

System Logging Fields

In VTA Configuration Manager, you can edit the following fields in the syslog section of the Logging screen.

Filter

- Filter that determines the type of messages that this log file contains.
- Value—Expression. The software filters events by evaluating each subexpression from left to right. When the software finds a match, it logs or ignores the message accordingly. You can specify an unlimited number of subexpressions. The order in which you specify the subexpressions affects the result. Expressions have the format:

singlematch [,singlematch]

where

singlematch—[!] (< category > | ([< category >]/[< severity >] |
[< minimumSeverity >]-[< maximumSeverity >]))

- !—Do not log matching events
- < category > —SRC component that generated the event message. To log only events in a specific category, you can define the category, which is a text string that matches the name of a category. The text string is not case sensitive. For the names of categories, view a log file for a default filter. Juniper Networks Technical Assistance Center (JTAC) can also provide category names.
- [< severity >] | [< minimumSeverity >]-[< maximumSeverity >] —Name or number in the range 1–127. A higher number indicates a higher severity level. Table 1 on page 1 shows common severity levels that you can specify by name.

Table 1: Named Severity Levels

Name	Severity Level
logmin	1
debug	10
info	20
notice	30
warning	40
error	50
crit	60
alert	70

Table 1: Named Severity Levels *(continued)*

Name	Severity Level
emerg	80
panic	90
logmax	127

Enabling debug log messages has a negative affect on system performance. Do not enable debug log messages unless JTAC instructs you to do so.

You can define a severity level as follows:

- Specify an explicit severity. For example:
warning—Defines only warning messages
- Specify a minimum severity and a maximum severity. For example:
info-warning—Defines messages of minimum severity level of info and a maximum severity level of warning
- Accept the default minimum (logmin) or maximum (logmax) severity by omitting the minimum or maximum severity. For example:
info—Defines messages of minimum severity level info and maximum severity level logmax

-warning—Defines messages of minimum severity level logmin and maximum severity level warning

- Specify no severity to log all event messages.
- Guidelines—This field is mandatory.
- Default—No value
- Example—Table 2 on page 3 shows some examples of filters.

Table 2: Examples of Filters for Event Messages

Syntax	Event Messages Saved
/	All event messages
/info-	Event messages of level info and above from all categories
vta/debug	Debug events from the VTA category only
!vta,/debug	All debug events except those from the VTA category
!VtaMsg/info-,vtaMsg,vta	All messages from the VTA category, except those from VtaMsg category with level less than info

Syslog Host

- IP address or name of a host that collects event messages with a standard system logging daemon.
- Value—IP address or text string
- Default—No value

Syslog Facility

- Type of system log in accordance with the system logging protocol.
- Value—Integer in the range 0–23; each integer corresponds to the standard number for a system logging client. See The syslog Protocol—draft-ietf-syslog-protocol-16.txt (July 2006 expiration).
- Default—No value

