Include and Exclude Rules

You can use **include** and **exclude processing rules** to specify what data is sent to Sumo Logic.

- An exclude rule functions as an allowlist filter where the matching data is not sent to Sumo Logic.
- An include rule functions as a denylist filter where only matching data is sent to Sumo Logic.

As a best practice, specify these rules to match the lesser volume of data.

- If you want to **collect the majority of data** from the Source’s path provide **exclude** rules to match (filter out) the lesser volume of data.
- If you want to **collect a small set of data** from the Source’s path provide **include** rules to match (filter in) the lesser volume of data.

For example, to include only messages coming from a Cisco ASA firewall, you could use the following:

```
Name: Cisco ASA firewall messages
Filter: .+ASA.-d.-d.(\w+) +
Type: Include messages that match
```

Rules and Limitations

When writing regular expression rules, you must follow these rules:

- Your rule must be **RE2 compliant**.

- Your rule must match the **entire message**, from the start to the end of any log message rather than addressing only a section.

- For **single line messages**, you must prefix and suffix the regex expression with .* if the matching string pattern is not at the beginning or end of the line. For example, if you want to exclude any message containing the words "secure" or "security", write the rule:

  ```
  .*secur.*
  ```

- For **multiline messages**, add single line modifiers (?s) to the beginning and end of the expression to simplify
matching your string, regardless of where it occurs in the message. For example, if you want to exclude any Windows Event message containing the Event Code 5156, write the rule like this:

```
(?s).*EventCode = 5156.*(?!s)
```

- Syslog UDP messages may contain a trailing newline character, which will require the above regular expression to properly match your string.

- Exclude rules take priority over include rules. Include rules are processed first, however, if an exclude rule matches data that matched the include rule filter, the data is excluded.

- If two or more rules are listed, the assumed Boolean operator is OR.

- The processing rule name must be less than 32 characters.

- A rule will process single line log messages until 1MB of data is processed and multiline log messages until 2,000 lines or 512KB of data is processed, whichever comes first. Once these limits are reached the processing rule will ignore the rest of the log message and move on to the next log.