

ORF + IMF Guide

How to redirect spam to the Junk folder
on Exchange 2003

Revision: 1.1
Date: June 15, 2009

■ Preface

WHAT IS THIS GUIDE ABOUT?

This documentation provides step-by-step instructions regarding the setup of ORF and IMF on Exchange 2003 SP2 or newer.

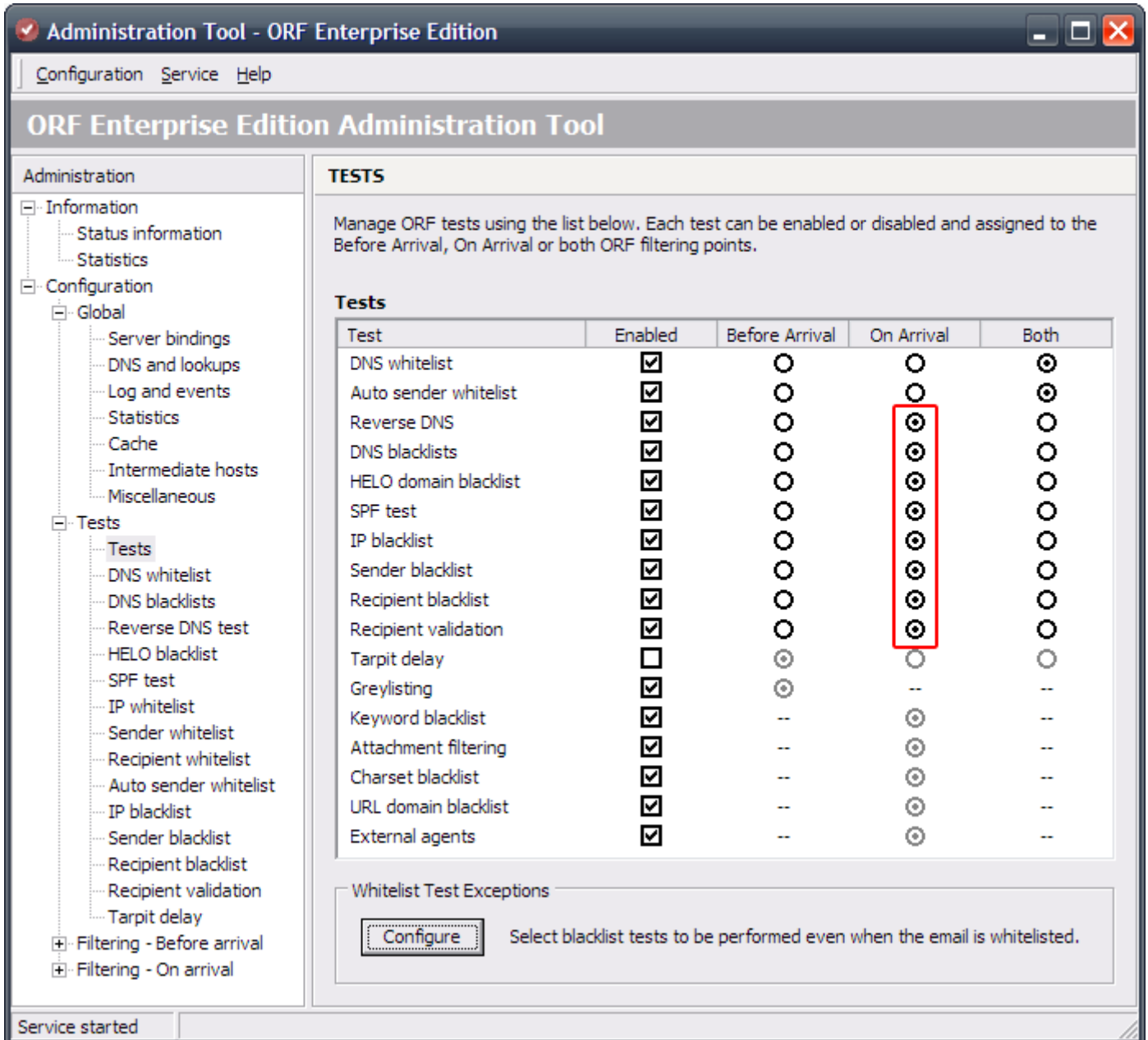
WHO SHOULD READ THIS?

The guide targets readers who would like to **redirect all emails blacklisted by ORF to the users' Junk folder instead of rejecting them**. This could be useful if you would like to apply some aggressive rules or your users want to make sure no legitimate was rejected for them. In the following method, we will use the **Custom Weighting feature of IMF v2 to achieve this goal, which is available since Exchange 2003 SP2**. Please consult the documentation of this service pack for installation instructions.

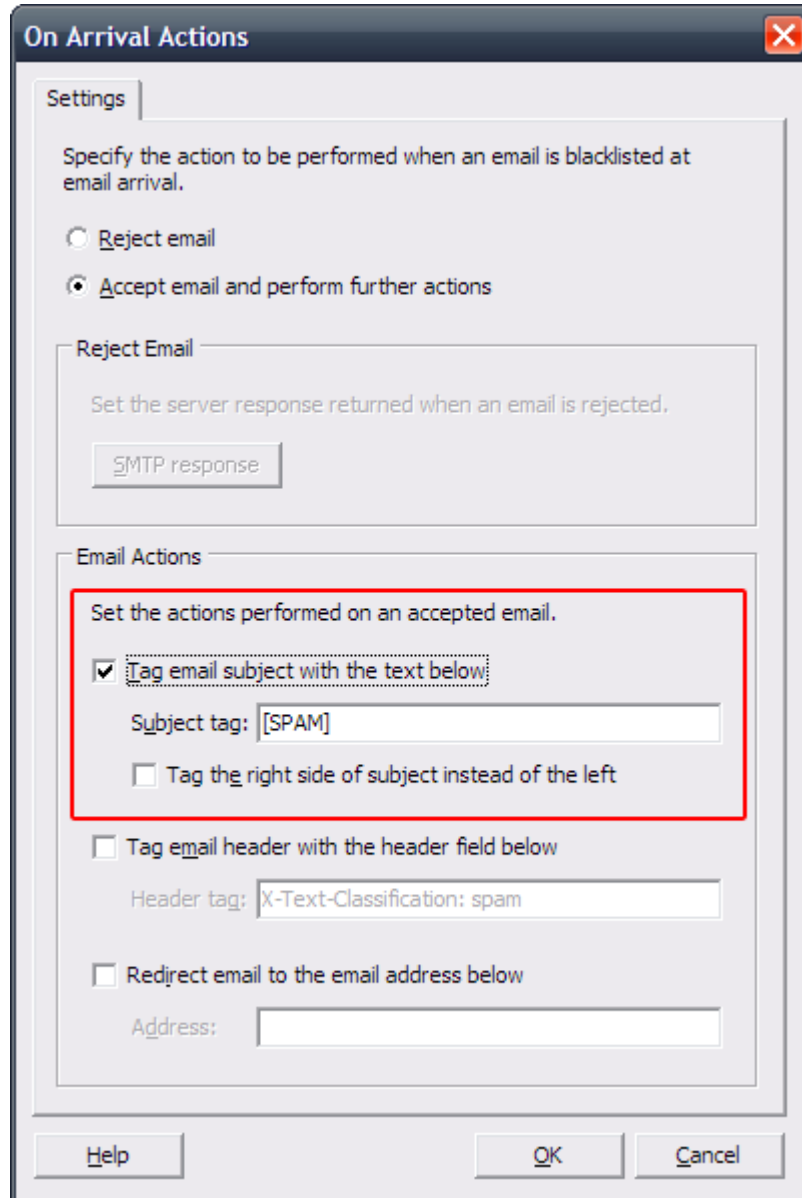
■ ORF Settings

First, you should configure ORF not to reject blacklisted emails, but to tag their subject line with [SPAM] instead. To achieve this, you should do the following:

- 1) Start the **ORF Administration Tool**.
- 2) Assign all blacklist tests to the **On Arrival filtering point** in *Configuration / Tests / Tests* (because if the email gets blacklisted at Before Arrival, the only option is to reject it, but we want to accept and tag it)



3) Configure ORF to tag the subject of all blacklisted emails in *Configuration / Filtering - On Arrival / Actions*



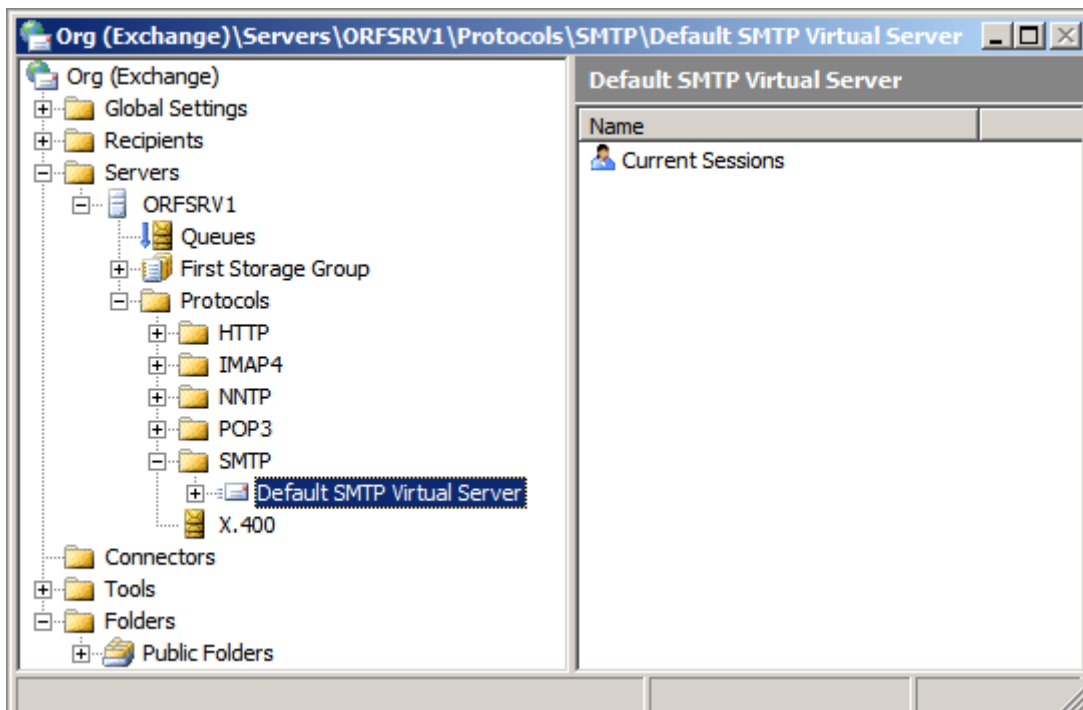
- 4) Click **OK**.
- 5) Finally, save your settings and restart the ORF Service (by pressing **Ctrl + U** in the **Administration Tool**) in order to apply the configuration changes.

IMF Settings

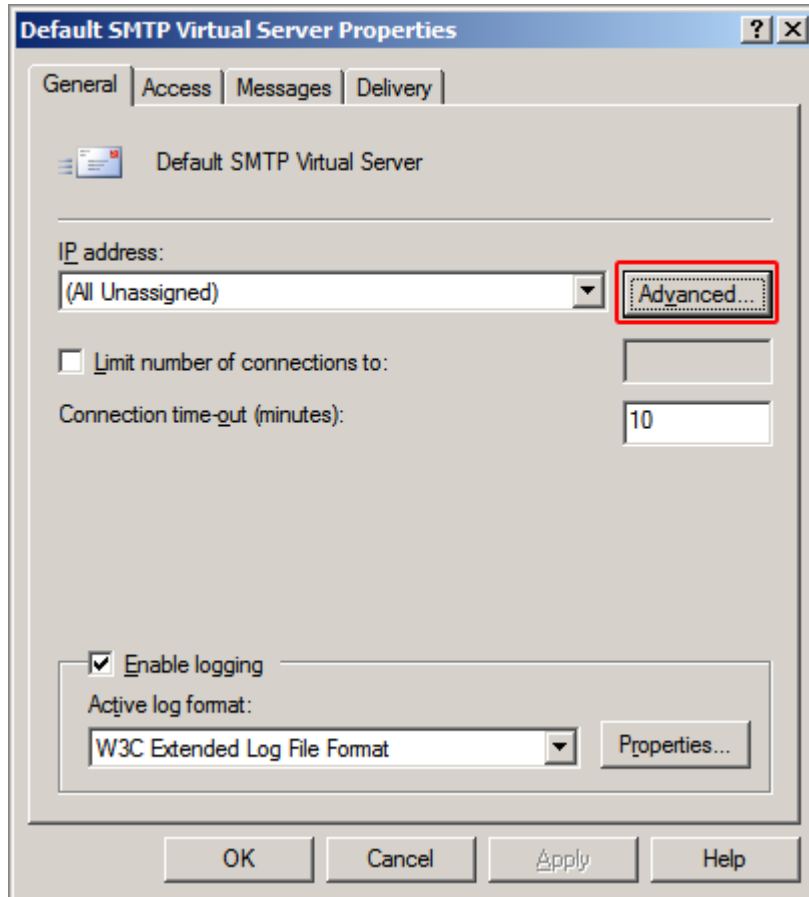
ENABLING IMF

We should make sure IMF is enabled on our SMTP server instance.

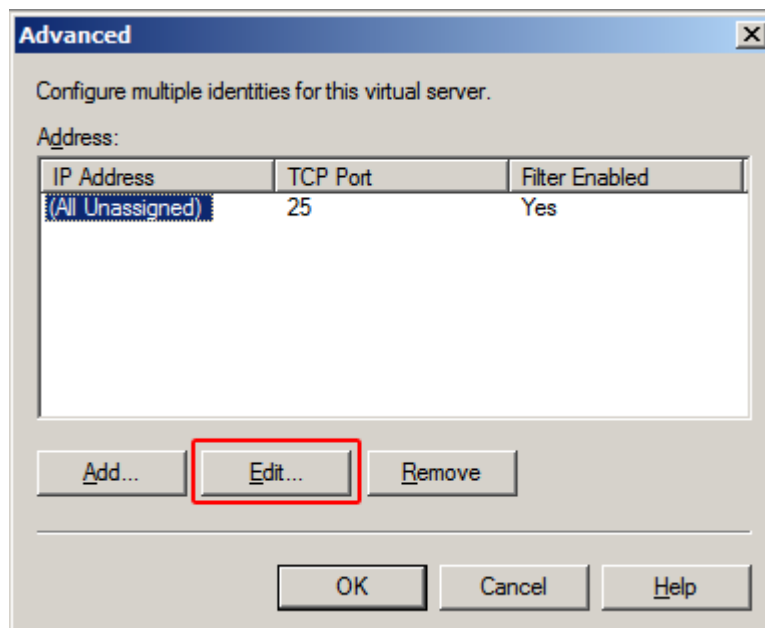
- 1) Start the **Exchange System Manager**
- 2) Under **Servers**, expand your server
- 3) Select **Protocols**, then **SMTP**
- 4) Right click on your **SMTP** server and select **Properties**



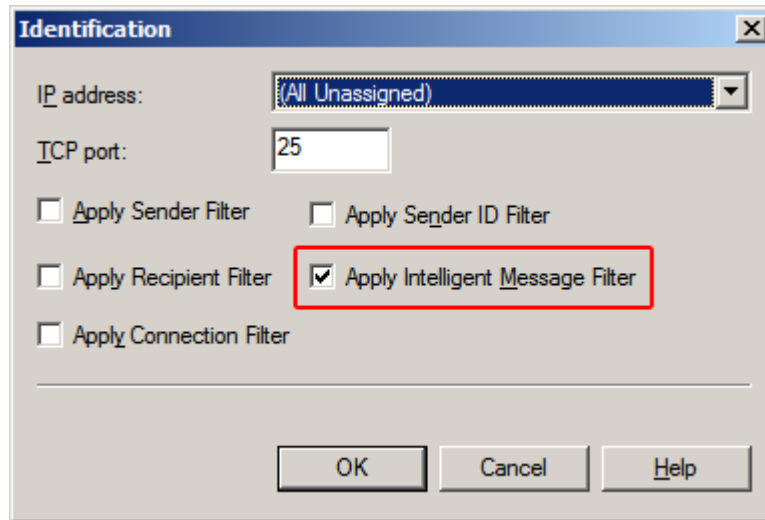
- 5) On the **General** tab, click the **Advanced...** button



- 6) Select the SMTP port on which the mails are coming in (25 by default) and click the **Edit button**



- 7) Finally, check the *Apply Intelligent Message Filter* check box and click **OK**.



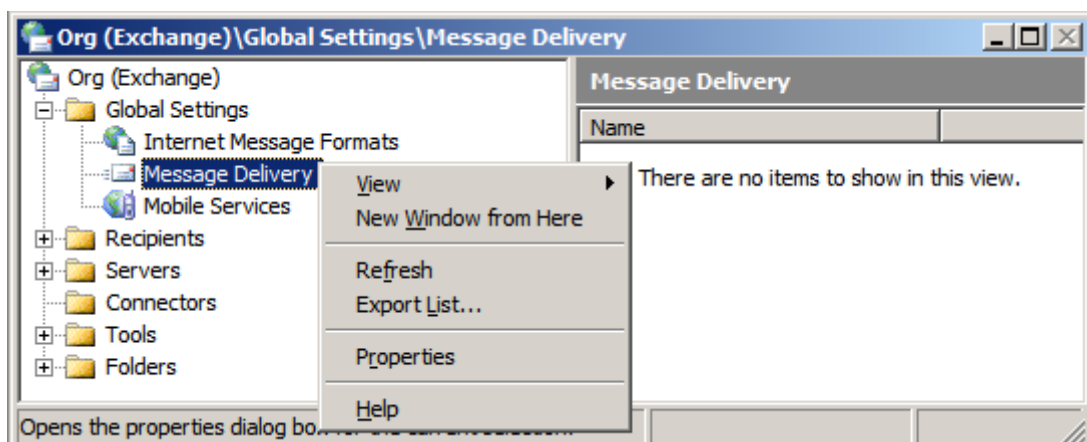
SETTING THE SCL THRESHOLDS

Next, we will configure *IMF* to move all emails with SCL score 8 or higher to the Junk folder of the user.

What is SCL?

Spam confidence level (SCL) is a numerical value indicating the likelihood that an incoming email message is spam. IMF evaluates message headers, content and other components of incoming mail and assigns an SCL ranking between zero and nine. An SCL of nine identifies a message that is almost certainly spam and an SCL of zero a message that is highly unlikely to be spam.

- 1) Start the **Exchange System Manager**
- 2) Select **Global Settings > Message Delivery**



- 3) Right click on it and select **Properties**

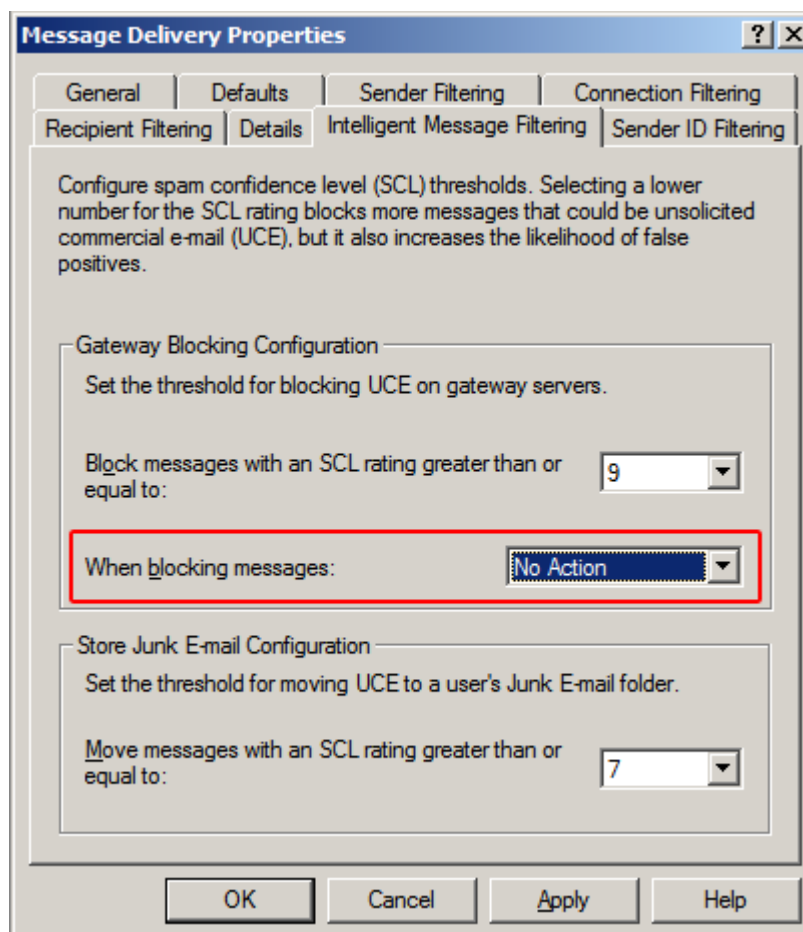
4) Select the *Intelligent Message Filter tab*

There are two (quite confusing) threshold settings for the SCL scores: the *Store Junk Email Configuration* SCL threshold tells IMF which ones should be redirected to the Junk folder, while the *Gateway Blocking Configuration* threshold tells which ones should be rejected (or archived, depending on your settings).

If you set **9** for *Gateway Blocking Configuration* and **6** for the *Store Junk Email Configuration*, the following will happen:

- Emails with SCL score **0-6** will be delivered
- Emails with SCL score **7-8** will be redirected to the **Junk folder**
- Emails with SCL score **9** will be blocked

Let's set **7** for *Store Junk Email Configuration* and **9** for *Gateway Blocking Configuration*. As we would like to redirect all messages to the Junk folder and reject none, you should choose **No Action** to be performed (*When blocking messages:*), so no email will be archived or rejected by IMF, all will go to the Junk folder (with SCL score higher than 7).



THE CUSTOM WEIGHTING FEATURE

IMF has a so called **Custom Weighting Feature (CWF)**, which can be used to setup some manual rules in order to increase or decrease the SCL score of an email based on certain criteria. The plan is to configure the CWF to set the SCL score to the maximum (9) for all emails blacklisted by ORF (i.e. which has been tagged with the phrase [SPAM]), thus IMF will redirect them the Junk folder.

Enabling The Custom Weighting Feature

First, in order to enable CWF, we need to register the *MSEExchange.UceContentFilter.dll* file in its folder (Program Files\Exchsrvr\bin\MSCFV2\ by default):

- 1) Open a command prompt
- 2) Navigate to the folder where the DLL file resides
- 3) Issue the following command:

```
regsvr32 MSEExchange.UceContentFilter.dll
```

You should receive a “DllRegisterServer in *MSEExchange.UceContentFilter.dll* succeeded” message.

Creating The Configuration File

The Custom Weighting feature has no graphical user interface, the configuration is stored in an XML file called *MSEExchange.UceContentFilter.xml*. The XML file is read by IMF upon initialization, and reloaded every time it is modified. The configuration file should be stored in the same folder where the *MSEExchange.UceContentFilter.dll* and .dat files reside.

The configuration file can be created in any text editor (e.g. Notepad), just make sure you save the file in Unicode format (Save as... | Encoding) and the filename matches the name of the DLL (but with XML extension). Here is a sample how the XML file should look like:

```
<?xml version="1.0" encoding="UTF-16"?>
<CustomWeightEntries xmlns="http://schemas.microsoft.com/2005/CustomWeight">
  <CustomWeightEntry Type="SUBJECT" Change="MAX" Text="[SPAM]"/>
</CustomWeightEntries>
```

This tells IMF set the SCL score to the maximum (9), if the text [SPAM] exists in the subject line of the email. To ease things, we ship a sample XML file with this guide.

WARNING! If the schema of the custom weighting file is broken or malformed, it will cause IMF to fail loading, so make sure it is correct. If the custom weighting file does not exist, IMF will continue to load and function normally, without the use of the **Custom Weighting Feature**.

After first creating a custom weighting file, the **SMTP service must be restarted to pick it up**. When the filter has been loaded with a valid custom weighting file, any changes that you made to the file are immediately picked up, no service restart is required.

■ Changing The Filtering Order

By default, IMF filters the incoming email flow first, because it has higher filtering priority. This is not ideal in our case, because we want ORF to tag spam emails first before IMF would assign an SCL score. To solve this problem, we should configure ORF to filter before the CWF feature of IMF would be triggered.

On Exchange 2003, the order of the filtering depends on so-called event sink priorities. By default, IMF has higher event sink priority (*MSExchange Content Filter EOD Sink*) than ORF, so it runs before ORF would run, as ORF uses protocol event sinks hooking the RCPT and EOD events with the default priority.

To check the SMTP event sink bindings (and the priorities), download a script from <http://www.vamsoft.com/downloads/smtpreg.zip>. Extract the ZIP archive contents to any folder on your server, then start a command prompt and enter to the directory where you extracted the archive contents to. Run the script as "cscript smtpreg.vbs /enum > sinks.txt" (without the quotes). A new file called 'sinks.txt' will be created in the current folder, which contains the event sink binding list of IIS SMTP/Exchange. ORF binds with the following names: VS_ORFEnterprise_RCPT, VS_ORFEnterprise_EOD and VS_ORFEnterprise_OUTBOUND.

In case IMF has higher priority (lower number indicates higher priority), you should change the event sink priorities of ORF. This could be done using the `smtpreg.vbs`. Note that ORF event sink bindings are restored to the default when they are changed (e.g. when upgrading to a newer version and when you re-bind the SMTP Module).

You can use the commands below to change the ORF SMTP Module bindings to priority 1000 on the first SMTP virtual server instance:

```
cscript smtpreg.vbs /setprop 1 OnInboundCommand "VS_ORFEnterprise_RCPT" Source Priority 1000
cscript smtpreg.vbs /setprop 1 OnInboundCommand "VS_ORFEnterprise_EOD" Source Priority 1000
```

If we are lucky, we are done with the configuration and can proceed with testing.

■ Testing

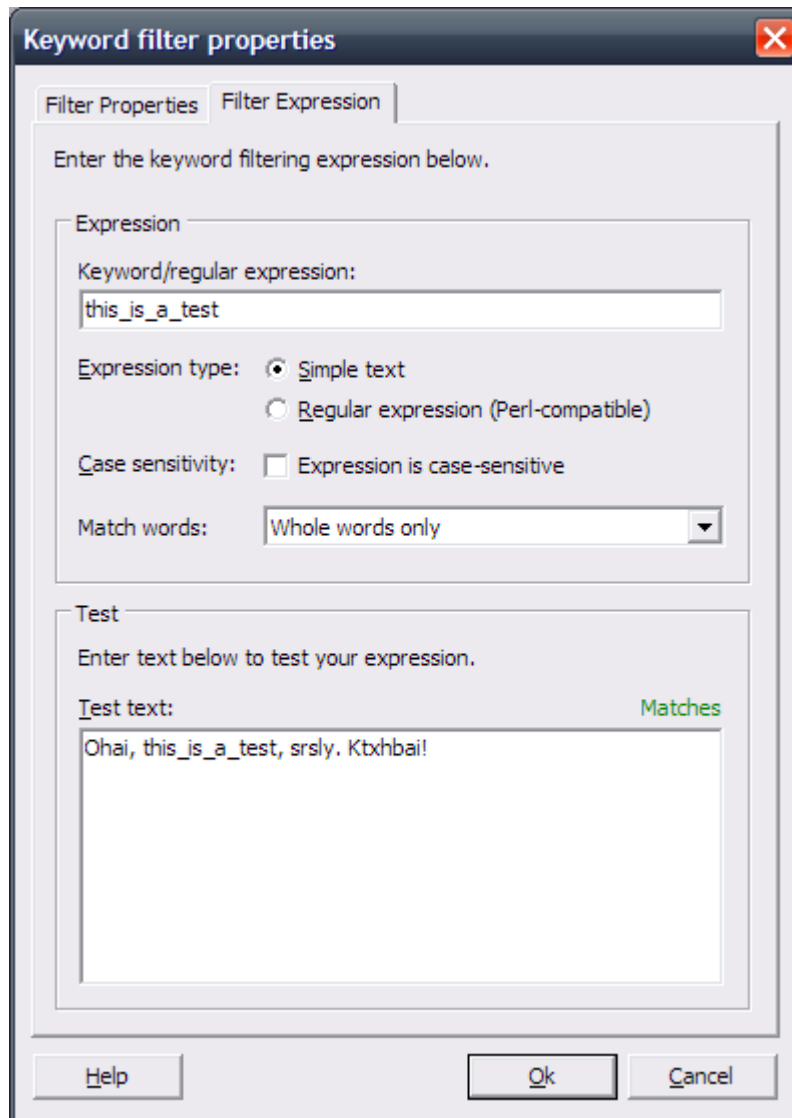
The easiest way to test is creating a **Keyword Blacklist** entry in ORF and sending a test mail from an external IP address (or using a loopback interface with an external IP) with the blacklisted word in it. According to our settings

- ORF should tag the subject with [SPAM]
- The CWF should recognize the [SPAM] tag in the subject line and should increase the SCL score to the maximum (9)

- Finally, IMF should redirect the mail to the Junk folder

PREPARING FOR THE TEST

1. Add a keyword blacklist entry in ORF (**Configuration / On Arrival / Keyword Blacklist / New...**)
2. On the **Filter Properties** tab, set the Search scope to “**Email subject**” and enter something in the **Comment** field (e.g. “*Test*”)
3. On the **Filter Expression** tab, enter the test phrase and set the expression type. Make sure it works as it should. See an example below:

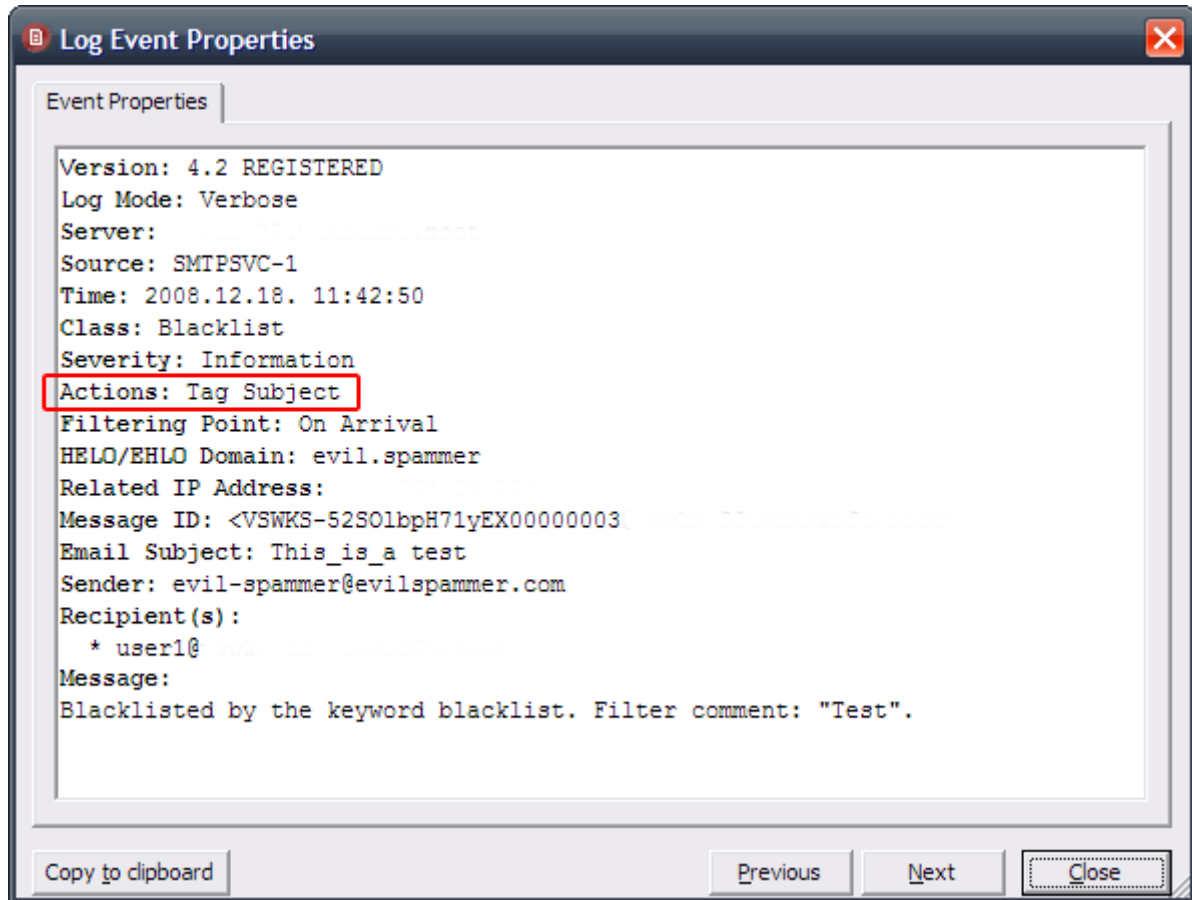


4. Click **OK**.
5. Make sure you have the **Keyword Blacklist test enabled**.
6. Save your settings and restart the ORF Service (**Ctrl + U** in the **Administration Tool**).

TESTING

1. Send a mail from an external email account. The blacklisted phrase should be included in it.

2. Check the ORF log in the **Log Viewer**. You should see the mail was tagged:



3. Finally, check the user's mailbox. *The tagged message should be in the Junk folder.*

■ Troubleshooting

PROBLEM: The email subject is not tagged by ORF

SOLUTION: Make sure you set everything in ORF correctly, save your settings and restart the ORF Service. If it does not solve the problem, check the ORF log to find out what happened: it's possible that the email was whitelisted for some reason.

PROBLEM: The mail was tagged, but it was delivered to the user's Inbox instead of the Junk E-mail folder

SOLUTION: Make sure the **Content Weighting Feature** increased the SCL score of the tagged email to **9**. Unfortunately, the SCL score is not indicated anywhere in the email client, but with a little trick, you can create an SCL column in your Outlook view:

- 1) Copy the *scl.cfg* file shipped with this guide to the directory where *IPML.ico* and *IPMS.ico* reside (`ProgramFiles\Microsoft Office\OFFICE11\FORMS\<Language_ID>\` by default. For the English version, the language ID is 1033, for other versions this may differ).
- 2) Open **Outlook**
- 3) From the main menu, select **Tools > Options > Other > Advanced Options > Custom Forms > Manage Forms**
- 4) Click on **Install** and select the *scl.cfg* file
- 5) Install it into your **Personal Forms Library**
- 6) Press **OK** several times until you return to the main **Outlook** screen
- 7) Right-click on the column headings in your Inbox (or any other folder) and select **Customize Current View...**
- 8) Click **Fields...**
- 9) In *Select available fields*, scroll down and choose **Forms**
- 10) Under **Personal Forms**, choose the **SCL Extension Form**, click **Add**, then **Close**

Now you have an SCL column displaying the SCL rating of messages. Drag the SCL column where you want it.

PROBLEM: The emails are tagged and have the maximum SCL score (9), still, they are delivered to the user's Inbox instead of the Junk E-mail folder

SOLUTION: This may happen because **Outlook** does not use the **IMF** provided SCL values for its client-side (cached-mode only) anti-spam determination. Instead, it does its own Junk E-mail evaluation and determines whether or not to move the mail to the Junk E-mail folder based on its own settings.

You can read more about the problem on this website:

<http://blogs.technet.com/evand/archive/2005/01/31/363935.aspx>

The problem seems to affect mostly those mailboxes which were not fired up in Exchange cache mode at first. If the problem appears to affect only a few mailboxes, you can do the following:

- 1) Login to the mailbox using **Outlook Web Access (OWA)**
- 2) Check the **"Filter Junk E-mail. Check the Junk E-mail folder regularly to ensure that you do not miss messages that you want to receive"** checkbox in **Options**
- 3) Click **Save & Exit**

This will fix the Junk folder issue in both in **Outlook** and **OWA**. Sometimes poking the Junk E-mail settings in **Outlook** might also help. If you have many mailboxes with this problem, you should use [Evan Dodds' script](#) to set this for multiple mailboxes at once.

FAQ

Q: I have multiple subfolders in `Program Files\Exchsrvr\bin\MSCFV2` with different `MSExchange.UceContentFilter.dll` files in each. Where should I put the XML file?

A: Exchange Updates create new folders for each new version of CWF. You can use either of them, just make sure you save the XML file to the same folder where the DLL you registered with regsvr32 resides.

Q: *The Custom Weighting List does not seem to be working and I have error messages (error 7514) in the Event Log saying “An error occurred while loading Microsoft Exchange Intelligent Message Filter. The error code is 0x80004005.”*

A: Most likely the XML file is saved in ANSI and not Unicode (or in a different Unicode format). The quickest way to verify this is trying to load it in **Internet Explorer**. If you get a “**Cannot view XML input using style sheet**” error, then it was probably saved in the wrong format. Re-save it in Unicode in your text editor. If you still get error 7514, try deleting the XML file entirely. If the error still occurs, something else may be wrong: for instance, the IMF DLLs may not be registered correctly.

Q: *No mail arrives to the users’ mailboxes. Why?*

A: Make sure you have set “**No Action**” in *Gateway Blocking Configuration*, otherwise IMF will archive or block all emails tagged by ORF.

Q: *Emails are tagged by ORF, but they arrive to the users’ inboxes instead of the Junk folder. Why?*

A: Make sure the filtering order and priorities are correct and the CWF configuration is OK.

■ Technical Support

Please contact our technical support using contact options below. Using the [Community Forums](#) is recommended (we are active there as well).

Before contacting us, please check the product documentation and the [ORF FAQ](#), you may find a quick answer for your question there.

Email:	orf-support@vamssoft.com
Community Forums	http://www.vamssoft.com/forum
Phone:	(+36) 1 279 2299
Fax:	(+36) 1 279 1260
World Wide Web:	http://www.vamssoft.com
Postal Address:	Vamssoft Ltd. Budapest Györök utca 11. H-1113 HUNGARY