

Re: Using IMF in conjunction with Trend CSM

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-10/msg05425.html>

- *From:* "Gregg Hill" <bogus@xxxxxxxxxxxx>
 - *Date:* Fri, 27 Oct 2006 09:21:18 -0700
-

Hi, Les!

I had forgotten that I actually do have the Junk email set to "No Protection" via a GPO to prevent them having to look in two places. It must not be working, because some users have spam in their junk email folder.

I will look at their setup again next week.

Gregg Hill

"Les Connor [SBS Community Member – SBS MVP]" <les.connor@xxxxxxxxxxxx> wrote in message news:evrSQjI%23GHA.1168@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

I'd recommend not using the Outlook JMF if you're using EUQ – it just confuses the issue (and the end user).

1. Connection filtering (spamhaus is good).
2. IMF set to reject at whatever number you feel good about *and* set the JMF to the same number.
3. Recipient filtering
4. Trend Anti-Spam <high>
5. Turn JMF *off* in Outlook.

Use the JMF folder in Outlook *only* for spam or unwanted email that makes it through to the inbox – the end user then only needs to r-click the message and send to JMF folder.

This way, EUQ and JMF don't fight over spam, spreading it over both folders. And, it's a good way to see how much spam actually makes it through to the Inbox, as these are stored in Outlooks JMF by the user.

If you're getting more than 5–10 spams a day into the inbox, then IMHO the solution isn't working and you may need to tighten up if you can, or implement other measures. Same with EUQ, you should be able to achieve 10–20 per day there.

Re: Using IMF in conjunction with Trend CSM

Les Connor [SBS Community Member – SBS MVP]

SBS Rocks !

"Tell me and I'll forget. Show me and I'll remember. Involve me and I'll understand." – Confucius

"Gregg Hill" <bogus@xxxxxxxxxxxx> wrote in message
news:%23a9Ts5H%23GHA.4404@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello!

I have Trend CSM 3.0 SP1 (build 1147) on my SBS 2003 server and some of my clients' SBS 2003 servers.

By default, the SMEX portion of Trend CSM will create a "Spam Folder" in each users' mailbox. This is the End User Quarantine, or EUQ. What I found was that most users failed to check that folder for possible false positives, or they did not even see the folder in Outlook because they had so many folders above it. "Out of sight, out of mind" seems to be the phrase that applies here.

So what I have done is remove the EUQ and then re-install it, but I named the folder as * Possible Spam during the re-installation of the EUQ (that is "* Possible Spam" without the quotation marks) so it stays at the top of the Outlook folders. Now everyone sees it and checks it.

The problem now is that some users get 5000 messages every two weeks (according to the SBS usage report) and most of that is spam. In order to reduce the time they spend looking for legitimate messages, I have implemented Connection Filtering (sbl-xbl.spamhaus.org) as well as the IMF in Exchange SP2. Recipient Filtering was added a long time ago with tarpitting (I know the end user never sees the result).

I have the IMF set to archive messages over SCL 6 (I may go to 7) and move to Junk at 5. So far, an SCL of 6 has only trapped one valid message, and that was from Backup Exec running on the same server (see thread "Strange IMF Behavior").

Trend EUQ still has a bunch of spam in it as well. I have Outlook set to show the SCL and I am reviewing those caught by Trend to see if I can safely lower the gateway SCL in IMF.

Currently, users have to look in two places to make sure no valid message got flagged as spam. I wish Trend's product would integrate better into Outlook so users could look in one location and use one method to approve and/or block mail. I thought about naming the Trend EUQ as "Junk E-mail" folder so everything goes into one box, but then I get the "out of sight..." problem again, and I am not sure what would happen if both IMF

Re: Using IMF in conjunction with Trend CSM

and Trend dumped into that folder, since they have different methods of approving users.

How have the rest of you Trend CSM users been handling this concern?

Gregg Hill