMfighter Mail Gateway will utilize a highly asynchronous communication model. The software is however *compatible* with Microsoft Windows 2000 and later. For optimal performance, make sure that the machine is fully updated with all available service packs.

Operating system	Microsoft Windows 2003 Server Microsoft Windows 2008 Server Microsoft Windows 2000 Server Microsoft Windows 2000 Client Microsoft Windows Vista Microsoft Windows XP Installation in virtual environments supported
E-mail server	Any SMTP based e-mail server
Additional software	Microsoft .NET framework 2.0 SP1 (*) Microsoft Internet Explorer 6.0 or newer (**)
Memory	128 MB minimum
Disk space	20 MB minimum (***)
CPU	1000 MHz minimum Support for both 32 bit and 64 bit Support for multiple cpu cores

(*) Will be offered during installation of SPAMfighter Mail Gateway if missing
(**) Any JavaScript enabled browser can be used to connect to the Administration Module
(***) Additional space may be required for runtime database-files used internally by SPAMfighter Mail Gateway

4.2 Before installation

As mentioned in paragraph “3. How it works”, an existing SMTP server is required for SPAMfighter Mail Gateway to be able to function properly.

If SPAMfighter Mail Gateway is to be installed on the same machine as the existing SMTP server, then this needs to be reconfigured to listen on another network port than the default port 25 or on a secondary network interface that uses an independent IP address. Please see the manual for the existing SMTP server on how to do this. Configuration of routing to the existing SMTP server can also be done after installation of SPAMfighter Mail Gateway has been completed.

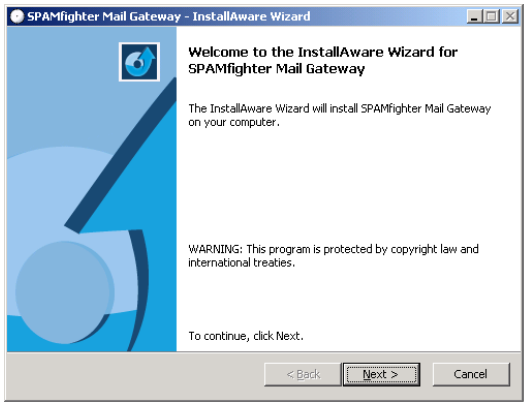
If SPAMfighter Mail Gateway is to be installed on another machine than the existing SMTP server, then no pre-configuration is needed.

4.3 Installation procedure

To install SPAMfighter Mail Gateway, download and run the latest installation file from SPAMfighter's website:

http://www.spamfighter.com

The actual installation process is as follows:

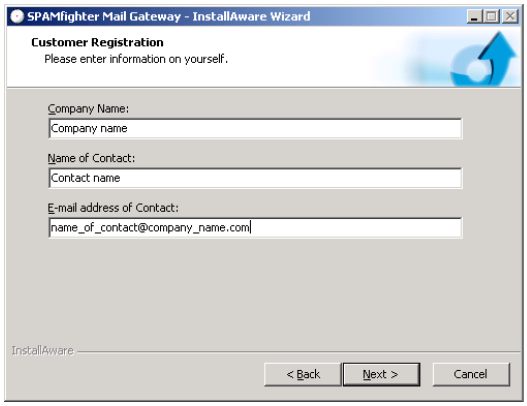


Welcome screen

Click the "Next >" button to begin installation of SPAMfighter Mail Gateway

License agreement

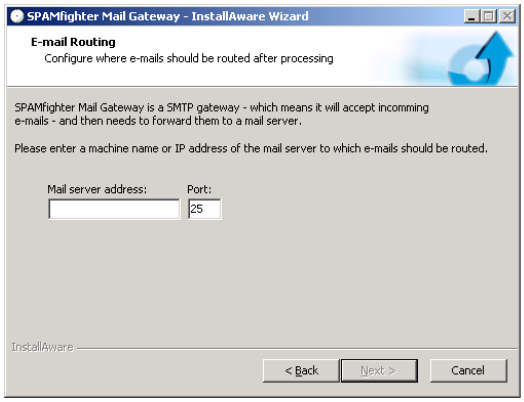
Please read and accept the license agreement before proceeding by clicking the "Next > " button



Registration

To be able to provide you with the best support and up-to-date information about SPAMfighter Mail Gateway, it is necessary for SPAMfighter to be able to identify you.

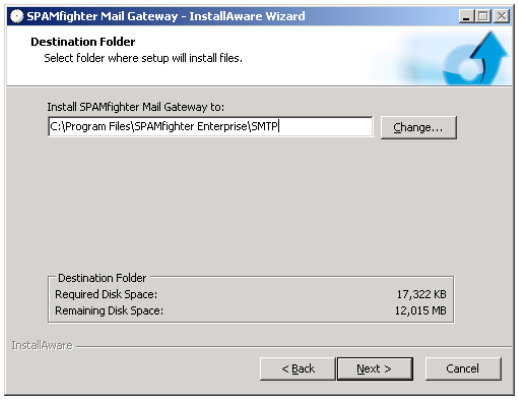
Please fill out the information with the required details. This information is strictly for SPAMfighter use only – and will never be given to any third party.



E-mail Routing

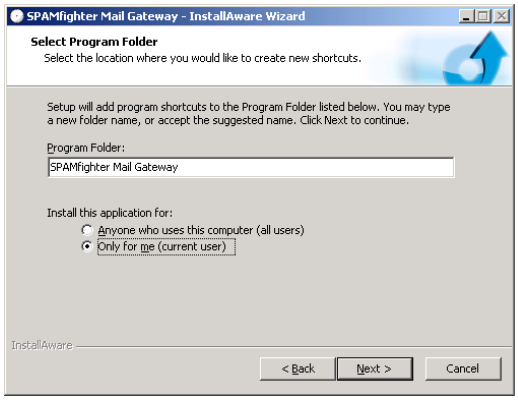
SPAMfighter Mail Gateway needs to know where to route legitimate e-mails. Please enter the network address or IP-address of the existing SMTP server in your e-mail infrastructure.

This information can always be changed through the Administration Module



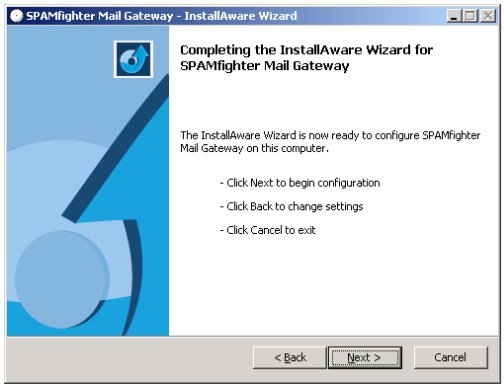
Destination folder

Please choose where on the file system SPAMfighter Mail Gateway should be installed



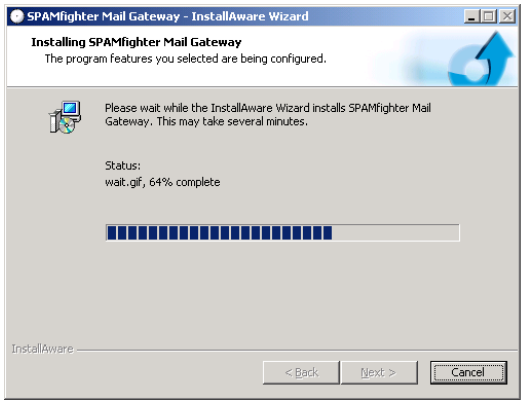
Shortcuts folder

Please select where in the Windows Start menu SPAMfighter should insert shortcuts to the various services SPAMfighter Mail Gateway provides



Completing installation

Please confirm that SPAMfighter Mail Gateway should be installed by clicking the “Next >” button



Installation

The installation will now complete – this may take several minutes to complete

Installation completed

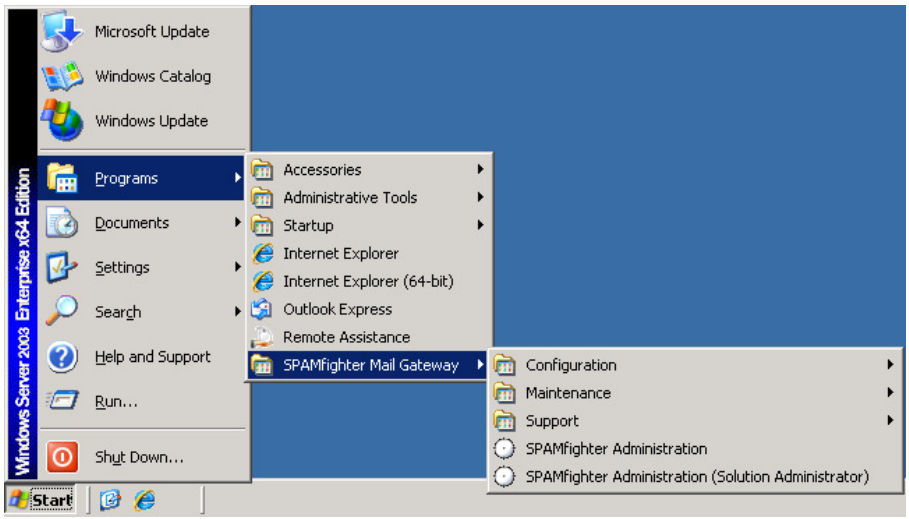
SPAMfighter Mail Gateway has now been successfully installed.

To begin using SPAMfighter Mail Gateway right away, leave the checkbox “Run SPAMfighter Mail Gateway now” checked.

Close the installation by clicking “Finish”

5. Use of SPAMfighter Mail Gateway

SPAMfighter Mail Gateway runs as a windows service – and has as such no graphical user interface. In order to configure SPAMfighter Mail Gateway, a dedicated web application is used which can be accessed through the Start menu in Windows:



Two main entries have been created in the "SPAMfighter Mail Gateway" folder in the start menu:

- *SPAMfighter Administration* opens the Administration Module as a normal user – and requires login.

- *SPAMfighter Administration (Solution Administrator)* opens the Administration Module in a special "Solution Administrator" mode. This does not require login, however the user *must* be member of the Administrators group in Windows and this mode is only available locally on the machine.

The first time the Administration Module is opened, it is necessary to run it in the special "Solution Administrator" mode – as no users exist, and thus no login information is available for use.

The following paragraphs will give a basic introduction to the core features of the Administration Module.

5.1 Front page

The first page presented in the Administration Module is the “Front page”. This page is a dashboard where basic information about the installation is presented.

The Administration Module is divided up into 2 parts – the menu part which is shown to the left, categorized in the groups described below – and the right part which will change depending on the current section chosen in the menu. Depending on the “*security type*” of the user logged in, the menu may show more or less sections and sub-entries.

The different menu sections are:

- General: This section provides various general information about the solution
- Configuration: This section provides all kinds of filtering related information
- Statistics: This section provides statistical information collected during filtering
- Administration: This section provides access administrative tasks
- Help: This section provides various support related information

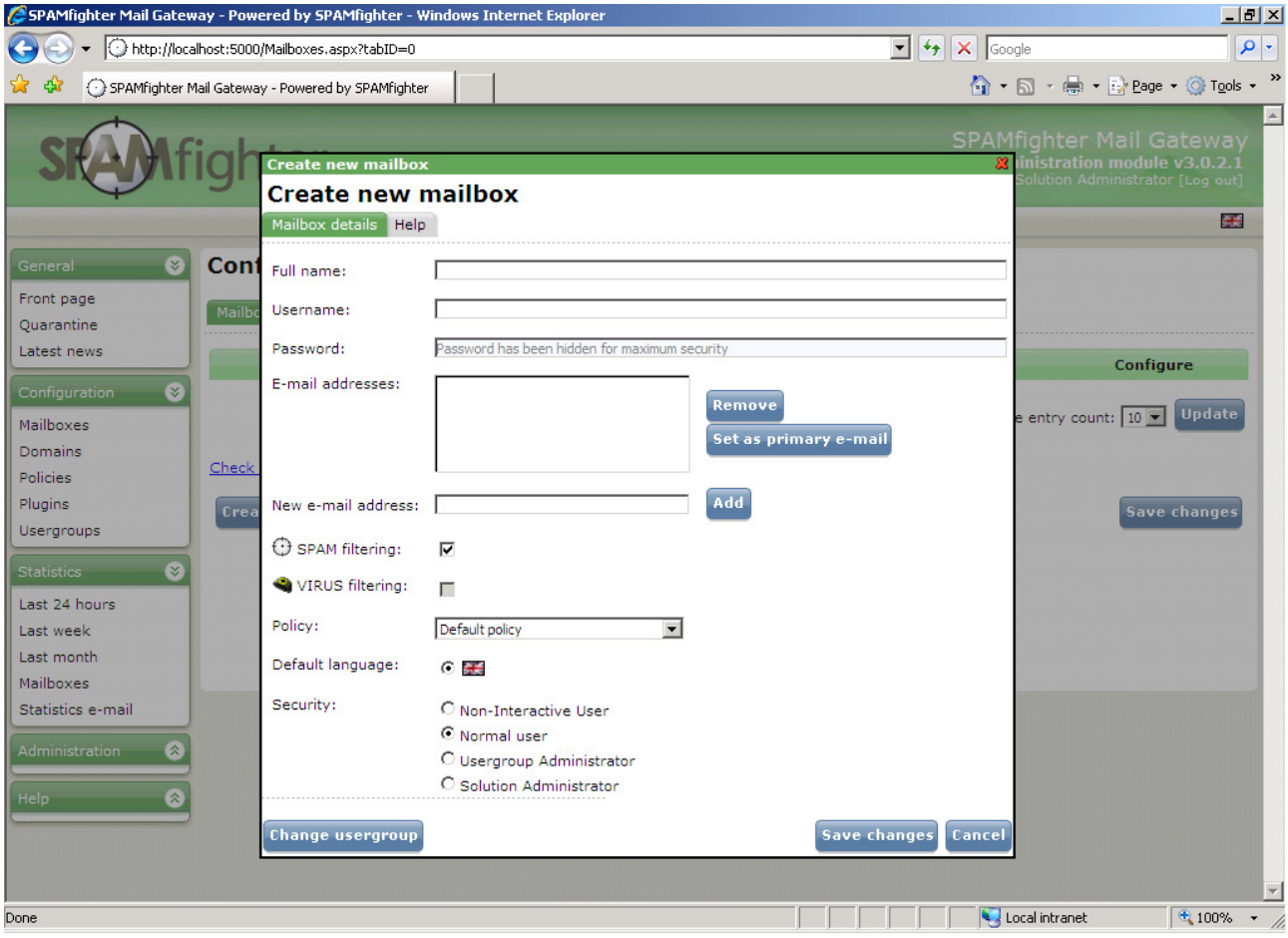
5.2 Mailboxes

SPAMfighter Mail Gateway needs to know about recipient mailboxes in order to know how a particular user would like his or her e-mails filtered.

SPAMfighter Mail Gateway currently provides 2 ways of managing mailboxes: Database driven or Active Directory driven. The default mailbox provider is “Database driven” – but if Active Directory is already used in the organisation, one can with benefit change the mailbox provider to that of “Active Directory” (please see paragraph “5.5 Advanced administration” how to do this).

In order to create a new mailbox or configure the settings of an existing mailbox, use the menu to the left and click “Mailboxes” in the “Configuration” section. All current mailboxes will be shown, with appropriate buttons next to them in order to configure / delete mailboxes.

If the mailbox provider is that of “Database driven” a button named “Create new mailbox” will be shown in the bottom of the list. Clicking this will open a “Create new mailbox” dialog, in which you can enter all relevant details of a given mailbox. It is strongly advised to configure at least 1 mailbox as “Solution Administrator” if you wish to be able to configure the solution remotely.



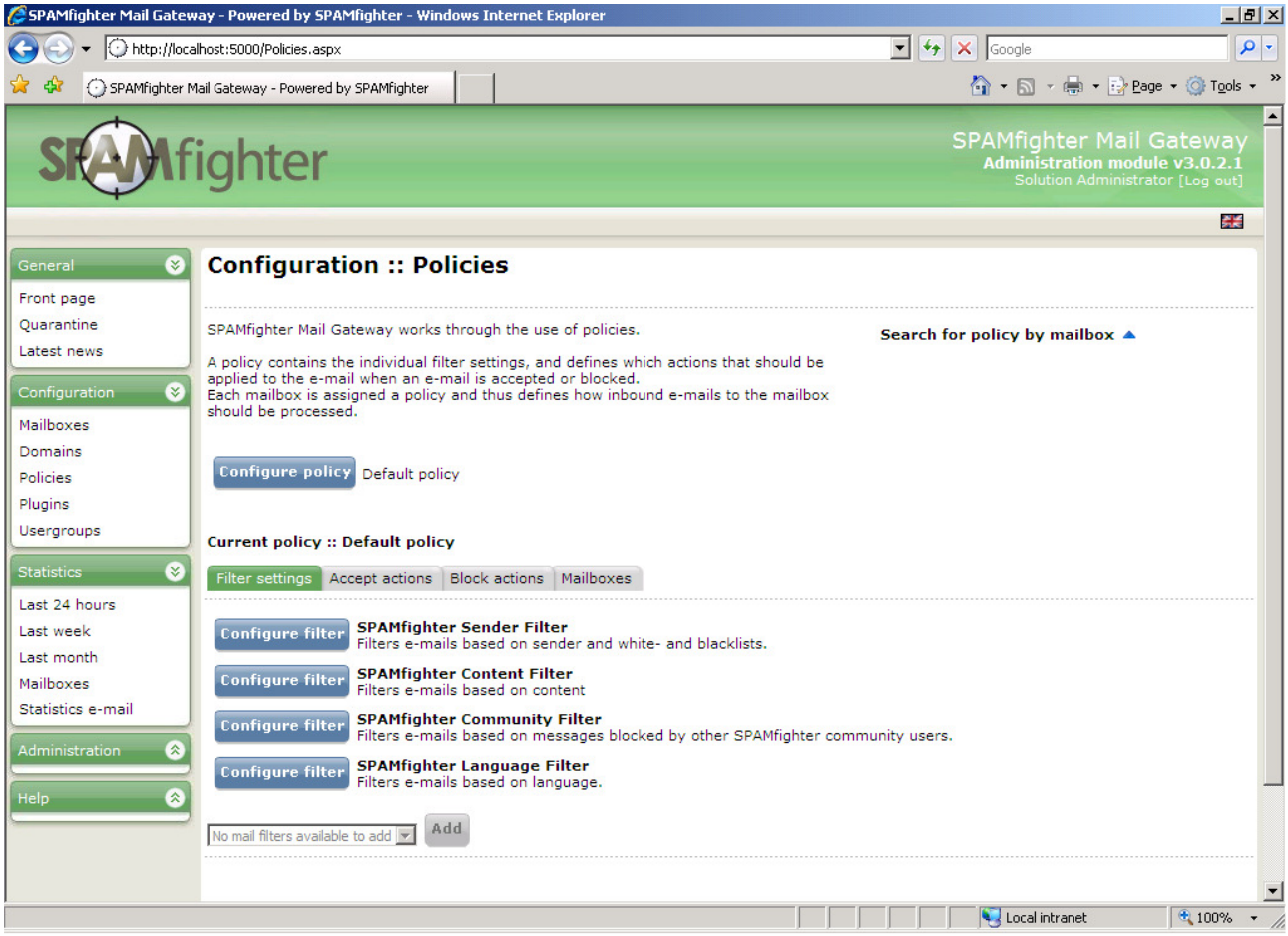
5.3 Policies

SPAMfighter Mail Gateway uses a concept named “Policies”. A policy is a collection of filter settings and details about what to do about spam e-mails and legitimate e-mails after a scan. SPAMfighter Mail Gateway provides a “Default policy” in which the most common settings are preconfigured.

Every mailbox will be given a policy – which thus dictates how e-mails sent to this mailbox should be filtered. You can always change the policy of a mailbox by opening the “Configure mailbox” dialog found on the Mailboxes page.

The concept of “Policies” enables you to easily divide your organisation’s mailboxes up into different groups, which thus can be filtered differently. One could for example have one policy for the sales department and another one for the marketing department.

To configure policies use the menu to the left and click “Policies” in the “Configuration” section. All policies will now be listed, and by clicking the “Configure policy” button next to a policy opens up the configuration of a given policy:



4 tabs will be shown for each policy:

- *Filter settings:* This displays all filters used by the policy, and buttons to open the configuration dialog for each filter.
- *Accept actions:* This displays all actions that are applied to an e-mail when it is classified as legitimate by the filters.
- *Block actions:* This displays all actions that are applied to an e-mail when it is classified as spam by the filters.
- *Mailboxes:* This list all mailboxes that uses the given policy

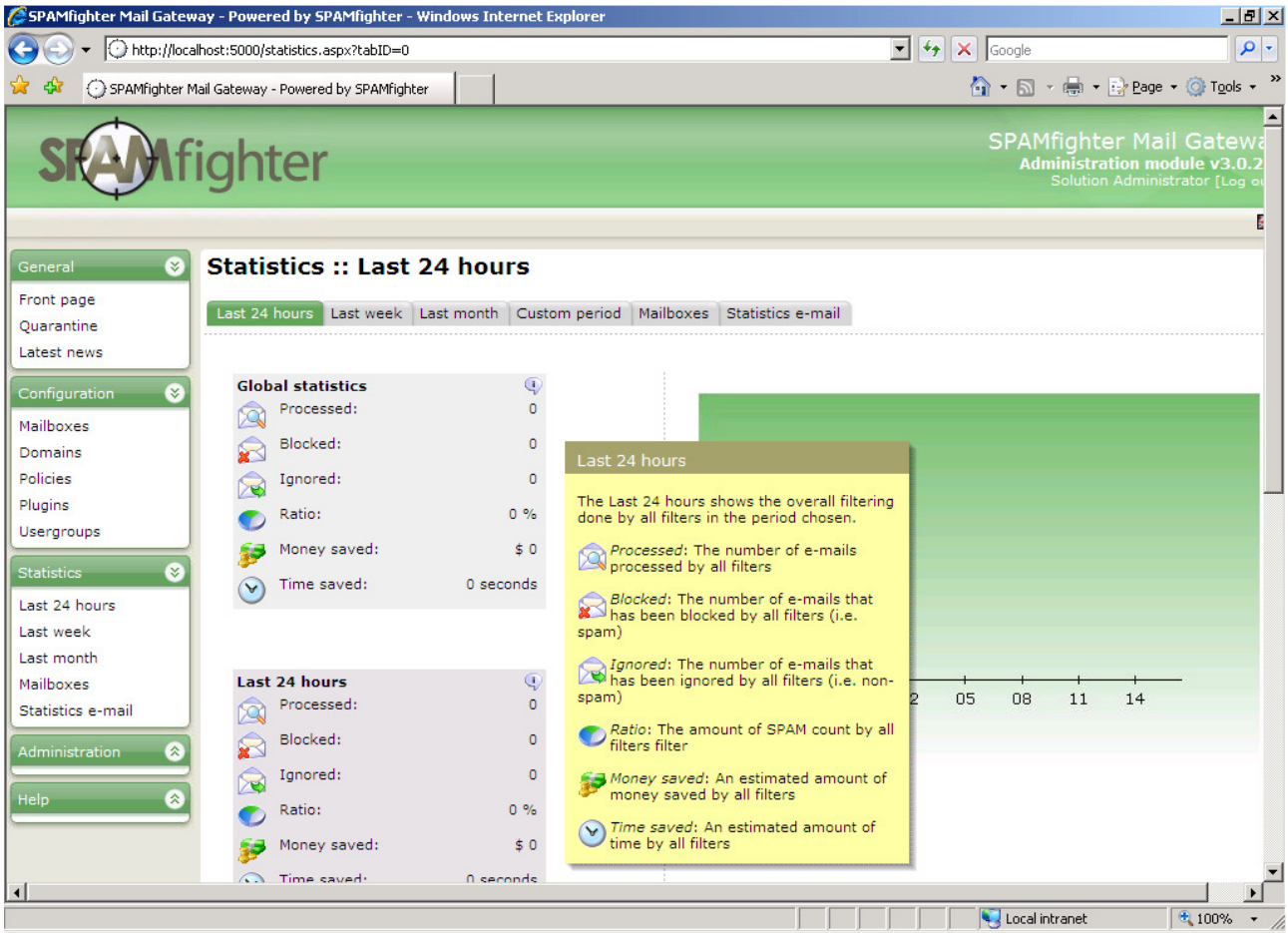
5.4 Statistics

SPAMfighter Mail Gateway maintains statistical information about e-mails that are scanned. This statistical information is available in the “Statistics” section of the menu to the left.

The Administration Module will always provide you with an up-to-date collection of relevant statistical information collected through the “Last 24 hours”.

The time period can be extended from “Last 24 hours” to “Last week” or “Last month” by clicking the appropriate entries in the Administration Module – or one could choose to use the “Custom period” feature to display a specific period in time.

Lastly the statistical information can be browsed by mailboxes. Per default the system will display the top most processing, blocking and ignoring mailboxes – but also enables you to search for a particular mailbox.



There is no need to use the Administration Module to get information about the processing of SPAMfighter Mail Gateway. Navigating to “Statistics e-mail” gives you choice of entering one or more e-mail addresses that should receive daily / weekly / monthly statistical information sent directly to your chosen mailboxes.

5.5 Advanced administration

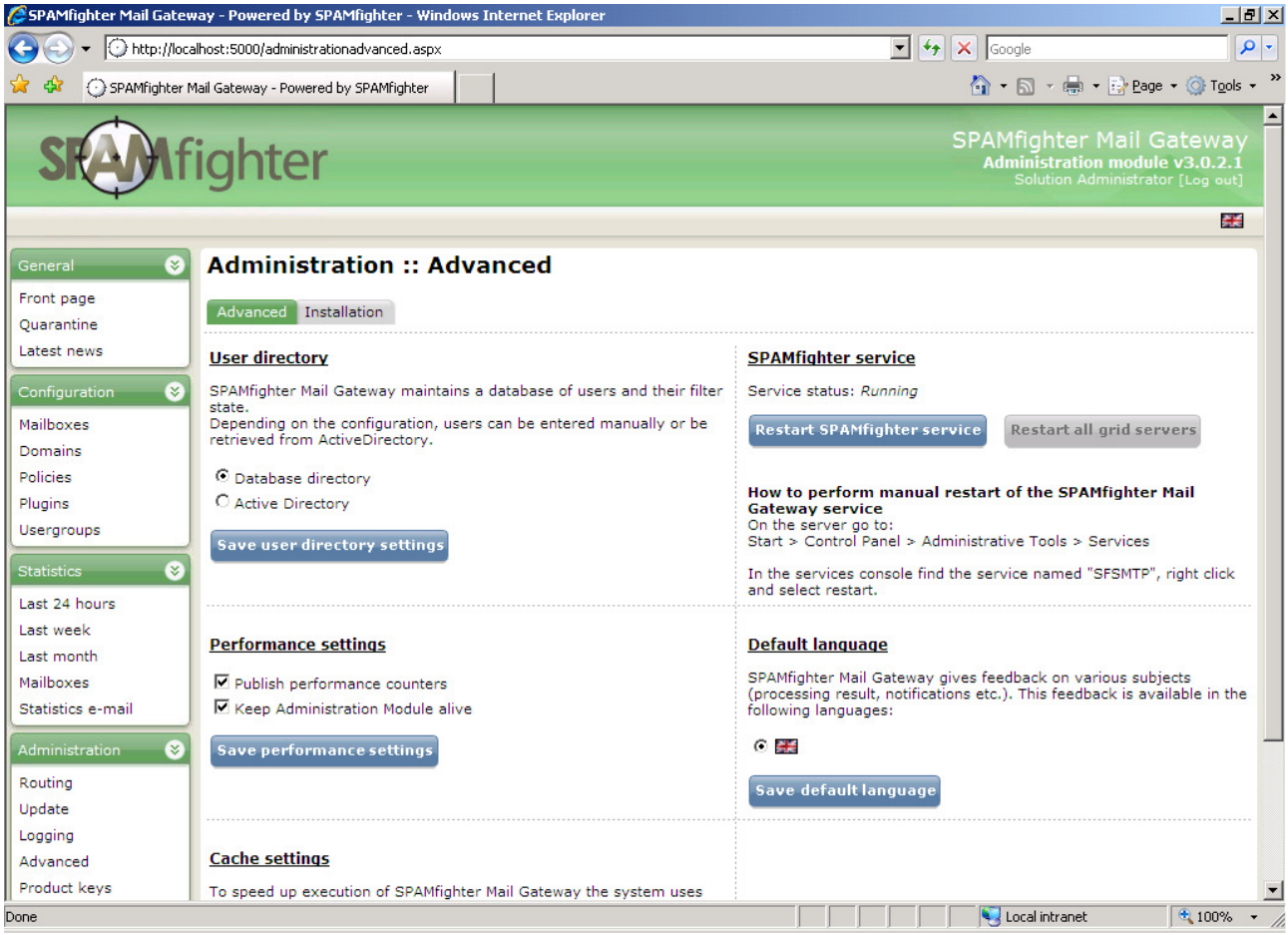
When the Administration Module runs in "Solution Administration" mode – either by accessing it through the "*SPAMfighter Administration (Solution Administrator)*" entry in the Windows Start menu – or by logging in as a mailbox user with security type as "*Solution Administrator*" – a menu section named "Administration" will be shown.

This menu section enables you to configure how e-mails should be routed, configure the update engine, enabling logging, entering product keys and configure the more advanced features of SPAMfighter Mail Gateway.

Paragraph "5.2 Mailboxes" mentioned that SPAMfighter Mail Gateway currently provides 2 ways of managing / storing mailbox information: Database driven or Active Directory driven.

The "Advanced" section in the "Administration" menu section enables you to configure the "User directory" type and various other properties of SPAMfighter Mail Gateway.

Please note changing the type of user directory (either from Database to Active Directory or vice versa) will clear all existing mailbox information and related data.



6. Network, security and machine impact

SPAMfighter Mail Gateway use state-of-the-art techniques to provide the best e-mail filtering with the highest level of security and the lowest machine impact.

6.1 Network Impact

SPAMfighter Mail Gateway needs to be able to communicate with the global SPAMfighter server network, however the actual requirements are minimal:

Required	
UDP port 2409	servers.backend.spamfighter.com
TCP port 2409	servers.backend.spamfighter.com
TCP port 80	http://login.spamfighter.com
Optional – *but strongly recommended*	
TCP port 80	http://download.spamfighter.com
TCP port 80	http://www.spamfighter.com

6.2 Security

Your e-mail security and privacy is our top priority. SPAMfighter Mail Gateway will never send sensitive information to the Internet. All information that is sent and received is validated in order to avoid manipulation. Legitimate e-mails on the server are never sent further or shared with anyone – your legitimate e-mails will never leave your server. Only a few blocks of e-mail compiled hash-values will be sent to the SPAMfighter server during e-mail filtering.

SPAMfighter Mail Gateway will periodically send details regarding application registration and login-information in order to receive up-to-date license key information.

The Administration Module for SPAMfighter Mail Gateway uses form-based login which is encrypted using a 1024 bit public key encryption scheme. All sensitive data is hashed before storage. When logging onto the Administration Module, the user is assigned a "*security type*" which dictates which resources that are made available for the user, and what type of changes the user is allowed to make. If a user attempts to access a resource or function in violation with his or her "*security type*" the user will immediately be logged out.

The Administration Module for SPAMfighter Mail Gateway runs in a dedicated web server, which per default listens on port 5000 and accepts all incoming request. If needed, the dedicated web server can be configured to only allow / disallow certain IP-addresses or only allow local traffic.

6.3 Machine impact

SPAMfighter Mail Gateway installs the following two Windows services:

"*SPAMfighter Mail Gateway*" (SFSMTP) is the actual application.

"*SPAMfighter Mail Gateway – Administration Module*" (SFSMTPW3) runs a dedicated web server that serves the Administration Module.

SPAMfighter Mail Gateway will when started spawn a number of threads, which will be assigned to any physical CPU, at the discretion of the operating system. In addition to this, SPAMfighter Mail Gateway will pre-initialize a buffer of memory. The operating system may reserve more memory than what SPAMfighter Mail Gateway request – but this will be released / rearranged / acquired in the most optimal way possible solely by the operating system. Spikes of memory usage may be observed, but this is expected and is to be considered normal behaviour as this either is caused by large e-mail(s) being loaded into memory at runtime for scanning or the operating system that based on system metrics sees fit to acquire / rearrange / release memory, without any intervention, request or control by SPAMfighter Mail Gateway.

7. Support and sale

SPAMfighter has a large and dedicated sales and support department. SPAMfighter will gladly help you by answering any questions you might have – or help you correct any technical issues you might encounter. Everything is of course free of charge.

SPAMfighter support department has great experience with Microsoft Windows and other server related issues – and will be able to fix almost all technical issues in regards to SPAMfighter Mail Gateway at no cost for our customers.

SPAMfighter sales department will be able to answer all questions regarding purchase of licenses and / or products and services.

You can contact SPAMfighter through the "Help" section in the Administration Module or through the "Support" menu in the Windows Start menu.

Finally you can contact SPAMfighter directly either by phone or e-mail:

SPAMfighter sales
E-mail: sales@spamfighter.com
Telephone: +45 7022 1551

SPAMfighter support
E-mail: smgsupport@spamfighter.com
Telephone: +45 7022 1551