

XpoLog Analytics

XpoLog provides users the ability to initiate their own investigation of problems in the system by using the Search console, Monitors, and Dashboards. However, users don't always know what to search for, and may spend valuable time investigating huge amount of data from multiple sources while troubleshooting a problem. XpoLog Analytics is a proactive console that helps users to see all problems from the log sources in a unified console over time.

XpoLog Analytics is an automatic Log Analysis and Monitoring console, which automatically scans all logs that enter the system for errors, risks, statistical problems, and predefined rules. Its Problem Analysis dashboard generates dynamic reports on the detected errors, maps problems over time, and tagging them according to their severity. From the Problems Analysis dashboard, users have immediate access to the analysis reports, with easy navigation and zoom-in capabilities to the relevant log data to accelerate problems isolation.

XpoLog's Analytics console analyzes log data for the following two types of problems:

- **Predefined Errors** – Detects problems that have been predefined as a saved search. Severity can be assigned to saved searches in XpoLog Search. Once a severity is assigned to a saved search, it will be presented in the Analytics console as a predefined problems.
- **Auto-Detected Errors** – Uses Semantic Content Analysis. Based on semantic analysis of the logs' contents and predefined knowledge-base, XpoLog Analytics detects in the logs thousands of errors and events that contain information related to a fault (for example, events containing the word *failure* or *error*). Analytics immediately generates a very high percentage of the problems in the logs of any application, without any configuration.

If In addition, the Analytics console runs **statistical analysis** on multiple use cases to identify unusual behavior in the Application logs. Problems such as high/low logging activity, applications/servers that stop logging normally, an IP that extensively calls the same URL, are captured and presented automatically.

