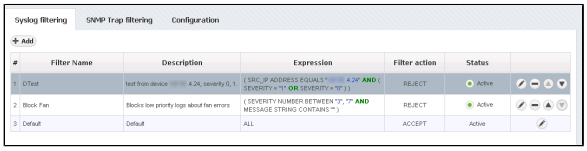
Filtering Settings (ELA)

Syslog Filters are used to make explicit rules to filter out unwanted syslog messages. Filtered out messages will not be processed, stored and showed in the EventLog charts and tables. To access Syslog Filters, go to blocked URL **> Settings > EventLog Settings > Syslog filtering**.



By default, there is only one Syslog Filter named Default that accepts all syslog messages. On the Figure 15: Syslog Filter Table you can see Syslog Filter list together with some filter examples. As you can see, each filter has:

1. Filter number
2. Description
3. Filter expression – condition for the filter expressed in text format
4. Filter action - reject or accept messages that match filter expression
5. Status – filter can be active or inactive

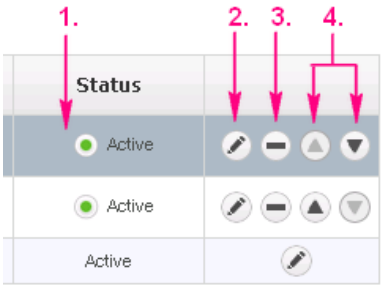
Looking at the second filter named “Block Fan” you can see that it is used to block (reject) fan related logs (log message contains the word “fan”) of low priority (severity levels between 3 and 7) from any device.

Filter table is ordered which means that filters are applied in the order of the table: filter with the filter number 1 will be applied first, then rest will follow. Note that default filter is always the last one to be applied.

Ordering and Default filter allows you to have two filter strategies:

- Explicit reject: default filter accepts all messages, filters reject specific messages
- Explicit accept: default filter rejects all messages, filters accept specific messages

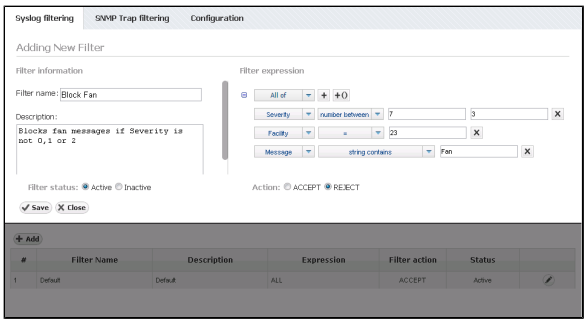
> ⚠ Default filter is always active, always the last to be applied, and the only change you can make to it is to change its Filter action (to accept or reject all messages).



Filter table has several quick options:

1. To make a filter active/inactive, click the Inactive/Active icon
2. To edit filter, click the edit icon or double click on the filter table row
3. To remove filter, click remove icon
4. To change the position of the filter in the table, use the Up and Down icons

To Add a new filter, click the Add button at the top of the Filter table.



Filter expression is a set of conditions that need to be met in order for filter action to be triggered. Condition are based on the Syslog message severity, facility, message content or device(s) that sent it (based on source IP address). Each condition type has several condition operands depending on the possible values, for instance Severity has options >, <, =, !=, >=, <= and “between” operands.

The conditions are added by clicking on the “+” icon and composite conditions are added by clicking on the “+()“ icon. Composite conditions will appear in the filter expression in the brackets, and are generally used if you need a condition in the form of Cond1 AND (Cond2 OR Cond3).

Logical operator between condition are set by the drop-down list next to “+” and “+()” options: Match All (AND), Match Any (OR), Match None (NAND).

By default, filter action is set to Accept and filter status to Active.