

Alliance LogAgent for IBM i

Data Sheet



Compliance Logging for the IBM i Platform

Meet PCI, SOX, HIPAA, GLBA and other security compliance regulations for log collection and monitoring. Alliance LogAgent collects security journal (QAUDJRN), system operator, QHST, and user security messages for distribution to a syslog server, or to a Security Information Management monitoring product. Alliance LogAgent supports both syslog and Common Event Format (CEF) messages. Alliance LogAgent integrates with Alliance encryption and Internet communications solutions.

High Speed Event Management

Poor performance can consume CPU resources and slow event management, defeating your security strategy. On an entry level IBM i platform, Alliance LogAgent processed over 800 events per second with minimal impact on CPU.



Meet Compliance Regulations

Collect security system logs and transmit to a log collection server

Formats QAUDJRN Security Journal

Format to syslog (RFC3164) or Common Event Format (CEF)

Communicates Securely

Communicates with log collection servers and Security Information & Event (SIEM) solutions

High Performance

Event management protects CPU resources with high event processing speeds

Affordable Solution

Protects your investment in IBM i hardware and software

www.townsendsecurity.com

Log Collection

- System security journal QAUDJRN
- User entries in security journal QAUDJRN
- Operator message queue QSYSOPR
- QHST system log messages
- User application messages
- SNMP network management trap alerts
- Apache, Websphere, PHP, MySQL, OpenSSH and other messages with syslog-ng

Syslog-ng

- IBM i version for Apache, Websphere, PHP, OpenSSH, log collection

Storage Management

- Remote archival for QAUDJRN entries reduces System storage
- Use system management for QAUDJRN journal receivers

Communications

- Standard syslogd UDP protocol
- Syslog-ng TCP communications
- Syslog-ng TLS secure communications

Log Filtering

- Select System audit journal entries by type
- Selectively enable operator message collection

Contact Us

Townsend Security
www.townsendsecurity.com
800.357.1019
360.359.4400

API's

- Supports direct user application QAUDJRN entries
- Commands to send syslog and Common Event Format (CEF) messages
- Bindable service program for syslog message creation
- Bindable service program for ArcSight CEF message creation

Security Assessment

- Identify and report privileged users
- Identify and report privileged applications

Supported SIEM Solutions

Compatible with any SIM solution using syslog including: Symantec SIM, ArcSight ESM, LogRhythm, LogLogic LX, Alert Logic, Novell Sentinel, CrossTec Activeworx

System Requirements

- IBM i OS/400 or i5/OS V5R2 or later. Syslog-ng requires V5R4 or later

Support

- Software maintenance
- Technical support
- 24/7/365 support available
- On site installation available
- Contract services available