

## Configuring Load-Time Parameters (NSM Procedure)

Load-time parameters include options for tuning IDP performance. In general, you modify these settings only if you encounter performance issues. These options control the security module functions when it first powers on.

To configure load-time parameters:

1. In NSM Device Manager, double-click the IDP device for which you want to configure load-time parameters. The device configuration editor appears.
2. Click **Sensor Settings**.
3. Click the **Load Time Parameters** tab.
4. Configure load-time parameters using Table 1.
5. Click **Apply**.
6. Click **OK**.

**Table 1: IDP Device Configuration: Load Time Parameters**

Setting	Description
Flow table size (requires sensor restart)	For improved IDP performance, set the flow table size to limit the size of the connection table. This setting should reflect the maximum number of concurrent flows you expect to have at any one time. A TCP connection has about two flows per session, and a UDP connection has about three flows per session. The default setting is 100,000 concurrent flows. If you change this value, you have to restart the IDP device.
Enable log suppression	Log suppression reduces the number of logs displayed in the Log Viewer by displaying a single record for multiple occurrences of the same event.  <b>NOTE:</b> If the reporting interval is set too high, log suppression can negatively impact IDP performance.
Include destination IP's while 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 16,384 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.
Enable application identification	The application identification feature is used to detect the session application regardless of port. We recommend you disable this feature only when troubleshooting.

**Table 1: IDP Device Configuration: Load Time Parameters** (continued)

Setting	Description
Maximum number of Application Identification sessions	Specifies the maximum number of sessions where application identification is in use. The default is 100,000. Valid values are 0 - 200,000. We recommend you tune this setting only if you encounter issues.
Enable policy sharing	This option allows two CPUs on a security module to share a policy. This enables the policy with all attacks to withhold maximum memory. Also the memory usage increases while the attacks database grows.

- Related Topics**
- Pushing Security Policy Updates to an IDP Device (NSM Procedure)
  - Troubleshooting Configuration Push Errors (NSM Procedure)
  - Configuring Run-Time Parameters (NSM Procedure)

---

Published: 2009-08-20