

Administrator Guide

XpoLog Administrator guide is designed to help administrators to manage XpoLog:

- Add and organize data from sources
- Define data parsing (normalization) rules
- Define Monitors
- Define Dashboards/Applications
- Define and manage Users and Groups

General Structure

XpoLog consoles are available via the top navigation bar: Applications, Search, Analytics and Manager (administrators main console):



XpoLog Manager Navigation

By clicking in the XpoLog Manager icon, the management console will be displayed with an overview screen summarizing the deployment's status.

All the management screens are available via the left navigation panel in the Manager section:

The screenshot shows the XpoLog Manager Overview screen. The top navigation bar includes the XpoLog logo, 'APPLICATIONS', 'SEARCH', and 'ANALYTICS', along with 'Admin | Logout', 'ADD DATA', and a settings gear. The left navigation panel is titled 'XPOLOG MANAGER' and lists: Overview, Folders and Logs, Data, Tags, Monitors and Tasks, Search, Analytics, Security, Settings, and System. The main content area is titled 'Overview' and contains several sections:

- Data trend** (Over 30 days): A bar chart showing data volume over time, with a peak of 2.4.
- TOP SOURCES**: A line chart showing data volume from various sources. A legend lists: Fortigate (Local), system audit (Local), xpologlog (Local), S3 Access xplignet (Local), and catalina log (SSH).
- Active log data** (Last updated): A table with columns for Log Name, Host, Collector, and Size.
- Listeners**: A table with columns for Name, Type, Ip Port, Logs, and Status.
- License**: Shows '1,000 GB DAY' package and '654.51 MB' used today.
- System Status**: Shows 'Overview' as 'Terrible' and 'Data' as '21 May 05:25:54'.
- Storage**: Shows '51.46 GB USED' and '46.84 GB' free.
- Monitors**: Shows '25' monitors and '4' alerts.

Log Name	Host	Collector	Size
Fortigate	gateway	Local	2.67 GB
system audit	localhost	Local	24 GB
xpologlog	localhost	Local	719.18 MB
S3 Access xplignet	localhost	Local	0 Bytes
catalina log	id.xpolog.com	SSH	823.74 MB

Name	Type	Ip Port	Logs	Status
Syslog UDP	Syslog UDP	514		Running
HTTP Listener Logstash	HTTP Listener			Running
HTTP Listener	HTTP Listener			Running
Syslog TCP	Syslog TCP	1468	1	Running