

# Implementing Spamhaus Datafeed Query Service in Exchange 2007

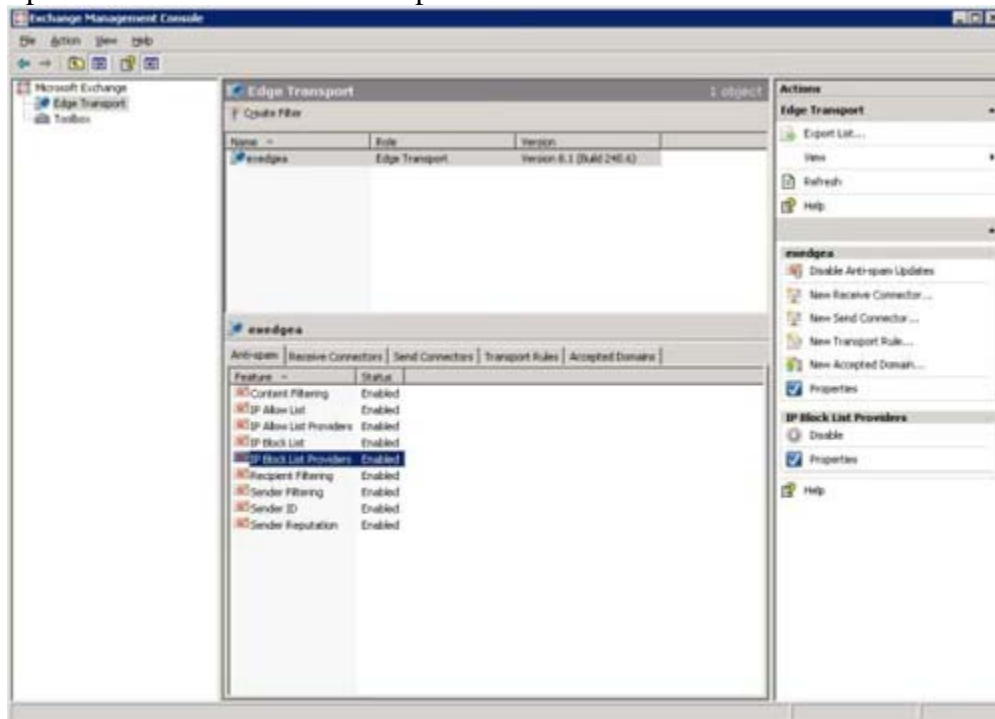
## About

The Spamhaus Datafeed Query Service is designed to run on the Exchange Edge Server (or Hub Transport if Edge is not being used). The steps below assume that Edge Services are being used and steps are to be performed from the console of the Edge Server. The same steps would also be performed on the Hub Transport server however the screen shots will differ slightly.

[Click here to download this tutorial as a PDF.](#)

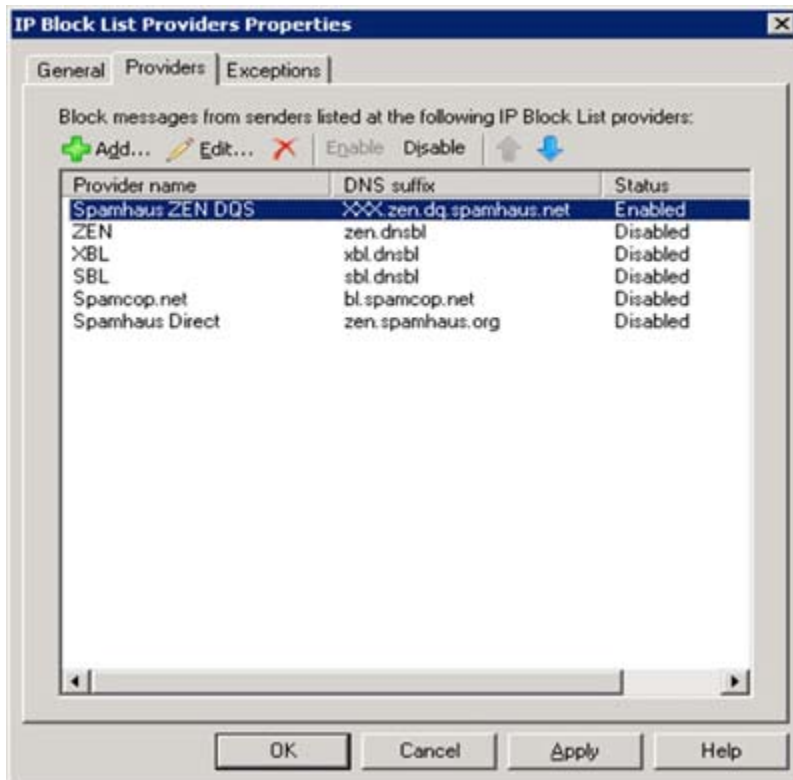
## Step by Step:

1. Open Exchange Management Console
2. Open IP Blocklist Providers Properties



3. Go to Providers Tab

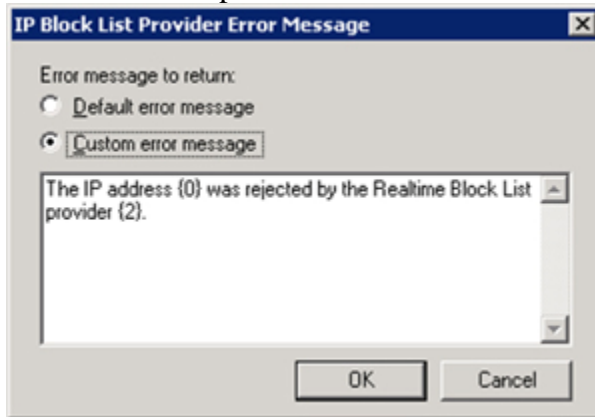
4. Click Add



5. Type the Spamhaus DQS lookup domain



6. Click OK
7. For extra diagnostic information click "Error Messages..." and insert a custom message such as the example below.



(Please note this is completely optional and it will provide the sender information on why the message was rejected.)

8. Click OK
9. Click OK on more time to return to the Exchange Management Console.
10. To test, send a blank email message to [nelson-sbl-test@crynwr.com](mailto:nelson-sbl-test@crynwr.com). A message similar to the example below should be received:

Testing your SBL block:

Visit <http://www.crynwr.com/spam/> for more info. Please note that this test will not tell you if your server is open for relaying. Instead, it tests to see if your server blocks email from IP addresses listed in various blocking lists; in this case, the SBL list.

Here's how the conversation looked from [sbl.crynwr.com](http://sbl.crynwr.com).

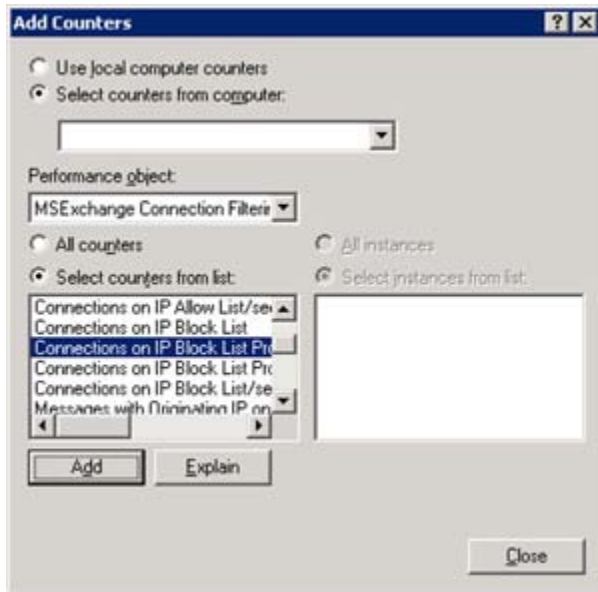
Note that some sites don't apply the SBL block to postmaster, so I use your envelope sender as the To: address.

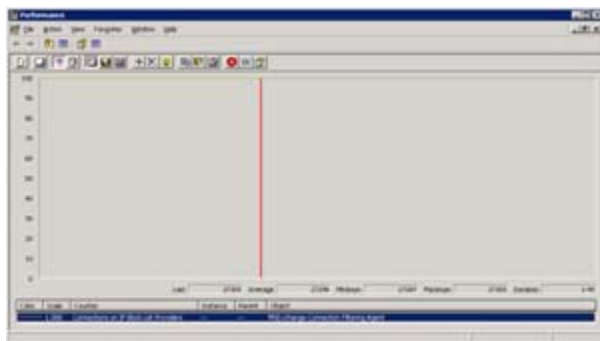
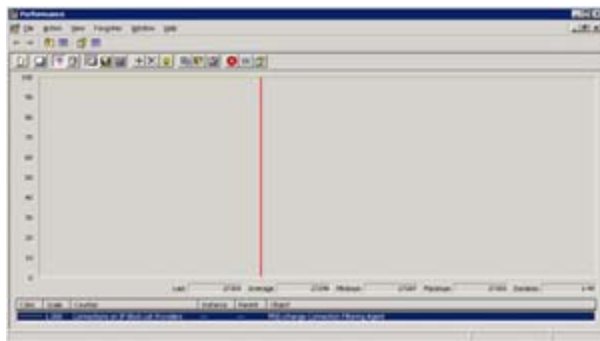
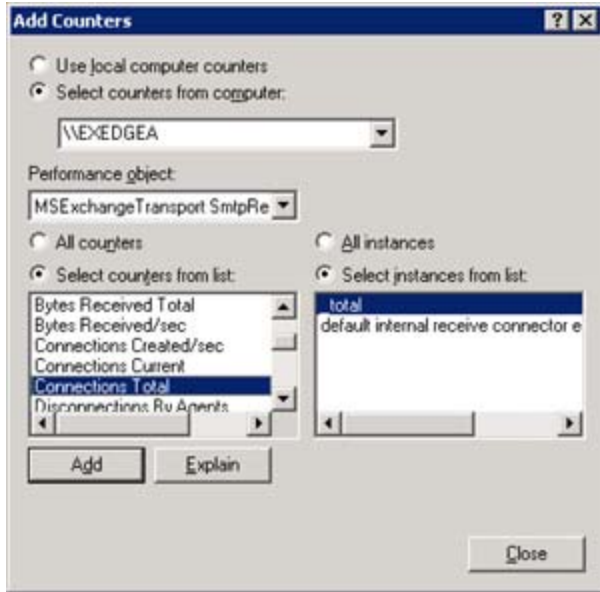
I connected to XXX.XXX.XXX.XXX and here's the conversation I had:

```
220 mail.server.com Microsoft ESMTP MAIL Service ready at Tue, 30 Jun 2009
06:01:44 -0500 helo sbl.crynwr.com 250 mail.server.com Hello [192.203.178.107] mail
from:<> 250 2.1.0 Sender OK rcpt to:< user@server.com> 550 5.7.1 The IP address
192.203.178.107 was rejected by one of Spamhaus' block lists. For further information,
visit http://www.spamhaus.org/lookup.lasso.
Terminating conversation
```

## Accountability

There is a performance counter for tracking how many connections are being dropped by the IP Block List Provider. The counter shows the total number of connections dropped since the Edge Transport service was last restarted. The exact name of the counter is "Connections on IP Block List Providers" from the "MSEExchange Connection Filtering" Performance Object. There is another counter called "Messages with Originating IP on IP Block List Providers". This counter is useless as the connection is dropped, no messages are received. Another valuable counter to see how many total connections have been made to the server is "Connections Total" from the "MSEExchangeTransport SMTPReceive". So the counters show how many connections are dropped but there is no way to accurately gauge how many messages were dropped because one connection could consist of one or a million messages potentially. Alternatively Microsoft System Center Operations Manager "SCOM", formerly Microsoft Operations Manager "MOM", will produce reports on how many connections are being dropped. No information is provided in this document on SCOM or MOM. However, screen shots are below of the counter in Performance Monitor.





As you can see from above comparing the two Performance Monitor windows; 178,817 connections have been made since the last reboot and 103,791 of those connections have been dropped from being found in Spamhaus!

**Customer Quote:**

The demise of WRBLDNSD prompted us to revisit the solution and found DQS on Spamhaus and said "This is what we need!"

The Spamhaus Datafeed Query Service is VERY easy to use, a "plug and play" solution for Microsoft Exchange 2007.

Installed in seconds!