

Data integrity techniques and security measures adopted by EventLog Analyzer for the PCI DSS

Requirement 10.5 of the PCI DSS states that the audit trails must be secure and tamper-proof. Integrity of log data is important to ensure there is reliable event information available to conduct a forensic investigation.

EventLog Analyzer has several mechanisms to ensure that the security and integrity of log data is maintained at every stage of the log management process. This document elaborates the data integrity methods adopted by EventLog Analyzer to secure log data that is collected, processed, and archived.

Log collection

- **Secure and reliable log collection:** Secure communication protocols - WMI/DCOM, TLS, and HTTPS (HTTP secured with SSL/TLS) are used to ensure protection of data. Reliable delivery of log messages is ensured with the TCP communication protocol. These protocols (except for WMI/DCOM) are not enabled by default and need to be configured separately.
- **Peak log volume handling:** During peak log volumes, EventLog Analyzer makes use of a 'data buffer' to store logs which exceed its threshold. These logs are processed when the log volume drops, thereby ensuring that no logs are dropped.
- **High availability:** EventLog Analyzer allows you to designate a secondary server to take over in case of primary server failure, to ensure that no log data is lost.

Other security measures

- **Secure web communication:** EventLog Analyzer is a web-based solution with a web client that can be accessed from anywhere in the network. Enabling HTTPS protocol ensures that all web communication is secure.
- **Role Based Access Control (RBAC):** EventLog Analyzer allows you to compartmentalize your data among the product's technicians. Three access levels are provided: administrator, operator, and guest, in order to limit user access and control to specific features and device information. This way, you can ensure that data is accessed only by authorized personnel.

- **Audit EventLog Analyzer technician actions:** EventLog Analyzer provides a built-in option to generate the audit trail of all user actions performed in the product. This allows you to ensure accountability within the solution itself.
- **Session termination after idle time:** The session termination requirement as stated by PCI DSS requirement 8.1.8. states, "If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session." With EventLog Analyzer, you can set up a session expiry time and if the session is idle for more than 10 minutes (which is the minimum time), then the session will be terminated. Users can change the default setting of 30 minutes for session expiry to 10 minutes by following the below steps:

1. Login to EventLog Analyzer web-console as an **admin**.
2. Navigate to **Settings tab > System Settings > Connection Settings**.
3. In the 'Session Expiry Time Field' provide value as '10'

Log archival

EventLog Analyzer ensures the integrity of archived logs with three crucial technical measures that are described below. The solution runs both log archival and analysis process in parallel. When log data is received, it is processed by the elastic search engine and is also encrypted and archived in the user specified location.

- 1 **Archive encryption:** Archived data is secured using the AES 256 encryption mechanism. To enable encryption for archived data:
 1. Navigate to **Settings > Admin Settings > Archive Settings**.
 2. Click on the **Settings** icon.
 3. Choose the **Enable** option corresponding to **Encrypt Archive Data**.
- 2 **Time-stamping:** EventLog Analyzer ensures that the log data is tamper-proof by using time-stamping techniques. To enable time-stamping for archived data:
 1. Navigate to **Settings > Admin Settings > Archive Settings**.
 2. Click on the **Settings** icon.
 3. Choose the **Enable** option corresponding to **Archive Time Stamping**.

3 Tamper detection in archived data: EventLog Analyzer has an option to detect tampered log archives. When you enable the Archive Integrity option, the solution shows the status of the archived file as Tampered if it's mishandled. To enable the archive integrity option:

1. Navigate to **Settings > Admin Settings > Archive Settings**.
2. Click on the **Settings** icon.
3. Choose the **Enable option** corresponding to **Archive Integrity**.

EventLog Analyzer's file integrity monitoring feature can be implemented on the archived log files to get instant notifications for changes made to the archived log data.

Contact support for more details

For further details, please contact support: support@eventloganalyzer.com

ManageEngine
EventLog Analyzer

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandate requirements with ease. For more information about EventLog Analyzer, visit manageengine.com/eventloganalyzer.

\$ Get Quote

↓ Download