Configuring AntiSpam Features for Exchange Server 2010

Overview

Exchange 2010 has a variety of tools available for reducing spam messages to an organization. Traditionally, schools have had the options of using either the State Spam Filter as a filtering method, or using third-party devices. Each has its benefits and drawbacks: the State Filter, while offered at no charge, offers no options for customization or fine-tuning, and third-party filters add to the overhead costs of the technology department while at the same time offer many options for customization.

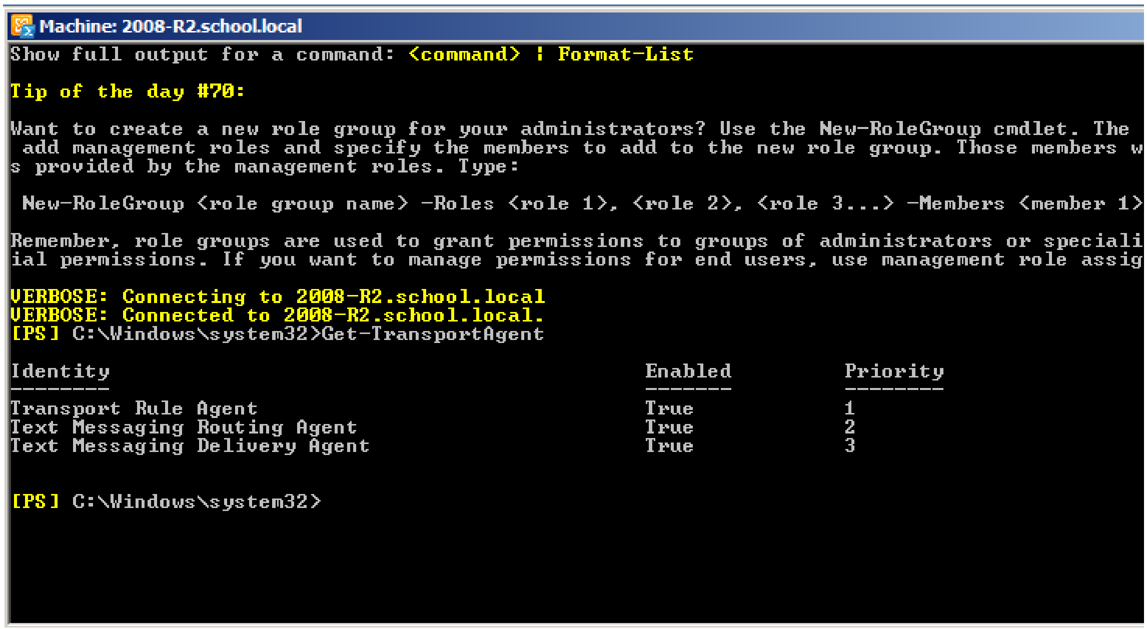
By installing and utilizing the Exchange Anti-Spam agents, you can gain both the flexibility that third-party options offer while at the same time cutting costs once allocated to filtering.

Installation

While the anti-spam agents are always installed by default on Edge Servers, most schools tend to use a single server that provides both edge connectivity to the Internet and hub services for delivering mail to users. On these single-server installations, the agents are NOT installed by default. To check if the AntiSpam agents are installed and enabled on the server, open Exchange Management Shell and type:

Get-TransportAgents

If the AntiSpam agents are not installed (by default) you will see the following output:

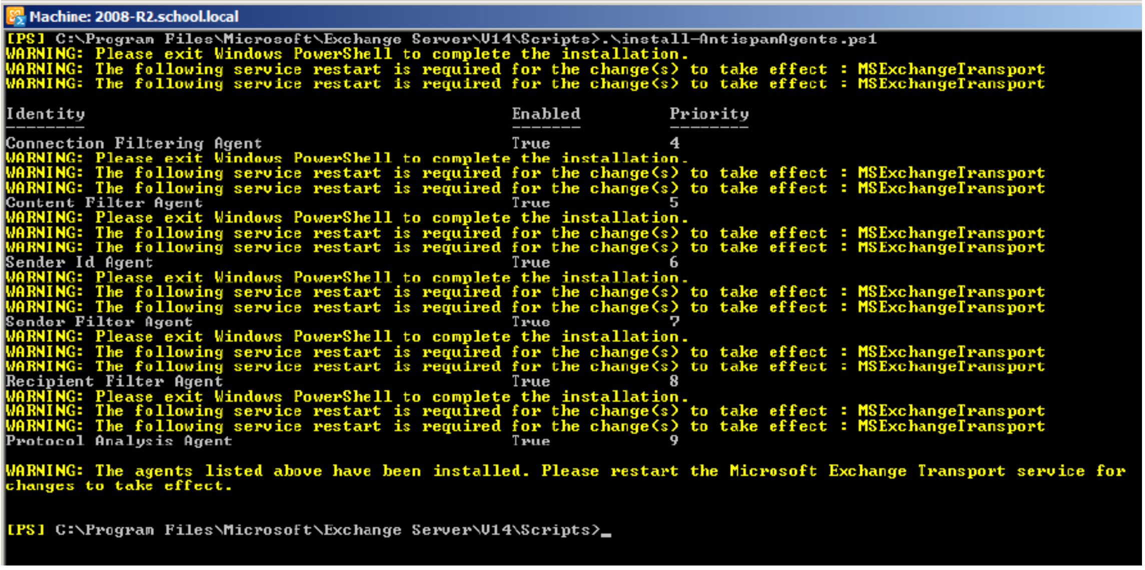


Machine: 2008-R2.school.local

```
Show full output for a command: <command> | Format-List

Tip of the day #70:

Want to create a new role group for your administrators? Use the New-RoleGroup cmdlet. The
 add management roles and specify the members to add to the new role group. Those members w
s provided by the management roles. Type:

 New-RoleGroup <role group name> -Roles <role 1>, <role 2>, <role 3...> -Members <member 1>

Remember, role groups are used to grant permissions to groups of administrators or speciali
ial permissions. If you want to manage permissions for end users, use management role assig

VERBOSE: Connecting to 2008-R2.school.local
VERBOSE: Connected to 2008-R2.school.local.
[PS] C:\Windows\system32>Get-TransportAgent

Identity                                          Enabled         Priority
--------                                          -------         --------
Transport Rule Agent                              True            1
Text Messaging Routing Agent                      True            2
Text Messaging Delivery Agent                     True            3


[PS] C:\Windows\system32>
```

To install the agent, you will need to open the Exchange Management Shell and navigate to the **Scripts** directory in your Exchange installation folder (**Program Files\Microsoft\Exchange Server\V14**) and then execute the following command:

./Install-AntiSpamAgents.ps1



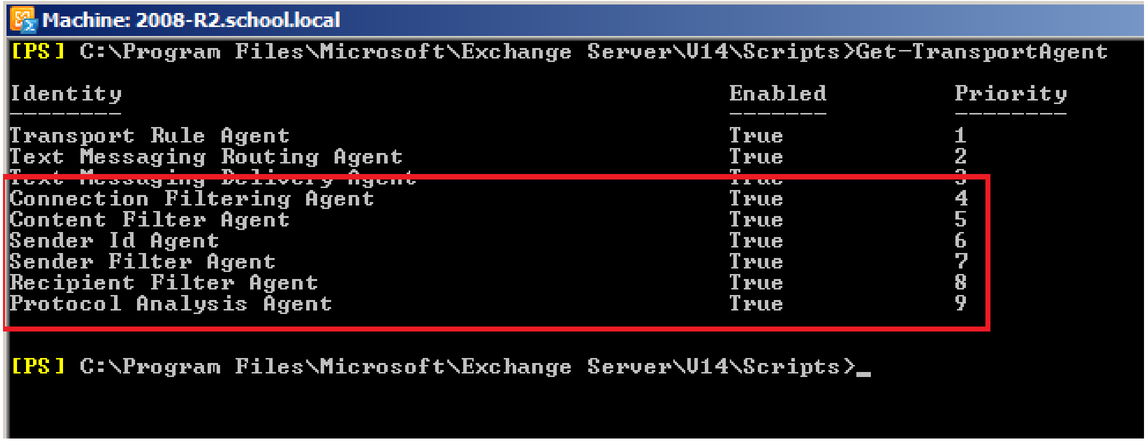
```
[PS] C:\Program Files\Microsoft\Exchange Server\V14\Scripts>.\install-AntispamAgents.ps1
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport

Identity                                                   Enabled          Priority
--------                                                   -------          --------
Connection Filtering Agent                                 True             4
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
Content Filter Agent                                       True             5
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
Sender Id Agent                                            True             6
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
Sender Filter Agent                                        True             7
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
Recipient Filter Agent                                     True             8
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
Protocol Analysis Agent                                    True             9

WARNING: The agents listed above have been installed. Please restart the Microsoft Exchange Transport service for
changes to take effect.

[PS] C:\Program Files\Microsoft\Exchange Server\V14\Scripts>_
```

When the script completes, it will prompt you to restart the Microsoft Exchange Transport Service. This can be accomplished with the following command:

Restart-Service MSExchangeTransport

Once the service is restarted, close the Exchange Management Shell and re-launch it for the changes to take effect.

To check if the AntiSpam agents are installed and enabled on the server, open Exchange Management Shell and type **Get-TransportAgent**. The output should show all the AntiSpam agents installed and enabled.



```
[PS] C:\Program Files\Microsoft\Exchange Server\V14\Scripts>Get-TransportAgent

Identity                                            Enabled         Priority
--------                                            -------         --------
Transport Rule Agent                                True            1
Text Messaging Routing Agent                        True            2
Text Messaging Delivery Agent                       True            3
Connection Filtering Agent                          True            4
Content Filter Agent                                True            5
Sender Id Agent                                     True            6
Sender Filter Agent                                 True            7
Recipient Filter Agent                              True            8
Protocol Analysis Agent                             True            9


[PS] C:\Program Files\Microsoft\Exchange Server\V14\Scripts>_
```

Now we will add the Server list which is bound to receive email (Internal SMTP Servers) using the following command:

```
Set-TransportConfig  -InternalSMTPServers  @{Add="165.29.108.2”,”10.10.10.1"}
```

Use IP addresses assigned to your Exchange server rather than the example above.

With this, the services are installed, and are ready to be configured. Before doing so, it is important to understand the order in which the filters are applied:

Regarding Filtering Order

Exchange filters apply in a specific order. Understanding this order will make it easier to troubleshoot how seemingly whitelisted e-mails are getting blocked. Filtering occurs in this order:

1. Connection Filtering: This includes the IP Block List and the IP Allow List
2. Sender Filtering: This includes blocking and/or whitelisting by the sender's domain name.
3. Recipient Filtering: This can be used to block mail that is sent to invalid addresses, saving server resources, as well as blocking mail from outside from going to certain users.
4. Sender ID Filtering: This includes SPF record checks, which are records in the DNS records associated with the sender's alleged domain. If present, an SPF record gives a list of servers authorized to send mail on their behalf. Mail from unauthorized sources, such as a spoofed server, can be eliminated.
5. Content Filtering: Along with the possibility of filtering out unwanted attachment types (such as executables), this portion of the filtering also uses information from Microsoft as well as from the domain's users to decide how to grade mail as 'junk' or 'not junk'. This generates a Spam Confidence Level for each message on a scale of 0-9, with the higher numbers representing the most suspicious messages.

Configuration of the Filtering Agents

Connection Filtering

Open the Exchange Management Console (EMC). Navigate to **Organization Configuration > Hub Transport**, then choose the tab marked **Anti-Spam**.

First, as the state spam relay is critical for communications from other districts as well as ADE, you will want to whitelist the state relay addresses. Choose **IP Allow List**. In the Action Pane to the right of the screen, choose **Enable** if it is not already enabled.

To add IP numbers in the allowed list type open Exchange Management Shell and type:

Add-IPAllowListEntry -IPRange 165.29.1.14-165.29.1.15

To check to make sure the entry was successfully added, type the following command in the Exchange Management Shell:

Get-IPAllowListEntry

This is also similar to the process needed if it is necessary to block a single IP address or block of addresses from sending mail to your server. However, it is recommended to instead use a blacklist provider, such as Spamhaus or Sorbs.

As the settings for blacklists differ from provider to provider, it is important to consult the vendor for the settings to be used. If using blacklists, it is especially important to whitelist the state mail relay (*see above*) as it is vulnerable to being blacklisted due to the quantity of mail that is processed by it.

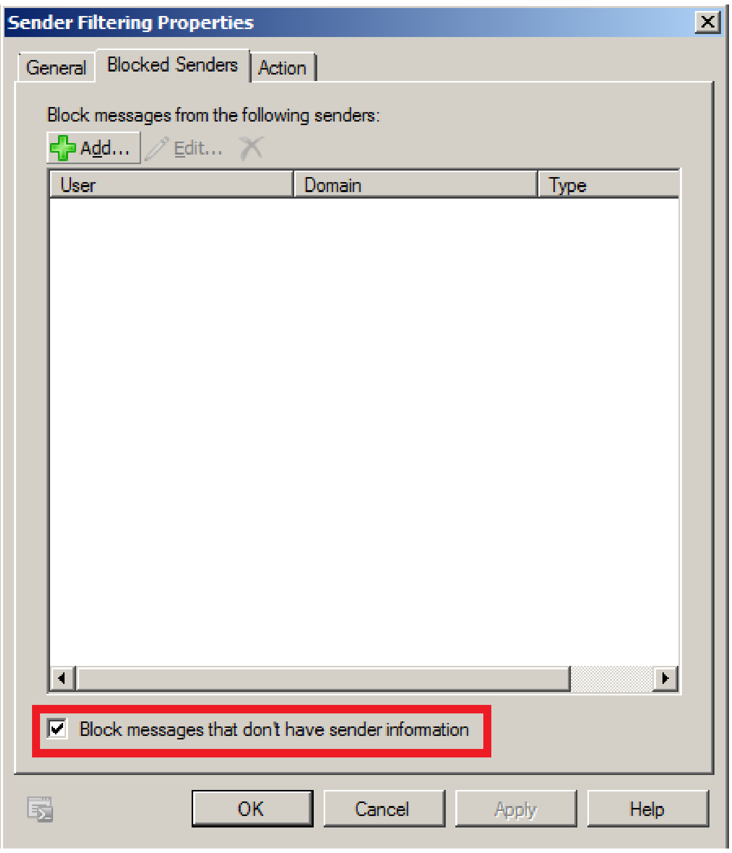
Sender Filtering

Open the Exchange Management Console (EMC). Navigate to **Organization Configuration > Hub Transport**, then choose the tab marked **Anti-Spam.** Select **Sender Filtering**, then choose Enable from the action pane on the right side of the screen.

In the main pane, right-click on **Sender Filtering** and choose **Properties.**

You may then add individual addresses, individual domains, or individual domains including subdomains, depending on your needs.

One that is highly recommended is **Block Messages that do not include Sender Information**.



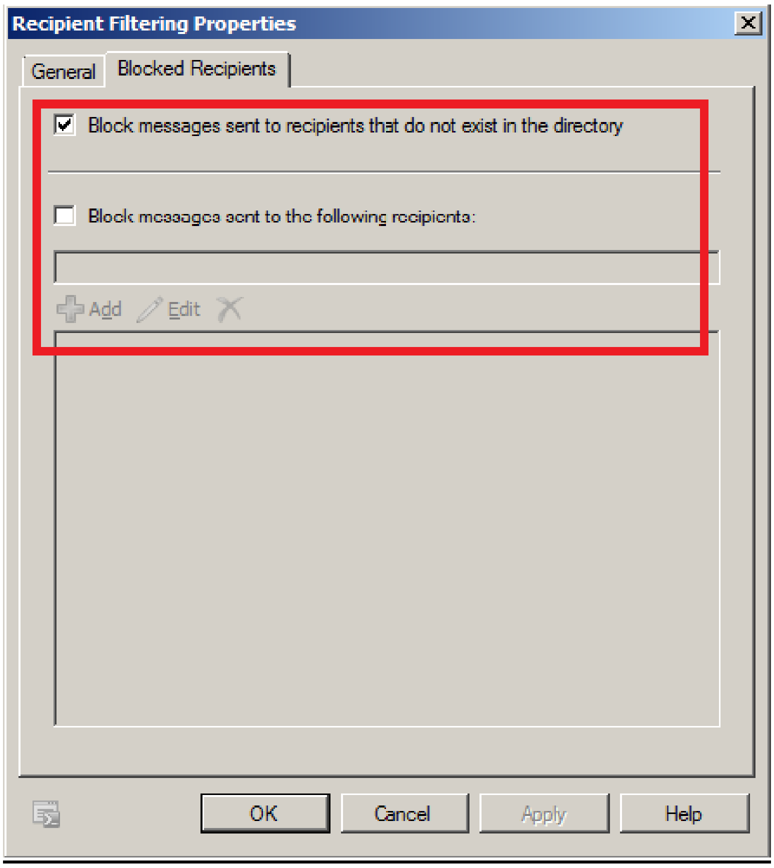
Block messages from the following senders:

☑ Block messages that don't have sender information

Once this is set, you can choose what to do with the messages from these senders under the **Action** tab. Our recommendation is to deny messages that do not include sender information, then stamp the messages from blocked addresses. These marks will be used by Exchange AntiSpam to calculate the likelihood of this message being spam.

Recipient Filtering:

Again, this is enabled the same way as the other types above, and the settings are configured similarly. Unfortunately, there are some drawbacks to using this for limiting student access to e-mail, namely that the list is not configured against organizational units, but instead each address must be typed manually, and there is a limit of 800 users.



☑ Block messages sent to recipients that do not exist in the directory

☐ Block messages sent to the following recipients:

Sender ID Filtering:

The recommended settings for the Sender ID action for spoofed messages is to **Stamp the Message with the Sender ID result and continue processing**. These will be used to help Exchange make an intelligent decision on whether or not the message is spam.

NOTE: If you need to exempt a specific domain for this, you will need to use the following command in the Exchange Management Shell:

```
Set-SenderIDConfig -BypassedSenderDomains domaintowhitelist.com
```

Content Filtering:

The content filtering may likewise be used to block e-mails containing specific keywords. It is recommended that this be used cautiously.

Enabling Attachment Filtering (Only on Edge Role):

Attachment filtering, unfortunately, cannot be managed by the Exchange Management Console, and instead must be done from the Exchange Management Shell.

To enable it, open the Exchange Management Shell and use the following commands:

```
Enable-TransportAgent -Identity "Attachment Filter Agent"

Set-AttachmentFilterListConfig -Action -Reject -RejectResponse "This message was
rejected due to an unaccepted attachment.  Please remove the attachment and retry."
```

Once these are in place, Exchange is ready to accept filter entries for the types of files to be blocked. This can be done by file extension or by MIME type. For example, to block all EXE files by extension:

```
Add-AttachmentFilterEntry -Name *.EXE -Type FileName
```

Of course, this only blocks users from sending files with the EXE extension on them, and is often circumvented by changing the filename accordingly. However, this can be circumvented by using the MIME type instead. These are available with a quick web search.

This example will block all JPEG images and executables, regardless of the actual extension used:

```
Add-AttachmentFilterEntry -Name image/jpeg -Type ContentType
Add-AttachmentFilterEntry -Name application/octet-stream –Type ContentType
```