

How do I add a new message filter to my Cisco Email Security Appliance (ESA)?



Document ID: 118145

Contributed by John Yu and Stephan Bayer, Cisco TAC Engineers.

Aug 05, 2014

Contents

Message filters allow you to create special rules describing how to handle messages and attachments as they are received. Message filters are applied earlier in the Email Pipeline than content filters and before message splintering occurs. Message filters are particularly useful when you want to skip Anti-Virus and Anti-Spam, which occur before Content Filters in the Email Pipeline, or to apply actions to a broad range of messages, such as all messages crossing a particular listener. A message filter is comprised of a filter name, filter rule, and at least one filter action. Message filters can be written using a text editor and imported or pasted directly using the `filters` command from the ESA Command Line Interface (CLI).

Below is an example showing how paste a filter using the ESA CLI.

```
mail.example.com> filters
```

```
Choose the operation you want to perform:
```

- NEW - Create a new filter.
 - IMPORT - Import a filter script from a file.
- ```
[]> new
```

```
Enter filter script. Enter '.' on its own line to end.
```

```
example: if (mail-from == user@example\\.com$) {
bcc ('admin@example.com');
deliver();
.
1 filters added.
```

```
mail.example.com>commit
```

**Note** – Use the `commit` command to apply the filter once it has been added.

For more information about message filters, see the Advanced Configuration Guide.