

## Capturing SNMP Secure Audit Logs

---

SNMP secure audit logging enables administrators to collect the SNMP audit logs for mirror traps and Mirror-MIB get/set operations with the protection of the mirror enabling feature. Secure audit logging facilitates the debugging of issues related to SNMP packet mirror traps.

All normal SNMP console and syslog audit logs (including snmpTrap, snmpPduAudit, and snmpSetPduAudit) for secure traps and Mirror-MIB are suppressed due to security concerns. When you have issued the **mirror enable** command, you can issue the **snmp secure-log** command to capture secure audit logs. Configuration, storage, and display of the SNMP secure logging is on global basis rather than a per-VR basis.

The SNMP agent captures and stores the audit logs for secure traps. The SNMP agent also captures PDU audit logs for Mirror-MIB operations. Configure the snmpTrap, snmpPduAudit, and snmpSetPduAudit logs at the proper severity level to capture the secure audit logs.

You can use the **show snmp secure-log** command to display the captured secure logs. Secure logs are stored in a string format similar to SNMP trap audit logs. You can use the **snmp-server clear secure-log** command to reset the secure logs.

The secure log configuration and data are not persistent. Secure audit logs are not available after a warm or cold restart of the SNMP agent, because the SNMP agent does not store the secure logs in NVS. The SNMP agent can store a maximum of 100 secure logs before overwriting the logs.

To enhance security, you can configure and display the secure audit logs only through the CLI. You cannot use SNMP to configure and display the logs. Secure trap logs are not populated in the notification logs MIB. From the perspective of the notification log MIB, secure traps do not exist.

- Related Topics**
- snmp-server clear secure-log
  - snmp-server secure-log
  - show snmp secure-log
  - show snmp trap

