

Configuring Log Suppression

You can configure log suppression if you want to reduce the number of logs displayed in the NSM log viewer. If you enable log suppression, NSM displays a single record for multiple occurrences of similar events, along with a count of all such occurrences.

To enable and configure log suppression:

1. In the NSM Device Manager, double-click the IDP device to display the configuration editor.
2. Click **Sensor Settings**.
3. Click **Load-Time Parameters**.
4. Complete the settings related to log suppression using Table 1 on page 1.

Table 1: IDP Configuration: Log Suppression Settings

Setting	Description
Enable log suppression	Log suppression is enabled by default. Use this setting to turn log suppression off and on.
Include destination IPs when performing log suppression	When log suppression is enabled, multiple occurrences of events with the same source IP, service, and matching attack object generate a single log record with a count of occurrences. If you enable this option, log suppression combines log records for events with the same destination IP.
Number of log occurrences after which log suppression begins	This number represents the number of identical log records received before suppression starts. The default is 1 (meaning log suppression begins with the first redundancy).
Maximum number of logs that log suppression can operate on	When log suppression is enabled, IDP must cache log records so that it can identify when multiple occurrences of the same event occur. This number represents the number of log records in the IDP Management Server that IDP tracks for log suppression. The default is 16384 log records.
Time (seconds) after which suppressed logs will be reported	When log suppression is enabled, the IDP device maintains a count of multiple occurrences of the same event. This number represents the number of seconds that pass before IDP reports a single log entry containing the count of occurrences. The default is 10 seconds.

- Related Topics**
- NSM Logs and Reports Overview
 - Configuring Syslog Collection (NSM Procedure)

