



Simply better network security.™

SMTP RECIPIENT VERIFICATION WITH EXCHANGE 2007 AND 2010



COPYRIGHT NOTICES

©eSoft Inc. 2010. eSoft, InstaGate, and ThreatWall are registered trademarks, and SoftPak and SoftPak Director are trademarks of eSoft, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation. Adobe, the Adobe logo, and Acrobat are registered trademarks of Adobe Systems Inc. UNIX is a registered trademark of UNIX Systems Laboratories, Inc. All other brand and/or product names are the property of their respective holders.

Portions of this software are covered under the GNU General Public License. You may freely obtain source code versions of the software covered by the GNU General Public License through the Internet at <http://www.redhat.com>. However, some applications remain the property of their owners, and require their permission to redistribute. For more information, access the eSoft web site at <http://www.esoft.com>.

Portions of this software are Copyright © The Regents of the University of California. A complete copy of the copyright notice follows:

Copyright © The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment:
“This product includes software developed by the University of California, Berkeley and its contributors.”

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software are Copyright © The Apache Group. A complete copy of the copyright notice follows:
Copyright © 1995-1997 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment:
“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”

The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission.

Redistributions of any form whatsoever must retain the following acknowledgment:
“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”

INTRODUCTION

Recipient address verification is a critical tool in fighting spam. It allows the Spamfilter to reject messages that are sent for invalid recipients (users) on your network. Rejecting messages to invalid recipients before Spamfilter and Anti-Virus processing reduces the volume of mail processed by your mail server, which enhances system performance and reduces load.

When the InstaGate or ThreatWall is set for Mail Relay mode, the recommended method for rejecting invalid recipients is to use SMTP Recipient Filtering on your internal Exchange Server. You must also enable Address Verification on the InstaGate or ThreatWall in order to complete the configuration. This document details the eSoft appliance configuration, as well as the Exchange server configuration for both Edge Transport mode and the default Hub Transport mode.

INSTAGATE OR THREATWALL CONFIGURATION

1.1 Verify the Relay Server Configuration

The Email Server on the InstaGate or ThreatWall must be set to relay mail to an internal SMTP server. Email Settings can be found under Email Server > Settings. Without the Complete Mail Server SoftPak 'Relay' is the only mode of operation. With the Complete Mail Server you must select 'Relay' from the drop down menu. Enter the IP address of the Exchange server in the Mail Server Address field. Address verification will not work if email is being relayed using a firewall redirect policy or if relay is set under the Advanced Email Settings.

Email: Settings

Email Server Settings

Server Enabled

Server Type **Relay** (dropdown menu open showing: Relay, Stand-Alone, Mirrored, Multi-Drop, ETRN, Mailbagging)

Domain Name

Trusted Networks
Only clients on listed networks are allowed to send mail without authentication.

Send Incoming Email To

Mail Server Address

Mail Server Requires Authentication

Send Outgoing Email To Relay Server (optional)
Enter server address only if you want all outbound mail directed to a single relay server.

Relay Server Address

Relay Server Requires Authentication

Advanced (highlighted button)

Apply **Cancel**

1.2 Activating SMTP Address Verification

Next, enable SMTP Address Verification. Choose Address Verification under Email settings and enable 'SMTP via Incoming Email Server' as shown below. The InstaGate or ThreatWall will now check addresses against the mail server you specified on the settings page.

Email: Address Verification

Rejection Settings
These settings help ensure incoming email is legitimate by verifying the existence of sending and receiving users and servers.

SPF violation Enabled
Sender domain does not exist Enabled
Non-local message contains invalid headers Enabled

Local Recipient Verification Settings

SMTP via incoming email server Enabled
LDAP Enabled
Fixed addresses

Match all server domains Enabled

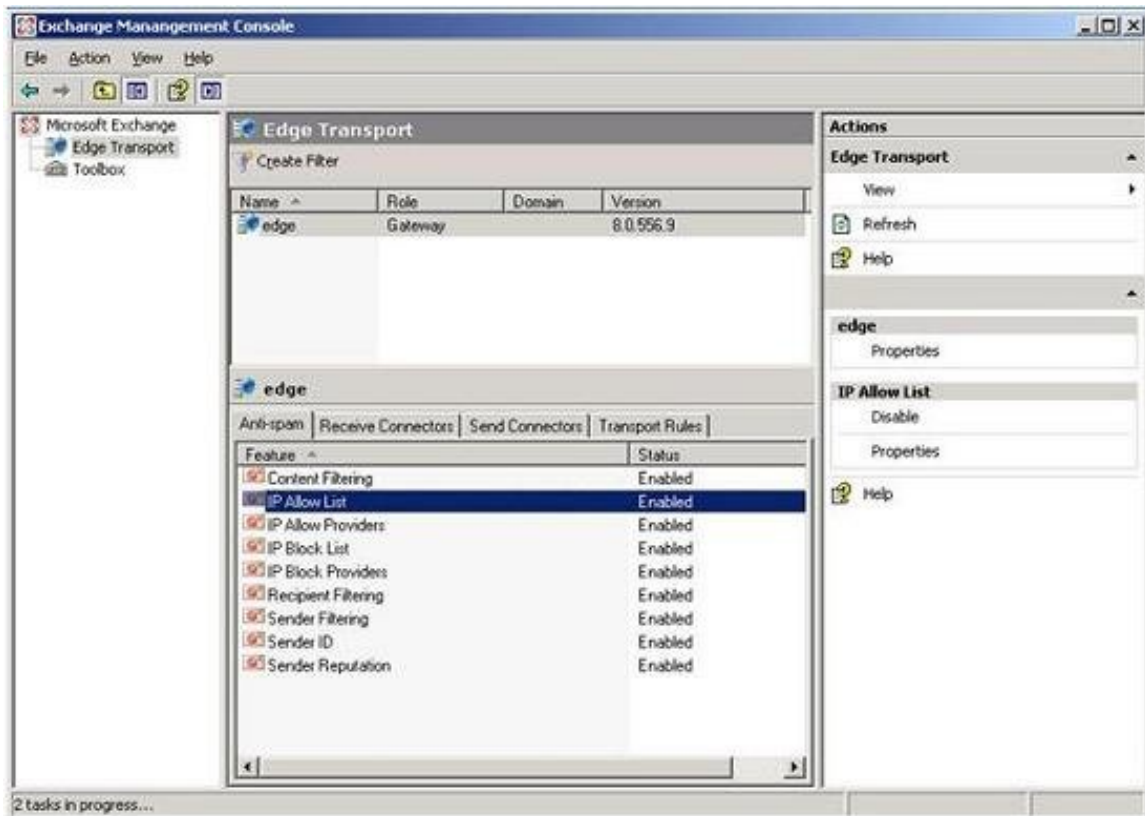
Apply Cancel

Note: Be sure to enable only one Verify Recipient setting. If you enable more than one setting, the Address Verification may not work correctly.

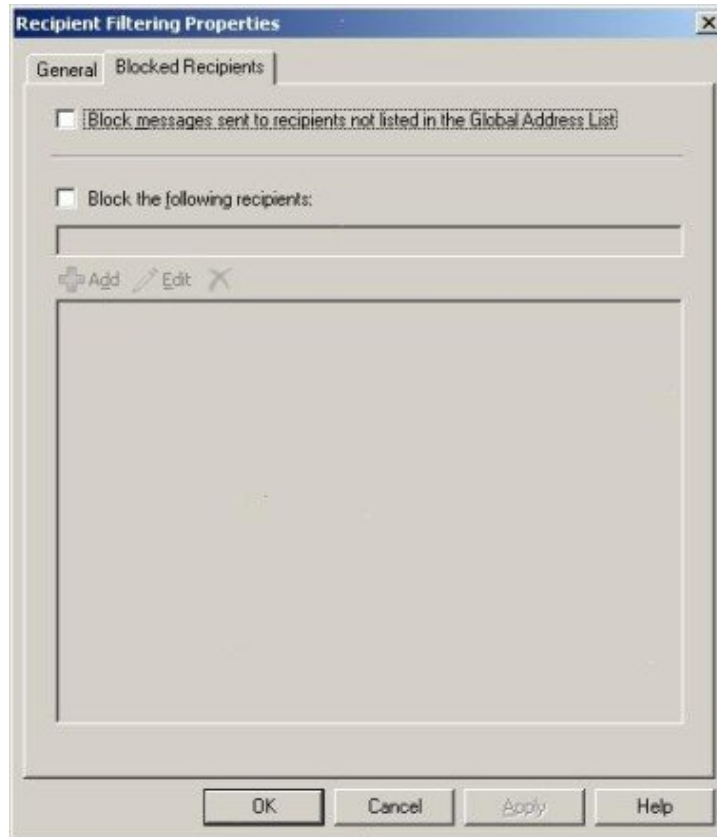
EXCHANGE CONFIGURATION WITH EDGE TRANSPORT SERVER

2.1 Enable the Recipient Filter

The recipient filter is enabled by default on servers with Edge Transport installed. If Edge Transport is not installed, skip to the next section to configure without Edge Transport. To verify the recipient filter is enabled, open the Exchange Management Console. Choose Edge Transport, and then the Anti-Spam tab.



On the Anti-Spam tab, right click the Recipient Filtering option and select Properties. Make sure the box is checked to 'Block messages sent to recipients not listed in the Global Address List'.



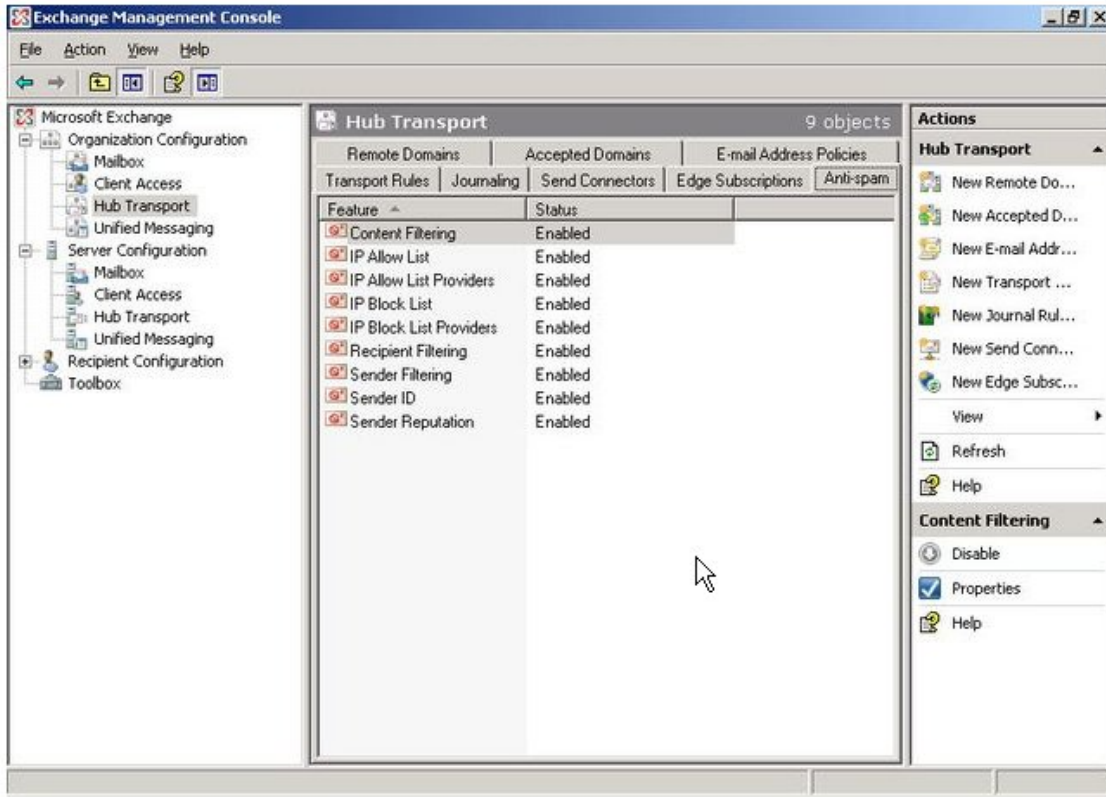
Note: The information contained in part two was taken directly from the following URL:
<http://technet.microsoft.com/en-us/library/bb125187%28EXCHG.80%29.aspx>

EXCHANGE CONFIGURATION WITHOUT EDGE TRANSPORT SERVER

3.1 Anti-Spam Agents

On servers without Edge Transport installed, Hub Transport is used. The Anti-Spam agents are not installed by default and recipient filtering is not enabled. To find out if the Anti-Spam agents are installed open the Exchange Management Console. Choose Hub Transport, and locate the Anti-Spam tab.

If there is an Anti-Spam tab proceed to step 3.3 to enable the recipient filter. If there is no Anti-Spam tab, follow the directions in section 3.2 to install the Anti-Spam Agents first.



3.2 Anti-Spam Agents

To install the anti-spam features on a Hub Transport server, you must run an install script and restart the Microsoft Exchange Transport service.

- 1) Run the following shell command from the Microsoft\Exchange Server\Scripts folder:

```
./ install-AntispamAgents.ps1
```

- 2) Restart the Microsoft Exchange Transport service by running the following command:

```
Restart-Service MExchangeTransport
```

After the service restart, you should be able to reload the Exchange Management Console and view the Anti-Spam tab from the Hub Transport configuration. Please contact Microsoft technical support for further assistance if the Anti-Spam Agents are not correctly installed.

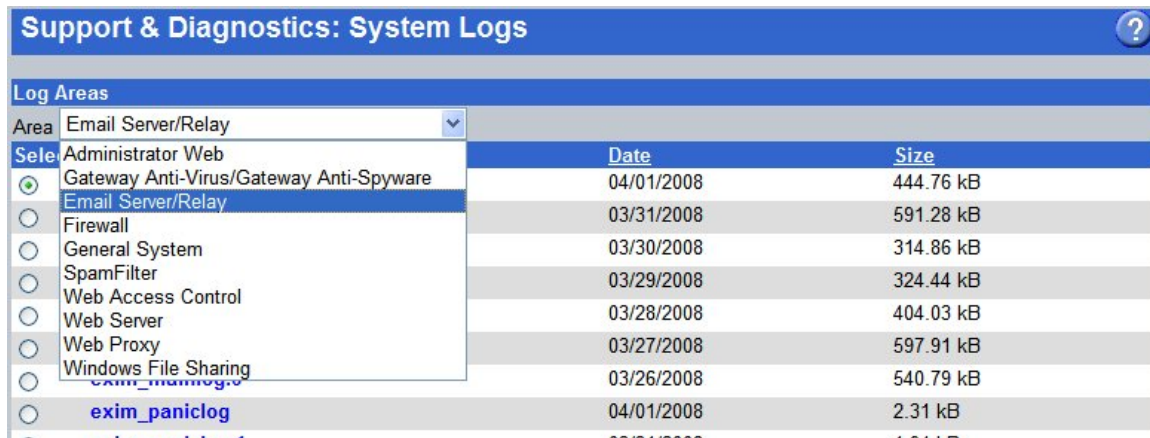
3.3 Enable the Recipient Filter

Open the Exchange Management Console. Choose Hub Transport, and then the Anti-Spam tab. Right click the Recipient Filtering option and select Properties. This properties page should look the same as in section 2.1. Check the box labeled 'Block messages sent to recipients not listed in the Global Address List'.

Note: The information contained in part three was taken directly from the following URL:
<http://technet.microsoft.com/en-us/library/bb201691.aspx>

TROUBLESHOOTING

If you are still receiving messages to invalid users, check the email server logs on your InstaGate or ThreatWall to determine if email is being rejected due to 'Unknown local part'. These logs can be found under Support and Diagnostics->System Logs for an InstaGate, and Reports & Logs->System Logs for a ThreatWall. Similar information can also be obtained from the ThreatMonitor.



Area	Date	Size
Administrator Web	04/01/2008	444.76 kB
Gateway Anti-Virus/Gateway Anti-Spyware	03/31/2008	591.28 kB
Email Server/Relay	03/31/2008	591.28 kB
Firewall	03/30/2008	314.86 kB
General System	03/29/2008	324.44 kB
SpamFilter	03/29/2008	324.44 kB
Web Access Control	03/28/2008	404.03 kB
Web Server	03/27/2008	597.91 kB
Web Proxy	03/27/2008	597.91 kB
Windows File Sharing	03/26/2008	540.79 kB
exim_mainlog	04/01/2008	2.31 kB
exim_paniclog	04/01/2008	2.31 kB

After selecting the Email Server/Relay logs, choose either the exim_mainlog or the exim_rejectlog. Once the log file has opened, look for the keywords "rejected RCPT" or "Unknown local part." You should see a log entry similar to the one below confirming that recipient verification is working.

```
2008-04-01 00:00:41 H=(3.142.76-86.rev.gaoland.net) [86.76.138.222]
F=<lleksak_1983@CHCBEIRA.MIN-SAUDE.PT> rejected RCPT <cks@testdomain.com>: Unknown local
part cks in <cks@testdomain.com>
```

For faster performance, the InstaGate or ThreatWall stores all successful verifications in a call-out cache. If the InstaGate or ThreatWall was not verifying recipient addresses correctly due to an improper setup, a bad address may be cached. Email addresses will remain cached for up to 4 hours.

If you still having problems setting up address verification after completing the previous steps please open a ticket with eSoft Technical Support at 877-754-2986 or online at <http://support.esoft.com>.