User Guide

XpoLog User guide is designed to help users use the different consoles of XpoLog:

- View and analyze data
- Use XpoLog Search console and search syntax
- Understand Monitors
- Use Dashboards/Applications

XpoLog Center Main Features

XpoLog features multiple modules that offer proactive analysis, problem isolation, log correlation, log analysis, log search engine, data visualization, and proactive monitoring. The solution offers the following main features:

- Advanced Logs Search Engine
- Web based Log Viewer for any log
- Comprehensive Live Data Visualization
- Logs correlation
- Logs Monitoring
- Out of the Box Errors Detection - trends, anomalies, stats, etc.
- Enterprise Security Integration

See XpoLog summary sheet for more information

See XpoLog data sheet for more information

XpoLog Center Modules

XpoLog Center includes three modules: XpoLog Apps, XpoLog Search, XpoLog Analytics and XpoLog Manager.

XpoLog Apps

XpoLog Apps centralizes the data visualization capabilities of the platform. Under each App a set of Live Dashboards can be managed to create a live visualization of the data that is managed in XpoLog. The Apps provide an easy way to manage multiple visualizations under a logical structure that makes it easier to identify issues, trends in the organization.

Accessible via the Apps tab in the main screen on the top left corner.

XpoLog Search

XpoLog Search (XpoSearch) allows you to perform centralized searches across multiple data sources. Using the XpoSearch interface, you can search all the logs in XpoLog Center, including applications, servers, network devices, and database tables. You can search values using common search syntax such as Boolean operators, wild cards, and regular expressions. Through its intuitive language, you can search specific terms, combined phrases, any text, IP addresses, numbers, and more, and then view and analyze the results, while creating monitors, filters, and reports. Advanced capabilities include complex search syntax for measuring time of events, computing averages, calculating aggregation in time bucketing, and more.

Accessible via the Search tab in the main screen on the top left corner.

XpoLog Analytics

XpoLog Analytics offers automated monitoring and problem isolation. It automatically scans the logs for errors, risks, and anomalies according to predefined rules. It generates dynamic reports and sends alerts as soon as new risks or problems are detected. Each event is mapped to a risk level according to the error message. Analytics also aggregates and computes statistics of many dimensions in the log events: the amount of events over time, type of message over time, risks, anomalies, and more. When these aggregated statistics exceed the normal thresholds, XpoLog alerts the relevant user.

Accessible via the Analytics tab in the main screen on the top left corner.

XpoLog Manager - Platform Administration

XpoLog Manager includes the administration screens for managing the information, which is covered in the Administrator Guide, as well as

several features for the end-user:

- Log Viewer – A dedicated real-time log viewer that allows basic navigation through the various logs, opening specific logs, displaying specific log records, filtering, customizing a log, and exporting a log.
- Log Monitor – A monitoring engine that verifies the logs' contents and alerts when a rule matches the log records.

Accessible via the Manager entry in the main screen on the top right corner.