

September 23, 2005

10<sup>th</sup> July 2007 Update – Include updates for configuration steps in IMF Tune v3.0.

IMF Tune enables any anti-spam filter to integrate into Exchange 2003. Filters running on any platform, on firewall appliances, and even at external service providers, suddenly become an integral part of Exchange.

The same level of integration offered by the Intelligent Message Filter is achievable with the help of IMF Tune. Spam is routed to the Junk Email folder at the client mailbox. Outlook Safe Senders, Safe Recipients and Blocked Senders are also applied.



The overall system setup is illustrated above. Emails are first processed by the anti-spam filter. This adds its "spaminess" classification and forwards them to Exchange. Here both IMF and IMF Tune are installed. IMF Tune extracts the filtering result and converts it to a Spam Confidence Level (SCL). Exchange now correctly recognizes the spam classification. Emails can thus be routed to the Inbox or Junk Email folder accordingly.

## **System Configuration**

Here are the basic configuration steps:

- 1. Route inbound emails to the anti-spam filtering solution.
- 2. Configure the anti-spam filter to analyze emails and tag them with the filtering result. Different solutions may offer differing email tagging mechanisms. We will look into these in a moment.
- 3. Set the anti-spam filter to forward emails to the Exchange server.
- 4. On Exchange install IMF and IMF Tune. Follow the Exchange Configuration section to setup these components.

## **Email Tagging Formats**

The anti-spam solution must publish its email classification through some tagging mechanism. Most filters support the insertion of custom headers or editing the email subject for this purpose.

Most commonly a flag may be set through a custom header. For example the following could be inserted whenever an email is classified to be spam:

X-SPAM: Yes

to 'No'.

A more complicated scenario is when the filter adopts a broader range of values rather than a Yes/No flag. For example a percentage rating is sometimes specified.

Another fairly common case is the insertion of tags within the email subject. Typically this is composed entirely (or in-part) of some fixed text. Through this text it is then possible to extract the filtering outcome.

## **Exchange Configuration**

On the Exchange Server both IMF and IMF Tune must be installed. Follow these steps to configure IMF.

- 1. Up to Exchange 2003 SP1, IMF is available as a separate install from the Microsoft download centre. Exchange SP2 includes IMF within it, eliminating the need for this step.
- 2. From the Exchange System Manager open the Message Delivery properties under Global Settings.



WinDeveloper Software

as follows:

3. Select the Intelligent Message Filtering property sheet and configure it

Gateway Action	No Action
Gateway Blocking Threshold	9 (not relevant)
Store Junk Email Threshold	6

Note that here we are focusing on the integration of an external antispam filter. Thus we go for a simple IMF setup by disabling Gateway Blocking.

ssage Delivery Properties	1
General   Defaults   Seno	der Filtering   Connection Filtering
Configure spam confidence level (SC number for the SCL rating blocks mor commercial e-mail (UCE), but it also in positives.	CL) thresholds. Selecting a lower ore messages that could be unsolicited increases the likelihood of false
- Gateway Blocking Configuration -	
Set the threshold for blocking UCE	E on gateway servers.
Block messages with an SCL ratin equal to:	ng greater than or 9 💌
When blocking messages:	No Action
- Store Junk E-mail Configuration	
Set the threshold for moving UCE	to a user's Junk E-mail folder.
Move messages with an SCL ratio equal to:	ng greater than or 6 💌
	-
OK Car	ncel Apply Help

4. Enable IMF.

In Exchange 2003 SP1 and earlier this is done from: <Organization> | Servers | <Exchange Server> | Protocols | SMTP | Intelligent Message Filtering. Here set the checkbox for the SMTP Virtual server receiving emails from the anti-spam filter.

WinDeveloper Software

neral		
Thtelligent Message Filt	ering	
pply intelligent message <u>f</u> ikering Idresses:	to the following vir	tual servers' IP
Virtual Server	IP Address	TCP Port
Thereor print Aurora pervery	10,0,0,100	23

Otherwise as from SP2 enablement is done from: <Organization> | Servers | <Exchange Server> | Protocols | SMTP | SMTP Virtual Server | General | Advanced. From here set the 'Apply Intelligent Message Filter' checkbox.

I <u>P</u> address:	[All Unassigned]
ICP port;	
F Apply Sender Filter	Apply Sender ID Filter
Apply Recipient Filt	er 🔲 Apply Intelligent <u>M</u> essage Filter
Apply Connection F	iker

5. It is now wise to test IMF and make sure it works correctly. Leave the system running for some time. Spam should start being deposited to the Junk Email folder at the recipient mailboxes.

Note: The IMF Junk Email threshold was set to a relatively high value. Thus a fair amount of spam will still be delivered to the Inbox at this stage.

Note: If email is not delivered to the Junk Email folder, check that this functionality is enabled at the client mailbox. Refer to the IMF Tune FAQs for details on how to do this.

## **IMF Tune Configuration**

- 1. Download IMF Tune from the WinDeveloper site at: <u>http://www.windeveloper.com/imftune/downimftune.htm</u>
- 2. Install the application on the same Exchange server running IMF.
- 3. From the IMF Tune configuration General category, set the 'Enable IMF Tune' checkbox.

Global Thresholds	Global Thresholds	4				
Whitelests     Accept Senders     Accept Recipients	🔽 Egable IMF Tune					
- Accept Subjects	SCL	Action	Archive	Auto-Reply	Logging	
Accept Bodies		Accept	disabled	disabled	disabled	_
Accept Subjects/Bodi	Witelisted	Accept	disabled	disabled	disabled	
Blacklists	Ø\$0-6	Accept	disabled	disabled	disabled	
Disk Maintenance	27-9	Accept	disabled	disabled	disabled	
Archives Logs/Reports Keyword Reporting SCL Rules Simple Advanced	<b>₩ŧ</b> łackisted	Accept	disabled	disabled	disabled	
Exchange System Manag Unprocessed Emails Details						
Elicensing WinDeveloper	Add   E	a.	Series -	4		8

- 4. Configure the IMF Tune action for SCL rating 7 and higher to 'Accept' as shown above. If you followed this whitepaper to the letter, this should already be the case. Otherwise, select the list entries and click on Edit to change the action setting.
- 5. Next select the SCL Rules | Simple category and set the 'Apply simple SCL Rules' checkbox.
- 6. You may now want to delete all the pre-configured SCL Rules that the installation creates for demonstration purposes. Do this by selecting the list entries and hit the delete button.

WinDeveloper Software

Global Thresholds	Simple				
Whitelists Accept Senders Accept Recipients Accept Subjects Accept Bubjects	Specify a cond Emails can be	iltion to match sta whitelisted, black le SCL Rules	ndard/custom headers, 5 isted or have their SCL ra	SMTP protocol data ting adjusted as re	and IP. equired.
Blacklists	Header	Match	Value	Operation	sa
Disk Maintenance     Archives     Logs/Reports     Keyword Reporting     SCL Rules     Sinclo     Advanced     Exchange System Manag     Unprocessed Emails     Details     Locening	X-SPAM X-SPAM	contains contains	no yes	set value to	0 7
WinDeveloper	Add	<u><u> </u></u>	<u>Derror</u>		

- 7. Click on the Add button to create a new SCL Rule.
- 8. Rule configuration depends on the type of tagging adopted by the antispam filter. Considering the Yes/No flag discussed earlier, we could configure two rules as follow:

Header Name:	X-SPAM
Matching Type:	contains
Header Value:	yes
Operation Type:	set value to
SCL Value:	7

Details	SCL Mapping		
121202030	Header/SMTP Command:	Match Type:	
	X-SPAM	✓ contains	3
	Operation:	SCL Change:	
	set value to	• 7	
	sensitive. Enclose phrases containing v	white space in double quotes.	Advanced
	Expression to match. Operators who, sensitive. Enclose phrases containing o yes Description:	white space in double quotes.	Advanced
	Description:	white space in double quotes.	Advanced

The second rule would match X-SPAM header value "no". In this manner legitimate emails are forced to the inbox:

Header Name:	X-SPAM
Matching Type:	contains
Header Value:	no
Operation Type:	set value to
SCL Value:	0

Some anti-spam filters only tag spam emails. Legitimate emails can then be identified by the absence of a header. In this case we could configure a rule that matches a missing header. Here is an example of how the configuration would look like:

Header Name:	X-SPAM
Matching Type:	is empty/missing
Header Value:	
Operation Type:	set value to
SCL Value:	0

Cl. Mapping	SCL Mapping		
	Header/SMTP Command:	Match Type:	
	X-SPAM	→ is empty/missing	
	Operation:	SCL Change:	
	set value to	• 0	
	Expression to Match, Operators AND, sensitive, Enclose process containing	OR, NOT ere supported. Matching is no of ite space in double quotes.	rt cane Isanced, /
	Expression to Match. Operators AAD, sensitive: Enclose process containing Description:	OR, NOT ere susported. Matching is no of ite space in double guides.	rt case
	Expression to Match, Operators AND, sensitive, Enclose process containing Description: IF X-SPAM is empty/missing set value	OR, NOT ere supported. Matching is no white space in double quotes.	rt case Jeanced. /

Let's instead consider subject tagging. If the filter identifies spam by inserting the text: '[SPAM]' the settings become:

Header Name:	Subject
Matching Type:	contains
Header Value:	[SPAM]
Operation Type:	set value to
SCL Value:	7

WinDeveloper Software

oct. Mapping Details	SCL Mapping		
	Header/SMTP Command:	Match Type:	
	Subject	- contains	-
	Operation:	SCL Change:	
	set value to	7	
	Expression to Match. Operators AND sensitive. Enclose phrases containing [[SPAM]	, OR, NOT are supported. Matching white space in double quotes,	is not case
	Expression to Match. Operators AND sensitive. Enclose phrases containing [SPAM] Description:	, OR, NOT are supported. Matching white space in double quotes.	is not case
	Expression to Match. Operators AND sensitive. Enclose phrases containing [[SPAM] Description: [If Subject contains "[SPAM]" set value	, OR, NOT are supported. Matching white space in double quotes.	is not case

9. Save Changes and test the complete system.

Through IMF Tune you may also cater for more complex tagging scenarios. If the filter produces a range of value tags, multiple SCL Rules could be created. We could also make use of Advanced Rules where multiple conditions and exceptions can be combined in order to match the tags as necessary.

Finally if you need assistance with configuring the rules contact WinDeveloper support on <a href="mailto:support@windeveloper.com">support@windeveloper.com</a>

### **Final Tips**

Filtering spam to the Junk Email folder enables users to maintain focus on their Inbox. Emails still reach their destination but the final separation minimizes the disruption caused by spam.

Users through Outlook may further customize filtering. Safe Senders, Safe Recipients and Blocked Senders may be specified from Tools | Options | Preferences | Junk E-mail.

All the client-side functionality is available through Outlook/OWA. No clientside extensions or custom rules are involved. Thus deployment is centralized and involves minimal disruptions.