2015

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

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:

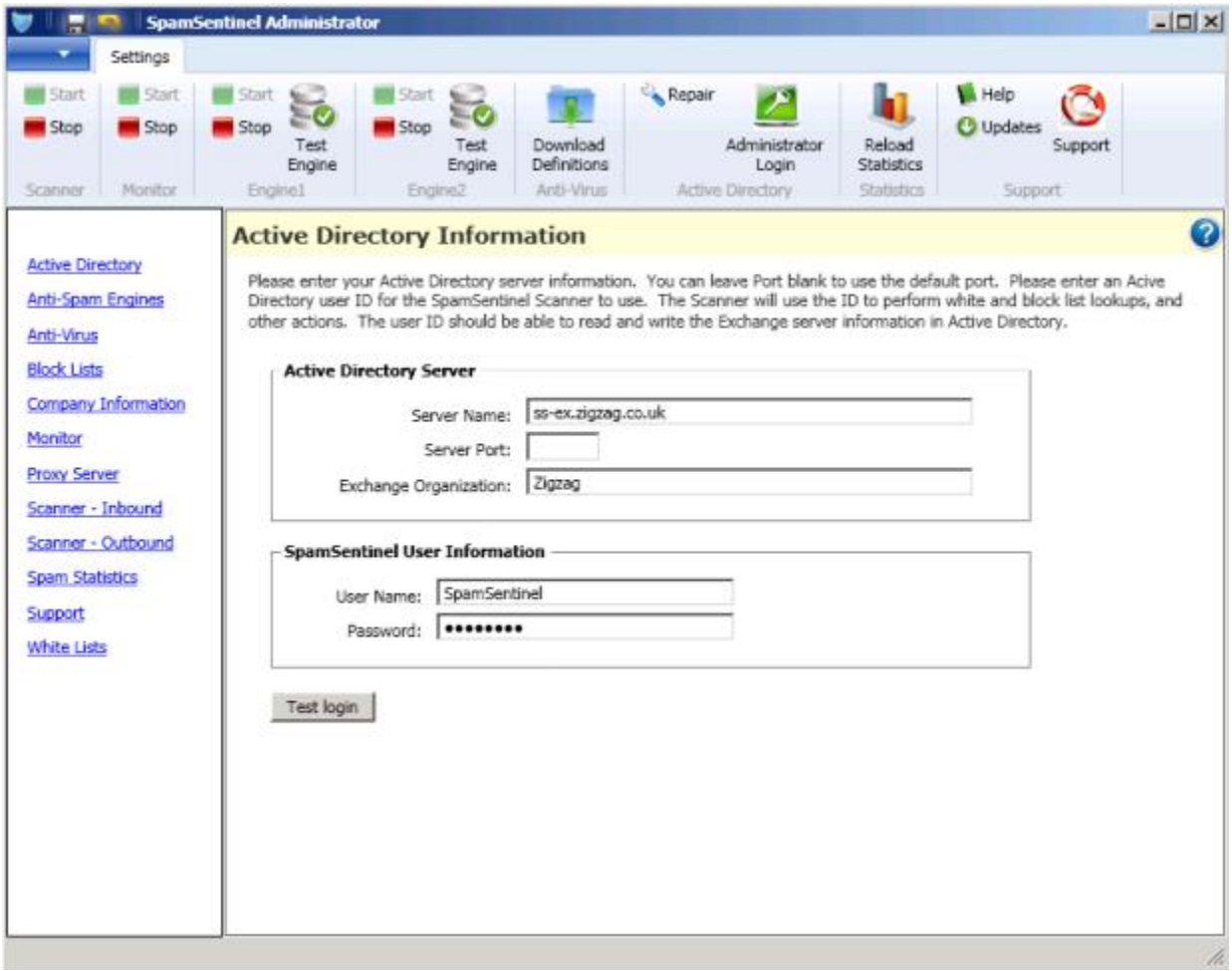
Exchange 64-bit 2007, 2010 or 2013
Windows Server 64-bit 2003, 2008 or 2012
Microsoft .Net 3.5 (4.0 or higher for Win 2012)
Microsoft Visual C++ SP1 Redistributable Package

Administration

The Administrator Interface

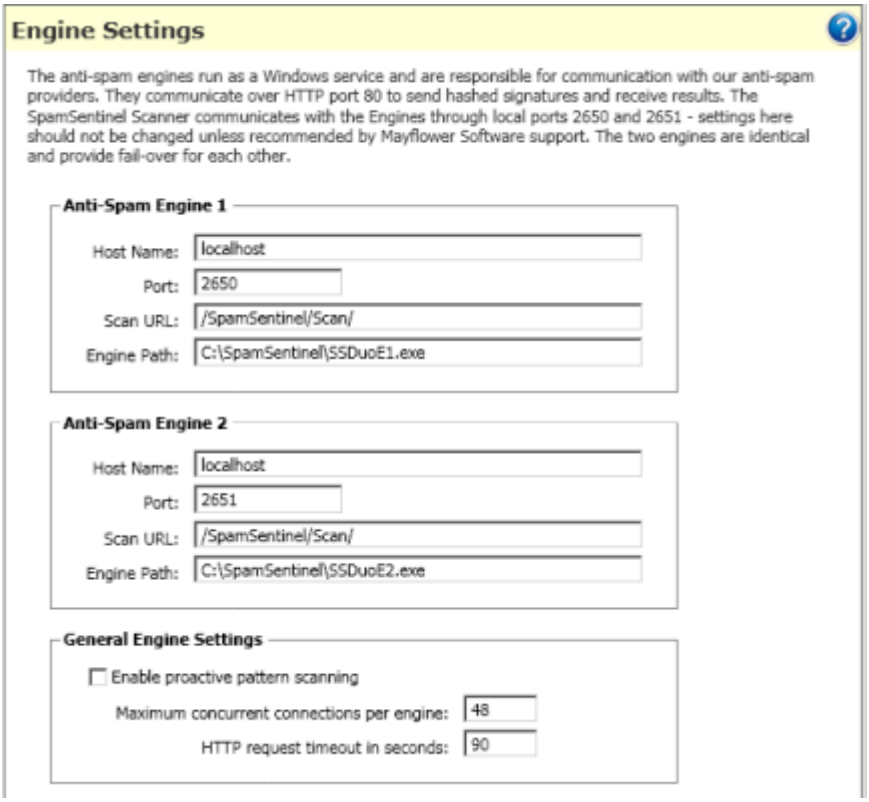
This is where all of the SpamSentinel configuration is entered. The list on the left takes you to the relevant pane on the right. See below for descriptions of each pane. Also note the symbol which will display context sensitive help. The button bar across the top performs various functions such as starting/stopping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

Active Directory



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

Anti-Spam Engines

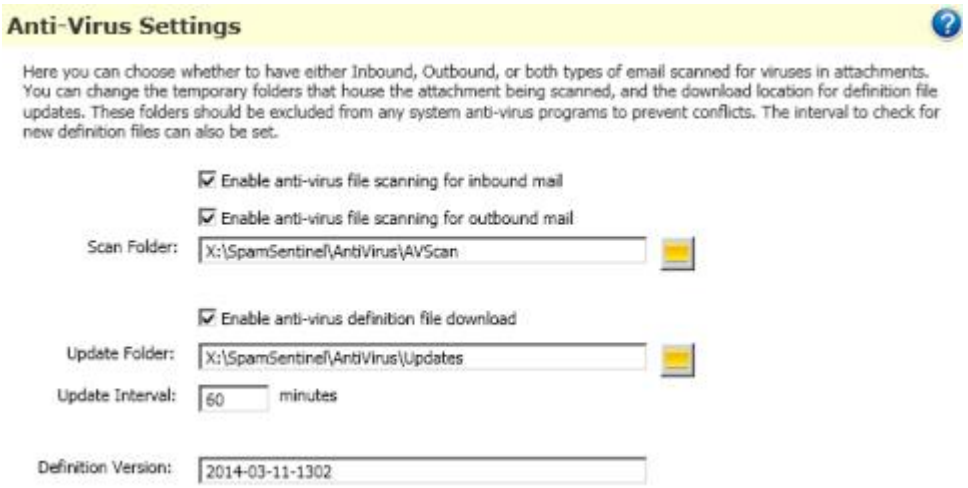


Contains the port and path settings for the anti-spam Duo Engines. These parameters should only be changed on the advice of Mayflower Software support.
'Enable proactive pattern scanning' allows SpamSentinel to identify and block new spam messages before the recurrent pattern is added to the spam database. 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.

Anti-Virus

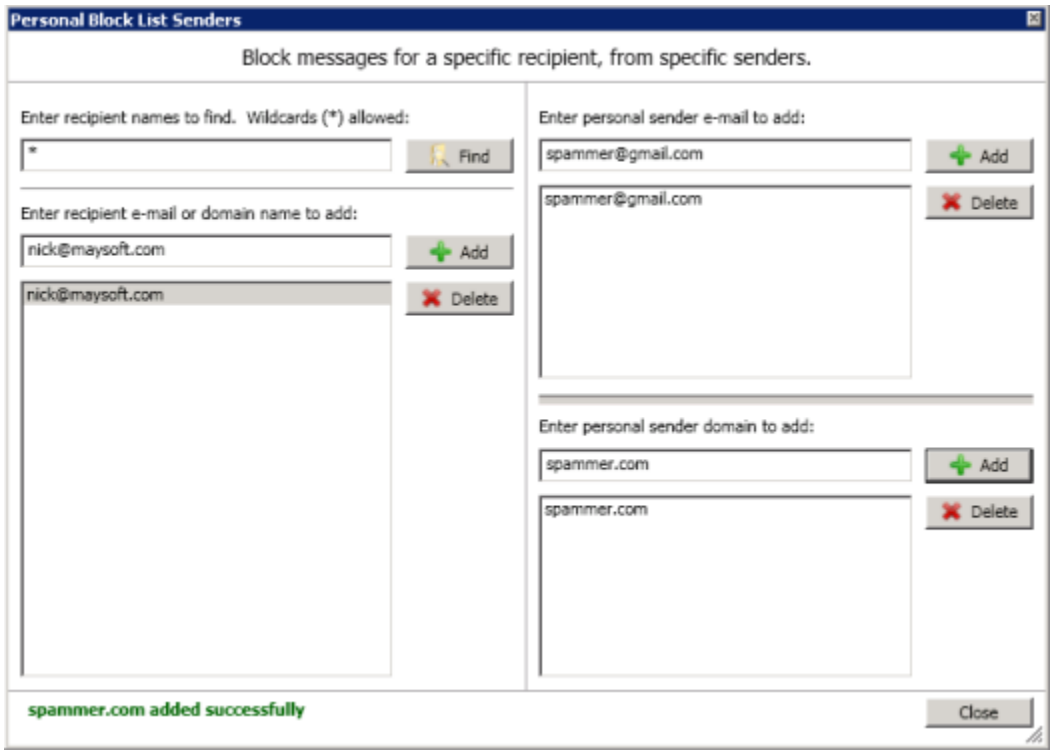


Enable/disable inbound and outbound anti-virus scanning. You can also change the unpack location of the definition updates, set the update interval and check the latest definition version.

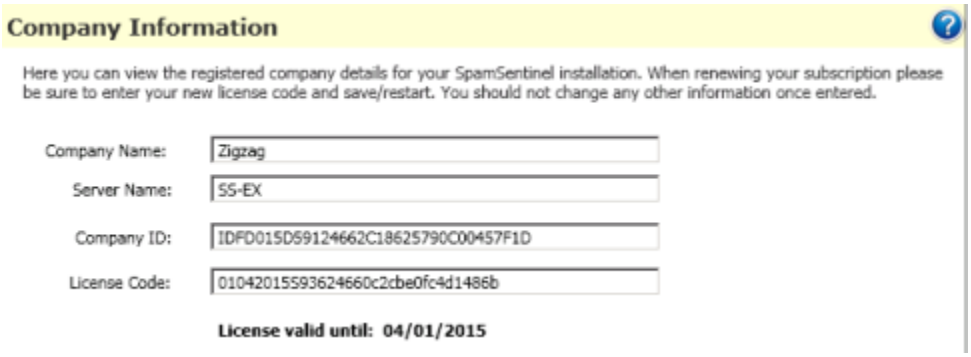
Block Lists

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

- 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):

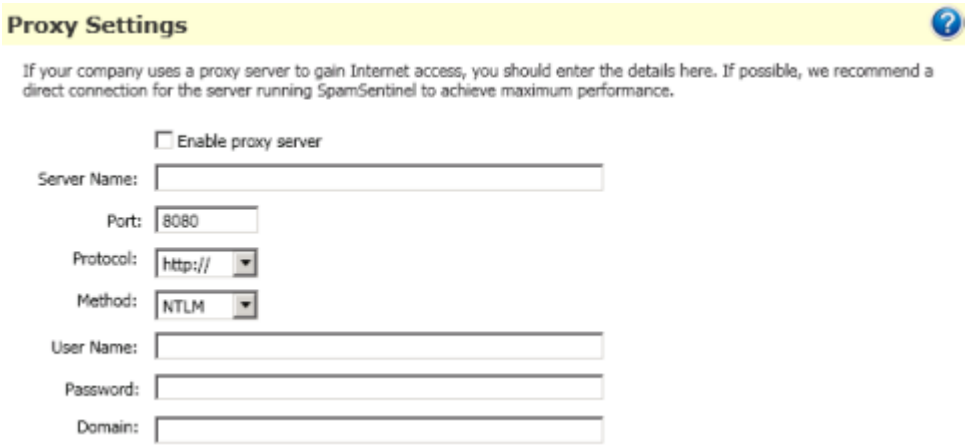


Company Information



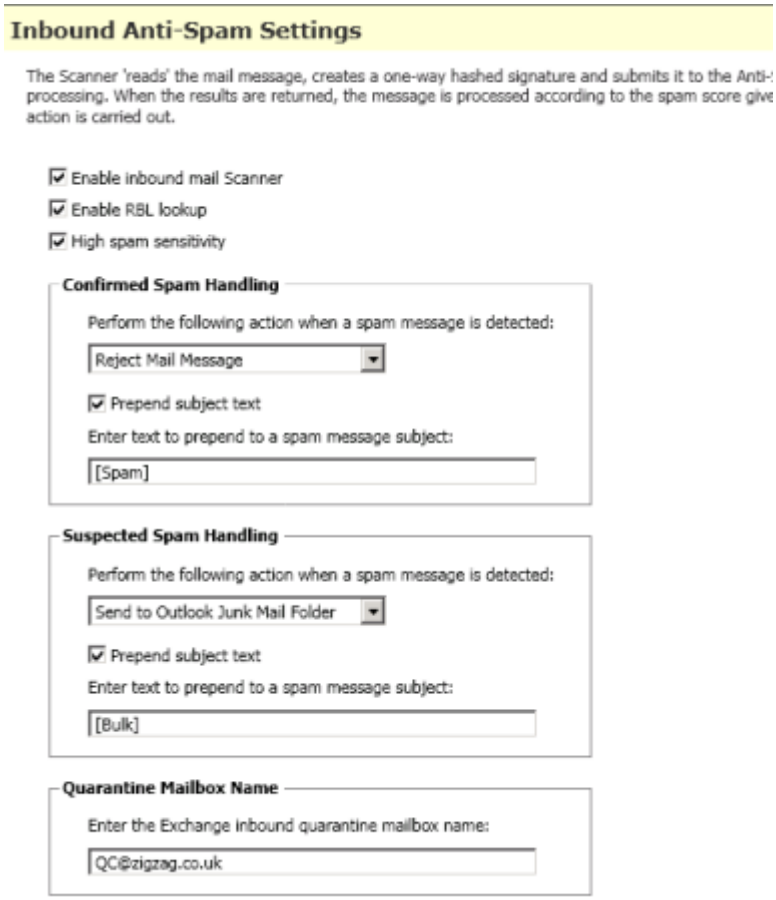
These values are carried over from the initial install. The only value that you need to change would be the license code on renewal.

Proxy Server



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



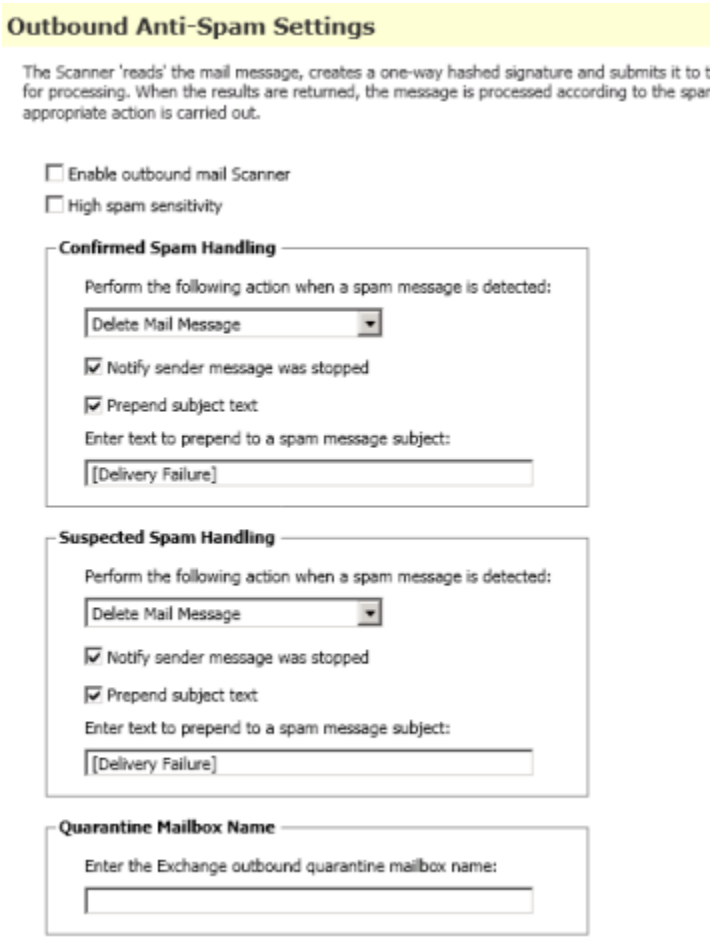
Settings here relate to the inbound scanning of messages. The inbound scanner is enabled by default.

- 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).

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.

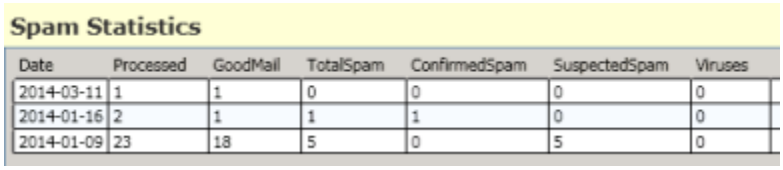


The Windows Event Viewer can be used to view the action taken on spam messages:

Explanation of Message Categories

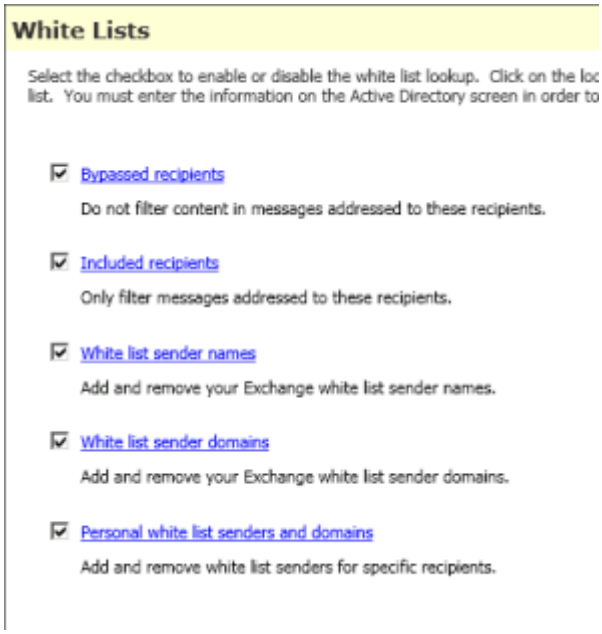
Message Category	Description
Good Mail	Messages considered to be good mail that is sent to the end user.
Suspect	Messages where both engines do not agree this is spam or valid - it is 'suspect', perhaps a news-letter but does require verification. These messages are immediately sent to the user's Junk folder for end-user verification. "Suspect" is a very small number of messages per day, consist-ing 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 "Sus-pect". It is recommended that this category is rejected.

Spam Statistics



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

White Lists



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

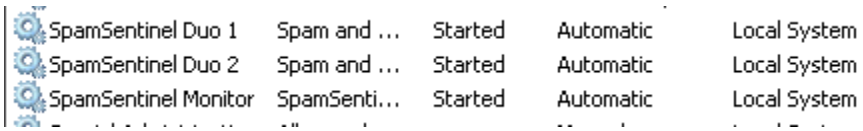
NOTE: Whitelists will ALWAYS override blacklists.

- 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 'spoof' 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:



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:

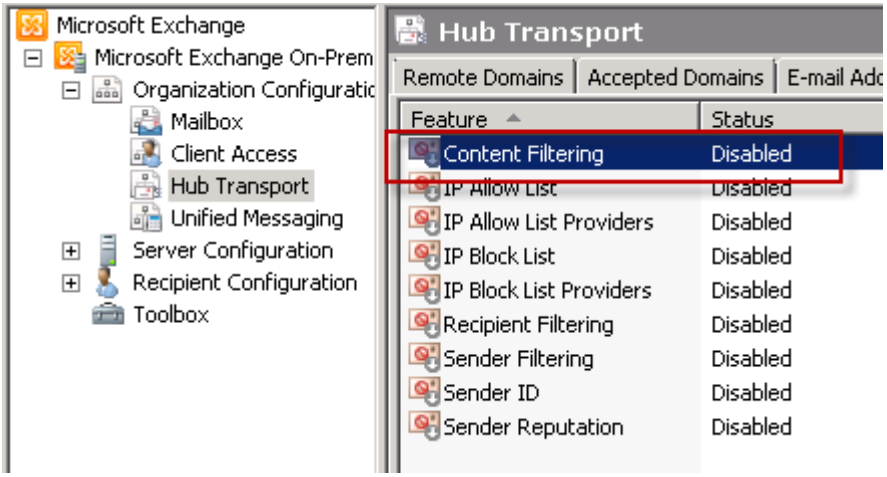
Get-TransportAgent

Which produces the following output:

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.