



SpamSentinel for Exchange

ADMINISTRATORS GUIDE

Contents

Contents.....	1
Contact Us:.....	2
Requirements and Pre-requisites:.....	2
Administration.....	3
The Administrator Interface.....	3
Active Directory.....	3
Anti-Spam Engines.....	4
Anti-Virus.....	5
Block Lists.....	5
Company Information.....	7
Proxy Server.....	7
Scanner – Inbound/Outbound.....	8
Explanation of Message Categories.....	10
Spam Statistics.....	10
White Lists.....	10
Installed Components.....	11
Microsoft Exchange Content Filter.....	12

SpamSentinel for Exchange

Contact Us:

For technical support please contact support@maysoft.com

For licensing and sales questions please contact Allison Cote at allison.cote@maysoft.com

Please feel free to call us at +1-978-635-1700 if you have any questions or require support.

Requirements and Pre-requisites:

Exchange 64-bit 2007, 2010 or 2013

Windows Server 64-bit 2003, 2008 or 2012

Microsoft .Net 3.5 (4.0 or higher for Win 2012)

Microsoft Visual C++ SP1 Redistributable Package

SpamSentinel for Exchange



Administration

The Administrator Interface

This is where all of the SpamSentinel configuration is entered. The list on the left takes you to the relevant pane on the right. See below for descriptions of each pane. Also note the  symbol which will display context sensitive help. The button bar across the top performs various functions such as starting/stopping services, testing the communication with the anti-spam engines, logging in to Active Directory etc.

Active Directory

The screenshot shows the SpamSentinel Administrator application window. The title bar reads "SpamSentinel Administrator". Below the title bar is a "Settings" menu and a toolbar with various icons: Start/Stop for Scanner, Monitor, Engine1, and Engine2; Download Definitions for Anti-Virus; Repair; Administrator Login; Reload Statistics; Help/Updates; and Support. The main content area is divided into a left sidebar and a right pane. The sidebar contains a list of links: Active Directory, Anti-Spam Engines, Anti-Virus, Block Lists, Company Information, Monitor, Proxy Server, Scanner - Inbound, Scanner - Outbound, Spam Statistics, Support, and White Lists. The right pane is titled "Active Directory Information" and contains a help icon. Below the title is a paragraph of instructions: "Please enter your Active Directory server information. You can leave Port blank to use the default port. Please enter an Active Directory user ID for the SpamSentinel Scanner to use. The Scanner will use the ID to perform white and block list lookups, and other actions. The user ID should be able to read and write the Exchange server information in Active Directory." Below this text are two form sections. The first is "Active Directory Server" with fields for "Server Name" (containing "ss-ex.zigzag.co.uk"), "Server Port" (empty), and "Exchange Organization" (containing "Zigzag"). The second is "SpamSentinel User Information" with fields for "User Name" (containing "SpamSentinel") and "Password" (containing "*****"). A "Test login" button is located below the password field.

This information is carried over from the initial install and can be changed here. Use the 'Test Login' button to verify your credentials.

SpamSentinel for Exchange

Anti-Spam Engines

Engine Settings

The anti-spam engines run as a Windows service and are responsible for communication with our anti-spam providers. They communicate over HTTP port 80 to send hashed signatures and receive results. The SpamSentinel Scanner communicates with the Engines through local ports 2650 and 2651 - settings here should not be changed unless recommended by Mayflower Software support. The two engines are identical and provide fail-over for each other.

Anti-Spam Engine 1

Host Name:

Port:

Scan URL:

Engine Path:

Anti-Spam Engine 2

Host Name:

Port:

Scan URL:

Engine Path:

General Engine Settings

Enable proactive pattern scanning

Maximum concurrent connections per engine:

HTTP request timeout in seconds:

Contains the port and path settings for the anti-spam Duo Engines. These parameters should only be changed on the advice of Mayflower Software support.

‘Enable proactive pattern scanning’ allows SpamSentinel to identify and block new spam messages before the recurrent pattern is added to the spam database. This should be enabled if you experience spam misses that are then blocked a short time later.

The ‘Maximum concurrent connections per engine’ should be in the region of twelve times the number of processors on the server- the default is 48 (i.e. 4 processors).

If your server has a high load – contact Mayflower Support, as we can add extra engines manually to spread the load further.

SpamSentinel for Exchange

Anti-Virus

Anti-Virus Settings

Here you can choose whether to have either Inbound, Outbound, or both types of email scanned for viruses in attachments. You can change the temporary folders that house the attachment being scanned, and the download location for definition file updates. These folders should be excluded from any system anti-virus programs to prevent conflicts. The interval to check for new definition files can also be set.

Enable anti-virus file scanning for inbound mail

Enable anti-virus file scanning for outbound mail

Scan Folder: 

Enable anti-virus definition file download

Update Folder: 

Update Interval: minutes

Definition Version:

Enable/disable inbound and outbound anti-virus scanning. You can also change the unpack location of the definition updates, set the update interval and check the latest definition version.

Block Lists

Block Lists

Select the checkbox to enable or disable the block list lookup. Click on the lookup name to add or remove items from the list. You must enter the information on the Active Directory screen in order to update the block lists.

[Blocked sender names](#)
Add and remove your Exchange blocked sender names

[Blocked sender domains](#)
Add and remove your Exchange blocked sender domains

[Blocked subjects](#)
Add and remove message subjects that will be blocked

[Blocked character sets](#)
Add and remove message character sets that will be blocked

[Blocked file attachment extensions](#)
Add and remove blocked file attachment extensions

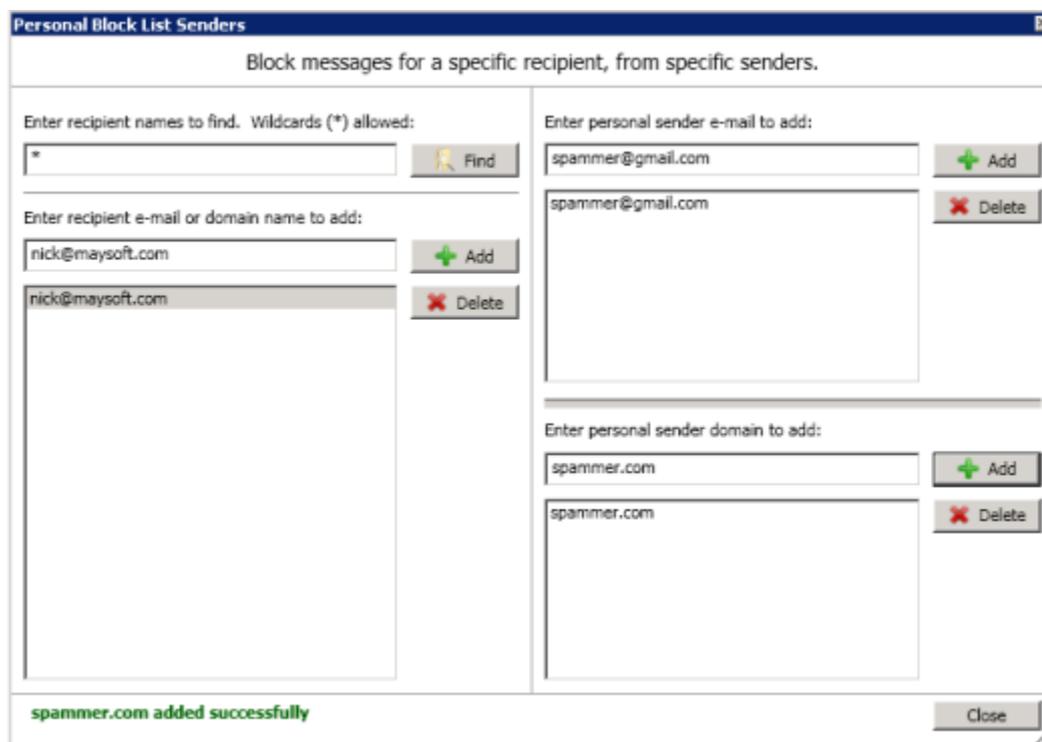
[Blocked file extensions in Zip files](#)
Add and remove blocked file extensions in Zip files

[Personal block list senders and domains](#)
Add and remove block list senders for specific recipients

Enables you to add various criteria for blocking mails. SpamSentinel will block most spam 'out-of-the-box' and these settings should be used sparingly to prevent false positives. Select the checkbox to enable that feature. Enabling/disabling these options require a save of the configuration, click the disk icon to save . Adding or removing an entry from the lists are performed in real time on Active Directory

SpamSentinel for Exchange

- Blocked sender names – Reject email from these senders (e.g. joe@example.com).
- Blocked sender domains – Reject mail from these sender domains (e.g. example.com).
- Blocked subjects – Mark messages with certain subjects as spam. This requires an exact match.
- Blocked character sets – Choose from a list of predefined character sets to block (e.g. Cyrillic (KOI8-R)). If there is a set that you require but is not on the list, please contact support for assistance.
- Blocked file attachment extensions – Remove attachments with the specified extensions (e.g. exe, pif, scr).
- Blocked file extensions in Zip files – Allows you to accept Zip files overall but block any containing specific files (e.g. a .exe file inside a .zip file).
- Personal block lists – This allows you to block certain senders and domains for selected users only. Add or select the user/domain in the left hand pane and then add the required address/domain to block on the right side (see below):



SpamSentinel for Exchange

Company Information

Company Information

Here you can view the registered company details for your SpamSentinel installation. When renewing your subscription please be sure to enter your new license code and save/restart. You should not change any other information once entered.

Company Name:	<input type="text" value="Zigzag"/>
Server Name:	<input type="text" value="SS-EX"/>
Company ID:	<input type="text" value="IDFD015D59124662C18625790C00457F1D"/>
License Code:	<input type="text" value="01042015593624660c2cbe0fc4d1486b"/>

License valid until: 04/01/2015

These values are carried over from the initial install. The only value that you need to change would be the license code on renewal.

Proxy Server

Proxy Settings

If your company uses a proxy server to gain Internet access, you should enter the details here. If possible, we recommend a direct connection for the server running SpamSentinel to achieve maximum performance.

Enable proxy server

Server Name:	<input type="text"/>
Port:	<input type="text" value="8080"/>
Protocol:	<input type="text" value="http://"/>
Method:	<input type="text" value="NTLM"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Domain:	<input type="text"/>

We recommend that where possible, SpamSentinel is given direct access to the Internet via port 80 (http) outbound. If this is not possible, enter your proxy server settings here.

Scanner – Inbound/Outbound

Inbound Anti-Spam Settings

The Scanner 'reads' the mail message, creates a one-way hashed signature and submits it to the Anti-spam processing. When the results are returned, the message is processed according to the spam score given and action is carried out.

Enable inbound mail Scanner

Enable RBL lookup

High spam sensitivity

Confirmed Spam Handling

Perform the following action when a spam message is detected:

Reject Mail Message

Prepend subject text

Enter text to prepend to a spam message subject:

[Spam]

Suspected Spam Handling

Perform the following action when a spam message is detected:

Send to Outlook Junk Mail Folder

Prepend subject text

Enter text to prepend to a spam message subject:

[Bulk]

Quarantine Mailbox Name

Enter the Exchange inbound quarantine mailbox name:

QC@zigzag.co.uk

Settings here relate to the inbound scanning of messages. The inbound scanner is enabled by default.

- Enable inbound mail scanner – turn the inbound scanning on/off.
- Enable RBL lookup – Use the Spamhaus RBL to conduct extra IP checks.
- High spam sensitivity – When selected, you will only receive a few 'Suspect' messages per day. If disabled then more messages will be suspect but with a lower chance of a false positive in the 'Confirmed' category.
- Confirmed Spam Handling – choose your preference for handling confirmed spam.
 - Send to the Outlook Junk Email folder
 - Send to the Quarantine mail box
 - Reject the message at the server - with notification sent to the sender (Recommended).
 - Delete the message (no notification is sent)
 - No action
 - Prepend subject text – adds a word or phrase to the beginning of the subject
- Suspected Spam Handling – Choose the options to apply to suspect messages. The choices are the same as above and we recommend sending these messages to the user's Junk Email folder for instant verification.
- Quarantine mail box name – The email address to which quarantined mail is sent (if that option is selected).

SpamSentinel for Exchange

The Outbound Scanner tab has similar options but with fewer choices due to the properties of this type of email. The outbound scanner is disabled by default. We recommend deletion of the mail message with a notification sent back to the sender if outbound scanning is enabled.

Outbound Anti-Spam Settings

The Scanner 'reads' the mail message, creates a one-way hashed signature and submits it to t for processing. When the results are returned, the message is processed according to the spar appropriate action is carried out.

Enable outbound mail Scanner
 High spam sensitivity

Confirmed Spam Handling

Perform the following action when a spam message is detected:
Delete Mail Message

Notify sender message was stopped
 Prepend subject text

Enter text to prepend to a spam message subject:
[Delivery Failure]

Suspected Spam Handling

Perform the following action when a spam message is detected:
Delete Mail Message

Notify sender message was stopped
 Prepend subject text

Enter text to prepend to a spam message subject:
[Delivery Failure]

Quarantine Mailbox Name

Enter the Exchange outbound quarantine mailbox name:
[]

The Windows Event Viewer can be used to view the action taken on spam messages:

The screenshot shows the Windows Event Viewer interface. On the left, the tree view is expanded to 'Microsoft > Monitor SpamSentinel > MExchange Management > Scanner SpamSentinel'. The main pane displays 'Event 0, ESSScanner1' with two tabs: 'General' and 'Details'. The 'Details' tab is active, showing the following information:

- Action: Spam message Rejected (highlighted with a red box)
- Category: Spam-D
- MessageID: <391608240-RVDSWSYJSHJXIEBIRUAP@dns4.learningmetrics.net>
- Subject: [Spam]Buy Meds cheap only here

SpamSentinel for Exchange

Explanation of Message Categories

Message Category Description	
Good Mail	Messages considered to be good mail that is sent to the end user.
Suspect	Messages where both engines do not agree this is spam or valid - it is 'suspect', perhaps a newsletter but does require verification. These messages are immediately sent to the user's Junk folder for end-user verification. "Suspect" is a very small number of messages per day, consisting of 2-4% of overall spam volume.
Confirmed Spam	Messages where both engines agree the message is spam. In addition, if the 'High Sensitivity' level is set, any message flagged by one engine as "Confirmed" (rather than "Suspect" or "Bulk") will be in this category. With the 'Low Sensitivity' set, those messages would be classed as "Suspect". It is recommended that this category is rejected.

Spam Statistics

Spam Statistics						
Date	Processed	GoodMail	TotalSpam	ConfirmedSpam	SuspectedSpam	Viruses
2014-03-11	1	1	0	0	0	0
2014-01-16	2	1	1	1	0	0
2014-01-09	23	18	5	0	5	0

An overview of the number of emails falling into certain categories by date. Click the 'Reload Statistics' button to refresh the table.

White Lists

White Lists

Select the checkbox to enable or disable the white list lookup. Click on the link. You must enter the information on the Active Directory screen in order to

- [Bypassed recipients](#)
Do not filter content in messages addressed to these recipients.
- [Included recipients](#)
Only filter messages addressed to these recipients.
- [White list sender names](#)
Add and remove your Exchange white list sender names.
- [White list sender domains](#)
Add and remove your Exchange white list sender domains.
- [Personal white list senders and domains](#)
Add and remove white list senders for specific recipients.

This tab allows the setting of various methods to bypass spam checking for both senders and recipients. Select the checkbox to enable the feature.

NOTE: Whitelists will ALWAYS override blacklists.

- Bypassed recipients – any email addresses added here will mean that SpamSentinel does not check messages for spam when sent to these recipients.
- Included recipients – if any email addresses are added here then SpamSentinel will ONLY check spam for these recipients. This is useful for setting up an initial pilot group during evaluation.
- White list sender names – do not check messages from these senders (e.g. joe@example.com).
- White list sender domains – do not check any messages from these domains (e.g. example.com).
- Personal white lists – Allows the addition of white lists for selected users/domains only. This works in the same way as the Personal block lists above.

NOTE: Be careful when adding whitelists, especially domains, as this can lead to missing a lot of spam. In particular you should NEVER add your own domain to the whitelist as the spam senders will often ‘spoo’ a sending address to make it seem that the message came from your domain. Domains that commonly host free email accounts, such as Gmail and Hotmail should also be avoided (you should white list specific senders instead).



Installed Components

Three Windows services are installed with the SpamSentinel suite:

SpamSentinel Duo 1	Spam and ...	Started	Automatic	Local System
SpamSentinel Duo 2	Spam and ...	Started	Automatic	Local System
SpamSentinel Monitor	SpamSenti...	Started	Automatic	Local System

In addition to these, the scanning components are added to the Microsoft Transport Agent. These can be viewed by entering the following command at the Exchange Management Shell:

Get-TransportAgent

Which produces the following output:

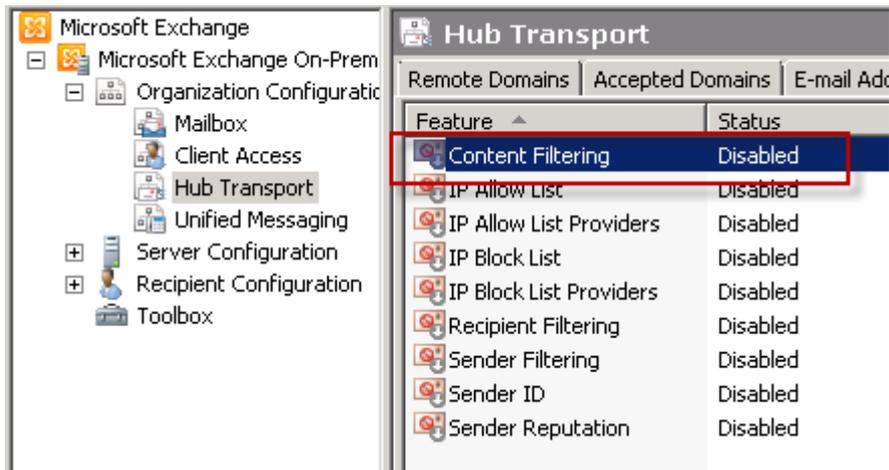
```
[PS] C:\Windows\system32>Get-TransportAgent
```

Identity	Enabled	Priority
Transport Rule Agent	True	1
Text Messaging Routing Agent	True	2
Text Messaging Delivery Agent	True	3
SpamSentinel Outbound	True	4
Connection Filtering Agent	True	5
Content Filter Agent	True	6
SpamSentinel Scanner	True	7
Sender Id Agent	True	8
Sender Filter Agent	True	9
Recipient Filter Agent	True	10
Protocol Analysis Agent	True	11

Microsoft Exchange Content Filter

SpamSentinel replaces the Microsoft Exchange server content filter but reads/writes to Active Directory in the same way. **You should therefore ensure that any black/white list features that were enabled in Exchange (such as whitelist domains/senders) are enabled in SpamSentinel after installation.** SpamSentinel will then read those entries and continue to block or skip specified senders.

NOTE: The Microsoft content filter will be disabled during the installation of SpamSentinel. It should not be necessary to re-enable it.



If you have any questions or require support, please email support@maysoft.com or call +1-978-635-1700

We would also like to hear from you if you have any feature requests or ideas for improvement.