

Using Exchange Management Shell to Configure Content Filtering

A Curious thing about Exchange Server 2007 is that the Exchange Management Console was built on top of the Exchange Management Shell. therefore, anything that you can do through the console can also be done from a command line. For the most part, I have always preferred to use a graphical user interface to accomplish administrative tasks in windows, and yet in Linux I always prefer the shell for practicality reasons and now windows has found a reason to shell!

For example, it's easy to think of content filtering as a set it and forget it proposition. However, some organizations may find themselves constantly making adjustments to the content filters as the spam flow dictates. If an organization happens to have a lot of servers, then fine tuning the spam filters can turn into a really big job. Fortunately, Exchange Server 2007 makes it relatively easy to create a script that you can use to set up content filtering on a server. In this article, I will show you how. Before I Begin Before I get started, I just want to quickly mention that Exchange Server 2007 offers an extensive number of anti spam mechanisms. As such, there is no way that I can possibly cover all of them within the confines of an article. As such, I'm going to show you some of the basic techniques that you can use to configure content filtering from the command line. Viewing the Current Configuration The first thing that you'll probably want to do is to get an idea of how the servers are configured right now. To do so, just enter the following command into the Exchange Management Shell: `Get-ContentFilterConfig` When you do, you will see a summary of all of the content filter settings, as shown in Figure A. Figure A - The `Get-ContentFilterConfig` command allows you to see the current state of the content filter Setting the Content Filter Configuration Just as the `Get-ContentFilterConfig` command allows you to see the status of the content filter, the `Set-ContentFilterConfig` command allows you to make modifications to the content filter configuration. Of course you have to know which content filtering mechanism you want to configure. Even so, the filtering process is fairly easy. If you look at Figure A, you will notice that when I entered the `Get-ContentFilterConfig` command, Exchange listed a number of different content filtering attributes, and the values associated with them. Any of these attribute names can be used in conjunction with the `Set-ContentFilterConfig` command. For example, if you look at Figure A, you will notice that the `BypassedSenderDomains` option is set to `Microsoft.com`. I tend to get a lot of e-mail from Microsoft, so I wanted to configure Exchange 2007's content filtering so that it would not scrutinize any of the messages that are coming from `Microsoft.com`. To Add `Microsoft.com` to the `BypassedSenderDomains` list, I used the following command: `Set-ContentFilterConfig –BypassedSenderDomains Microsoft.com` That works well enough, but what happens if all of a sudden you decide that you don't trust messages from Microsoft and want to remove `Microsoft.com` from the `Bypassed Sender Domain` list? Well, here is where things get tricky. The Exchange Management Shell works by allowing you to enter commands in a verb-noun format. One of the most commonly used verbs is `Remove`, so it would therefore stand to reason that you could enter the following command: `Remove-ContentFilterConfig –BypassedSenderDomains Microsoft.com` For many of the Exchange Management Shell commands, this reasoning would be perfectly valid. However, Microsoft decided to limit the verbs that can be used with the `ContentFilterConfig` command as a way of simplifying things. As such, the `Remove` command is invalid. The easiest way to clear the `Bypassed Sender Domain` list is to replace `Microsoft.com` with something else. For example, you might replace `Microsoft.com` with the word `null`. `Null` doesn't really have any meaning to Exchange in this context, but using it will replace `Microsoft.com` with an invalid domain name, thus accomplishing your goal. That technique works great if you only add a single domain to the `BypassedSenderDomain` list, and then decide to remove it. In real life though, you will probably have several sender domains that you want to bypass. When you start working with multiple sender domains things get a bit trickier. The reason for this is that you can't just re-issue the `Set-ContentFilterConfig` command every time you want to add a `BypassedSenderDomain`, because doing so will cause the current list to be overwritten. Likewise, you can't use the `Add-ContentFilterConfig` command, because Microsoft has disallowed the use of the `Add` verb. The trick to being able to add and remove domains from the `BypassedSenderDomain` list is to make use of variables.