XpoLog Home

<table>
<thead>
<tr>
<th>Latest XpoLog Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online documentation</td>
</tr>
<tr>
<td>XpoLog Latest</td>
</tr>
<tr>
<td>XpoLog 5.0.x</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setup XpoLog</th>
<th>XpoLog Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Data to platform</td>
<td>XpoLog Analytics</td>
</tr>
<tr>
<td>XpoLog Manager</td>
<td>Out of the Box Applications</td>
</tr>
<tr>
<td>XpoLog Search</td>
<td></td>
</tr>
</tbody>
</table>

Latest XpoLog Documentation

About XpoLog

XpoLog is the platform for management and analysis of any log data in the environment - Powerful search, analysis and visualizations of any log.

XpoLog makes it extremely easy to store, analyze and monitor any log data from your IT systems and technology infrastructure. Troubleshoot problems in minutes and Monitor your entire environment to avoid outages or service level issue. Gain real-time visibility and critical insights into customer experience, transactions and behavior. XpoLog will make all your logs data accessible, usable and valuable.
This site contains several sections

- **Introduction** - General information about XpoLog and the help site, main features and modules summary as well as general architecture details

- **Installation** - Information regarding which server to use to run XpoLog and installation procedures

- **XpoLog Home** - A detailed explanation of the application's home page

- **Administrator guide** - A detailed explanations and examples for system administrators on how to configure an environment

- **User guide** - A detailed explanations and examples of the user's available operations in an existing environment

- **Getting Assistance** - ways to get assistance from the XpoLog team

**Introduction**

XpoLog is a Log Analysis Platform that helps applications and operations teams to quickly search, investigate, and navigate through application problems and IT metrics. It offers a centralized perspective covering multiple logs from local and remote infrastructure, including servers, applications, machines, and data centers, all in real-time through a standard web-browser. XpoLog is a non-intrusive, agent-less solution, which does not require any changes to the IT configuration or code.

With XpoLog, operation/production support personnel can:

- Collect and analyze end-user transaction logs
- Perform advanced searches on consolidated logs
- Correlate log events by transactions
- Accelerate problem isolation and troubleshooting
- Automatically detect errors and risks without prior configuration
- Receive alerts based on risk levels and other predefined rules

With XpoLog, application teams can:

- Analyze software logs during testing
- Detect bugs before going live
- Automatically detect risks and monitor problems
- Correlate log events by transactions

See XpoLog summary sheet for more information

See XpoLog data sheet for more information

**Main Features and Product Modules**

**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 four 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.

**About this Help**

This Help is divided into three parts: Installation Guide, Administrator Guide, and User Guide.

**Installation Guide**

The Installation Guide provides instructions for:

- Planning your XpoLog Center installation
- Installing XpoLog Center on your machine
- Tuning XpoLog Center

**Administrator Guide**

The Administrator Guide provides instructions for:

- Adding data to XpoLog
- Mapping applications in XpoLog
- Defining monitors
- Building Apps and Dashboards
- Creating users/groups and applying permissions
User Guide

The User Guide provides instructions for:

- Browsing logs with Log Viewer
- Searching logs with XpoSearch
- Generating statistics and aggregations using XpoSearch
- Viewing Analytics
- View and use Apps and Dashboards

Getting Started

In order to begin working with XpoLog, the Administrator has to do the following:

1. Plan the XpoLog installation (see System Requirements).
2. Install XpoLog (see Installation).
3. Perform post installation recommendations (see Post Installation Recommendations).
4. Add data to the system (see Adding Data to the XpoLog Platform).
5. Set up important settings (see Settings).

Release Notes

This topic contains the release notes of XpoLog version releases and software update releases.

Installations files are available at www.xpolog.com

Latest update/upgrade patch is available at: XpoLog 6 Upgrade and Updates page

XpoLog 6 - Release Notes

Welcome to XpoLog 6

This article contains details on new features, enhancements, and general information related to the release of XpoLog Center 6

Contents

Planning a New Installation or Upgrade?

Documentation

General System Enhancements

- Home page modifications
- SDK/API Enhancements
- System Monitoring and Alerting

Apps - NEW*

XpoLog Manager

- XpoLog Manager Tab
- AppTags
- URL Validator
- Remote XpoLog Enhancements
- Monitors Alerts Enhancements
- Templates Enhancements
- Reports - End of life (replaced by Dashboards)

Search

- New Search Functions
- Enhanced Zoom In from Search Results
Planning a New Installation or Upgrade?

Setups are available at www.xpolog.com. Please review Plan a Deployment for details on system requirements, installation procedures, and getting started.
If you plan an upgrade from an earlier XpoLog version, please contact our support team at support@xpolog.com to get more details - we will be releasing the upgrade patch for existing environments shortly.

Documentation

All technical documentation is available at http://wiki.xpolog.com, and in our technical support site – http://support.xpolog.com. We are working hard to update the resources to provide as detailed and accurate documentation as possible.

General System Enhancements

Home page modifications

XpoLog homepage was replaced to present a quick actions panel and a selected dashboard. More>

SDK/API Enhancements

XpoLog System Status console XpoLog SDK and XpoLog API were enhanced to support more remote based operations. The SDK and API provide more methods for accessing and managing more features in the product.

System Monitoring and Alerting

XpoLog System Status console was enhanced to support SNMP trap based alerts to report NOCs on issues with XpoLog. XpoLog Alert MIB can be reviewed here.

XpoLog Apps (formerly Dashboards) - NEW*

An XpoLog App is a container that contains one or more dashboards. Each dashboard in the App is used to display visual or textual information from the logs that exist in the XpoLog environment.
The entire visualization layer of XpoLog was replaced and is now available under Apps context management. V6 introduces 50+ advanced visualization types that can be defined on the managed data in XpoLog.
Apps and Dashboards simplify and expedite analysis of an Application or Environment. The Dashboards provide live visualization of the data to quickly expose and understand faults and outages. XpoLog has an engine that enables customizing multiple dashboards. For example, multiple dashboards can be defined under an App one for displaying application problems, performance problems, network issues, and security - see XpoLog Apps for more information.

For Administration related topics - see Apps Administration

XpoLog Manager

XpoLog Manager Tab

XpoLog Manager tab was moved to the right hand side of the Tab bar. The Manager tab is focusing on the platform's administration and management.
XpoLog’s formerly Application is now replaced to be AppTag.

URL Validator
GET MORE INFO...

Remote XpoLog Enhancements
Remote XpoLog’s accounts were enhanced to support automated synchronization of logs from a remote XpoLog instance to the center as well as time zone of the remote XpoLog’s instance that can be automatically applied on all logs of a given Remote XpoLog instance.

Monitors Alerts Enhancements
XpoLog Monitors alerts were enhanced to support a REST call when a certain threshold is met.

Templates Enhancements
Templates management enhancements. More>

Reports End of Life - Replaced by Dashboards Enhancements
The previous reports section is no longer available. All capabilities are support in a much more efficient and advanced ways in the Dashboards. More>

XpoLog Search

New Search Functions
XpoLog’s Search syntax was enhanced with implementation of more mathematical, statistical and complex functions. More>

Enhanced Zoom In from Search Results
XpoLog’s Search zoom in was enhanced in a way that performing a zoom in from the search results will redirect the user to the log viewer in a non filtered view with the selected record highlighted.

6.4254 Release Notes

General System Fixes and Optimizations

XpoLog Manager
Event Meta-Data: Added events meta-data when exporting data to CSV via Monitors.
Tuning of export PDF: Handling multiple fields scenarios and Look & Feel improvements.

XpoLog Search
Share Search Action: The Search The share search action provides users with a link that contains the exact search query and time frame to be shared with our users.
Event Meta-Data: Added events meta-data when exporting results to CSV.
Syntax Fixes: display values

XpoLog Apps
**Live Mode:** Added Live mode to dashboards/gadgets.

**Event Meta-Data:** Added events meta-data when exporting gadgets to CSV.

6.4318 Release Notes

Installations files are available at www.xpolog.com

Latest update/upgrade patch is available at: XpoLog 6 Upgrade and Updates page

---

General System Fixes and Optimizations

Indexing Optimizations

---

**XpoLog Manager**

---

**XpoLog Search**

**Share Search Action:** The Share search action provides users with a link that contains the exact search query and time frame to be shared with our users.

**Syntax Enhancements:** new complex functions. Read More>

---

**XpoLog Apps**

**Live Mode:** Added Live mode to dashboards/gadgets.

**Interactive Dashboards - User Inputs:** Users Inputs provide an interface for users to supply values that effect gadgets search terms and displayed results based on their selection. Typically, the inputs are displayed in a checkbox, text area, dropdown menus or radio buttons.

The forms allow users to visually make selections which impact the underlying searches and focus only on points of interest while viewing dashboard's results. Read More>

**Multi Export Scheduler:** XpoLog dashboards support definition of multiple export schedulers. Using more than one export scheduler allows a configuration of a specific date range and specified user inputs for each scheduled export. Read More - Apps> / Read More - Dashboards>

6.4319 Release Notes

Installations files are available at www.xpolog.com

Latest update/upgrade patch is available at: XpoLog 6 Upgrade and Updates page

---

General System Fixes and Optimizations

Indexing Optimizations

6.4473 Release Notes

Installations files are available at www.xpolog.com

Latest update/upgrade patch is available at: XpoLog 6 Upgrade and Updates page

**General**

**SDK/API Enhancements** Read More>

**Bug Fixes**

**Optimizations**
XpoLog Manager

**XpoLog Listeners Enhancements**: new supported protocols such as HTTP/s transport protocol and XpoLog transport protocol. Read More>

**Data Forwarding**: XpoLog instances support forwarding logs data over variety of protocols (Syslog UDP/TCP, HTTP/S, etc.) – the data can be received by either other XpoLog instances or any other supported device. Read More>

**Improvement of the Environment Variables mechanism** Read More>

**Batch Configuration**: New console for massive changes in the configurations of logs. Read More>

XpoLog Search

**Syntax Enhancements**: new simple and complex functions. Read More>

XpoLog Apps

**New Gadgets**: Scatter Gadget, Distribution Chart. Read More>

**Interactive Dashboards - User Inputs Enhancements**: Input dependencies improvements including reflection of all of the inputs according to a given value. Read More>

6.4555 Release Notes

Installations files are available at www.xpolog.com

Latest update/upgrade patch is available at: XpoLog 6 Upgrade and Updates page

General

Bug Fixes

Optimizations

XpoLog Manager

**XpoLog Listeners Enhancements**: new supported protocols such as HTTP/s transport protocol and XpoLog transport protocol. Read More>

**AWS S3 Integration**: Add AWS S3 as source. Read More>

XpoLog Search

**Syntax Enhancements**: milliseconds interval support

XpoLog Apps

**Gadgets**: milliseconds support

6.4611 - Release Notes

Installations files are available at www.xpolog.com

Latest update/upgrade patch is available at: XpoLog 6 Upgrade and Updates page

General

Bug Fixes - CRITICAL BUG fix of version 6.4610 (Analytics graph is not loaded)

Optimizations
6.4618 - Release Notes

Installations files are available at www.xpolog.com

Latest update/upgrade patch is available at: XpoLog 6 Upgrade and Updates page

General

TCP Listeners Optimizations

6.4818 - Release Notes

XpoLog Manager

Data Tagging: Added more tagging capabilities for logs (logtype) and field (ftype) - see more.

Listeners:
- Split incoming data by a custom regular expression - see more.
- Add NetFlow version 9 Listener - see more.

XpoLog Search

Syntax Enhancements: Added more functions for data analysis.

XpoLog Analytics

Servers Metrics: deprecated as of this release.

XpoLog Apps

New Marketplace for using XpoLog Out of the Box Application: predefined applications to be used on various systems/devices - see more

New Gadgets:
- Heat Map Chart - see more
- Stacked Column Grouped Chart - see more
- Google Map Chart - see more

General System Fixes and Optimizations

6.5020 - Release Notes

General System Fixes and Optimizations

6.5028 - Release Notes

Listeners optimizations

Dashboards Layouts and GUI optimizations

Bug fixes and optimizations

Plan a Deployment

This topic explains the steps required to plan and install XpoLog in your environment. High level actions you need to consider and/or perform are listed below.

General
- Review the system requirements in order to decide which XpoLog you need (Windows/Linux/Solaris), decide whether a cluster is required, ensure required ports are opened, etc.
- Install XpoLog server/cluster. The main questions to ask are what is the daily logs volume and what the concurrent number of users is. Note: Although in small environments (less than 10GB/Day), it might be sustainable to a single XpoLog process for processing and
search, it is highly recommended that you run the processor process on a dedicated instance and the UI process on a dedicated instance when managing higher volumes. For more information about deployment server sizing, read system requirements.

- Review and configure the relevant post installation recommendations
- Configure log sources as detailed in the Administrator Guide. Suggested procedure is described below:
  - Determine your remote configuration needs. Questions to ask include:
    - What types of sources do I need to connect to? For example: direct access, databases, SSH, etc. to plan required connectivity to the sources.
    - Within each source type, what characteristics dictate the configuration needs? For example: machine type, geographic location, etc.
  - Determine how to group your sources to best fit your needs. You can group source by applications, machines, or any other criteria that make sense for your deployment topology. A source may be a member of multiple groups. For example, source A might be a member of Application A, under the North America folder, and source B might be a member of the Application B, also under the North America folder.
  - The Applications and Folders structure in XpoLog form the basis for easy navigation and hierarchy management of sources in XpoLog. These tags also enable users to easily manage and execute tag oriented dashboards, searches, and monitors (defined on folder, log, server or application).
- Create detailed log templates for your main log types in advance. Note that you may update templates any time later on as well.

Once you've completed this planning and initial configuration process, you can start adding data to XpoLog platform from multiple sources in the environment as detailed in the Administrator Guide

Please read this topic thoroughly before starting a deployment, if you have any questions or concerns don't hesitate to contact XpoLog Support Team - make sure you perform complete tests on your staging environment before deploying or updating XpoLog in production

System Requirements

Supported Operating Systems (standalone installation)

The following operating systems are supported for standalone installation:

- Linux Kernel versions 2.6.x and later (x86: 32-bit, 64-bit)
- Windows Server 2008 / 2012
- Windows XP, 7, 10
- Mac OS X 10.5 and 10.6 (32-bit, 64-bit)
- Solaris 9, 10 (x86, SPARC)

Supported Application Servers

The following are supported Application Servers for deployment of XpoLog as an application (requires JAVA 1.6+):

- Tomcat 5.5+
- JBoss 4+
- WebSphere 6.1+
- WebLogic 9+

Note: XpoLog is known to run on additional application servers. However, it was tested only on the above servers.

JAVA

JAVA 1.7 or later is required. JAVA 1.8 is recommended.

Supported Browsers

The following browsers are supported:

- Google Chrome (Version 50+) - recommended
- Mozilla Firefox (Version 50+)
- MS Internet Explorer (Version 11+)
- MS Edge

Required Ports

The following are the default ports which should be opened:
- 30303 - HTTP client access to XpoLog web interface and communication between different XpoLog instances (can be modified if needed)
- 30443 - HTTPS client access to XpoLog web interface and communication between different XpoLog instances (can be modified if needed)
- 22 - In order to enable XpoLog to establish connections to remote machines over SSH (can be modified if needed)
- 25 - In order to enable XpoLog to use a SMTP server to send emails (can be modified if needed)
- Alerting:
  - 162 - In order to enable XpoLog to send SNMP traps (can be modified if needed)
  - 7676 - In order to enable XpoLog to send JMS messages (can be modified if needed)
- 389 - In order to enable XpoLog to authenticate users against an Active Directory (can be modified if needed)
- JDBC - In case XpoLog is planned to connect to databases using JDBC drivers, it is mandatory to open the relevant ports:
  - Oracle - 1521 (can be modified if needed)
  - MSSQL - 1433 (can be modified if needed)
  - MySQL - 3306 (can be modified if needed)
  - DB2 - 50000 (can be modified if needed)
  - Postgres - 5432 (can be modified if needed)
- Windows Only:
  - 135-139, 445 - Share and UNC access to remote servers

Hardware Recommendations

**Standard**

The following is hardware recommendation for up to 3 concurrent users, and < 10 GB of daily logs volume:

- 4 CPU cores (2.5-3 GHz per core)
- Standard Linux or Windows 64-bit or 32-bit distribution
- 8 GB RAM

**Recommended**

The following is hardware recommendation for up to 5 concurrent users, and < 10 GB of daily logs volume:

- 8 CPU cores (3 GHz per core)
- Standard Linux or Windows 64-bit OS
- 16 GB RAM

**Cluster**

The following is hardware recommendation for up to 25 concurrent users, and higher daily logs volume:

(contact support@xpolog.com to determine if a cluster is needed. More information about clustering can be found here. See installations details at XpoLog Cluster Installation)

- **Processor node**
  - <25 GB/day (minimum): 4 CPU cores, 8 GB memory, 64-bit OS
  - <100 GB/day: 8 CPU cores, 16 GB memory, 64-bit OS
  - <500 GB/day: 16 CPU cores, 16 GB memory, 64-bit OS

- **UI node**
  - <25 GB/day (minimum): 4 CPU cores, 8 GB memory, 64-bit OS
  - <100 GB/day: 4 CPU cores, 16 GB memory, 64-bit OS
  - <500 GB/day: 8 CPU cores, 16 GB memory, 64-bit OS

**Storage**

XpoLog collection, index and search operations benefit from a disk subsystem that is designed to the system's needs.

**Capacity:** Generally, the total required storage is calculated based on \[\text{DAILY AVERAGE LOG} \times \text{RETENTION POLICY}\] x 1/2

The required storage for standard application logs may be closer to 35%. It is possible to tune the indexing density to reduce the required storage down to 15%.

**Architecture:** RAID 0, 10, 01, 0+1 will give the best performance, while RAID 5 will offer the worst performance.

**Performance:** XpoLog does many bulk reads/writes and many disk seeks. We recommend storage that provides high number (1000+) of random input/output operations per second (IOPS).
As faster the storage is, XpoLog will present better performance. XpoLog processing engines mostly perform write operations but not only, while XpoLog UI engines mostly perform read operations but not only. It is mandatory to perform tests on your set of data and configuration deployment to determine optimized performance since it may vary between different types of data and searches XpoLog performs.

Note: In Linux/Solaris standalone installations, it is recommended to allocate a high number of open files and processes to the user that runs XpoLog.
For more information please see Post Installation Recommendations or contact support@xpolog.com for more details.

**System Architecture**

This article discusses XpoLog's architecture and different deployment scenarios. The key parameters that helps deciding which deployment architecture are daily logs volumes, retention policy, number of monitors, number of dashboards, etc. for the required processing power and mainly number of concurrent users for the required WEB Interface nodes.

Clustering XpoLog has several key advantages for enterprises environments:

- **Multiple points of failure** - all cluster nodes may function as alerting and processing nodes in cases of failures to avoid loss of data / loss of service.
- **Fast Disaster Recovery (DR)** - XpoLog has automated procedures to maintain configuration backups that may be easily used to restore a system.
- **High Availability (HA)** - Upon cluster node failure the cluster manager immediately identifies it and alerts. Until the failed node resumes, its processes are automatically assigned to another node to ensure all activities are performed.
- **Fault tolerance** - During a cluster node failure or following an entire cluster failure, XpoLog recovers immediately and accurately to complete undigested data, reports and monitors.

It is recommended to consult with XpoLog support prior to setting up the clustered environment.

**Deployments Architecture**

**Basic Installation**

At its basic format, XpoLog installs as a single process. This process includes everything that is needed to run and use XpoLog including the WEB interface and data processing engines. XpoLog requires only a file system based storage to manage data and configurations. See more details at the installation guide.

The following diagram demonstrates XpoLog's single process main components:
XpoLog Single Machine Cluster

XpoLog scales easily by separating the web interface and back end processing engines. The XpoLog Center cluster is composed of several instances, using a common storage in order to share the system tasks load and users’ activity. Some of the instances function as processor nodes, taking care of back-end tasks (indexing, analysis, monitoring, and more), while the rest of the instances function as UI nodes. This architecture enables easy scaling of XpoLog Center in heavily loaded environments, without influencing the users’ front-end experience. See more details at the basic cluster installation guide.

A basic cluster of XpoLog may be consisted of 2 such separated processes running on the same machine (commonly, this will be suitable for smaller environments as an initial clustered deployment):
**XpoLog Multiple Machines Cluster**

A more advanced clustering deployment would be usage of 1-N UI nodes and 1-M Processor nodes to support users load and high daily volumes while preserving excellent service. See more details at the [cluster installation guide](#).

The machines that runs XpoLog may be physical or virtual:

---

* UI Process - Dedicated for users activity  
** MASTER Process - Manages back-end activity  
*** Local Disk - Used by UI/MASTER locally
Advanced Architecture

This article discusses XpoLog's architecture for advanced deployment scenarios, which are usually used in highly busy environments, due to enterprise regulations or multiple geographical locations.

An important part of the considerations when planning a full HA deployment including ELB, nodes array and storage replication is recovery time / tolerable loss vs. complexity and cost.

It is recommended to consult with XpoLog support prior to setting up the clustered environment.

**Advanced Deployments Architecture**

**Full HA Installation**

XpoLog cluster configuration supports high availability for both UI nodes by using a load balancer in front of the cluster that redirects users to 1 out of N nodes, and for Processor nodes by assigning an Active/Passive MASTER node and 1-M Processor nodes as described in the system architecture article.

The following diagram demonstrates XpoLog's full HA cluster including UI nodes array, Processor node array and storage replication. Multiple nodes supports full HA of the cluster usage and functionality and normally the cluster would work against its hot storage. In case of a storage failure that cluster nodes will switch to use the (replicated) cold storage which is a mirror of the Hot Storage which is normally used.
Clusters Array Installation

Some scenarios do not allow a single XpoLog cluster to process all data into a centralized silo (closed network segments, network limitation over remote geographical locations, single share storage limitations, etc.). In such cases it is possible to distribute XpoLog deployment to multiple instances / simple clusters / HA clusters across the organization.

The following diagram demonstrates XpoLog’s full HA clusters array across an enterprise environment with a centralized cluster which provides access to the data stored on each remote cluster. In this case data is managed by each cluster independently and the centralized cluster only queries the remote clusters to provide users with the required information:
Installation Guide

This topic explains the steps required to install XpoLog in your environment.

All XpoLog setups can be downloaded from www.xpolog.com

Installation steps include:

1. Planning the XpoLog installation (see System Requirements).
2. Installing XpoLog, including advanced installation, when relevant.
3. Performing post installation recommendations.

Please read this topic thoroughly before installing XpoLog.

Accessibility to XpoLog

XpoLog invests efforts in constantly enhancing its accessibility and usability for users of assistive technology (AT), both in accordance with Section 508 of the United States, and in terms of best practices.

This article discusses how XpoLog addresses accessibility within the product for users of AT.

VPAT™ - Voluntary Product Accessibility Template® - View XpoLog VPAT

Accessibility of XpoLog Web and the CLI

The XpoLog CLI and SDK is fully accessible, and covers many of the functions available in XpoLog GUI. The CLI is text-only by definition and designed for usability for all users, regardless of accessibility needs.

As GUI is sometime preferred, XpoLog GUI is designed with the following accessibility features:
• Form fields are labeled, and ALT text describes elements and images.
• Form fields and dialog boxes have on-screen indication of focus, as supported by the Web browser.
• XpoLog GUI does not override user-defined style sheets.
• No additional on-screen focus is implemented for links, buttons or other elements that do not have browser-implemented visual focus.
• Analyzed data and gadgets results are available via CSV for text only view without style sheets.
• Most data tables implemented with HTML use headers and markup to identify data as needed.

Accessibility and real-time search

Generally, XpoLog GUI does not include any blinking or flashing components. However, using real-time search or real-time gadgets causes the page to update constantly. Real-time search is easily disabled to avoid such behavior.

Installation

General

This topic includes installation instructions for the following operating systems:

• Windows
• Linux
• Solaris
• WAR Deployment
• Any JAVA supported OS (JAVA should be provided externally)

Installing on Windows

You may want to print these instructions. When you are ready to install, go to XpoLog site www.xpolog.com to the Download Center.

Part One: Downloading Your New Software

To download your new software:

1. On the XpoLog download page, click the link or button for the product that you want to download.
2. When you are done, click the Download link or the Download Now button.
   Note: Be sure to click the Download Now button for the product you want to install.
3. Do one of the following:
   • If the software is downloaded automatically into a default folder, you see a download progress dialog box. Make a note of the directory (folder) and filename for the software that you are downloading.
   • If a "Save As" dialog box appears, choose a folder and filename for the software that you are downloading.

Part Two: Installing Your New Software

To install your new software:

1. After downloading is complete, you may see a "Download successful" dialog box. If you see this dialog box, click Install and proceed to step 3. Otherwise, continue with step 2.
2. (Skip this step if installation has already started.) Open the folder into which the new software was downloaded, copy it to the target machine, and double-click the file that you downloaded. For instance, if you downloaded XpoLog Center, double-click the file named "XpoLogCenterSetup.exe". Depending on what you are installing, you may see the Install Anywhere dialog box.
3. When the XpoLog Setup Welcome screen appears, read the information and click Next.
   Note: Read the instructions on the following screens. The screens vary depending on what you are installing, but in general you are asked to do some or all of the instructions in the following steps.
4. Choose a destination directory (folder). This is the location where the new software will be installed, normally C:\Program Files\XpoLogCenter. If you install your new software into the XpoLog folder that contains your current version of the software, your current version will be overwritten. If you wish to keep a copy of the old version as a backup, simply choose or create a new folder for the software that you are about to install.
5. Choose a name for the program group; the default is XpoLog. Then, click Next.
6. Verify all the details in the preview screen and click Install.
   Note: if you want to edit any of the details that are presented in the preview screen, click Previous to return to the desired location.
7. When you see the prompt telling you that installation is complete, click Done.
   XpoLog starts automatically.
Important: At any step, you can click **cancel** to quit the installation.

**Silent Mode:**

1. Open the folder that the new software was downloaded into, copy it to the target machine.
2. In the folder that the new software was downloaded into create a file installer.properties, with the following contents:
   - Mandatory Parameters:
     - INSTALLER_UI=SILENT
     - USER_INSTALL_DIR=<FULL_PATH_TO_INSTALLATION_DIRECTORY> (For example: C:\Program Files\XpoLogCenter4.5\)
   - Optional Parameters:
     - USER_INPUT_AGENT_MODE="Agent Mode Active" (use "Agent Mode Not Active" for a regular installation)
     - USER_INPUT_START_XPOLOG=1 (use 0 to prevent XpoLog from starting once the installation completes)
     - USER_INPUT_SERVICE_NAME=XpoLogCenter (use a different service name if needed)
     - Note: ensure there are no spaces at the end of any of the lines in the file installer.properties
3. Execute command: XpoLogCenterSetup.exe -f installer.properties
4. XpoLog will be installed in the background and will be started automatically, unless you specified otherwise during installation.

**Part Three: Running Your New Software**

XpoLog starts automatically after installation. There is a single process - XpoLogCenter, which is presented in the Windows Services panel. It is highly recommended to configure a user on the XpoLogCenter service, which XpoLog can use while reading logs from machines in the environment.

To run your new software:

1. Recommended: In the Windows Services panel, under the **log on** tab, type a username that XpoLog service can use in order to connect and read logs over the Windows network authentication in your organization.
2. Open a browser with the following URL: [http://MACHINE_NAME:30303](http://MACHINE_NAME:30303) and you will be redirected to XpoLog Center homepage.

**Installing on Linux/Solaris**

You may want to print these instructions. When you are ready to install, go to XpoLog site [www.xplg.com](http://www.xplg.com) to the Download Center.

**Part One: Downloading Your New Software**

To download your new software:

1. On the XpoLog download page, click the link or button for the product that you want to download.
2. When you are done, click the **Download** link or the **Download Now** button.
   - **Note:** Be sure to click the Download Now button for the product that you want to install.
3. Do one of the following:
   - If the software is downloaded automatically into a default folder, you see a download progress dialog box. Make a note of the directory (folder) and filename for the software that you are downloading.
   - If a “Save As” dialog box appears, choose a folder and filename for the software that you are downloading.

**Part Two: Installing Your New Software**

To install your new software:

After downloading is complete, you may see a "Download successful" dialog box. If you see this dialog box, click **Install** and go on to step 3. Otherwise, continue with step 2.

1. (Skip this step if installation has already started.) Open the folder that the new software was downloaded into, copy it to the target machine, and gunzip the file that you downloaded. For instance, if you downloaded XpoLog Center, gunzip the downloaded file (gunzip XpoLogCenterSetup.bin.gz | for x64 gunzip XpoLogCenterSetup-64.bin.gz).
2. After unzipping the file, execute the .bin file (sh XpoLogCenterSetup.bin | for x64 sh XpoLogCenterSetup-64.bin).
   - The installation wizard will start.
3. When the XpoLog Setup message appears, read the information and follow the installation process.
4. Read the instructions on each step.
5. When you see the prompt telling you that installation is complete, XpoLog will be started automatically.

**Important:** At any step, you can click **cancel** to quit the installation.

**Silent Mode:**
1. Open the folder that the new software was downloaded into, copy it to the target machine, and gunzip the file that you downloaded. For instance, if you downloaded XpoLog Center, gunzip the downloaded file (gunzip XpoLogCenterSetup.bin.gz | for x64 gunzip XpoLogCenterSetup-64.bin.gz).

2. In the folder that the new software was downloaded into create a file installer.properties, with the following contents:

   Mandatory Parameters:
   INSTALLER_UI=SILENT
   USER_INSTALL_DIR=<FULL_PATH_TO_INSTALLATION_DIRECTORY> (For example: /apps/XpoLogCenter/)

   Optional Parameters:
   USER_INPUT_AGENT_MODE="Agent Mode Active" (use "Agent Mode Not Active" for a regular installation)
   USER_INPUT_START_XPOLOG_CONSOLE="Yes" (use "No" to prevent XpoLog from starting once the installation is complete)

   - Note: ensure there are no spaces at the end of any of the lines in the file installer.properties

3. Execute command: sh XpoLogCenterSetup.bin -f installer.properties.

   XpoLog will be installed in the background and will be started automatically, unless you specified otherwise during installation.

Part Three: Running Your New Software

   XpoLog starts automatically after installation. There are several useful commands for starting, stopping, restarting, or finding out the status of the server:

   - cd to XPOLOG_HOME
   - Run: `sh runXpoLog.sh start|stop|restart|stat`
     start = starting XpoLog
     stop = stopping XpoLog
     restart = restarting XpoLog
     stat = finding out whether XpoLog is running or not

   To run your new software:

   1. Go to the installation directory.
   2. XpoLog should start automatically after installation. To control and verify, use these commands:
      - Start XpoLog – sh /.../XpoLogCenter/runXpoLog start
      - Stop XpoLog – sh /.../XpoLogCenter/runXpoLog stop
      - Check Status – sh /.../XpoLogCenter/runXpoLog stat
   3. Open a browser with the following URL: [http://MACHINE_NAME:30303](http://MACHINE_NAME:30303)
      You will be redirected to the XpoLog Center homepage.

Installing on UNIX without internal JVM (JAVA Provided Externally)

   You may want to print these instructions. When you are ready to install, go to XpoLog site www.xpolog.com to the Download Center.
   This XpoLog Installer does not contain JAVA and uses an external JAVA which should already be available on the machine that you plan to run XpoLog on. Important: JAVA 1.6+ is required.

Part One: Downloading Your New Software

To download your new software:

1. On the XpoLog download page, click the link or button for the product that you want to download (without internal JVM).
2. Log in to the target machine with the same user you plan to run XpoLog with to ensure JAVA is available. Run the command `java -version` and confirm the output is JAVA 1.6+
   - If the java command does not return result or the JAVA version is prior to JAVA 1.6 please contact XpoLog Support for additional information.
3. Do one of the following:
   - If the software is downloaded automatically into a default folder, you see a download progress dialog box. Make a note of the directory (folder) and filename for the software that you are downloading.
   - If a "Save As" dialog box appears, choose a folder and filename for the software that you are downloading.

Part Two: Installing Your New Software

To install your new software:

After downloading is complete, you may see a "Download successful" dialog box. If you see this dialog box, click Install and go on to step 3. Otherwise, continue with step 2.
1. (Skip this step if installation has already started.) Open the folder that the new software was downloaded into, copy it to the target machine, and gunzip the file that you downloaded. For instance, if you downloaded XpoLog Center, gunzip the downloaded file (gunzip XpoLogCenterSetupNoJava.bin.gz).
2. After unzipping the file, execute the .bin file (sh XpoLogCenterSetup.bin).
   The installation wizard will start.
   **Note:** the installation wizard looks for a local JAVA to be used, it is possible to specify the full JAVA path that should be used, by executing the installation with a specified JAVA full path (sh XpoLogCenterSetupNoJava.bin LAX_VM"/FULL/PATH/TO/JAVA/EXECUTABLE")
3. When the XpoLog Setup message appears, read the information and follow the installation process.
4. Read the instructions on each step.
5. When you see the prompt telling you that installation is complete, XpoLog will be started automatically, unless you specified otherwise during installation.

**Important:** At any step, you can click cancel to quit the installation.

---

**Silent Mode:**

1. Open the folder that the new software was downloaded into, copy it to the target machine, and gunzip the file that you downloaded. For instance, if you downloaded XpoLog Center, gunzip the downloaded file (gunzip XpoLogCenterSetupNoJava.bin.gz or in case of x64 gunzip XpoLogCenterSetupNoJava-64.bin.gz).
2. In the folder that the new software was downloaded into create a file installer.properties, with the following contents:

   **Mandatory Parameters:**
   - INSTALLER_UI=SILENT
   - USER_INSTALL_DIR=<FULL_PATH_TO_INSTALLATION_DIRECTORY> (For example: /apps/XpoLogCenter/)

   **Optional Parameters:**
   - USER_INPUT_AGENT_MODE="Agent Mode Active" (use "Agent Mode Not Active" for a regular installation)
   - USER_INPUT_START_XPOLOG_CONSOLE="Yes" (use "No" to prevent XpoLog from starting once the installation is complete)

   - Note: ensure there are no spaces at the end of any of the lines in the file installer.properties
3. Execute command: sh XpoLogCenterSetup.bin -f installer.properties
4. XpoLog will be installed in the background and will be started automatically.

**Part Three: Running Your New Software**

XpoLog starts automatically after installation. There are several useful commands for starting, stopping, restarting, or finding out the status of the server:

- cd to XPOLOG_HOME
- Run: 'sh runXpolog.sh start|stop|restart|stat'
  - start = starting XpoLog
  - stop = stopping XpoLog
  - restart = restarting XpoLog
  - stat = finding out whether XpoLog is running or not

To run your new software:

1. Go to the installation directory.
2. XpoLog should start automatically after installation. To control and verify, use these commands:
   - Start XpoLog – sh ../XpoLogCenter/runXpolog start
   - Stop XpoLog – sh ../XpoLogCenter/runXpolog stop
   - Check Status – sh ../XpoLogCenter/runXpolog stat
3. Open a browser with the following URL: http://MACHINE_NAME:30303.
   You will be redirected to the XpoLog Center homepage.

---

**Deploying XpoLog as a Web Application**

**Part One: Downloading Your New Software**

To download your new software:

1. On the XpoLog download page, click the link or button for the product that you want to download.
2. When you are done, click the Download link or the Download Now button.
   **Note:** Be sure to click the Download Now button for the product that you want to install.

**Part Two: Installing Your New Software**

XpoLog can be deployed on most application servers. The deployment is standard, according to the application server that you are using.
Part Three: Running Your New Software

Start/stop/restart the application on the application server on which you deployed XpoLog.

Note: XpoLog default context is ‘logeye’.

Thank you for installing XpoLog Center.

Post Installation Recommendations

Configuring XpoLog to Storage

It is highly recommended to configure XpoLog to work against an external storage location / directory. XpoLog requires full permissions (read/write) on this location with direct/fast access.

To configure XpoLog to storage:

1. Create a folder under the name “XpoLogConfig”.
2. Go to XpoLog > Settings > General.
3. Select the Use external configuration directory checkbox and type the absolute path into XpoLogConfig – “…/XpoLogConfig/”
   XpoLog saves the information and requests a restart.
4. Restart XpoLog, and go once again to XpoLog > Settings > General, and ensure that the configuration was saved successfully. XpoLog saves all the information into this external folder.
   Note: It is recommended to back it up occasionally. If you remove your XpoLog version and redeploy, you can always point the new XpoLog instance to this folder to use the existing configuration or for clustering purposes.
   For further information, contact the support team at support@xplg.com

Allocating More Memory to XpoLog (64-bit installations)

It is highly recommended to install XpoLog on a 64 bit OS, which enables higher allocation of memory than the default.

To allocate more memory:

1. Stop XpoLog.
2. Edit the file /.../XPOLOG_INSTALL_DIR/XpoLog.lax (Windows) OR /.../XPOLOG_INSTALL_DIR/XpoLog.sh.lax (Linux/Solaris).
3. Look for -Xmx1024m (default allocation is 1024 MB) and allocate more memory based on the available memory of the machine. For example, to allocate 4096 MB change the value to be -Xmx4096m and save.
   Note: it is recommended to allocate 75% of the machine's memory.
4. Start XpoLog.

Setting a default Character Encoding (Optional)

In case XpoLog should be able to support special characters which are different from the machine's default (Especially Chinese, Japanese, Korean, etc.) it is recommended to modify the default encoding as follows.

To change default encoding:

1. Stop XpoLog.
2. Edit the file /.../XPOLOG_INSTALL_DIR/XpoLog.lax (Windows) OR /.../XPOLOG_INSTALL_DIR/XpoLog.sh.lax (Linux/Solaris).
3. Edit the parameter -Dfile.encoding=UTF-8 at the end of the LAX.NL.JAVA.OPTION.ADDITIONAL parameters line to any desired default encoding.
   Note: the encoding can be any of the JAVA supported encoding
4. Start XpoLog.

Setting a default locale (Optional)

In case XpoLog should be capable of displaying content in different languages and normalize dates from different regions, it is possible to assign a JVM locale. By default, the JVM locale is the locale of the platform where XpoLog is installed. To override the default JVM locale, you must set the appropriate language and region (country) arguments in XpoLog.

To change default locale:

1. Stop XpoLog.
2. Edit the file /.../XPOLOG_INSTALL_DIR/XpoLog.lax (Windows) OR /.../XPOLOG_INSTALL_DIR/XpoLog.sh.lax (Linux/Solaris).
3. Add the parameters -Duser.language=en_US -Duser.region=en_US at the end of the LAX.NL.JAVA.OPTION.ADDITIONAL parameters line
Note: The above example is for English US locale, the complete locale list that JAVA supports can be found here: [JAVA locale list](#).

4. Start XpoLog.

**Windows Specific - Assign a service account**

After installation, XpoLog service is available under the Windows services panel (XpoLogCenter). It is highly recommended, after installation, to assign an account on the service for optimized connectivity between XpoLog and remote log sources over the Windows network.

To assign a service account:

1. Go to the Windows Services Panel.
2. Right click the XpoLogCenter service > Properties
3. Go to the ‘Log On’ tab (by default, XpoLog is installed with a Local System Account). Select ‘This account’ radio button and enter a specific account with sufficient privileges that XpoLog can use to read remote log sources.
4. Save and restart.

This will allow Administrators adding logs over the Windows network as if they were local (direct access) using UNC paths: \\<server-name>\<drive-name>$\...\<log> (for example: \server1\c\logs\log4j.log{string})

**Linux Specific - Allocating Allowed Open Files / Number of Processes**

It is very important to allocate 10,000 allowed open files and allowed number of processes to XpoLog that runs on Linux (default is usually 1024).

The allocation can be done specifically to the user who runs XpoLog:

To check the limitation for the user who runs XpoLog:

1. Open SSH terminal to XpoLog's machine and log in using the same user that runs XpoLog (for example, Putty).
2. Run the command: 'ulimit -n' and then the command: 'ulimit -u'
   - The recommended output should be 10000.

To allocate the required number of open files:

- Log in to the machine that runs XpoLog, as superuser if needed, and edit the file /etc/security/limits.conf, by adding the following line:
  ```
  [USER_THAT_RUNS_XPOLOG] - nofile [MAX_NUMBER_OF_FILES]
  ```
  - Where
  - [USER_THAT_RUNS_XPOLOG] is the user who you are using to run the XpoLog process (superuser, if you logged in as such).
  - [MAX_NUMBER_OF_FILES] is the new limitation that has to be set to 10000.
  - For instance, you can add the line: xpolog - nofile 10000

To allocate the required number of processes:

- Log in to the machine that runs XpoLog, as superuser if needed, and edit the file /etc/security/limits.conf, by adding the following line:
  ```
  [USER_THAT_RUNS_XPOLOG] - nproc [MAX_NUMBER_OF_PROCESSES]
  ```
  - Where
  - [USER_THAT_RUNS_XPOLOG] is the user who you are using to run the XpoLog process (superuser, if you logged in as such).
  - [MAX_NUMBER_OF_PROCESSES] is the new limitation that has to be set to 10000.
  - For instance, you can add the line: xpolog - nproc 10000

**IMPORTANT:** After making this change, log out and then log in again so that the changes take effect, verify by getting 10000 as a result of running 'ulimit -n' and 'ulimit -u' again using the same user which runs XpoLog, and then restart XpoLog.

**Solaris Specific - Allocating Allowed Open Files**

It is very important to allocate 10,000 allowed open files to XpoLog that runs on Solaris (default is usually 1024).

To check the limitation for the user who runs XpoLog:

1. Open SSH terminal to XpoLog's machine and log in using the same user that runs XpoLog (for example, Putty).
2. Run the command: 'ulimit -a'
   - The recommended output should be 10000.

To allocate the required number of open files:

- Log in to the machine that runs XpoLog, as superuser if needed, and edit the file /etc/security, by adding the following line:
  ```
  [MAX_NUMBER_OF_FILES]
  ```
  - set rlim_fd_max = [MAX_NUMBER_OF_FILES]
  - Where
  - [MAX_NUMBER_OF_FILES] is the new limitation that has to be set to 10000.

- Once the above hard limit is set reboot the system once. You can then increase the value of this property explicitly (up to this limit) using the following command:
ulimit -n [MAX_NUMBER_OF_FILES]

IMPORTANT: After making this change, log out and then log in again so that the changes take effect, verify by getting 10000 as a result of running `ulimit -a` again using the same user which is used to run XpoLog, and then restart XpoLog.

WAR Deployment Specific - Configuring XpoLog to Storage

It is highly recommended to configure XpoLog that is deployed as a war on an application server to an external configuration directory (storage) - instructions are available at the top of this page.

In case you need to update your XpoLog version, the war file will be replaced and if an external storage is not configured all the data and configuration will be removed.

Advanced Installation Procedures

This topic discusses advanced installation procedures of XpoLog.

Please read it carefully before installing XpoLog.

The following advanced installations can be performed:

- Installing a cluster of several XpoLog instances to process larger volumes of data (see XpoLog Cluster Installation)
- Installing and using XpoLog to XpoLog deployment – usage of remote XpoLog instances scenarios (see Remote XpoLog Installation)

XpoLog Cluster Installation

General

When deploying XpoLog Center in busy environments, it is recommended to deploy several XpoLog Center instances as a cluster, for high availability and load balancing.

The XpoLog Center cluster is composed of several instances, using a common storage in order to share the system tasks load and users' activity. Some of the instances function as processor nodes, taking care of back-end tasks (indexing, analysis, monitoring, and more), while the rest of the instances function as UI nodes. This architecture enables easy scaling of XpoLog Center in heavily loaded environments, without influencing the users' front-end experience. A load balancer can be used if more than one UI node is deployed.

It is highly recommended to consult with XpoLog support prior to setting up the clustered environment. Review the System Architecture diagrams that explain the XpoLog Center Cluster architecture, and below a step-by-step cluster deployment instructions.

XpoLog Center Cluster Deployment Instructions

The following are instructions for installing XpoLog Center in a clustered environment, with two UI nodes and a single processor node.

Preparations

1. Decide if XpoLog Center will be installed in a Windows or Linux environment. In case there is a need to analyze log data from Windows machines, XpoLog Center must be installed on Windows machines.
2. Prepare 2+ machines (physical or virtual); one for the UI nodes and one for the processor node, based on the XpoLog Center hardware requirements.
3. Prepare a shared storage device that can be accessed by all XpoLog Center nodes, based on the XpoLog Center hardware requirements. It is mandatory that ALL XpoLog instances in the cluster will have full permissions (READ/WRITE) on the allocated shared storage.

Note: XpoLog Center performs heavy read/write operations. It is highly recommended that the fastest storage connectivity is allocated to the UI node.

Installation

1. Download the XpoLog Center installer from the XpoLog website at http://www.xpolog.com
2. Run the installer on each node machine - See installation instructions for more details
3. Once completed, open a web browser directly to each node at: http://[NODE_HOST_NAME]:30303 to verify that XpoLog Center was installed successfully.

Configuration

1. Create a folder that will store XpoLog Center's data on the shared storage device (referred to as EXTERNAL_CONFIGURATION_DIRECTORY).
2. Open a web browser to each node at http://[NODE_HOST_NAME]:30303, go to XpoLog > Settings > General, and do the following:
   a. Select the Use external configuration directory checkbox.
   b. Enter the full path to the EXTERNAL_CONFIGURATION_DIRECTORY in the 'Configuration full path' field.
c. Select the **Cluster Mode** checkbox.
d. Click **Save**.
e. Wait until receiving a message that the configuration was saved successfully and a restart request but don’t restart XpoLog Center yet.
g. Under the Mail tab, specify the SMTP details and system administrator email address. XpoLog Center will send an alert in case the active processor node changes.

3. On each node (starting with the processor node), go to `XPOLOG_CENTER_INSTALLATION_DIRECTORY`, edit the lax file (`XpoLog.lax` on Windows installation; `XpoLog.sh.lax` on Linux installation), and perform the following changes to the line that starts with `lax.nl.java.option.additional=`

   a. By default, XpoLog Center is allocated with 1024 MB of memory. It is recommended to increase this value to about 75% of the machine’s memory. To do so, replace `-Xmx1024m` with `-XmxNEW_VALUE`

   b. In a clustered environment, each node should be assigned a unique name for it to be identified in the system. To do so, append the following to the end of the line `-Dxpolog.uid.structure=[NODE_NAME]`  

   example node name: PROCESSOR1, PROCESSOR2, UI01, UI02, etc.

c. Save the file.
d. Restart XpoLog Center (on a Windows installation, restart the XpoLogCenter service; on a Linux installation, run the script `XPOLOG_CENTER_INSTALLATION_DIRECTORY/runXpoLog.sh restart`).

4. In a clustered environment, some configuration properties should be tuned. To do so, open a web browser to the processor node at `http://[PROCESSOR_NODE_HOST_NAME]:30303/logeye/support`, select ‘Advanced Settings’ in the select box.

   For each of the following properties, enter the property name in the text box of the ‘Name’ column, right-click the row, click ‘Edit’, enter the custom value and click **Save**:

   - **Property name: cluster.allowedMasters**
     - Purpose: used to determine the name of the processor node.
     - Should be customized: always
     - Custom value: `[NODE_NAME_1],[NODE_NAME_2]...,[NODE_NAME_N]` (of the processor nodes)

   - **Property name: htmlUtil.BaseUrl**
     - Purpose: used by the processor node when exporting information on the server side
     - Should be customized: always
     - Custom value: `http://[PROCESSOR_NODE_HOST_NAME]:[PROCESSOR_NODE_PORT]/logeye/`

   - **Property name: htmlUtil.ui.BaseUrl**
     - Purpose: used by the UI node when exporting information on the server side
     - Should be customized: always
     - Custom value: `http://[UI_NODE_HOST_NAME]:[UI_NODE_PORT]/logeye/`

   - **Property name: mail.link.baseUrl**
     - Purpose: used in links that point back to XpoLog from an email
     - Should be customized: always
     - Custom value: `http://[UI_NODE_HOST_NAME]:[UI_NODE_PORT]/logeye/` (in multiple UI nodes environments, consider pointing the link to a load balancer, if exists)

   Note that it is highly recommended to consult XpoLog support before editing any of the following properties:

   - **Property name: cluster.shouldCheckForMaster**
     - Purpose: used to indicate whether the UI nodes should take over the processor node activity in case the processor node is down
     - Should be customized: only if UI nodes should never take over the processor activity
     - Custom value: false

   - **Property name: cluster.takeOverAttempts.notAllowedMaster**
     - Purpose: used to indicate the number of minutes that should pass before a UI node attempts to take over the processor activity in case the processor node is down
     - Should be customized: only when there’s a need to allow the processor node to be down for more than 5 minutes without a UI node taking over its activity
     - Custom value: numeric value larger than 5

Note: in case there is an XpoLog instance which is dedicated to be a listener then the following has to be done for that specific instance:

- Allocate 2GB of memory (there is no need in more)
- Set this specific instance to run in agent mode:
  - Open a browser to the instance directly
  - Go to Manager > Settings > General
  - Check the ‘Agent Mode’ and save
- Set this specific instance not to be recycled:
- Edit the file LISTENER_INSTALL_DIR/xpologInit.prop
- Add the line (empty recycle cron expression):
  recycleCronExpression=
- Restart Listener instance
- Go to the Listener Account (Manager > Administration > Listeners):
  - Stop the listener account
  - Edit the listener account
  - Set Listening node to be the Listener instance
  - Set the Indexing node to be the MASTER or one of the PROCESSORS
  - Save the listener account
  - Start the listener account

**Verification**

1. Open a web browser to each node at http://[NODE_HOST_NAME]:30303, go to XpoLog > Settings > General, and verify that the external configuration directory and cluster mode are active.
2. On the shared storage device, go to EXTERNAL_CONFIGURATION_DIRECTORY/conf/general/cluster and verify that the file with suffix .masterNode is called [PROCESSOR_NODE_NAME].masterNode. In case the file is named differently, wait two minutes and check again. If the file still does not exist nor has a different name, verify configuration steps 3b and 4a once again.

**Please review the system architecture overview for additional information:** [XpoLog-Center-Architecture](#)

**Installing XpoLog Cluster on a single machine**

It is possible to run 2 or more instances of XpoLog on a single machine as a cluster similar to the usage of multiple machines. The procedure is similar with a few mandatory additional steps as listed below

**Installation**

Follow the same steps as described in the [cluster installation guide](#) with the following changes during installation:

1. During installation set the installation directory name to be XpoLog Center UI (for the UI node) and XpoLog Center PROCESSOR (for the PROCESSOR node). At first step you will not be able to run both instances as there will be a port a collision since both instance use the same ports by defaults.
2. Go to PROCESSOR_INSTALL_DIR/ServletContainer/conf/ and rename the file server.xml to be server.xml.orig and the file server.xml.processor to server.xml (this will change the ports of the processor node so that both instances will be able to run simultaneously on the same machine).
4. Please continue with the configuration section at [cluster installation guide](#)
5. If you plan to install more instances make sure all ports are changed in the INSTALL_DIR/ServletContainer/conf/server.xml as each instance must use different ports

- Note: the HTTP/S ports of all nodes can be changed in the **settings** section.

**Windows Specifics**

If you are running multiple nodes on a Windows machine then it is mandatory to give a unique name to each node during installation. During installation ensure you specify a different installation directory and a different service name to each instance. For example:

- XpoLogCenterProcessor and XpoLogCenterUI

At the end of the process, you should have a installation directory and a unique service name per each installed instance.

**Note:**

It is also possible to manually remove/create services but recommended to do it directly in the installation wizard:

- Remove service: sc delete [SERVICE_NAME]
- Create service: sc create [SERVICE_NAME] binpath= "C:\PROGRA~1\XPOLOG~1\XpoLog.exe -zglaxservice XpoLogCenter" start= auto DisplayName= "[SERVICE_DISPLAY_NAME]"
  For example: sc create XpoLogProcessor binpath= "C:\PROGRA~1\XPOLOG~1\XpoLog.exe -zglaxservice XpoLogCenter" start= auto DisplayName= "XpoLogProcessor"

It is recommended to set a service account on each of the services for an optimized connectivity to machines across the network - [Windows Post Installation](#)

**Linux/SunOS Specifics**
If you are running multiple nodes on a Linux/SunOS machine then it is recommended to allocate a specific range of CPU cores to be used by the Processor and a specific range for the UI. For example, if there are 12 CPU cores available on the machine that the cluster is running on, the recommended configuration should be as follows:

1. Go to PROCESSOR_INSTALL_DIR and edit the file runXpoLog.prop:
   a. For Linux, specify a CPUs range, for example 0-3 for the first 4 CPUs or 4-7 for the second 4 CPUs
      For SunOS, specify a space separated list of processor IDs, for example 0 1 2 3 for the first 4 CPUs or 4 5 6 7 for the second 4 CPUs
      un-comment the line #cpus= with the allocated range. For example cpus=0-7
   b. Save and restart the PROCESSOR_NODE and you should see a message after restart indicating that the configured range has been applied.
2. Go to UI_INSTALL_DIR and edit the file runXpoLog.prop:
   a. For Linux, specify a CPUs range, for example 0-3 for the first 4 CPUs or 4-7 for the second 4 CPUs
      For SunOS, specify a space separated list of processor IDs, for example 0 1 2 3 for the first 4 CPUs or 4 5 6 7 for the second 4 CPUs
      un-comment the line #cpus= with the allocated range. For example cpus=8-11
   b. Save and restart the UI_NODE and you should see a message after restart indicating that the configured range has been applied.

Using Load Balancer

If XpoLog cluster is running with multiple UI nodes, it is recommended to install a Load Balancer in front of the XpoLog cluster so that users will be automatically redirected to the UI nodes.

For more details on how to set up XpoLog Cluster, please see [here](#)

The following example explains how to set up Apache Httpd server as a load Load Balancer:

1. Set up Apache httpd server on Linux
2. Download the latest version of mod_jk from Apache web site. Copy this file into the Apache modules/ directory and rename it to mod_jk.so.
3. Configure Apache:
   a. Edit the file httpd.conf (Apache configuration path usually: /etc/httpd/conf/httpd.conf)
      Note that the default port is usually 80, change it if needed but make sure that the ports you use are available.
      Add the following right after the other LoadModule directives:
      LoadModule jk_module modules/mod_jk.so
   Add the following at the end of the httpd.conf file:
   # Where to find workers.properties
   JkWorkersFile /etc/httpd/conf/workers.properties
   # Where to put jk shared memory
   JkShmFile /var/log/httpd/mod_jk.shm
   # Where to put jk logs
   JkLogFile /var/log/httpd/mod_jk.log
   # Set the jk log level [debug/error/info]
   JkLogLevel info

   # Select the timestamp log format
   JkLogStampFormat "[%a %b %d %H:%M:%S %Y] "
   JkMount /* balancer
   JkMount /*/* balancer

   b. Create workers.properties
      The worker.properties file should be located in the /etc/httpd/conf/ directory. In the file you should have the following parameters set for the UI1, UI2 nodes:
      Define the list of workers that will be used
      worker.list=balancer
      worker.balancer.type=lb
      worker.balancer.balance_workers=ui1,ui2
Configure Tomcat on each of the UI nodes:

4. On each of the XpoLog UI nodes, edit the file
   `<UI1_NODE_INSTALLATION_DIR>/ServletContainer/conf/server.xml`
   Go to the following XML Tag:
   ```xml
   <!-- Define an AJP 1.3 Connector on port 8009 -->
   <Connector port="8011" enableLookups="false" redirectPort="30445" protocol="AJP/1.3" />
   ```
   Set up the port to the same as `<UI1_JK_PORT>`
   Go to the following Engine tag to set the ui node name must be like the one in the Apache
   workers.properties used name:
   ```xml
   <!-- You should set jvmRoute to support load-balancing via AJP ie :–>
   <Engine name="Catalina" defaultHost="localhost" jvmRoute="ui1">
   ```
   Activate and Verify:
   After completing the above step - restart UI1, UI2 and the Apache server
   Users should use the URL to the Apache
   `http://<HTTPD-IP>:<HTTPD-PORT>`

Remote XpoLog Installation

Background

While XpoLog is fully functional as an agentless application, i.e., you can install it anywhere in the environment and import logs into its platform, it is also possible to install XpoLog as an agent or structure the deployment to several instances for several reasons which are specified below. If you choose to run multiple instances of XpoLog in the environment, it is possible to connect the different instances over HTTP/S (XpoLog to XpoLog).

When should XpoLog to XpoLog usage be considered?

There are several key reasons to consider installing multiple instances of XpoLog to manage an environment:

- **Inaccessible network segments** – Sometimes, when logs are collected from multiple network segments, there is no direct access between the location of the centralized XpoLog to other network segments (for instance, different domains in Windows).
- **Data load balancing (Map Reduce)** – In cases where a regular cluster is insufficient, it is possible to manage several XpoLog instances of several separate machines, and each will be managing a selected group of logs, and on top of all instances, there will be an instance which users can access to view all logs from all instances.
- **Keeping main console on Linux in a mixed Linux/Windows environment** – In case the main XpoLog instance runs on Linux/Solaris, but there is a need to add logs from Windows machines (Windows event logs, logs on shared locations, Windows machines), it is mandatory to deploy a Windows instance of XpoLog which will be able to manage all logs from Windows machines and connect it to the centralized XpoLog instances.
- **Different data centers** – Organizations which manage multiple data centers may consider an XpoLog cluster-instance per data center to get optimized connectivity and performance within each data center and then connect all data centers instances to a centralized XpoLog instance for the users.
- **Need of an agent to collect data** – While XpoLog is completely agentless, in cases where there is no available connectivity to the sources with the standard protocols, it is recommended to install XpoLog as an agent on the remote sources and collect the data from using XpoLog to XpoLog communication over HTTP/S protocol. The agent is also required for Log Synchronization to collect data as is from multiple sources into a central repository.
How to install a remote XpoLog?

Remote XpoLog installation is a regular installation, only with selected features activated. For example, if the remote XpoLog is used only to collect data to a centralized XpoLog then 'agent mode' is activated and no operations will be performed by the agent besides access to the data. In case a Map Reduce / multiple data centers deployment is required, then the remote XpoLog may be fully functional and all its log processing can be done independently. If the remote XpoLog is only used for Log Synchronization then 'agent mode' should be activated. When deploying multiple remote XpoLog instances, it is possible to use a silent installation in order to distributed multiple setups and then remotely configure them by using the SDK commands.

How to connect between XpoLog instances?

In order to connect XpoLog instances and add the remote XpoLog's log to the centralized XpoLog instance, first ensure that there is communication over HTTP/S on the port which is used to run XpoLog between the instances:

1. Go to XpoLog>Tools>Address Book, and add a remote XpoLog account with all the required details (a user name and password are also required if security is activate on the remote XpoLog).
2. To add logs which are configured on the remote XpoLog follow information here: Adding Data to the XpoLog Platform / Adding a Log to XpoLog
3. To use the agent for a LogSync task, see Log Synchronization

Uninstall

General

This topic includes uninstall instructions for the following operating systems:

- Windows
- Linux
- Solaris
- WAR Deployment
- Any JAVA supported OS (JAVA should be provided externally)

Uninstalling from Windows

Removing XpoLog from Windows OS

To remove your XpoLog setup:

1. Go to the XpoLog setup directory, in it you will find the "UninstallerData" directory.
2. In this directory you will execute the .exe file "Uninstall XpoLog".
   
   **Note:** You can remove the XpoLog software from the add/remove program console in Windows control panel.
3. Follow the uninstall wizard, when the wizard will finish, the XpoLog software will removed from the machine.

Important: Once XpoLog is uninstalled no traces will remain on the machine.

Uninstalling from Linux/Solaris

Part One: Downloading Your New Software

To remove your XpoLog setup:

1. Go to the XpoLog setup directory, in it you will find the "UninstallerData" directory.
2. In this directory you will execute the .bin file "Uninstall XpoLog" (.sh "Uninstall XpoLog.bin")
   
   **Note:** You can also remove the XpoLog software by simply removing the XpoLog setup directory.
3. Follow the command line uninstall wizard, when the wizard will finish, the XpoLog software will removed from the machine.

Important: Once XpoLog is uninstalled no traces will remain on the machine.

XpoLog Updates

XpoLog releases versions and maintenance patches several times a year which includes new features, enhancements, optimizations and bug fixes.

This topic covers the steps required to update XpoLog with the latest available update if applicable.

For additional details please contact us support@xpolog.com

XpoLog 6 Upgrade and Updates

- This patch is compatible only to XpoLog versions 5.3911 or higher
- Please note that if you are upgrading XpoLog 5.0.x using this patch you will be required to save a valid 6 license to activate
Before you proceed - Verify your version at XpoLog Manager > Settings > About - Installed version. Please contact us if you have any questions.

Review the release notes of V6 version and latest updates under: V6 Release Notes / Latest Patch Notes

Deployment instructions:

1. Download the update - XpoLog 6 Upgrade & Update Patch (save it to your desktop - do not extract).
2. XpoLog will automatically deploy the update, and should present a message indicating a successful deployment once done.
3. Apply a valid XpoLog 6 license (if upgrading from an earlier version)
4. Verify at XpoLog Manager > Settings > About that the update is listed and the installed version is 6.5028

Important - the above procedures cannot be implemented if XpoLog is deployed on an application server as WAR file on a J2EE Application Server, please contact us for more details on how to update/upgrade.

Administrator Guide

Adding Data to the XpoLog Platform

Log files can be loaded into the XpoLog servers from the following types of data sources:

- Any Textual files in any format
- Windows Event Logs
- Syslog
- Database tables

The XpoLog server can read log files into XpoLog from the following types of servers:

- **Direct access (Local or Remote)** - XpoLog can access a local log file, i.e. a log file that resides on the same server as XpoLog, and read it into XpoLog. XpoLog can also access a log file on a remote server to which it has been provided direct access (i.e. the server has a service account that enables remote access to these servers), if XpoLog is provided with the UNC path (\hostname\dirname) to the log files on the remote server or on UNIX based machines direct access to mounted directories.
- **SSH (Secure shell)** - XpoLog can access a log file on remote servers over SSH agent-less, provided that XpoLog has an account with a username and password for connecting to the SSH server on which the log files reside. Usually used for connecting to Unix servers (Linux systems).
- **Windows Network** - XpoLog can access a server in a Windows Network, provided that XpoLog has an account with a username and password for connecting to the Windows server on which the log files reside and XpoLog is installed on a server that runs on Windows.
- **Hadoop HDFS** - XpoLog contains an integration to Hadoop HDFS and can access logs which reside on the Hadoop environment
- **Google App Engine** - XpoLog contains integration to Google App Engine and can access logs from applications that run on the Google App Engine cloud
- **Amazon Web Services (AWS)** - XpoLog contains integration to Amazon Web Services (AWS) and can access machines which are hosted on the Amazon cloud
- **Database** - XpoLog can connect to any Database which supports JDBC connectivity to add database tables as logs in XpoLog
- **Windows Events** - XpoLog support Windows Event logs (evt, evtx) which can be added from remote servers in the Windows environment
- **Remote XpoLog** - XpoLog can communicate over HTTP/S with other XpoLog instances in the environment to collect data from multiple XpoLog instances into a centralized viewer
- **Local XpoLog** - In case there is a need to filter specific data from existing Log, XpoLog can collect logs from its local data repository.
- **Merge XpoLog** - Any log in XpoLog system (regardless of its source location) can be merged to a unified view with other logs, all data will be presented in a single view sorted chronologically
- **Listeners** - XpoLog also functions as a Syslog server, it can use UPD or TCP to receive events from sources/devices which send Syslog message

Note: XpoLog requires Read permission for any log that it reads, regardless of the source of the log file.

While the logs are being copied into the XpoLog server's repository, XpoLog indexes the log files and performs on them Analytics. It saves the data, index and analysis of the log files in XpoLog make them available for searching, analysis and visualization. It is possible to define a storage policy on each log to determine the time XpoLog should keep its data available.

See Adding a Log to XpoLog for detailed instructions on how to add a single log file to XpoLog, or Adding a Logs Directory to XpoLog for detailed instructions on how to add a directory of log files to XpoLog.

Adding a Logs Directory to XpoLog

The Add Logs Directory wizard enables users to add to XpoLog multiple logs that are located in a local or remote directory. The user can scan their local or remote directory for the log directory from which they want to capture logs into XpoLog. The added Logs Directory appears under Folders and Logs in the left panel.
Note: The Add Logs Directory feature described here enables adding a single logs directory to XpoLog. It is also possible to add multiple logs directories and automate a single or multiple logs directory, by adding an Add Logs Directory task (see Adding an Add Logs Directory Task).

Adding a logs directory to XpoLog is performed in the following stages:

1. Selecting the directory location type, and defining connectivity settings accordingly.
2. Specifying the location of the added logs directory in XpoLog.
3. Tagging the newly added log directory to application(s) (optional).
4. Selecting the folders and logs in the logs directory to add to XpoLog.

As logs are written in free format, XpoLog uses its built-in mechanism to guess the structure of the log, also called a pattern. For example, Xpolog guesses which is the date field, the time field, and more, parses the data, and then adds the log records as bulk. Users can normalize or tune the results of parsing. For example, if the results of parsing data is a log with columns Date, Text2, and Text3, the user can open the log under Folders and Logs, and click the log to open it and tune the parsing results. For example, Text2 column heading can be changed to Host, and Text3 column heading to Server Name. Next time you add a log of a similar type to the one that you edited, it uses the last structure that you applied to the new log.

To add a logs directory to XpoLog:

1. Open the XpoLog tab, and in XpoLog Manager, click Add Logs Directory
2. Set the connectivity details to the logs directory (see Defining Connectivity Settings).
3. Click the Next button.
   A Progress box displays the status of the system as it scans the directory for logs, a process that can take several minutes. When the scan completes, the Add Logs Directory Wizard presents the General and Folders and Logs sections.
4. Define the general settings of the logs directory in XpoLog (see Setting Logs Directory General Information).
5. Select the folders and logs of the logs directory to add to XpoLog (see Selecting Logs Directory to Add to XpoLog).
6. Click the Save button.
   The selected folders and logs are created and placed in XpoLog. By default, they are indexed and Analytics is performed on them.
   The Log Viewer opens with the following message: Select a log from the Folders and Logs panel on the left or Create a New Log.

Defining Connectivity Settings

You can add to XpoLog Center a logs directory that resides on a local or remote machine. The selectable directory locations are:

- **Local** – The logs directory is on the same machine as XpoLog Center.
- **Windows Network** – The logs directory is on a remote Windows machine.
- **Over SSH** – The logs directory is on a remote UNIX machine (with SSH connecting protocol).
- **Hadoop HDFS** – The logs directory is in a Hadoop environment.
- **AWS S3 Bucket** – The logs directory is in AWS S3 bucket.

Connecting to a Local Logs Directory

To add a local logs directory to XpoLog:

1. In Directory Location, select Local.
2. In Select Directory, type the path to the directory that contains the log files
3. Optionally, configure Advanced Settings (see Configuring Advanced Settings).
4. Click the Next button.
   A Progress box displays the status of the system as it scans the selected local directory for logs, a process that can take several minutes. When the scan completes, XpoLog presents the General and Folders and Logs sections of the Add Logs Directory Wizard.

Connecting to a Remote Logs Directory

You can add to XpoLog a logs directory residing in any of the following remote locations: Windows Network, Over SSH, Hadoop HDFS and AWS S3 Bucket.

To add a remote logs directory to XpoLog:
1. In Directory Location, select one of the following remote logs directory locations: Windows Network, Over SSH, Hadoop HDFS or AWS S3 Bucket.
2. Under Wizard Settings, in Connection Details, select the authentication account required to connect to the remote location where the selected directory resides, or click the new link to add an authentication account to the system (see Address Book).
3. In Select Directory, type the path to the logs directory
   OR
   Click Browse and in the System Files Browser that opens, expand the folders to get to the desired directory, and then click Select to display the path to the remote logs directory in Select Directory.
4. Optionally, configure Advanced Settings (see Configuring Advanced Settings).
5. Click Next.
   A Progress box displays the status of the system as it scans the selected remote directory for logs, a process that can take several minutes. When the scan completes, XpoLog presents the General and Folders and Logs sections of the Add Logs Directory Wizard.

Configuring Advanced Settings

When adding a Logs Directory to XpoLog, you can configure any of the following advanced settings:

- **Files Filters** – enables specifying which files in the logs directory are to be scanned
- **Scan Method** – enables selecting the mechanisms used to match patterns to the logs during scanning
- **Files Name Pattern** – enables defining how to process files of similar names

**Defining the Files Filters**

By default, XpoLog scans all files from the selected directory. Especially in cases where the directory has many files, you may want to limit the number of files that XpoLog scans. In the File Filters advanced option, you can specify the names of the files to include and/or exclude in the scan, define to add only log files with last updated time that is within the specified time interval, and also define the number of subdirectory levels to scan.

To define the files filters:

1. Under Advanced Settings, click Files Filters.
   The Files Filters definitions open.
2. In Include Files, type the names of the files to include in the scan, separated by commas.
3. In Exclude Files, type the names of the files to exclude from the scan, separated by commas.
4. In Include files from the last, type the time interval and select the time interval unit.
5. In Include the last, type the maximum number of log files that are added per log type.
6. In Subdirectories levels to scan, select Unlimited or a number from 1 to 10.

**Defining the Scan Method**

By default, during scanning, the automatic patterns that are matched to the logs are taken from an existing configuration that is based on log names, log content, and an automatic patterns generator. You can select to activate all these mechanisms (the default), or select the mechanisms to use.

To define the scan method:

1. Under Advanced Settings, click Scan Method.
   The Scan Method options open.
2. Select one of the following options:
   Use existing configuration (file names and content) and automatic matching (the default) – Select this option to try and match patterns to detected logs by matching existing log patterns and log templates. In case no match is detected, runs automatic assignment of patterns. This method captures all readable files during scanning; however, it is the slowest method.
   Use existing configuration (file names and content) – Select this option to try and match patterns to detected logs by matching existing log patterns and log templates. Files for which no existing log patterns or templates are matched are not captured.
   Use existing configuration (file names only) – Select this option to try and match patterns by log templates only. Files for which no templates are matched are not captured.

**Defining Files Name Patterns**

By default, XpoLog applies generic name patterns to files with the same naming convention. However, XpoLog enables you to set the wizard to capture each file separately.

To define files name patterns:

1. Under Advanced Settings, click Files Name Pattern.
   The Files Name Pattern options open.
2. Select one of the following options:
   Unite files with similar names (apply name pattern automatically) (the default) – All files with similar names (such as rotating files, files with date suffixes, and files with numerical prefixes) will be captured as a single log type using a general name pattern.
   Unite files with similar suffix (apply name pattern only at the end of the file name) – All files with similar name suffixes (such as rotating files, files with date suffixes) will be captured as a single log type using a general name pattern.
   Capture each file separately (without name pattern) – A log type will be created for each file.
After XpoLog connects to the logs directory in the local or remote machine and scans it for logs, you can now define under which parent folder in XpoLog to place the newly added logs directory, the collection policy to use, and optionally, the applications to tag to the logs directory.

### Selecting the Logs Directory Location in XpoLog

By default, the logs directory is placed under Folders and Logs in XpoLog Center directly under **Folders and Logs** in the left pane of the Log Viewer. However, you can select or create another parent folder for the newly added logs directory. In this case, the logs directory is placed under the selected parent folder located under **Folders and Logs**.

To select the added logs directory's parent folder:

1. In the **General** section of the Add Logs Directory Wizard, if you want to select for the new log a Parent folder other than the default (**Folders and Logs**), near **Parent Folder**, click **select**.
   
   The Parent Folder page opens, displaying the available parent folders.

2. In the Parent Folder page, do one of the following:
   
   - Select an existing folder to be the parent of the new log, by clicking the folder on the Parent Folder page.
   - Click the **Create New** button, and in **Enter new folder name**, type the name of the new parent folder, and then click the **Save** button. The selected folder appears in Parent Folder.

### Tagging the Logs Directory to Application(s)

Optionally, you can tag the newly added logs directory to applications.

To tag the added logs directory to application(s):

1. Near **Tag to Application(s)**, click **select**.
   
   The Tag to Application(s) page is displayed.

2. In the Tag to Application(s) page, do one of the following:
   
   - Select the checkboxes of the applications to tag to the log.
   - Click the **Create New** button, and in the New Application dialog box, in **Name**, type the name of the new application, and then click the **Add** button. The application is added to the New Application list, and its checkbox is marked.

### Selecting the Log Collection Policy

XpoLog uses a log collection policy to determine how XpoLog server should collect the log directory information into its repository, and how long the logs should be archived. By default, XpoLog uses the default log collection policy. However, you can also use a predefined log collection policy (see **Defining a Log Collection Policy**).

To define a log collection policy:

- In **Collection Policy**, select the collection policy to use.

### Selecting Logs Directory to Add to XpoLog

After the logs directory on the local or remote machine is scanned, a tree of its folders and logs is displayed under the **Folders and Logs** section. By default, all these folders and logs are added to XpoLog. However, you can select to add only some of the directory logs and folders.

To select the logs and folders to add to XpoLog:

- Under the **Folders and Logs** section, clear the checkboxes of the folders and logs that you do not want to add to XpoLog.

### Add Logs Directory Use Case

The Add Logs Directory wizard enables users to add to XpoLog multiple logs that are located in a local or remote directories. The user can scan their local or remote directory for the log directory from which they want to capture logs into XpoLog. Using this wizard may result with adding huge amount of logs and data to XpoLog, therefore it is critical to review the configuration properly prior to completing the execution of collection and indexing of data.

This procedure is important due to two main reasons: if XpoLog process data prior to major configuration changes such as data patterns, data will be reconstructed using the new configuration after it was already processed, which may take time based on the environment sizing. In addition, in order to get optimized search and analysis results it is mandatory to to get data parsed properly (it is not mandatory to parse all log fields however at least ensure the date/time stamp is parsed properly and the rest of the log record can be under a single message field).

### Recommended steps:

1. Prepare and save templates to log samples - use as many log types as possible that will be added during the environment processing and ensure data is parsed properly.
2. Define a new collection policy (temp) with schedule set to ‘Never’. This way no data will be processed before review.
3. Scan the required directory/directories using templates (by setting **Scan Method to use existing configuration**) so the predefined configuration will be applied on the detected logs. Set the temporary collection policy on the scan result so no data will be collected and indexed before reviewing the scan results.
4. Review the results on the scanning by entering selected log types that were detected by the scanner and ensure that all data is parsed and presented properly.
In case you identify log(s) which are not parsed well, make the required changes and replace / save a new template. Use the apply template on logs function to update all required logs based on the templates configuration. At the end of this process all logs should be parsed and presented properly.

5. Apply the required collection policy on the logs that were added by the scan process, so that data will be collected and indexed using the accurate configuration.

The above steps will ensure that data is thoroughly reviewed prior to being processed by XpoLog resulting with a single data execution processing and optimized performance.

Adding a Log to XpoLog

You can add a log to XpoLog Center from any of the following sources:

- **Local** – The log is on the same machine as XpoLog Center or can be directly accessed from a remote server (in the case of Windows) or a mounted directory (in the case of UNIX).
- **Windows Network** – The log is on a remote Windows machine.
- **Over SSH** – The log is on a remote UNIX machine (with SSH connecting protocol).
- **Hadoop HDFS** – The log is in a Hadoop environment.
- **AWS S3 Bucket** - The log is in Amazon Web Services S3 storage.
- **Google App Engine** – The log is on a Google cloud.
- **Database** – Connection is made to a database to import a table from the database as a log.
- **Windows Events** – The log is a Windows Events log.
- **Remote XpoLog** – Connection is made with http (protocol of navigating) or https (secure protocol of navigating, as in a bank) between XpoLog instances.
- **Merge Logs** – Multiple logs in the system are combined into a single unified view log and sorted chronologically.

**Note:** Windows Network and Windows Events logs are only available when Xpolog Center is installed on a Windows machine.

A single log can include many files of the same type or rotated files. For example, a messages log can include the files messages.1, messages.2, and more. It is recommended to capture multiple files of the same log type as one log, using a generic path. This can be done by appending a name pattern to the log path. For example, if a log type contains multiple files that follow a similar name pattern such as mylog.log.20110101_1, mylog.log.20110101_2, mylog.log.20110101_3, ..., mylog.log.20110101_n, you can enter the generic log path: mylog.log.(date,yyyy-MM-dd)_{string}.

Examples:

- `/var/log/messages[string]`  
  - log.1.log, log.2.log, and log.3.log can be represented by the name pattern log.(string).log.
- `myapp.25-8-2009-22:30:00, myapp.26-8-2009-22:30:00, and myapp.27-8-2009-22:30:00` can be represented by the name pattern myapp.(date,dd-MM-yyyy-HH:mm:ss).

As logs are written in free format, XpoLog uses its built-in mechanism to guess the structure of the incoming log, also called a pattern. For example, Xpolog guesses which field is the Date, the Time, and more, parses the data, and then adds the log records in bulk to XpoLog. Users can further normalize or tune the results of parsing. For example, if the results of parsing data is a log with columns Date, Text2, and Text3, the user can open the log under Folders and Logs, and click the log to open it and tune the parsing results. For example, Text2 column heading can be changed to Host, and Text3 column heading to Server Name. Next time you add a log of a similar type to the one that you edited, it uses the last structure that you applied to the new log.

Once a log is brought into XpoLog it is indexed and undergoes Analytics. You can also run searches on it, and perform all log actions on it. To add a log to XpoLog:

1. Open the XpoLog tab, and in XpoLog Manager, click Add Log
   OR
   Open the XpoLog tab, and in the Administration menu, select Add Log
   OR
   In the XpoLog homepage, in the left pane under More Actions, click Add log
   OR
   In the XpoLog homepage, in the left pane under More Actions, click Quick start wizard, and in the Quick Start Wizard that opens, click Add Log
   OR
   Open the XpoLog tab, and in the Administration menu, select Folders and Logs, and in the Folders and Logs console that opens, click the New Log button.
   The Add Log Wizard opens.
2. Set the basic information of the log being added to XpoLog, including log name, location, and tagging to applications (see Setting Log General Information).
3. In Log Source, select the log source of the log to add to XpoLog
4. Fill in the connectivity information for the selected log type, as follows:
   a. For a Local log, complete the information as described in Adding a Local Log.
   b. For a Windows Network log, complete the information as described in Adding a Windows Network Log.
   c. For an Over SSH log, complete the information as described in Adding an Over SSH Log.
   d. For a Hadoop HDFS log, complete the information as described in Adding a Hadoop HDFS Log.
   e. For a AWS S3 Bucket log, complete the information as described in Adding an AWS S3 Bucket Log.
   f. For a Google App Engine log, complete the information as described in Adding a Google App Engine.
g. For a **Database** log, complete the information as described in **Adding a Database Log**.

h. For a **Windows Events** log, complete the information as described in **Adding a Windows Events Log**.

i. For a **Remote XpoLog** log, complete the information as described in **Adding a Remote XpoLog Log**.

j. For a **Merge Logs** log, complete the information as described in **Adding a Merged Log**.

5. At this point it is possible to save the log, or going “Next” if applicable to review the Data Pattern Configuration.

6. Once the log is added to XpoLog, validate the log configuration (see **Verifying Added Log Configuration**).

---

### Setting Log General Information

The first screen of the Add Log wizard includes the Basic Info section for defining the basic information of the new log in XpoLog Center, including:

- **Log Name** – the name of the log in XpoLog Center
- **Parent Folder** – the folder where to locate the newly added log
- **Tag to Application(s)** – optional; the applications to tag to the log
- **Log Type(s)** – optional; the log type of the added log
- **Collection Policy** – the collection policy for the added log

### Setting the Log Name and Location in XpoLog

By default, the log is placed under Folders and Logs in XpoLog Center directly under **Folders and Logs** in the left pane of the Log Viewer. However, you can select or create another parent folder for the newly added log. In this case, the log is placed under the selected parent folder located under **Folders and Logs**.

To set the name and location of the newly added log:

1. In the **Basic Info** section of the Add Log Wizard, in **Log Name**, type a meaningful name for the new log.
2. If you want to select for the new log a Parent folder other than the default (**Folders and Logs**), near **Parent Folder**, click **select**. The Parent Folder page opens, displaying the available parent folders.
3. In the Parent Folder page, do one of the following:
   - Select an existing folder to be the parent of the new log, by clicking the folder on the Parent Folder page.
   - Click the **Create New** button, and in **Enter new folder name**, type the name of the new parent folder, and then click the **Save** button. The selected folder appears in **Parent Folder**.

### Tagging the Log to Application(s)

Optionally, you can tag the newly added log to applications.

To tag the added logs directory to application(s):

1. Near **Tag to Application(s)**, click **select**. The Tag to Application(s) page is displayed.
2. In the Tag to Application(s) page, do one of the following:
   - Select the checkboxes of the applications to tag to the log.
   - Click the **Create New** button, and in **Name**, type the name of the new application, and then click the **Add** button. The application is added to the New Application list, and its checkbox is marked.
3. In the Tag to Application(s) page, click the **Apply** button. The selected applications, separated by commas, appear in **Tag to Application(s)**.

### Tagging the Log to Log Type(s)

Optionally, you can tag the newly added log to log type.

To tag the added logs directory to log type(s):

1. In the **Log Types**, type a meaningful name for the log type of the new log.

### Selecting the Log Collection Policy

XpoLog uses a log collection policy to determine how XpoLog server should collect the log information into its repository, and how long the log should be archived. By default, XpoLog uses the default log collection policy. However, you can also use a predefined log collection policy (see **Defining a Log Collection Policy**).

To define a log collection policy:

- In **Collection Policy**, select the collection policy to use.

### Adding a Local Log

On a Windows machine, you can bring into XpoLog local logs that reside on either of the following:

- The same Windows machine, provided that XpoLog has Read permissions on these logs. Example: **My Computer > C > Logs**
- A remote server to which you have direct access. This requires providing a UNC path (**\hostname\dir_name**) through which XpoLog can locate the files on these servers. Example: **\qaserver$**.

In cases where you want to view or search an archived log, you can restore it by adding it as a local log.
Note: To access a remote Windows server that requires authentication, see Adding a Windows Network Log.

To add a local log to XpoLog:

1. In Log Path, type the path to the log's location
   OR
   Click Browse and in the System Files Browser that opens, expand the folders to get to the desired log, and then click Select to display the log location in Log Path.
2. Optionally, append to the log path a name pattern to capture multiple files from the same log. (For pattern syntax, see XpoLog Patterns Language.)
3. Optionally, define advanced settings for the local log – Files Attributes, Files Filters, and/or Regional Settings (see Configuring Advanced Log Settings).
4. Click either of the following buttons:
   Save – XpoLog applies an automated pattern on the incoming log, and the Log Viewer opens displaying the parsed records of the new log. The log name is displayed in the left pane in its selected location under Folders and Logs. If you put in the log path a {string} pattern, the various files of the log appear in the left pane. Otherwise, only one file appears. You can perform regular actions on this log.
   Next – The Patterns administration screen opens. Apply patterns on the log data and save the log in XpoLog (see Applying Patterns on the Log).

Comments:

- On a Unix machine, you can bring into XpoLog local logs that reside on the same machine or in a mounted directory to which you have direct access.
- On a Windows machine you can define zipped logs (single/multiple files) without extracting them:
  If you have a file archive.zip, which contains inside a single file, it should be defined directly on that file archive.zip
  If you have a file archive.zip, which contains inside multiple files (log-name.log, log-name.log.1, log-name.log.2, ..., log-name.log.N) it should be defined using the name pattern: archive.zip?log-name.log{string}

Adding a Windows Network Log

If a Windows Network machine has security activated, you require an authentication account to access it. Otherwise, if authentication is not required, you can also access a Windows Network log from the Local log type page (see Adding a Local Log).

Note: Windows Network logs are only available when XpoLog Center is installed on a Windows machine.

Note: It is highly recommended to save a user on the XpoLog Service (Windows Services -> XpoLog Center Service -> Properties -> Log On tab). Once a user is applied on the XpoLog service it is possible to add remote Windows logs using type 'local' by providing a UNC path (\hostname\dir_name). Example: \qaserver\c$\Log Files\log.log.

To add a Windows Network Log to XpoLog:

1. In Connection Details, select the Windows Authentication account required to connect to the log, or click the new link to add an account to the system (see Address Book).
   Note: If you do not have any Windows authentication accounts defined in XpoLog, the Add Windows Authentication account page is presented automatically.
   Recommended: It is recommended to configure a service account (on the XpoLog Service in the Windows Services Panel) with the required permissions to read logs from remote machines in the network. Then all logs, local or any other machine in the network, can be defined as Local log type page (see Adding a Local Log).
2. In Log Path, type the path to the log's location
   OR
   Click Browse to open the System Files Browser of the Windows Network machine that you connected to, expand the folders to get to the desired log, and then click Select to display the log location in Log Path.
3. Optionally, append to the log path a name pattern to capture multiple files from the same log. (For pattern syntax, see XpoLog Patterns Language.)
4. Optionally, define advanced settings for the Windows Network log – Files Attributes, Files Filters, and/or Regional Settings (see Configuring Advanced Log Settings).
5. Click either of the following buttons:
   Save – XpoLog applies an automated pattern on the incoming log, and the Log Viewer opens displaying the parsed records of the new log. The log name is displayed in the left pane in its selected location under Folders and Logs. If you put in the log path a (string) pattern, the various files of the log appear in the left pane. Otherwise, only one file appears. You can perform regular actions on this log.
   Next – The Patterns administration screen opens. Apply patterns on the log data and save the log in XpoLog (see Applying Patterns on the Log).

Adding an Over SSH Log

To add an Over SSH log to XpoLog:

1. In Connection Details, select the SSH account required to connect to the log, or click the new link to add an account to the system (see Address Book).
   Note: If you do not have any SSH accounts defined in XpoLog, the Add SSH account page is presented automatically.
2. In Log Path, type the path to the log on the remote machine
   OR
   Click Browse to open the System Files Browser of the remote machine that you connected to, expand the folders to get to the desired
log, and then click **Select** to display the log location in **Log Path**.

3. Optionally, append to the log path a name pattern to capture multiple files from the same log. (For pattern syntax, see **XpoLog Patterns Language**.)

4. Optionally, define advanced settings for the SSH log – Files Filters, and/or Regional Settings (see **Configuring Advanced Log Settings**).

5. Click either of the following buttons:
   - **Save** – XpoLog applies an automated pattern on the incoming log, and the Log Viewer opens displaying the parsed records of the new log. The log name is displayed in the left pane in its selected location under Folders and Logs. If you put in the log path a (string) pattern, the various files of the log appear in the left pane. Otherwise, only one file appears. You can perform regular actions on this log.
   - **Next** – The Patterns administration screen opens. Apply patterns on the log data and save the log in XpoLog (see **Applying Patterns on the Log**).

**Comments:**

- XpoLog utilized some system commands on the remote server in order to read the logs without the need to deploy agents. In case XpoLog indicates that some of these commands are missing (mainly the ‘Less’ command), it is very easy to use **XpoLog LogAway** which replaces the native commands.
- Over SSH supports **gz**, **tar** and **tar.gz** logs without extracting them:
  - If you have a file **archive.gz** with a single file in it, it should be defined directly on that file **archive.gz**
  - If you have a file **archive.tar** / **archive.tar.gz** with a single file in it, it should be defined directly on that file **archive.tar** or **archive.tar.gz**
  - If you have a file **archive.tar** / **archive.tar.gz**, which contains inside multiple files (**log-name.log**, **log-name.log.1**, **log-name.log.2**, ..., **log-name.log.N**) it should be defined using the name pattern: **archive.tar?log-name.log{string}** or **archive.tar.gz?log-name.log{string}**

**SSH Log Using LogAway (V4.3+)**

**Note:** **LogAway Agent (compatible with XpoLog V4.3+)**

**Summary**

XpoLog’s agent-less architecture allows accessing logs located on remote machines over SSH, without the need to change or install anything on the remote machine. In order to do this, XpoLog utilizes the ‘less’ command on the remote machine, among other commands. In some environments, where the ‘less’ command is not available on the remote machine, XpoLog cannot work as described above.

XpoLog’s LogAway agent provides a solution for accessing logs located on remote machines over SSH where the ‘less’ command is not available. It is important to note that the agent is **passive**, and does not run any process on the remote machine unless requested to do so by the XpoLog server.

**Technical Details**

XpoLog’s LogAway agent is a JAR file located in the home directory of the user that is used by XpoLog to access the remote machine. After the JAR file is deployed on the remote machine, it does not run any process. Instead, the XpoLog server automatically identifies that the LogAway agent is available on the remote machine, and uses it instead of utilizing traditional system commands.

All the data which is transferred by the LogAway agent to the XpoLog server is compressed, to minimize network traffic.

**Deployment**

1. Verify that Java is installed on the remote machine:
   a. Log in to the remote machine using the same user that is used by XpoLog to access the remote machine.
   b. Run the command `java -version` (the LogAway agent requires Java version 1.3+ to run)
2. Download XpoLog’s LogAway package compatible to the Java version installed on the remote machine:
   a. Download LogAway for Java 1.3: **LogAway for JAVA 1.3**
   b. Download LogAway for Java 1.4+: **LogAway for JAVA 1.4+**
3. Copy XpoLog’s LogAway package to the remote machine (place it in the home directory of the user that is used by XpoLog to access the remote machine)
4. Unpack XpoLog’s LogAway package by running the following commands:
   a. `gunzip xpologAgent.tar.gz`
   b. `tar xvf xpologAgent.tar`
   c. Verify that a folder named `xpologAgent` was created and contains several files
5. Verify that XpoLog’s LogAway agent can be executed:
   a. Enter the `xpologAgent` folder
   b. Run the command `sh runAgent.sh -v`
   c. Verify that information regarding the agent is printed to the screen
6. In order to verify that the agent can be used by the XpoLog server, add a log over SSH on this machine using direct access mode and check that everything works as expected.
   - Open **XpoLog Support Portal > Activity Information and under SSH connections tab verify that the connection mode is Agent (instead of the default: Less).**

**SSH Log Using LogAway (V4.5+)**
Note: LogAway Agent (compatible with XpoLog 4.5+)

The new version of LogAway is compatible with XpoLog 4.5+, and supports a higher transfer log rate (~300MB/Minute)

Summary

XpoLog’s agent-less architecture allows accessing logs located on remote machines over SSH, without the need to change or install anything on the remote machine. In order to do this, XpoLog utilizes the ‘less’ command on the remote machine, among other commands. In some environments, where the ‘less’ command is not available on the remote machine, XpoLog cannot work as described above. XpoLog’s LogAway agent provides a solution for accessing logs located on remote machines over SSH where the ‘less’ command is not available. It is important to note that the agent is passive, and does not run any process on the remote machine unless requested to do so by the XpoLog server.

Technical Details

XpoLog’s LogAway agent is a JAR file located in the home directory of the user that is used by XpoLog to access the remote machine. After the JAR file is deployed on the remote machine, it does not run any process. Instead, the XpoLog server automatically identifies that the LogAway agent is available on the remote machine, and uses it instead of utilizing traditional system commands.

All the data which is transferred by the LogAway agent to the XpoLog server is compressed, to minimize network traffic.

Deployment

1. Verify that Java is installed on the remote machine:
   a. Log in to the remote machine using the same user that is used by XpoLog to access the remote machine.
   b. Run the command `java -version` (the LogAway agent requires Java version 1.4+ to run)
2. Download XpoLog’s LogAway package compatible to the Java version installed on the remote machine:
   [Download LogAway for Java 1.4+]
3. Copy XpoLog’s LogAway package to the remote machine (place it in the home directory of the user that is used by XpoLog to access the remote machine)
4. Unpack XpoLog’s LogAway package by running the following commands:
   a. `gunzip xpologAgent.tar.gz`
   b. `tar xvf xpologAgent.tar`
   c. Verify that a folder named `xpologAgent` was created and contains several files
5. Verify that XpoLog’s LogAway agent can be executed:
   a. Enter the `xpologAgent` folder
   b. Run the command `sh runAgent.sh -v`
   c. Verify that information regarding the agent is printed to the screen
6. Verify on the remote server that TCP port forwarding is enabled:
   a. View the file `/etc/ssh/sshd_config`
   b. The parameter ‘AllowTcpForwarding’ specifies whether TCP forwarding is permitted (the default is “yes”). Note that disabling TCP forwarding does not improve security unless users are also denied shell access, as they can always install their own forwarders. In case ‘AllowTcpForwarding’ is set to “no” change it to “yes” and restart the SSH service.
7. Go to XpoLog>Settings>General, and under the ‘Connection Policies’ configure the following:
   a. LogAway Agent forwarding port - a free port on the remote machine to use (try “netstat” to list ports in use). LogAway uses the port locally in order to use SSH port forwarding (for example: 5555). It is not recommended to use ports 0-1023, as these are usually system processes ports.
   b. LogAway Agent forwarding timeout - the allowed period of LogAway Agent inactivity before it’s connection is terminated (default 1 minute)
8. In order to verify that the agent can be used by the XpoLog server, add a log over SSH on this machine using direct access mode and check that everything works as expected.

Adding a Hadoop HDFS Log

To add a Hadoop log to XpoLog:

1. In Connection Details, select the Hadoop account required to connect to the log, or click the new link to add an account to the system (see Address Book).
   Note: If you do not have any Hadoop accounts defined in XpoLog, the Add Hadoop account page is presented automatically.
2. In Log Path, type the path to the Hadoop log
   OR
   Click Browse to open the System Files Browser of the Hadoop environment that you connected to, expand the folders to get to the desired log, and then click Select to display the path to the log in Log Path.
3. Optionally, append to the log path a name pattern to capture multiple files from the same log. (For pattern syntax, see XpoLog Patterns Language.)
4. Optionally, define advanced settings for the Hadoop log – Files Attributes, Files Filters, and/or Regional Settings (see Configuring Advanced Log Settings).
5. Click either of the following buttons:
   Save – XpoLog applies an automated pattern on the incoming log, and the Log Viewer opens displaying the parsed records of the new log. The log name is displayed in the left pane in its selected location under Folders and Logs. If you put in the log path a (string)
pattern, the various files of the log appear in the left pane. Otherwise, only one file appears. You can perform regular actions on this log. Next – The Patterns administration screen opens. Apply patterns on the log data and save the log in XpoLog (see Applying Patterns on the Log).

Adding a Google App Engine
To add a Google App Engine log to XpoLog:

1. In Connection Details, select the Google App Engine account required to connect to the log, or click the new link to add an account to the system (see Address Book).
2. A list of applications that Xpolog extracted from the Google App Engine is displayed.
3. Note: If you do not have any Google App Engine accounts defined in Xpolog, the Add Google App Engine account page is presented automatically.
4. Select the checkboxes of the applications to add to Xpolog.
5. Optionally, define advanced settings for the Google App Engine log – Regional Settings (see Configuring Advanced Log Settings).
6. Click Save.

Xpolog applies an automated pattern on the incoming log, and the Log Viewer opens displaying the parsed records of the new log. The log name is displayed in the left pane in its selected location under Folders and Logs. You can perform regular actions on this log.

Adding a Windows Events Log
Adding a Windows Events log (format evt/evtx) is similar to importing a local log, except that you are also required to enter a host name and set the type of events (Application/Security/System/Custom/*.evt).

Note: Windows Events logs are only available when Xpolog Center is installed on a Windows machine.

To add a Windows Events log to Xpolog:

1. In Connection Details, select the Windows authentication account required to connect to the remote log, or click the new link to add an account to the system.
2. Note: If you do not have any Windows Events account, the Add Windows Events account page is presented automatically.
3. In Host Name, type the IP address of the host. Leave blank for a local host.
4. Select the type of log events to bring into Xpolog:
   - Application – Select the Application option button.
   - Security – Select the Security option button.
   - System – Select the System option button.
   - Custom – Select the Custom option button, and type a Windows log type.
   - File – Select the File option button, type or browse and select a *.evt/*.evtx file, and select its type: Application, Security, or System.
5. Optionally, define Regional Settings for the Windows Events log (see Configuring Advanced Log Settings).
6. Click Save.

Xpolog applies an automated pattern on the incoming log, and the Log Viewer opens displaying the parsed records of the new log. The log name is displayed in the left pane in its selected location under Folders and Logs. You can perform regular actions on this log.

Adding Windows Events Logs from Multiple Machines
Xpolog provides a wizard that helps adding Windows Event logs from multiple machines based on an external configuration XML file.

Please follow the below steps:

1. Import Windows Event logs templates package into your Xpolog:
   a. Download the package here: Windows Event Logs Templates (do not extract)
   b. Go to Xpolog>Configuration>Import Templates, select the zip file and save
   c. Xpolog will import the templates of Application, Security and System Windows Event Logs
2. Prepare the Wizard:
   a. Download the package here: Windows Event logs Xpolog Package and extract it on your desktop
   b. Edit the following files:
      i. logsAdminClient.properties:
         xpologURL - should be the URL to your Xpolog instance. For example if you extracted it on the same machine that you are using to run Xpolog, use this: http://localhost:30303/logeye
         user / password - should be the administrator user of Xpolog in case security is activated (admin/admin by default) or leave empty if security is not active
         configFile - should be the configuration XML file (by default: logsAdminConfigurationWizard.xml)
      ii. logsAdminConfigurationWizard.xml:
         For each server that you wish to add it's Windows Event logs enter it's name under the <server> tag - the example contains 2 entries of servers which should be modified (add more / remove based on the machines in your environment)

DirectoryScanner XML General Structure

The following is the XML code of DirectoryScanner.
<ConfigurationWizard>
  <Defaults>
    <LogsGroup>
      <Log logTemplate="" />
      <Log logTemplate="" />
      <Log logTemplate="" />
    </LogsGroup>
    <Server targetName="" accountName="" >
      <LogsGroup target="" />
    </Server>
    <Server targetName="" >
      <LogsGroup target="" />
    </Server>
  </Defaults>
  <Servers>
    <Server target="" name="" collectionPolicy="" displayName="" />
    <Server target="" name="" collectionPolicy="" displayName="" />
  </Servers>
</ConfigurationWizard>

The following table describes the general structure of ConfigurationWizard.

<table>
<thead>
<tr>
<th>Tag Path</th>
<th>Mandatory/Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defaults</td>
<td>Mandatory</td>
<td>Contains the target name to use, logs names that will created, the location in the XpoLog Folders and Logs tree and the application which logs are tagged to when created.</td>
</tr>
<tr>
<td>Defaults/LogsGroup</td>
<td>Mandatory</td>
<td>The templates which will be used on each server to add the logs.</td>
</tr>
<tr>
<td>Defaults/LogsGroup/Log</td>
<td>Mandatory</td>
<td>Contains a target of server. If needed a the connectivity account that should be used to connect to a remote Windows server can be specified (Creating an Account).</td>
</tr>
<tr>
<td>Servers</td>
<td>Mandatory</td>
<td>Contains the list of servers which will be scanned.</td>
</tr>
<tr>
<td>Servers/Server</td>
<td>Mandatory</td>
<td>Contains the target that should be used in the server, server hostname/ip address, collection policy which will be tagged to the server's log and a server display name.</td>
</tr>
</tbody>
</table>

**XML Reference**

**Defaults/LogsGroup**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetName</td>
<td>Mandatory</td>
<td>The name of the target of this LogsGroup.</td>
<td>String</td>
</tr>
<tr>
<td>logNameStructure</td>
<td>Mandatory</td>
<td>The name structure of the logs that will created. Available placeholders that can be used: [TEMPLATE_NAME], [SERVER_NAME], [displayName]</td>
<td>String</td>
</tr>
<tr>
<td>folderNameStructure</td>
<td>Mandatory</td>
<td>The folder name and location that the logs will be tagged to in XpoLog's folders and logs tree. Root = Top Folder -&gt; = separator to the next folder in the hierarchy Available placeholders that can be used to tag/create folders: [TEMPLATE_NAME], [SERVER_NAME], [displayName]</td>
<td>String</td>
</tr>
<tr>
<td>applications</td>
<td>Optional</td>
<td>The name of the application which the logs will be tagged to. Leave empty or remove in order not to tag logs to an application</td>
<td>String</td>
</tr>
<tr>
<td>Log/logTemplate</td>
<td>Mandatory</td>
<td>The exact name of the template which will be used to create the log</td>
<td>String</td>
</tr>
</tbody>
</table>

Example
<LogsGroup targetName="default" logNameStructure="[displayName] [TEMPLATE_NAME]" folderNameStructure="Root->[displayName]" applications="Windows Event Logs" />
<Log logTemplate="Application" />
<Log logTemplate="Security" />
<Log logTemplate="System" />
</LogsGroup>

**Defaults/Server**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetName</td>
<td>Mandatory</td>
<td>The name of the target of this server.</td>
<td>String</td>
</tr>
<tr>
<td>accountName</td>
<td>Optional</td>
<td>If a connectivity account should be used to connect to a remote Windows server the account name can be specified (Creating an Account)</td>
<td>String</td>
</tr>
<tr>
<td>LogsGroup/target</td>
<td>Mandatory</td>
<td>The name of the LogsGroup's target that should be used</td>
<td>String</td>
</tr>
</tbody>
</table>

**Example**

```xml
<Server targetName="AuthAccountEnabled" accountName="AuthAccountName" />
<LogsGroup target="default" />
</Server>
```

**Servers**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server/target</td>
<td>Mandatory</td>
<td>The target that this server should use</td>
<td>String</td>
</tr>
<tr>
<td>Server/name</td>
<td>Mandatory</td>
<td>The ip or hostname of this server</td>
<td>String</td>
</tr>
<tr>
<td>Server/collectionPolicy</td>
<td>Optional</td>
<td>The collection policy that will be assigned on logs from this server. If used, the name should be the exact name of an existing collection policy in XpoLog</td>
<td>String</td>
</tr>
<tr>
<td>Server/displayName</td>
<td>Optional</td>
<td>The display name of the server. Usually used if the name and the display name of a server are different. The display name placeholder can be used in the folders/logs names structure</td>
<td>String</td>
</tr>
</tbody>
</table>

**Example**

```xml
<Server target="AuthAccountEnabled" name="ip/hostname" collectionPolicy="PolicyName" displayName="displayName1" />
<Server target="AuthAccountDisabled" name="ip/hostname" collectionPolicy="PolicyName" displayName="displayName2" />
</Servers>
```

3. Verify that JAVA is available on the machine you are running the wizard from:
   a. Open the command line console and run `java` - in case JAVA is installed please proceed to the next step
   b. In case JAVA is not installed, please edit the file run.bat and set a path to an available JAVA on the machine from which you're running this wizard from. For example if you are using the Wizard on the same machine that you are running XpoLog on, you can use XpoLog internal JAVA, for example modify the file run.bat and use: "C:\Program Files\XpoLogCenter6\jre\bin\java" instead of 'java'

4. Run the batch file run.bat

5. Once done, refresh XpoLog. The result will be a list of folders in XpoLog (one for each server) with the server's Windows Event logs configured under it.

**Adding a Database Table as Log Source**

You can add data (in table format) from a database into XpoLog as a log, provided that the database is connected to a JDBC driver. Database table configuration in XpoLog should be based on a common SQL query.

To add a database table into XpoLog as a log:

1. In **Connection Details**, select the account required to connect to the database, or click the **new** link to add an account to the system. **Note:** If you do not have any Database account, the Add Database account page is presented automatically.
2. Optionally, define advanced settings for the Database log – Data Access Mode and/or Regional Settings (see Configuring Advanced Log Settings).
3. Click **Next**.
The Database Query Administration screen opens, listing the tables in the database.

4. Select the table that you want to add to XpoLog as a log.

5. In the **Query Definition** textbox, write an expression based on SQL syntax to execute on the selected table(s).
   
   - **Note:** If you are not familiar with SQL syntax, leave the default expression.
   
   - **Advanced:** If you are interested to add functions that will run at the end of the query use at the end of the entered query XPLG_QUERY_INSERT and then the function. For example:
   
   ```
   Select * from TABLE_NAME XPLG_QUERY_INSERT with UR
   ```
   
6. Optionally, click **Verify Query** to preview on the lower half of the screen, the log records resulting from the query that you input. If you would like to change the resulting log, repeat step 5.

7. Select the maximum records that you want XpoLog to show.
   
   - **Note:** By default XpoLog will retrieve only 10000 records from the table. It is highly recommended to select 'Unlimit' and then click order by to specify which column should be used for the order by when querying the table. The selected column must be unique - either an ID or Date so that each collection cycle will start from the last record which was collected.

8. Click **Save**.

   The database logs are displayed in the Log Viewer.

---

**IBM DB2**

In order to add a table from IBM DB2 as a log source to XpoLog follow these steps:

**JDBC Driver**

1. Download the required driver from here
2. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
3. In the Database Types screen, click the 'Upload Driver' button and select the JDBC jar file and click the 'Upload' button.

**Database account**

1. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
2. The JDBC Status of DB2 should be ready, select it and click 'Create Account'.
3. Required details:

   - **Name**
   - **Description**
   - **Driver Name** should be left default (com.ibm.db2.jcc.DB2Driver)
   - **Host Address** - the database hostname or IP address
   - **Port** - the port that should be used to establish a connection (default 50000)
   - **Database Name** - the name of the target database
   - **User** - the user name that will be used for authentication
   - **Password** - the password that will be used for authentication

4. Save the account and click on the 'Verify' button to verify the connectivity.

   If verification fails - ensure all the details are accurate, and that the XpoLog machine can establish a connection to the database machine on port 50000.

5. Once connectivity is verified it is possible to add tables as log source from this database

---

**Microsoft SQL Server 2008+**

In order to add a table from Microsoft SQL Server 2008 or higher as a log source to XpoLog follow these steps:

**SQL Authentication**

**JDBC Driver**

1. Download the driver from here
2. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
3. In the Database Types screen, click the ‘Upload Driver’ button and select the JDBC jar file and click the 'Upload' button.

**Database account**

1. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
2. The JDBC Status of SQL Server 2008 should be ready, select it and click 'Create Account'.
3. Required details:

   - **Name**
   - **Description**
   - **Driver Name** should be left default (com.microsoft.sqlserver.jdbc.SQLServerDriver)
   - **Host Address** - the database hostname or IP address
   - **Port** - the port that should be used to establish a connection (default 1433)
   - **Database Name** - the name of the target database
   - **User** - the user name that will be used for authentication
   - **Password** - the password that will be used for authentication

4. Save the account and click on the 'Verify' button to verify the connectivity.
If verification fails - ensure all the details are accurate, and that the XpoLog machine can establish a connection to the database machine on port 1433.

5. Once connectivity is verified it is possible to **add tables as log source** from this database

Example:

### SQL Server 2008 Database Account

<table>
<thead>
<tr>
<th>Name *</th>
<th>SQL Server Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Driver Name *</td>
<td>com.microsoft.sqlserver.jdbc.SQLServerDriver</td>
</tr>
<tr>
<td>Host Address *</td>
<td>10.0.0.119</td>
</tr>
<tr>
<td>Port</td>
<td>1433</td>
</tr>
<tr>
<td>Database Name *</td>
<td>master</td>
</tr>
<tr>
<td>Username *</td>
<td>sa</td>
</tr>
<tr>
<td>Password</td>
<td>*********</td>
</tr>
</tbody>
</table>

* marks a mandatory field

**Windows Authentication**

**JDBC Driver**

1. Download the driver from [here](#).
2. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
3. In the Database Types screen, click the 'Upload Driver' button and select the jtds-1.2.2.jar and click the 'Upload' button.

**Database account**

1. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
2. Select type **Other** and click 'Create Account'.
3. Required details:

   - Name
   - Description
   - Driver Name should be: net.sourceforge.jtds.jdbc.Driver
   - Connection String - jdbc:jtds:sqlserver://<host-name>:<port>/<database-name>;domain=<domain-name>
   - User - the user name that will be used for authentication
   - Password - the password that will be used for authentication
   - Database Type - should be SQL Server

4. Save the account and click on the 'Verify' button to verify the connectivity.

If verification fails - ensure all the details are accurate, and that the XpoLog machine can establish a connection to the database machine on port 1433.

5. Once connectivity is verified it is possible to **add tables as log source** from this database

Example:
MySQL Database

In order to add a table from MySQL Database as a log source to XpoLog follow these steps:

**JDBC Driver**

1. Download the driver from [here](#)
2. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
3. In the Database Types screen, click the 'Upload Driver' button and select the JDBC jar file and click the 'Upload' button.

**Database account**

1. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
2. The JDBC Status of MySQL should be ready, select it and click 'Create Account'.
3. Required details:
   - Name
   - Description
   - Driver Name *should be left default (com.mysql.jdbc.Driver)*
   - Host Address - the database hostname or IP address
   - Port - the port that should be used to establish a connection (default 3306)
   - Database Name - the name of the target database
   - User - the user name that will be used for authentication
   - Password - the password that will be used for authentication

4. Save the account and click on the 'Verify' button to verify the connectivity.
   If verification fails - ensure all the details are accurate, and that the XpoLog machine can establish a connection to the database machine on port 3306.
5. Once connectivity is verified it is possible to add tables as log source from this database

Oracle Database

In order to add a table from Oracle Database as a log source to XpoLog follow these steps:

**JDBC Driver**

1. Download the driver from [here](#)
2. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
3. In the Database Types screen, click the 'Upload Driver' button and select the classes12.jar and click the 'Upload' button.

**Database account**

1. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
2. The JDBC Status of Oracle should be ready, select it and click 'Create Account'.
3. Required details:
   - Name
   - Description
   - Driver Name *should be left default (oracle.jdbc.driver.OracleDriver)*
   - Host Address - the database hostname or IP address
   - Port - the port that should be used to establish a connection (default 1521)
   - Database Name - the name of the target database
   - User - the user name that will be used for authentication
   - Password - the password that will be used for authentication
4. Save the account and click on the ‘Verify’ button to verify the connectivity. If verification fails - ensure all the details are accurate, and that the XpoLog machine can establish a connection to the database machine on port 1521.

5. Once connectivity is verified it is possible to add tables as log source from this database

**PostgreSQL**

In order to add a table from PostgreSQL as a log source to XpoLog follow these steps:

**JDBC Driver**

1. Download the driver from here
2. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
3. In the Database Types screen, click the ‘Upload Driver’ button and select the JDBC jar file and click the ‘Upload’ button.

**Database account**

1. Go to XpoLog Manager > Tools > Address Book, Add New Database Account.
2. The JDBC Status of PostgreSQL should be ready, select it and click ‘Create Account’.
3. Required details:
   - Name
   - Description
   - Driver Name - should be left default (org.postgresql.Driver)
   - Host Address - the database hostname or IP address
   - Port - the port that should be used to establish a connection (default 5432)
   - Database Name - the name of the target database
   - User - the user name that will be used for authentication
   - Password - the password that will be used for authentication
4. Save the account and click on the ‘Verify’ button to verify the connectivity. If verification fails - ensure all the details are accurate, and that the XpoLog machine can establish a connection to the database machine on port 5432.
5. Once connectivity is verified it is possible to add tables as log source from this database

**Adding a Merged Log**

You can created a merged log from local logs residing on your machine. The merged log records are sorted chronologically, and include information from the merged logs, with an additional leftmost column indicating the source of the record.

To add a merged log to XpoLog:

1. In the Select Logs to Merge page that opens upon selecting Merge Logs as the log type, select the checkboxes of the logs to merge, and then click Apply. The selected logs appear in the Logs to Merge field, separated by commas.
2. Optionally, define advanced settings for the merged log – Regional Settings (see Configuring Advanced Log Settings).
3. Click Save
   - The Log Viewer opens displaying the merged records of the new log. The log name is displayed in the left pane in its selected location under Folders and Logs. You can perform regular actions on this log.

**Adding a Remote XpoLog Log**

XpoLog is usually agentless. Remote XpoLog is an agent-based mode of XpoLog, which is supported in organizations that do not have direct access to a server, for example highly secured networks that do not allow direct connection to the server, mainframes, etc.. In this case, local XpoLog instances can communicate with each other over HTTP/S, and one XpoLog instance can connect to another and import from it log(s).

Logs that are added to your XpoLog system from a remote XpoLog system appear under the list of Folders and Logs in the left pane of your XpoLog system log viewer. There is no indication that these log(s) came from another XpoLog system for the users, only for administrators on edit mode.

To add a remote XpoLog log into your XpoLog system:

1. In **Connection Details**, select the authentication account required to connect to the server where the log resides, or click the **new** link to add an account to the system (see Address Book).
   - **Note**: If you do not have connectivity details for any Remote XpoLog accounts, the Add Remote XpoLog Account page is presented automatically.
   - Select the Remote XpoLog instance you wish to pull logs from.
2. In the Remote XpoLog instance, select the logs to add to your XpoLog instance (multiple logs may be selected).
3. Click **Save**.
   - The remote XpoLog logs are added to your XpoLog instance.

**Configuring Advanced Log Settings**

When adding a log to XpoLog, you can configure the advanced settings that are available for the log type of the log that you are adding. The available advanced settings are:

- **Data Filter** – enables filtering data during collection
Files Attributes – for local, Over SSH, and Hadoop HDFS logs
Files Filters – for local, Over SSH, and Hadoop HDFS logs; enables specifying which files in the logs directory are to be scanned
End of Line Representation – for local, Over SSH, and Hadoop HDFS logs; enables to define the end line of log records
Regional Settings – for local, Over SSH, Hadoop HDFS, Google App Engine, Database, and Merge Logs logs
Other Types – for Windows Events logs

Note: Advanced settings are not available for Remote XpoLog logs.

Data Filter

You can filter out log events during collection so that some of the logs data will not be collected and available in XpoLog (alternatively it is also possible to mask data)

To set the data filter:

1. Under Advanced Settings, click Data Filter.
   The Data Filter definitions open.
2. Enter a search query that filters only events that should be collected from the log (events that don't satisfy the query will be ignored).
   It is recommended to run the same query in the Search console prior to saving this filtering to ensure the result is the desired one.

Files Attributes

For local, Over SSH, or Hadoop HDFS log files, when using a generic name pattern that captures multiple files, it is important to define the following file attributes:

- **Sort physical files by** – specify the option that will ensure that all the files in the log that are being captured are sorted correctly: last update time (default) or filename.
  **Note:** It is recommended to order according to the last update time, because XpoLog assumes that one file is written and closed in the source log, before another is written and closed.
- **File rotation policy** – define the nature of rotation between the captured files of the log:
  - **Cyclic** – Files are overridden as part of the rotation cycle.
  - **New appending** – File names are unique and are not changed as part of the rotation; however, the list of files changes as new files are added.
  - **Static** – The list of files never changes. Relevant for logs repository where the files are not changed.
- **Get files information from** – XpoLog retrieves information on files that are being collected in order to keep continuous collection (last modified time, file's size, etc.). In order to maximize efficiency, it is done by default on the directory level however in some cases (seen many times on Windows) the directory returns wrong information such as file size zero or an older last modified time - in such cases it is recommended to retrieve the information directly from the collected files which usually solves the case.
  - **Parent directory (default)** – information retrieved from the parent directory.
  - **Each file directly** – information retrieved directly from the files

To set the file attributes:

1. Under Advanced Settings, click File Attributes.
   The File Attributes definitions open.
2. In Sort physical files by, select Last update time or File name.
3. In File rotation policy, select Cyclic, New appending, or Static.
4. In Get files information from, select Parent directory (default) or Each file directly.
5. If you want to import an additional log into the same XpoLog log, click Add another log path.
   An additional Log path field opens for selecting another log file to import into the same log.
6. Repeat step 4 for all the source logs that you want to capture under the same XpoLog log.

Files Filters

If you used in the log path a name pattern that captured multiple log files, you can filter the files list to add only some of these captured files to XpoLog by filtering the list according to any or all of the following criteria:

- Include or exclude the last specified number of files
- Include the files from the specified timeframe
- Include files of or within a specified size range
- Exclude specified name patterns

For example, you can filter the log files to include only those files from the last 7 days, or the last 50 files.

**Important:** XpoLog does not allow two files of a single captured log to contain data from the same timeframe. In such a scenario, it is not possible to execute time-based operations. When different files contain an identical timeframe, they should be defined separately and can be merged by the merge-logs wizard.

To define the file filters:

1. Under Advanced Settings, click Files Filters.
The Files Filters filtering criteria open.

1. Fill in any of the criteria that you want to use to filter the captured files:

   - In the textbox within **Include the last files**, type the number of last files to include in the log
   - OR
   - In the textbox within **Exclude the last files**, type the number of last files to exclude from the log.
   - In the **From the** filter, select to filter the files from the last (default) or previous specified number of units of time – in the textbox, type the number of units of time and in the following dropdown list, select minutes, hours (default), days, weeks, or months.
   - In **With size**, select **equals**, smaller than, smaller than or equals, greater than, greater than or equals, between, not equals, and in the following textbox, type the number of bytes.
     - **Note:** If you select between, type a range of bytes.
   - In **Exclude name patterns**, type the name patterns (separated by commas) of the files to exclude from the log. See XpoLog Patterns Language for syntax of name patterns.

**End of Line Representation**

Some logs contain special characters or methodology to end line of log records. When standard end of line characters are not used, it is possible to define the "logic" of different line separation:

- **Automatic (default) -** XpoLog uses standard end of line characters to identify end of lines. This option is the most common one, only special logs require one of the below options in order to be supported.
- **Dynamic Line Length -** Specify the number of characters at the beginning of each line which defines the line's length. XpoLog will use the first specified chars to calculate the line's length and then will read it on the next line to calculate its length and so on.
- **Fixed Line Length -** Specify the fixed number of characters which represent a line.
- **Line Fixed Suffix -** Specify the term which appears at the end of each line as is.
- **Line Fixed Prefix -** Specify the term which appears at the beginning of each line as is.

**Regional Settings**

In Regional Settings, you can set:

- The time zone of the added log. This is especially useful if you are managing more than one data center, and you want to view all logs of all data centers in the same time zone.
- The character set used in the added log. The default is the language of your machine.

To define the regional settings:

1. Under **Advanced Settings**, click **Regional Settings**.
   - The Regional Settings section opens.
2. In **Log Time Zone**, select the time zone of the added log (Default is **Default UTC**).
   - **Note:** If the log doesn't have a date field, the time zone setting is ignored.
3. In **Character Set**, select the charset of the added log (Default is **Default** (charset of your machine)).
   - **Note:** Use the charset that applies to the file encoding and machine charset support.

**Other Types**

Windows Events logs that are added to XpoLog are usually classified as system, application, or security logs. In the Advanced Settings section, under Other Types, XpoLog enables you to alternately classify the incoming log as a Custom log or *.evt file.

To define other types:

- Under **Advanced Settings**, click **Other Types**.
  - The Other Types options open.
- Select one of the following options:
  - **Custom** – Type the name of the custom log.
    - **Note:** If the custom registered log name cannot be found, the event logging service opens the Application log.
  - **File** – Browse for or type the name of the file, and select its type: **system**, **application**, or **security**.

**Applying Patterns on the Log**

Applying a pattern on a log enables viewing the log in organized tabular format, setting an alarm on a specific field, or aggregating on a certain field.

By default, when adding a log to XpoLog and clicking the Save button on the first page of the Add Log wizard, XpoLog applies an automated pattern to parse the logs.

For certain log types (local, Windows Network, Over SSH, and Hadoop HDFS), XpoLog enables you to tune the log and parse it more deeply to normalize the log records into tabular format, by applying patterns on the incoming log data.

This can be performed from the Patterns Administration page, accessed by clicking the Next button on the first page of the Add Log wizard or Edit Log wizard.

It may be necessary to configure more than one pattern for logs that have different types of records that cannot be represented by a single pattern. You can do so by clicking the **New** button in the central pane.
The Patterns Administration page is divided into three sections, as follows:

- **Upper pane** – Text sample from the selected log. This pane presents the first 20 records from the incoming log (original data). You can copy paste other records from the incoming log data into this section, and then view the results of applying a pattern on those records (see Verifying Patterns on Manually Selected Data).
- **Central pane** – There is a tab for each pattern that has been configured for the log, named Pattern1, Pattern2, and so on. There is also a New button, which can be clicked to configure a new pattern to apply on the log. On the right side, provides you with three different Pattern Editor methods for configuring the patterns to apply on the log data:
  - **Wizard** – Opens a wizard for creating or modifying a pattern. Using the wizard, you can set different indications on each column such as type, length, optional, column name and more (more information on each type is presented in the wizard itself).
  - **Manual** – For advanced users who are familiar with the Pattern language.
  - **Automatic** – XpoLog matches patterns automatically and suggests possible patterns for deeper parsing. This is only available when adding a log; not when editing a log.
- **Bottom pane** – Log records analysis results. Shows the results of each parsing, i.e. applying the pattern to the log data.

To apply a pattern on the log:

1. In the central pane of the Patterns Administration page, click the tab of a pattern to modify, or click the **New** button to configure a new pattern.
2. Click one of the available **Pattern Editor** options, and configure the pattern:
   - **Auto** – see Selecting an Automatic Pattern.
   - **Wizard** – see Creating a Pattern Using the Wizard.
   - **Manual** – see Configuring a Manual Pattern.
   - **Note**: You can also create a pattern in the wizard based on one of the automatic pattern suggestions (see Creating a Pattern Based On an Automatic Pattern Suggestion).
3. Repeat steps 1 and 2 for each pattern that you want to configure or modify.
4. After you have modified and configured all patterns, click the **Save** button.
   - XpoLog applies the pattern on the incoming log, and the Log Viewer opens displaying the parsed records of the new log. The log name is displayed in the left pane in its selected location under Folders and Logs. If you put in the log path a {string} pattern, the various files of the log appear in the left pane. Otherwise, only one file appears. You can perform regular actions on this log.

**Removing a Pattern**

You can remove a pattern that you no longer want to apply on the log.

To remove a pattern:

- In the central pane of the Patterns Administration page, click the down arrow on the tab of the pattern that you want to remove, and in the menu that appears, click **Remove**.
  - The pattern is removed. The renaming patterns are renumbered. For example, if there is a Pattern1 and Pattern2 and you remove Pattern1, Pattern2 now becomes Pattern1.

**Moving a Pattern to the Left or Right**

You can move a pattern one tab to the left or right.

To move a pattern one tab to the left:

- In the central pane of the Patterns Administration page, click the down arrow on the tab of the pattern that you want to move to the left, and in the menu that appears, click **Move left**.
  - The pattern moves one tab to the left and is highlighted.

**Note**: Nothing happens when you select to move left the leftmost tab.

To move a pattern one tab to the right:

- In the central pane of the Patterns Administration page, click the down arrow on the tab of the pattern that you want to move to the right, and in the menu that appears, click **Move right**.
  - The pattern moves one tab to the right and is highlighted.

**Note**: Nothing happens when you select to move right the rightmost tab.

**Duplicating a Pattern**

You can duplicate a pattern that you want to use as a basis for another pattern.

To duplicate a pattern:

- In the central pane of the Patterns Administration page, click the down arrow on the tab of the pattern that you want to duplicate, and in the menu that appears, click **Duplicate**.
  - A new pattern tab is created with the contents of the duplicated pattern.

**Verifying Patterns on Manually Selected Data**

By default, the Patterns Administration page shows the results of applying a pattern on the first 20 records of the incoming log. However, you can verify the results of applying a pattern on any records of the incoming log, by copy-pasting the records into the upper pane of the Patterns Administration page.
To verify patterns on manually selected data:

1. Copy-paste records from the incoming log into the upper pane of the Patterns Administration page.
2. After selecting the pattern to apply (in the middle pane), in the upper pane, click the Verify link.
   The results of applying the pattern on the selected records is presented in the lower pane.

**Refreshing the Incoming Log Records**

You can refresh the top pane to once again display the first 20 records of the incoming log.

- To refresh the top pane, click the Reset link.
  The top pane is refreshed to display the first 20 records of the incoming log.

**Selecting an Automatic Pattern**

XpoLog matches patterns automatically and in the central pane of the Patterns Administration page displays its suggested patterns for deeper parsing. Near each suggested pattern, is displayed in parentheses the level of accuracy of the system parsing using that pattern, i.e. the percentage of records that were successfully parsed.

**Note:** XpoLog suggests patterns automatically. However, it does not guarantee that all records are matched. Therefore, each automatic suggestion should be reviewed, and its parsing results verified.

To select an automatic pattern:

- Under **Automatic Pattern Suggestions**, select the option button of the automatic pattern to apply on the log data.

**Creating a Pattern Based On an Automatic Pattern Suggestion**

You can create a new pattern in the wizard based on an automatic pattern suggestion.

To create a pattern based on an automatic pattern suggestion:

1. In the central pane, under the Auto pattern editor, select the option button of a suggestion.
2. Click the Edit button.
   The Wizard pattern editor opens.
3. Modify the pattern using the wizard (see **Creating a Pattern Using the Wizard**), and then click the Verify button to see the parsing results in the bottom pane.

**Configuring a Manual Pattern**

Users can manually change or enter one or more patterns using the XpoLog Patterns Language, to apply on the log records. Applying a detailed pattern is not mandatory, as **all data is searchable either way**, however it may ease the search and allow to use more functionality on the log fields (correlations, average, minimum, maximum, group by, searching specific fields, etc.).

To open the patterns editor edit a log and go 'Next'. The pattern editor is presented:
To configure a manual pattern:

1. The upper part presents original data, taken from the first 50 lines of the log files. It is possible to modify the data in this area and click verify to check the pattern on different types of records.

2. In the toolbar of the central pane, near Pattern Editor, the wizard enables setting up patterns via suggested options by XpoLog. Click Manual to switch to manual mode when you can enter pattern using the Pattern language (see XpoLog Patterns Language).

   Note: if multiple patterns are configured, XpoLog tries to match records to a pattern starting from pattern 1, then pattern 2, etc. Therefore, the most narrowed pattern should be placed first and the widest last.

3. Click the 'Verify' button after any changes made in order to confirm that changes were applied correctly - result is presented at the lower part of the screen.

**Creating a Pattern Using the Wizard**

You can use the wizard to create or modify a pattern use the wizard to add and name columns that represent the structure of the records. The wizard includes features to set different indications on each column, such as type, length, optional, and column name. More information on each type is presented in the wizard itself.

**Inserting a Field or Separator**

To insert a field:

1. In the Wizard pattern editor, click the + button.
   The Add Field dialog box opens.

2. Follow the procedure in the following subsections that is relevant to the field or separator that you want to insert into the log record.

   **Note:** Adding a field or separator can result in an error, such as The marked field causes the log to be unparsed. In this case, edit or remove the field.

**Inserting a Separator**

You can insert between log fields one or more spaces or tabs, or any other separator that you choose.

To insert a separator:

1. In Type, select Separator.
2. In Separator, select Space, Tab, or Custom.
3. If you selected Custom, in Insert separator, type the character to be used as a separator.
4. In Num of repeats, type the number of the selected separator to insert.
5. To configure advanced settings for the separator, click Advanced. Otherwise, continue with step 7.
6. If the selected separator does not appear in all records, select the Optional checkbox.

7. Click Apply.
   The log records are refreshed in the bottom pane showing the added separator.

Inserting a String Field

The following procedure describes how to insert into a log record a field that has a string value.

To insert a string field:

1. In Type, select String.
2. In Name, type the name of the field (column heading).
3. To configure advanced settings for the field, click Advanced. Otherwise, continue with step 11.
4. In UI Message Length, type the maximum length of data displayed in a column. If the data is longer than this value, it continues onto the next line(s).
5. In Field Types, type the set of strings that describe the field.
6. In Char Length, type the length of the character string. If there are less characters for this field in a log record, characters are added to the string to force it to be this length.
7. In Trim Chars, type a character or string to delete from the column value. For example, typing $ means that $ will be deleted from log records with $ in this field.
8. In Delimiter Chars, type a character or string for delimiting the column.
9. In Mask Column, define the masking of column text by selecting one of the following:
   a. Don't mask (default) - entire column value is displayed
   b. Mask entire column text - entire column value is not displayed
   c. Mask part of column text - part of the column value will be masked, use a regular expression and include the part you wish to mask inside a round brackets (). Note all masked values are replaced with six * - regardless of the masked value length.
   Note:
   a. Admin user will see masking only in the patterns administration part, the values cannot be masked from users who are part of the XpoLog Administrators group.
   b. All users with patterns administration permissions (Edit log) will see all values in the patterns administration part.
   c. Users who are restricted from viewing masked data are not able to preform searches on this data, the masked data does not exist from these user's context.
10. Select the GeoIP checkbox to enable GeoIP for this field.
11. If this string does not appear in all records, select the Optional checkbox.
12. Click Apply.
   The log records are refreshed in the bottom pane showing the added field.

Inserting a Date Field

Inserting into a log record a field with a date value requires giving a name to the date field, and specifying how to format the date.

For example, if the text in the log is 2003-05-23 00:24:41.368, the format should be yyyy-MM-dd HH:mm:ss,SSS.

Examples of optional identifiers are:

- MM – numeric month
- MMMMM – full textual month
- dd – numeric day
- EEEEEE – full textual day
- EEE – textual day
- yy – two-digit year
- yyyy – four-digit year
- HH – 24 hour
- hh – 12 hour
- a – AM/PM marker
- mm – minute
- ss – second
- SSS – milliseconds
- z – general time zone
- Z – RFC 822 time zone
- "TEXT" – a constant text that appears in the date string

To insert a date field:

1. In Type, select Date.
2. In Name, type the name of the field (column heading).
3. In Format, type the format to be used to format the date.
4. To configure advanced settings for the field, click Advanced. Otherwise, continue with step 14.
5. In UI Message Length, type the maximum length of data displayed in a column. If the data is longer than this value, it continues onto the next line(s).
6. In Char Length, type the length of the character string. If there are less characters for this field in a log record, characters are added to the string to force it to be this length.
7. In Trim Chars, type a character or string to delete from the column value. For example, typing $ means that $ will be deleted from log records with $ in this field.
8. In Delimiter Chars, type a character or string for delimiting the column.
9. In Display Format, type the format in which to display the date.
10. In Time Diff, specify the time offset in milliseconds. For example, to subtract 5 seconds from the result in the log view, type -5000.
Text in log: 2003-05-23 00:24:41.368
Time Diff Value: -5000
Result in the log view: 2003-05-23 00:24:36.368
11. In **Locale**, specify the locale in which the log was written.
12. In **Locale View**, specify the locale in which the log should be displayed.
13. If this date field does not appear in all records, select the **Optional** checkbox.
14. Click **Apply**.
   The log records are refreshed in the bottom pane showing the added field.

Inserting a Text Field

Same as **Inserting a String Field** above.

Inserting a Priority Field

The following procedure describes how to insert into a log record a priority field.

To insert a priority field:

1. In **Type**, select **Priority**.
2. In **Name**, type the name of the field (column heading).
3. In **Set Priorities**, specify the set of priorities that can appear in the field, in a semi-colon separated list. Example: DEBUG;INFO;WARN;ERROR;FATAL
4. To configure advanced settings for the field, click **Advanced**. Otherwise, continue with step 9.
5. In **Chars Length**, type the length of the character string. If there are less characters for this field in a log record, characters are added to the string to force it to be this length.
6. In **Trim Chars**, type a character or string to delete from the column value. For example, typing $ means that $ will be deleted from log records with $ in this field.
7. In **Delimiter Chars**, type a character or string for delimiting the column.
8. In **Mask Column**, define the masking of column text by selecting one of the following:
   a. **Don't mask** (default) - entire column value is displayed
   b. **Mask entire column text** - entire column value is not displayed
   c. **Mask part of column text** - part of the column value will be masked, use a regular expression and include the part you wish to mask inside a round brackets (). Note all masked values are replaced with six * - regardless of the masked value length.
   
   **Note:**
   a. Admin user will see masking only in administration part, the values cannot be masked from users who are part of the XpoLog Administrators group.
   b. All users with patterns administration permissions (Edit log) will see all values in the patterns administration part.
   c. Users who are restricted from viewing masked data are not able to perform searches on this data, the masked data does not exist from these user's context.
9. If this field does not appear in all records, select the **Optional** checkbox.
10. Click **Apply**.
   The log records are refreshed in the bottom pane showing the added field.

Inserting a Choice Field

The following procedure describes how to insert into a log record a choice field.

To insert a choice field:

1. In **Type**, select **Choice**.
2. In **Name**, type the name of the field (column heading).
3. In **Set Choice**, specify the set of choices that can appear in the field, in a semi-colon separated list. Example: RED;YELLOW;GREEN
4. To configure advanced settings for the field, click **Advanced**. Otherwise, continue with step 10.
5. In **Chars Length**, type the length of the character string. If there are less characters for this field in a log record, characters are added to the string to force it to be this length.
6. In **Trim Chars**, type a character or string to delete from the column value. For example, typing $ means that $ will be deleted from log records with $ in this field.
7. In **Delimiter Chars**, type a character or string for delimiting the column.
8. In **Mask Column**, define the masking of column text by selecting one of the following:
   a. **Don't mask** (default) - entire column value is displayed
   b. **Mask entire column text** - entire column value is not displayed
   c. **Mask part of column text** - part of the column value will be masked, use a regular expression and include the part you wish to mask inside a round brackets (). Note all masked values are replaced with six * - regardless of the masked value length.
   
   **Note:**
   a. Admin user will see masking only in administration part, the values cannot be masked from users who are part of the XpoLog Administrators group.
   b. All users with patterns administration permissions (Edit log) will see all values in the patterns administration part.
   c. Users who are restricted from viewing masked data are not able to perform searches on this data, the masked data does not exist from these user's context.
9. If this field does not appear in all records, select the **Optional** checkbox.
10. Click **Apply**.
   The log records are refreshed in the bottom pane showing the added field.

Inserting a Numeric Field

The following procedure describes how to insert into a log record a numeric field.

To insert a numeric field:
1. In **Type**, select **Number**.
2. In **Name**, type the name of the field (column heading).
3. To configure advanced settings for the field, click **Advanced**. Otherwise, continue with step 9.
4. In **Chars Length**, type the length of the character string. If there are less characters for this field in a log record, characters are added to the string to force it to be this length.
5. In **Trim Chars**, type a character or string to delete from the column value. For example, typing $ means that $ will be deleted from log records with $ in this field.
6. In **Delimiter Chars**, type a character or string for delimiting the column.
7. In **Mask Column**, define the masking of column text by selecting one of the following:
   a. **Don't mask (default)** - entire column value is displayed
   b. **Mask entire column text** - entire column value is not displayed
   c. **Mask part of column text** - part of the column value will be masked, use a regular expression and include the part you wish to mask inside a round brackets (). Note all masked values are replaced with six * - regardless of the masked value length.

   **Note:**
   a. Admin user will see masking only in administration part, the values cannot be masked from users who are part of the XpoLog Administrators group.
   b. All users with patterns administration permissions (Edit log) will see all values in the patterns administration part.
   c. Users who are restricted from viewing masked data are not able to perform searches on this data, the masked data does not exist from these user's context.

8. If this numeric field does not appear in all records, select the **Optional** checkbox.
9. Click **Apply**. The log records are refreshed in the bottom pane showing the added field.

### Inserting a Timestamp Field

The following procedure describes how to insert into a log record a timestamp field.

To insert a timestamp field:

1. In **Type**, select **Timestamp**.
2. In **Name**, type the name of the field (column heading).
3. In **Display Format**, type the format in which to display the time zone.
   
   *For example:*
   
   Text in log: 56895633232
   Display Format: yyy/MM/dd
   
   Result in the log view: 2007/11/13

4. To configure advanced settings for the field, click **Advanced**. Otherwise, continue with step 9.
5. In **Product**, type the number by which to multiply the timestamp in the log to convert it into milliseconds. For example, to convert a timestamp in seconds to milliseconds, type 1000.
6. If this timestamp field does not appear in all records, select the **Optional** checkbox.
7. Click **Apply**. The log records are refreshed in the bottom pane showing the added field.

### Inserting a New Line Field

The following procedure describes how to insert into a log record a new line field.

To insert a new line field:

1. In **Type**, select **New Line**.
2. Click **Apply**. The log records are refreshed in the bottom pane showing the added field.

### Inserting an End of Event Field

The following procedure describes how to insert into a log record an End of Event field.

To insert an end of event field:

1. In **Type**, select **End of Event**.
2. Click **Apply**. The log records are refreshed in the bottom pane showing the added field.

### Inserting a GeoIP Field

The following procedure describes how to insert into a log record a GeoIP field.

To insert a GeoIP field:

1. In **Type**, select **GeoIP**.
2. In **Name**, type the name of the field (column heading).
3. In **Information**, type the information appearing in the field: **Country, Region, City; Country, Country Code; Region; City; None.**
4. To configure advanced settings for the field, click **Advanced**. Otherwise, continue with step 9.
5. In **Ref Index**, type the zero-based index of the source column. The regular expression will be extracted according to this reference.
6. In **Ref Name**, type the zero-based name of the source column. The regular expression will be extracted according to this reference.
7. In **Mask In Mask Column**, define the masking of column text by selecting one of the following:
   a. **Don't mask (default)** - entire column value is displayed
   b. **Mask entire column text** - entire column value is not displayed
   c. **Mask part of column text** - part of the column value will be masked, use a regular expression and include the part you wish to mask inside a round brackets (). Note all masked values are replaced with six * - regardless of the masked value length.

   **Note:**
a. Admin user will see masking only in administration part, the values cannot be masked from users who are part of the XpoLog Administrators group.
b. All users with patterns administration permissions (Edit log) will see all values in the patterns administration part.
c. Users who are restricted from viewing masked data are not able to perform searches on this data, the masked data does not exist from these user's context.

8. If this GeoIP field does not appear in all records, select the Optional checkbox.
9. Click Apply.
   The log records are refreshed in the bottom pane showing the added field.

Inserting a Term Field

A constant string that appears in a record and needs to be displayed in the log view. For example, assuming you have the next two records in your log:

03/07/2005 03:44:56 app1 IP=192.168.11.44 success (where IP is a source IP)
03/07/2005 03:44:57 app2 IP=192.168.12.33 failure (where IP is a destination IP)

The multi-pattern you should use is:

(date,dd/MM/yyyy HH:mm:ss) {term,app1} IP={text:Source IP} {string}

(date,dd/MM/yyyy HH:mm:ss) {term,app2} IP={text:Destination IP} {string}

This will result in the following log view:

03/07/2005 03:44:56 app1 192.168.11.44 success
03/07/2005 03:44:57 app2 192.168.12.33 failure

To insert a term field:

1. In Type, select Term.
2. In Name, type the name of the field (column heading).
3. To configure advanced settings for the field, click Advanced. Otherwise, continue with step 7.
4. In Mask Column, define the masking of column text by selecting one of the following:
   a. Don't mask (default) - entire column value is displayed
   b. Mask entire column text - entire column value is not displayed
   c. Mask part of column text - part of the column value will be masked, use a regular expression and include the part you wish to mask inside a round brackets (). Note all masked values are replaced with six * - regardless of the masked value length.

Note:
   a. Admin user will see masking only in administration part, the values cannot be masked from users who are part of the XpoLog Administrators group.
   b. All users with patterns administration permissions (Edit log) will see all values in the patterns administration part.
   c. Users who are restricted from viewing masked data are not able to perform searches on this data, the masked data does not exist from these user's context.

5. If this string does not appear in all records, select the Optional checkbox.
6. Click Apply.
   The log records are refreshed in the bottom pane showing the added field.

Inserting an IP Address Field

The following procedure describes how to insert into a log record an IP address field.

To insert an IP Address field:

1. In Type, select IP Address.
2. In Name, type the name of the field (column heading).
3. To configure advanced settings for the field, click Advanced. Otherwise, continue with step 7.
4. In Mask Column, define the masking of column text by selecting one of the following:
   a. Don't mask (default) - entire column value is displayed
   b. Mask entire column text - entire column value is not displayed
   c. Mask part of column text - part of the column value will be masked, use a regular expression and include the part you wish to mask inside a round brackets (). Note all masked values are replaced with six * - regardless of the masked value length.

Note:
   a. Admin user will see masking only in administration part, the values cannot be masked from users who are part of the XpoLog Administrators group.
   b. All users with patterns administration permissions (Edit log) will see all values in the patterns administration part.
   c. Users who are restricted from viewing masked data are not able to perform searches on this data, the masked data does not exist from these user's context.

5. Select the GeoIP checkbox to enable GeoIP for this field.
6. If this string does not appear in all records, select the Optional checkbox.
7. Click Apply.
   The log records are refreshed in the bottom pane showing the added field.

Modifying a Pattern Field

You can modify any field in a pattern.

To modify a field:
1. Click the down arrow in the field that you want to modify, and in the menu that appears, click **Edit**. The Edit Field dialog box is displayed.
2. Modify the parameters of the field as required, as when adding a field to a pattern (see Creating a Pattern Using the Wizard).
3. Click **Save**. The modified pattern is applied on the log.

### Removing a Pattern Field

You can remove a field from a pattern.

To remove a field:

- Click the down arrow in the field that you want to remove, and in the menu that appears, click **Remove**. The field is removed from the pattern.

### Adding an AWS S3 Bucket Log

To add an AWS S3 Bucket log to XpoLog:

1. In **Connection Details**, select the AWS S3 bucket account required to connect to the S3 repository, or click the new link to add an account to the system (see Address Book). **Note:** If you do not have any AWS S3 bucket accounts defined in XpoLog, the Add AWS S3 bucket account page is presented automatically.
2. In **Log Path**, type the path to the log on the S3 repository (Note: it is mandatory to start the path with slash /). OR Click **Browse** to open the System Files Browser of the S3 repository that you connected to, expand the folders to get to the desired log, and then click **Select** to display the log location in **Log Path**.
3. Optionally, append to the log path a name pattern to capture multiple files from the same log. (For pattern syntax, see XpoLog Patterns Language.)
4. Optionally, define advanced settings for the AWS S3 bucket log – Files Filters, and/or Regional Settings (see Configuring Advanced Log Settings).
5. Click either of the following buttons:
   - **Save** – XpoLog applies an automated pattern on the incoming log, and the Log Viewer opens displaying the parsed records of the new log. The log name is displayed in the left pane in its selected location under Folders and Logs. If you put in the log path a (string) pattern, the various files of the log appear in the left pane. Otherwise, only one file appears. You can perform regular actions on this log.
   - **Next** – The Patterns administration screen opens. Apply patterns on the log data and save the log in XpoLog (see Applying Patterns on the Log).

### Adding a Local XpoLog Log

When there is a need for second layer of aggregation over a log it is possible to use this option and collect any digested log in XpoLog.

To add a Local XpoLog log to XpoLog:

1. In **Local Log Path**, mark the checkbox with the relevant log from the logs tree and press **Apply**.
2. Optionally, define advanced settings – Files Filters, and/or Regional Settings (see Configuring Advanced Log Settings).
3. Click either of the following buttons:
   - **Save** – XpoLog applies an automated pattern on the incoming log, and the Log Viewer opens displaying the parsed records of the new log. The log name is displayed in the left pane in its selected location under Folders and Logs. If you put in the log path a (string) pattern, the various files of the log appear in the left pane. Otherwise, only one file appears. You can perform regular actions on this log.
   - **Next** – The Patterns administration screen opens. Apply patterns on the log data and save the log in XpoLog (see Applying Patterns on the Log).

### XpoLog Listeners

XpoLog may be configured to monitor incoming messages and decode the messages to be available in XpoLog over different protocols. XpoLog can listen to Syslog data (UDP or TCP) arriving from one or more source devices, HTTP/S arriving from one or more source device, data forwarded from XpoLog Agents and Cisco routers and switches that support NetFlow.

You can use XpoLog to receive data from these source devices for easy searching, reporting and alerting - XpoLog also provides several options to automatically split the incoming data and create a dedicated log per source device or a custom configuration (note that such changes in a listener configuration take place on incoming data from the change forward, and is not applied on already processed data).

#### Syslog - UDP vs. TCP transport protocol:

Syslog logging has been traditionally sent to port 514 using UDP. UDP is a connectionless protocol, hence unreliability is inherent. There is no acknowledgement, error detection, sequencing or re-transmission of missed packets when sending Syslog messages over the UDP protocol. Some devices implement the Syslog protocol over a TCP transport (When sending messages using TCP the
TCP is connection oriented. It relies on the destination host being there. The connection is built when the sending device is initialized, or prior to sending the first Syslog message. It’s slower to use TCP because of the initial time for the three-way handshake, and all packets get acknowledged by the server once they are received, and essentially before the next one can be sent. The TCP protocol offers reliability plus error correction; this is used to ensure messages are sent to the syslog server reliably.

**HTTP/s transport protocol:**
When an HTTP/S listener is configured and active, devices can send to the XpoLog server IP address and port data in JSON format and XpoLog will process the data and create log per device to be available in XpoLog. Since an HTTP listener is a combination of the XpoLog IP address and port, each listener also provide a unique token that may be used the the device that pushes data to be identified by XpoLog.

**XpoLog transport protocol:**
XpoLog instances and agents can forward data ("push") in a format that XpoLog is familiar with. In order to received the data that is being sent from other XpoLog instances, and get it processed automatically an XpoLog listener has to be configured and active on the instance/cluster that should receive and process the data.

**NetFlow transport protocol:**
Cisco routers and switches that have the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion. Routers and switches that support NetFlow can collect IP traffic statistics on all interfaces where NetFlow is enabled, and later export those statistics as NetFlow records toward XpoLog as a NetFlow collector - for traffic analysis. XpoLog supports NetFlow versions 5 and 9.

**Listeners Accounts Console:**
Available under Manager > Administration > Listeners, the listeners accounts console presents all the configured listeners and their statuses and provides access to their configuration.

- Adding TCP Listener account
- Adding UDP Listener account
- Adding HTTP/S Listener account
- Adding XpoLog Listener account
- Adding NetFlow Listener account
- The Syslog Protocol
- Syslog Facilities
  - The Facility value is a way of determining which process of the machine created the message. Since the Syslog protocol was originally written on BSD Unix, the Facilities reflect the names of Unix processes and Daemons. The priority value is calculated using the following formula: Priority = Facility * 8 + Level
  - The list of Facilities available:
    - 0 kernel messages
    - 1 user-level messages
    - 2 mail system
If you are receiving messages from a Unix system, it is recommended to use the 'User' Facility as your first choice. Local0 through to Local7 are not used by Unix and are traditionally used by networking equipment. Cisco routers for example use Local6 or Local7.

Syslog Levels

The list of severity Levels:

0 Emergency: system is unusable
1 Alert: action must be taken immediately
2 Critical: critical conditions
3 Error: error conditions
4 Warning: warning conditions
5 Notice: normal but significant condition
6 Informational: informational messages
7 Debug: debug-level messages

Recommended practice is to use the Notice or Informational level for normal messages.

Severity Levels Details:

DEBUG: Info useful to developers for debugging the app, not useful during operations

INFORMATIONAL: Normal operational messages - may be harvested for reporting, measuring throughput, etc - no action required

NOTICE: Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required

WARNING: Warning messages - not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time

ERROR: Non-urgent failures - these should be relayed to developers or admins; each item must be resolved within a given time

ALERT: Should be corrected immediately - notify staff who can fix the problem - example is loss of backup ISP connection

CRITICAL: Should be corrected immediately, but indicates failure in a primary system - fix CRITICAL problems before
ALERT - example is loss of primary ISP connection

**EMERGENCY**: A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.

Syslog Priority values

The `PRI` part is a number that is enclosed in angle brackets. This represents both the Facility and Severity of the message. This number is an eight bit number. The first 3 least significant bits represent the Severity of the message (with 3 bits you can represent 8 different severities) and the other 5 bits represent the Facility of the message. You can use the Facility and the Severity values to apply certain filters on the events in the Syslog Daemon. Note that Syslog Daemon cannot generate these Priority and Facility values. They are generated by the applications on which the event is generated. Following are the codes for Severity and Facility. Please note that the codes written below are the recommended codes that the applications should generate in the specified situations. You cannot, however, be 100% sure if it really is the correct code sent by the application. For example: An application can generate a numerical code for severity as 0 (Emergency) when it should have generated 4 (Warning) instead. Syslog Daemon can not do anything about it!! It will simply receive the message as it is.

**Calculating Priority Value**

The Priority value is calculated by first multiplying the Facility number by 8 and then adding the numerical value of the Severity. For example, a kernel message (Facility=0) with a Severity of Emergency (Severity=0) would have a Priority value of 0. Also, a "local use 4" message (Facility=20) with a Severity of Notice (Severity=5) would have a Priority value of 165. In the PRI part of a Syslog message, these values would be placed between the angle brackets as <0> and <165> respectively.

Syslog Header

The `HEADER` part contains the following things:

- **Timestamp** -- The Time stamp is the date and time at which the message was generated. Be warned, that this timestamp is picked up from the system time and if the system time is not correct, you might get a packet with totally incorrect time stamp
- **Hostname or IP address of the device.**

Syslog Message

The `MSG` part will fill the remainder of the Syslog packet. This will usually contain some additional information of the process that generated the message, and then the text of the message. The MSG part has two fields:

- **TAG field**
- **CONTENT field**

The value in the TAG field will be the name of the program or process that generated the message. The CONTENT contains the details of the message.

**Syslog - TCP**

To get Syslog data over TCP, configure XpoLog to listen on a network port for incoming Syslog:

1. Go to Manager > Administration > Listeners. The Listeners management console opens.
2. Add Syslog TCP account, for each account the following should be configured:
   a. **Name**: the name of the Listener account
   b. **Description**: the description of the Listener account
   c. **Listening Node**: the node in the cluster which will listen to the Syslog messages (appears only if a XpoLog cluster is deployed)
   d. **Port**: the port which will be used on the XpoLog machine to receive Syslog messages of this Listener account (usually 1468)

   e. **Advanced Settings**:

   **General Information:**
   - **Enabled**: determine whether this account is enabled or not
   - **Listening Interface**: the network interface (IP address) on which the XpoLog listener instance is listening

   **Dynamic Log Creation Configuration:**
   - **Parent Folder**: the parent folder which all logs from this listener will be place under in XpoLog Folders and Logs tree
   - **Collection Policy**: the collection policy which will be associated to all logs from this listener (used mainly for storage location and data retention)
   - **AppTags**: the AppTags which will be associated to all the logs from this listener (used mainly for data enrichment)
   - **Log Name Prefix**: a prefix which will be added to any of the the logs from this listener (used to easily distinguish between multiple listener accounts logs)
   - **Split by Source Device**:
     i. Do not split - by default, XpoLog will not split the incoming data. All data will be stored under a single log in XpoLog.
     ii. Create log by unique IP / host name - XpoLog will split the incoming data based on the source that sends it to different logs, the log name structure will be "Log_Name_Prefix Source_IP/Name"
     iii. Create log by IP mask - XpoLog will split the incoming data based on matched source to the configured IP mask that sends it to different logs, the log name structure will be "Log_Name_Prefix IP_Mask"
     iv. Create log with Regular expression - XpoLog will split the incoming data to different logs based on a regular expression
that will be applied on the Message field. The part in the regular expression that will be used to determine the split should be in (round parentheses).

Records that the regular expression does not return a value will be directed to the global Syslog TCP log.

**Listener Data:**
- **Listener Data Location:** the location which data will be stored to, by default XpoLog stores it in its data directory
- **Indexing Node:** the node in the cluster which will index the received Syslog messages (appears only if a XpoLog cluster is deployed)
- **Indexing Interval:** the frequency in which received Syslog messages are indexed

3. Save the account.
4. Data received to the Syslog listener account will be created under the configured parent folder and will be available for searching, reporting and alerting.

**Note:** multiple listeners accounts may be configured. However, listeners which run on the same machine must listen on a different network port.

**Syslog - UDP**

To get Syslog data over UDP, configure XpoLog to listen on a network port for incoming Syslog:

1. Go to Manager > Administration > Listeners. The Listeners management console opens.
2. Add Syslog UDP account, for each account the following should be configured:
   a. **Name:** the name of the Listener account
   b. **Description:** the description of the Listener account
   c. **Listening Node:** the node in the cluster which will listen to the Syslog messages (appears only if a XpoLog cluster is deployed)
   d. **Port:** the port which will be used on the XpoLog machine to receive Syslog messages of this Listener account (usually 514)

3. **Advanced Settings:**
   - **General Information:**
     - **Enabled:** determine whether this account is enabled or not
     - **Listening Interface:** the network interface (IP address) on which the XpoLog listener instance is listening
   - **Dynamic Log Creation Configuration:**
     - **Parent Folder:** the parent folder which all logs from this listener will be place under in XpoLog Folders and Logs tree
     - **Collection Policy:** the collection policy which will be associated to all logs from this listener (used mainly for storage location and data retention)
     - **AppTags:** the AppTags which will be associated to all the logs from this listener (used mainly for data enrichment)
     - **Log Name Prefix:** a prefix which will be added to any of the the logs from this listener (used to easily distinguish between multiple listener accounts logs)
     - **Split by Source Device:**
       i. Do not split - by default, XpoLog will not split the incoming data. All data will be stored under a single log in XpoLog.
       ii. Create log by unique IP / host name - XpoLog will split the incoming data based on the source that sends it to different logs, the log name structure will be "Log_Name_Prefix Source_IP/Name"
       iii. Create log by IP mask - XpoLog will split the incoming data based on matched source to the configured IP mask that sends it to different logs, the log name structure will be "Log_Name_Prefix IP_Mask"
       iv. Create log with Regular expression - XpoLog will split the incoming data to different logs based on a regular expression that will be applied on the Message field. The part in the regular expression that will be used to determine the split should be in (round parentheses).

   Records that the regular expression does not return a value will be directed to the global Syslog UDP log.

**Note:** multiple listeners accounts may be configured. However, listeners which run on the same machine must listen on a different network port.

**HTTP/S**

To get data over HTTP/S, configure an HTTP/S Listener account:

1. Go to Manager > Administration > Listeners. The Listeners management console opens.
2. Add HTTP account, for each account the following should be configured:
   a. **Name:** the name of the Listener account
To get data from remote XpoLog forwarders, configure an XpoLog Listener account:

1. Go to Manager > Administration > Listeners. The Listeners management console opens.
2. Add XpoLog account, for each account the following should be configured:
   a. Name: the name of the Listener account
   b. Description: the description of the Listener account
   c. Listening Node: the node in the cluster which will listen to the messages received from remote XpoLog instances/agents (appears only if a XpoLog cluster is deployed)
   d. Token: a unique token that is identified with this listener and must be included in the used URL when forwarding data to this account - the token ensures only permitted devices send data and also tags the sent data to the desired HTTP/S listener in XpoLog
   e. URL: the URL that devices that forward data to XpoLog should use - including the IP address/Hostname, port, path and token (in case of a cluster - the URL gets populated when selecting a Listening Node)

Advanced Settings:

General Information:
Enabled: determine whether this account is enabled or not

Dynamic Log Creation Configuration:
Note: It is optional to configure the dynamic log creation configuration in the listener XpoLog. Leave as default to recevie the data as is, or use the agent's configuration to send the information.
- Parent Folder: the parent folder which all logs from this listener will be place under in XpoLog Folders and Logs tree
- Collection Policy: the collection policy which will be associated to all logs from this listener (used mainly for storage location and data retention)
- AppTags: the AppTags which will be associated to all the logs from this listener (used mainly for data enrichment)
- Log Name Prefix: a prefix which will be added to any of the the logs from this listener (used to easily distinguish between multiple listener accounts logs. Leave empty for no prefix)
- Split by Source Device: check to create a log for each unique source device value in the received message (a log will be created per device)
- Message JSON Key: the JSON key of the message field. Used when sending a type to XpoLog Listener to match a template of that type - the key determine which one of the fields of the JSON contains the log message itself to be matched
- Split by JSON columns: A list of JSON keys, separated by ‘->’, denoting the log's path and name. Append ‘*’ to the key denoting the host.

Advanced Dynamic Log Creation Configuration:
It is possible to push information from the agents/devices sending the logs to XpoLog such as name, data type and their target Folders and Logs location in XpoLog. The Listener looks for the following JSON keys and, if any of them exists in the messages, uses them:
- xpologPath: a path of folders, separated by ‘->’, that the logs should be placed in, in XpoLog Folders and Logs
- xpologName: the name of the log in XpoLog (if another split type is selected then it will be added to the name)
- xpologType: the type of the log, if there's a template in XpoLog with the exact same type then XpoLog will automatically apply the template's pattern on the received message (note: in this case it is important to specify the 'Message JSON Key' detailed above).

Listener Data:
- Listener Data Location: the location which data will be stored to, by default XpoLog stores it in its data directory
- Indexing Node: the node in the cluster which will index the received Syslog messages (appears only if a XpoLog cluster is deployed)
- Indexing Interval: the frequency in which received Syslog messages are indexed

JSON Parsing:
- JSON Parsing Level: set the maximum depth in the JSON object for which data will be extracted into columns

Save the account.
3. Data received to the HTTP/S listener account will be created under the configured parent folder and will be available for searching, reporting and alerting

XpoLog
**Enabled:** determine whether this account is enabled or not

**Dynamic Log Creation Configuration:**
- **Parent Folder:** the parent folder which all logs from this listener will be placed under in XpoLog Folders and Logs tree
- **Collection Policy:** the collection policy which will be associated to all logs from this listener (used mainly for storage location and data retention)

**Listener Data:**
- **Listener Data Location:** the location where data will be stored to, by default XpoLog stores it in its data directory
- **Indexing Node:** the node in the cluster which will index the received Syslog messages (appears only if a XpoLog cluster is deployed)
- **Indexing Interval:** the frequency in which received Syslog messages are indexed

3. Save the account.
4. Data received to the XpoLog listener account will be created under the configured parent folder and will be available for searching, reporting and alerting.

**Cisco NetFlow**

To get routers and switches that support NetFlow IP traffic statistics (version 9), configure XpoLog to listen on a network port for incoming NetFlow data:

1. Go to Manager > Administration > Listeners. The Listeners management console opens.
2. Add NetFlow account, for each account the following should be configured:
   a. **Name:** the name of the Listener account
   b. **Description:** the description of the Listener account
   c. **Listening Node:** the node in the cluster which will listen to the received Syslog messages (appears only if a XpoLog cluster is deployed)
   d. **Port:** the port which will be used on the XpoLog machine to receive Syslog messages of this Listener account (usually 2055)
   e. **Advanced Settings:**
      - **General Information:**
        - **Enabled:** determine whether this account is enabled or not
        - **Listening Interface:** the network interface (IP address) on which the XpoLog listener instance is listening
      - **Dynamic Log Creation Configuration:**
        - **Parent Folder:** the parent folder which all logs from this listener will be placed under in XpoLog Folders and Logs tree
        - **Collection Policy:** the collection policy which will be associated to all logs from this listener (used mainly for storage location and data retention)
        - **AppTags:** the AppTags which will be associated to all the logs from this listener (used mainly for data enrichment)
        - **Log Name Prefix:** a prefix which will be added to any of the logs from this listener (used to easily distinguish between multiple listener accounts)
        - **Split by Source Device:**
          i. Do not split - by default, XpoLog will not split the incoming data. All data will be stored under a single log in XpoLog.
          ii. Create log by unique IP / host name - XpoLog will split the incoming data based on the source that sends it to different logs, the log name structure will be “Log_Name_Prefix Source_IP/Name”
          iii. Create log by IP mask - XpoLog will split the incoming data based on matched source to the configured IP mask that sends it to different logs, the log name structure will be “Log_Name_Prefix IP_Mask”
          iv. Create log with Regular expression - XpoLog will split the incoming data to different logs based on a regular expression that will be applied on the Message field. The part in the regular expression that will be used to determine the split should be in (round parentheses).
          Records that the regular expression does not return a value will be directed to the global NetFlow log.
      - **Listener Data:**
        - **Listener Data Location:** the location where data will be stored to, by default XpoLog stores it in its data directory
        - **Indexing Node:** the node in the cluster which will index the received Syslog messages (appears only if a XpoLog cluster is deployed)
        - **Indexing Interval:** the frequency in which received Syslog messages are indexed

3. Save the account.
4. Data received to the NetFlow listener account will be created under the configured parent folder and will be available for searching, reporting and alerting.

**Note:** multiple listeners accounts may be configured. However, listeners which run on the same machine must listen on a different network port.

**Verifying Added Log Configuration**

After a log is successfully added to XpoLog Center, it is recommended in the case of multiple files per log, to validate that the log files have been sorted properly. Also, when pattern(s) have been applied to the log, it is advisable to check that log records have been parsed as expected. Otherwise, some searches and filters that are run on the log may not return results.

**Files List Validation**
For logs that have multiple files, it is important to ensure that the files are sorted properly.
To validate the log file list:

1. In the Log Viewer, open the log file to validate.
2. In the top left panel, open Quick Filter, and select the Files List tab.
   The files in the selected log are listed.
3. Check that the files are sorted in the correct order.
   If not, return to Advanced Settings > Files Attributes, and select an appropriate value for Sort physical files by (see Configuring Advanced Log Settings).

Pattern Validation

The following procedure describes the recommended way of verifying that patterns have been applied correctly on a log.

If you have any doubts regarding the pattern configuration, you can use a simpler pattern for verification, such as date and string. If you still have any doubts, contact our support team to review or recommend a suitable configuration.

To validate log file contents:

1. In the Log Viewer, open the log file to validate.
2. Browse to the beginning of the log and verify that all records are parsed as expected (forward parsing).
3. Browse to the end of the log and verify that all records are parsed as expected (backwards parsing).
4. Open the files list (see section above), and click each of the files.
   XpoLog jumps to the first record of each selected file. Verify that all records in each file are parsed as expected.
5. Run a few test filters (string or date) to make sure the data is returned as expected.

Editing a Log Definition

You can edit the definition of logs that resides in XpoLog Center. Editable information includes the log’s basic information (log name, parent folder, and applications to which it is tagged), log type settings (besides for the log type, which cannot be changed), and the pattern applied on the log.

To edit a log:

1. In the left pane, under Folders and Logs, right-click a log that you want to edit, and in the menu that appears, click Edit.
   The Edit Log page appears.
2. Modify the log definition, as described in Adding a Log to XpoLog. The only field that you cannot modify is Log Type.

XpoLog Patterns Language

XpoLog enables users to use the Patterns language to normalize log records into tabular format.

Records in the log can usually be presented by a combination of types. It is recommended to present the logged information in as detailed way as possible. Doing so gives greater possibilities in manipulating and analyzing the data, such as filtering by a specific ip, priority, date, or specific text column. You should try to be as descriptive as possible.

Note that you can configure several patterns for one log using XpoLog multi pattern.
Each command will be treated as a column of data in the log view table.

Note: If a pattern is formulated incorrectly, the log records may display wrong data or no data at all.

IMPORTANT!!!
After defining a pattern, it is highly recommended to click the verify pattern link to see the results of your definition in the table at the bottom of the page.
If you do not see data at all or you see wrong data, check your pattern definition.
For any definition problem, send XpoLog support the log example by email to support@xplg.com, and we will help you define a pattern.

The following table describes the Patterns language:

<table>
<thead>
<tr>
<th>Pattern Type</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>any string of characters, including multi line strings</td>
</tr>
<tr>
<td></td>
<td>{string}</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Text</td>
<td>any single-line string of characters</td>
</tr>
<tr>
<td>Date</td>
<td>a date string</td>
</tr>
<tr>
<td>Timestamp</td>
<td>a timestamp representing a date string</td>
</tr>
<tr>
<td>Number</td>
<td>a numeric string</td>
</tr>
<tr>
<td>Choice</td>
<td>a set of strings that can appear in a record</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All optional choices should appear as a semicolon separated list inside the tag.</td>
</tr>
<tr>
<td>IP Address</td>
<td>An IP address</td>
</tr>
<tr>
<td>Geo IP Address</td>
<td>A Geo IP address</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All optional combinations of country, region and city are valid, for example: country:region, region:city, country etc.</td>
</tr>
<tr>
<td>Priority</td>
<td>A set of priorities that can appear in a record</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All optional priorities should appear as a semi-colon separated list inside the tag.</td>
</tr>
<tr>
<td>Expression</td>
<td>The expression that will be used according to the source columns given</td>
</tr>
<tr>
<td>Regular Expression</td>
<td>A regular expression, used to extract part of the data from another column read more about regular expressions in the regular expressions help page</td>
</tr>
<tr>
<td>Properties</td>
<td>A set of key-value properties that can appear in a record</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Json</td>
<td>A set of key-value pairs</td>
</tr>
</tbody>
</table>
| Term | a constant string that appears in a record and needs to be displayed in the log view | {term,TERM} 
TERM is the constant string |
| Free Text | any text you wish to display in the log view, usually used in multi-pattern logs to distinguish records | {freetext,FREETEXT} 
FREETEXT is the text that you wish to display in the log view. |
<p>| Value Mapping Option I (manual mapping) | maps an original value from log to a converted value | {map,val1=convertedVal1;val2=convertedVal2;val3=convertedVal3;...;valN=convertedValN} |
| Value Mapping Option II (mapping based on an external file) | maps an original value from log to a converted value | {map,refIndex=ORIG_COL_INDEX,file:FULL_PATH_TO_FILE} |
| Value Mapping Option III (regular expression manual mapping) | maps an original value from log to a converted value | {regexp,refIndex=index | refName=column_name;columnType=map;mapping=val1:convertedVal1^val2:convertedVal2^...^valN:convertedValN,(regular_expression_to_extract)} |
| Block | an optional string that does not appear in all records | {block,start,emptiness=true}XXX{block,end,emptiness=true} |
| Horizontal Tab | a tab delimiter | {tab} |
| End of Line | end of line, used in records that spread over more than one line | {eol} |</p>
<table>
<thead>
<tr>
<th>Identifier</th>
<th>Text in Log</th>
<th>Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM - numeric month</td>
<td>01-25-1986</td>
<td>{date,MM-dd-yyyy}</td>
</tr>
<tr>
<td>MMMMM - full textual month</td>
<td>25/July/1986</td>
<td>{date,dd/MMMMM/yyyy}</td>
</tr>
<tr>
<td>MMM - textual month</td>
<td>25/Jul/1986</td>
<td>{date,dd/MMM/yyyy}</td>
</tr>
<tr>
<td>dd - numeric day</td>
<td>01:25:1986</td>
<td>{date,MM:dd:yyyy}</td>
</tr>
<tr>
<td>EEEEE - full textual day</td>
<td>Friday 01-25-00</td>
<td>{date,EEEEE MM-dd-yy}</td>
</tr>
<tr>
<td>EEE - textual day</td>
<td>Fri 01-25-00</td>
<td>{date,EEE MM-dd-yy}</td>
</tr>
<tr>
<td>yy - 2 digit year</td>
<td>25/Jul/86</td>
<td>{date,dd/MMM/yy}</td>
</tr>
<tr>
<td>yyyy - 4 digit year</td>
<td>25/Jul/1986</td>
<td>{date,dd/MMM/yyyy}</td>
</tr>
<tr>
<td>HH - 24 hour</td>
<td>18:05:23</td>
<td>{date,HH:mm:ss}</td>
</tr>
<tr>
<td>hh - 12 hour</td>
<td>6:05:23 PM</td>
<td>{date,hh:mm:ss}</td>
</tr>
<tr>
<td>a - AM/PM marker</td>
<td>6:05:23 PM</td>
<td>{date,hh:mm:ss a}</td>
</tr>
<tr>
<td>mm - minute</td>
<td>18:05:23</td>
<td>{date,HH:mm:ss}</td>
</tr>
<tr>
<td>ss - second</td>
<td>18:05:23</td>
<td>{date,HH:mm:ss}</td>
</tr>
<tr>
<td>SSS - millisecond</td>
<td>18:05:23 253</td>
<td>{date,HH:mm:ss SSS}</td>
</tr>
<tr>
<td>z - general time zone</td>
<td>18:05:23 EST</td>
<td>{date,HH:mm:ss z}</td>
</tr>
<tr>
<td>Z - RFC 822 time zone</td>
<td>18:05:23 -0400</td>
<td>{date,HH:mm:ss Z}</td>
</tr>
<tr>
<td>X - ISO 8601 time zone</td>
<td>18:05:23 -04:00</td>
<td>{date,HH:mm:ss XXX}</td>
</tr>
<tr>
<td>'TEXT' - a constant text that appears in the date string</td>
<td>07-1986D25</td>
<td>{date,MM-yyyy'D'dd}</td>
</tr>
</tbody>
</table>

### Attributes Supported by All Types

All pattern types support the attributes described in the following table.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Remark</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Name                 | This attribute should always follow the tag name with a leading colon. | {string:Title}  
{date:Start Date,dd/mm/yyyy}  
{priority:Severity,DEBUG;INFO;ERROR}  
{number:Status Code} |
| uiMessageLength      | This attribute allows you to limit the length of data displayed in a specific column. If the data is longer than specified, it will be divided to several lines. | {string:Title,uiMessageLength=20} |
| charsLength          | This attribute allows you to force the existence of a fixed number of characters in a string, even if there are less characters in the record. | {string:Title,charsLength=10} |
This attribute allows you to set a regular expression that will serve as the column's delimiter. This is useful in case there is no natural delimiter (such as space or a non-word character) between two columns.

This attribute allows you to set a regular expression for masking the column's data. If a match is found for the column's value, then the matched part will be displayed as a string of asterisks (**).

Special Cases

- The right/left curly brackets characters ( { } ) are reserved in XpoLog syntax, therefore they can be used as literal only if as \u007B (left curly bracket) or \u007D (right curly bracket).
- The quote character ('') can be used as literal only if preceded by another quote ".

Examples of Patterns Used on Logs

The following are examples of patterns that can be used to tune the parsing results of logs.

<table>
<thead>
<tr>
<th>Log</th>
<th>Parsed Records</th>
<th>Data Pattern</th>
</tr>
</thead>
</table>
| Log 1 | 2003-02-12 12:37:26 ContextConfig[/examples]: Missing application web.xml, using defaults only | {date,yyyy-MM-dd HH:mm:ss} {string} 
2003-02-12 12:37:26 StandardManager[/examples]: Seeding random number generator class java.security.SecureRandom | {string} 
2003-02-12 12:37:30 StandardManager[/examples]: Seeding of random number generator has been completed | {string} 
2003-02-12 12:37:30 StandardWrapper[/examples:default]: Loading container servlet default | {string} 
2003-02-12 12:37:30 StandardWrapper[/examples:invoker]: Loading container servlet invoker | {string} |
| Log 2 | 127.0.0.1 - - [26/Dec/2001:19:49:23 +0200] "GET / HTTP/1.1" 200 1494 | {string} - - 
127.0.0.1 - - [26/Dec/2001:19:49:23 +0200] "GET /apache_pb.gif HTTP/1.1" 200 2326 | {string} - - 
127.0.0.1 - - [26/Dec/2001:19:52:48 +0200] "GET /examples/ HTTP/1.1" 404 277 | {string} - - 
127.0.0.1 - - [26/Dec/2001:19:54:37 +0200] "GET /examples/jsp/snp/snoop.jsp HTTP/1.1" 404 294 | {string} - - 
127.0.0.1 - - [28/Dec/2001:09:54:37 +0200] "GET /puga/main.html HTTP/1.1" 404 282 | {string} - - |
| Log 3 | [Wed Dec 26 19:52:48 2001] [error] [client 127.0.0.1] File does not exist: c:/devapp/apache/apache/htdocs/examples/ [Wed Dec 26 19:55:01 2001] [error] [client 127.0.0.1] File does not exist: c:/devapp/apache/apache/htdocs/_vti_bin/owssvr.dll [Wed Dec 26 19:55:01 2001] [error] [client 127.0.0.1] File does not exist: c:/devapp/apache/apache/htdocs/msoffice/cltrq.asp | {string} [date,EEE MMM dd HH:mm:ss yyyy] [priority,debug;info;warn;error;fatal] |
| Log 4 | 28/02/03 20:23:16 ERR Critical error on section 34 on module 5 [Channel 9] 4.4.4.4 | {date,dd/MM HH:mm:ss} [priority,DBG;FLW;WRN;ERR] {string} |
| Log 5 | 5 d MBGN Talk to port 9 f MLPT1 Port open 0 x MCOM Com port open | {number}{tab}{string}{tab}{string}{tab}{string}{tab}{string} |
XpoLog Regular Expressions Patterns Language

As part of XpoLog parsing language, users may apply a regular expression on another column in order to extract a specific value from that column.

Regular expressions language:

Characters
x The character x
\\ The backslash character
\0n The character with octal value 0n (0 <= n <= 7)
\0nn The character with octal value 0nn (0 <= n <= 7)
\0mnn The character with octal value 0mnn (0 <= m <= 3, 0 <= n <= 7)
\xhh The character with hexadecimal value 0xhh
\uhhhh The character with hexadecimal value 0xhhhh
\t The tab character (\u0009)
\n The newline (line feed) character (\u000A)
\r The carriage-return character (\u000D)
\f The form-feed character (\u000C)
\a The alert (bell) character (\u0007)
\e The escape character (\u001B)
\cx The control character corresponding to x

Character classes
[abc] a, b, or c (simple class)
[^abc] Any character except a, b, or c (negation)
[a-zA-Z] a through z or A through Z, inclusive (range)
[a-d[m-p]] a through d, or m through p: [a-dm-p] (union)
[a-zA-Z&&[def]] d, e, or f (intersection)
[a-z&&[^bc]] a through z, except for b and c: [ad-z] (subtraction)
[a-z&&[^m-p]] a through z, and not m through p: [a-lq-z] (subtraction)

Predefined character classes
. Any character (may or may not match line terminators)
[0-9] A digit: [0-9]
[^0-9] A non-digit:[^0-9]
[ ] A whitespace character: [ \t\n\x0B\f\r ]
[\s] A non-whitespace character: [\s]
[a-zA-Z] A word character: [a-zA-Z]
[\w] A non-word character: [\w]

POSIX character classes (US-ASCII only)
[\p{}{Lower}] A lower-case alphabetic character: [a-z]
[\p{}{Upper}] An upper-case alphabetic character: [A-Z]
[\p{}{ASCII}] All ASCII: [0x00-0x7F]
[\p{}{Alpha}] An alphabetic character: [\p{}{Lower}\p{}{Upper}]
[\p{}{Digit}] A decimal digit: [0-9]
[\p{}{Alnum}] An alphanumeric character: [\p{}{Alpha}\p{}{Digit}]
[\p{}{Punct}] Punctuation: One of "!"#$%&'()+,;-./:;<=>?@["]^`{|}~
[\p{}{Graph}] A visible character: [\p{}{Alnum}\p{}{Punct}]
[\p{}{Print}] A printable character: [\p{}{Graph}]
[\p{}{Blank}] A space or a tab: [\s]
[\p{}{Ctrl}] A control character: [\x00-\x1F\x7F]
[\p{}{XDigit}] A hexadecimal digit: [0-9a-fA-F]
[\p{}{Space}] A whitespace character: [\s]
Classes for Unicode blocks and categories

\p{InGreek} A character in the Greek block (simple block)
\p{Lu} An uppercase letter (simple category)
\p{Sc} A currency symbol
\P{InGreek} Any character except one in the Greek block (negation)
\[p{L}&&[^p{Lu}]\] Any letter except an uppercase letter (subtraction)

Boundary matchers

^ The beginning of a line
$ The end of a line
\b A word boundary
\B A non-word boundary
\A The beginning of the input
\G The end of the previous match
\Z The end of the input but for the final terminator, if any
\z The end of the input

Greedy quantifiers

? any character, once or not at all
* any character, zero or more times
+ any character, one or more times
X{n} X, exactly n times
X{[n,]} X, at least n times
X{[n,m]} X, at least n but not more than m times

Reluctant quantifiers

?? any character, once or not at all
?? any character, zero or more times
++ any character, one or more times
X{n}? X, exactly n times
X{[n,]}? X, at least n times
X{[n,m]}? X, at least n but not more than m times

Possessive quantifiers

?+ any character, once or not at all
*+ any character, zero or more times
++ any character, one or more times
X{n}+ X, exactly n times
X{[n,]}+ X, at least n times
X{[n,m]}+ X, at least n but not more than m times

Logical operators

XY X followed by Y
X|Y Either X or Y
(X) X, as a capturing group

Back references

\n Whatever the nth capturing group matched

Quotation

\ Nothing, but quotes the following character
\Q Nothing, but quotes all characters until \E
\E Nothing, but ends quoting started by \Q

Special constructs (non-capturing)

(?X) X, as a non-capturing group
(?idmsux-idmsux) Nothing, but turns match flags on - off
(?idmsux-idmsux:X) X, as a non-capturing group with the given flags on - off
(?=X) X, via zero-width positive lookahead
(?<=X) X, via zero-width negative lookahead
(?<X) X, via zero-width positive lookbehind
(? (?=X) X, as an independent, non-capturing group

Backslashes, escapes, and quoting

The backslash character ('\') serves to introduce escaped constructs, as defined above, as well as to quote characters that otherwise would be interpreted as un-escaped constructs. Thus the expression \ matches a single backslash.

One special case is right/left curly brackets since a curly bracket is used by XpoLog pattern syntax as a reserved sign to open/close field tags. To represent curly bracket which are not XpoLog reserved use: \u007B (left curly bracket) and \u007D (right curly bracket).
It is an error to use a backslash prior to any alphabetic character that does not denote an escaped construct; these are reserved for future extensions to the regular-expression language. A backslash may be used prior to a non-alphabetic character regardless of whether that character is part of an un-escaped construct.

Character Classes
Character classes may appear within other character classes, and may be composed by the union operator (implicit) and the intersection operator (&&). The union operator denotes a class that contains every character that is in at least one of its operand classes. The intersection operator denotes a class that contains every character that is in both of its operand classes.

The precedence of character-class operators is as follows, from highest to lowest:

1. Literal escape \x
2. Grouping [...]
3. Range a-z
4. Union [a-e][i-u]
5. Intersection [a-z&&[aeiou]]

Note that a different set of metacharacters are in effect inside a character class than outside a character class. For instance, the regular expression . loses its special meaning inside a character class, while the expression - becomes a range forming metacharacter.

Line terminators
A line terminator is a one- or two-character sequence that marks the end of a line of the input character sequence. The following are recognized as line terminators:

- A newline (line feed) character (\n'),
- A carriage-return character followed immediately by a newline character (\r\n'),
- A standalone carriage-return character (\r'),
- A next-line character (\u0085),
- A line-separator character (\u2028), or
- A paragraph-separator character (\u2029).

If UNIX_LINES mode is activated, then the only line terminators recognized are newline characters.

The regular expression . matches any character except a line terminator unless the DOTALL flag is specified.

By default, the regular expressions ^ and $ ignore line terminators and only match at the beginning and the end, respectively, of the entire input sequence. If MULTILINE mode is activated then ^ matches at the beginning of input and after any line terminator except at the end of input. When in MULTILINE mode $ matches just before a line terminator or the end of the input sequence.

For a more precise description of the behavior of regular expression constructs, please see Mastering Regular Expressions, 2nd Edition, Jeffrey E. F. Friedl, O'Reilly and Associates, 2002.

Syntax:
regexp - a regular expression, used to extract part of the data from another column will be extracted out of the value in the source column

| refIndex/refName (mandatory): the zero-based index of the source column |
| refName=column_name;columnType=date/timestamp/number;multiLine=true/false,(regular_expression_to_extract) |
| columnType (mandatory if date/timestamp only): columnType=timestamp;dateFormat=<the desired format of the date> |
| multiLine (optional): indicates whether the record spreads over more than one line |

Examples:
<table>
<thead>
<tr>
<th>Log Events Example</th>
<th>XpoLog Pattern</th>
<th>What will be extracted by the Regular Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Jul 10 04:33:51 2017 ALTER DATABASE ADD LOGFILE THREAD 2 GROUP 3 ('/oradata/PROD/redo.log') SIZE 200K, GROUP 4 ('/oradata/PROD/redo.log') SIZE 200K ORA-336 signalled during: ALTER DATABASE ADD LOGFILE THREAD 2 GROUP 3 ('/oradata/PROD/redo.log') SIZE 200K, GROUP 4 ('/oradata/PROD/redo.log') SIZE 200K...</td>
<td>{date:Date,EEE MMM dd HH:mm:ss yyyy}{regexp:Error Code,refName=Message,(ORA-\d+)}{string:Message}</td>
<td>ORA-336 will be extracted to a unique column</td>
</tr>
<tr>
<td>Log Message: Error in Application at &lt;2017-05-05 12:00:00.000&gt;</td>
<td>{text:type}:{string:Message}{regexp:Date,refName=Message;columnType=date;dateFormat=yyyy-MM-dd HH:mm:ss.SSS,&lt;(\d+)&gt;}</td>
<td>2017-05-05 12:00:00.000 will be extracted to a unique column of type date</td>
</tr>
<tr>
<td>Log Message: Error in Application at &lt;1399291200000&gt;</td>
<td>{text:type}:{string:Message}{regexp:Timestamp,refName=Message;columnType =timestamp,dateFormat=yyyy-MM-dd HH:mm:ss.SSS,&lt;(\d+)&gt;}</td>
<td>2017-05-05 12:00:00.000 will be extracted to a unique column of type date (which is a translation of the timestamp 1399291200000)</td>
</tr>
<tr>
<td>2017-05-05 12:00:00.000 ERROR Failed to run application, x=1</td>
<td>{date,yyyy-MM-dd HH:mm:ss.SSS} {text:Priority} {string:Message}{regexp:Error-Code,refName=Message,((x=)</td>
<td>(y=)</td>
</tr>
<tr>
<td>2017-05-05 12:00:00.000 ERROR Failed to run application, y=2</td>
<td>{date,yyyy-MM-dd HH:mm:ss.SSS} {text:Priority} {string:Message}{regexp:Processing-Time,refName=Message;columnType=number,Processing Time: (\d+))</td>
<td>875 will be extracted to a unique column of type number</td>
</tr>
<tr>
<td>2017-05-05 12:00:00.000 ERROR Invalid Processing Time: 875ms</td>
<td>{date,yyyy-MM-dd HH:mm:ss.SSS} {text:Priority} {string:Message}{regexp:Code-X,refName=Message,&quot;userCode&quot;:u007B(&quot;X&quot;)} {regexp:Code-Y,refName=Message,&quot;userCode&quot;:u007B(&quot;Y&quot;)}</td>
<td>YYYYYY will be extracted to a unique column (Code-Y)</td>
</tr>
<tr>
<td>2017-05-05 12:00:00.000 ERROR Message = &quot;userCode&quot;::{&quot;XXXX&quot;:&quot;YYYYYY&quot;}</td>
<td>{date,yyyy-MM-dd HH:mm:ss.SSS} {text:Priority} {string:Message}{regexp:Code-X,refName=Message,&quot;userCode&quot;:u007B(&quot;X&quot;)} {regexp:Code-Y,refName=Message,&quot;userCode&quot;:u007B(&quot;Y&quot;)}</td>
<td>XXXX will be extracted to a unique column (Code-X)</td>
</tr>
</tbody>
</table>

Patterns Knowledgebase

Under this section you can find reference to different patterns of known systems with 'how to' information.

Please note, that the suggested template may require some minor modifications based on the logs configuration in your environment.

Database Logs

Synopsis
The page contains patterns examples of Database Logs such as Oracle, SQL, and DB2. Each database generates log files containing messages that record all types of events, including startup and shutdown information, errors, warning messages, and access information.

Examples

Example 1 - Oracle Alert Log:

The alert log is a chronological log of all messages and errors that occur, including the administrative operations. The alert log is maintained as both an XML-formatted file and a text-formatted file.

Oracle Alert Log Sample (XML-formatted file):

```
<msg time='2014-08-18T05:23:58.391-05:00' org_id='oracle' comp_id='rdbms' msg_id='opistr_real:963:3971575317' type='NOTIFICATION' group='startup' pid='13599' version='1'>
  <txt>Starting ORACLE instance (normal)</txt>
</msg>
```

Oracle Alert Log Pattern (XML-formatted file):

```
```

Example 2 - DB2 Audit Log:

The audit log is an invaluable resource for security-conscious DBAs that need to monitor database events such as failed access attempts, database object modifications, and user validation. Auditing takes place at the instance level, meaning that once it is started, it audits the activity for all databases in that instance.

DB2 Audit Log Sample:

```
2014-08-14-23.59.01.914515", "AUDIT", "FLUSH", 0, 0, "db2p20", "DB2P20", "", 0, 0, "LOCAL_APPLICATION", "db2audit", "",="/sap" "
```

DB2 Audit Log Pattern:

```
{date:Date,yyyy-MM-dd-HH.mm.ss.SSSSSS} ,{text:Category},{text:Audit event},{text:Event correlator},{text:Event status},{text:Database Name},{text:User ID},{text:Authorization ID},{text:Execution ID},{text:Origin Node Number},{text:Coordinator Node Number},{text:Application Name},{text:Authentication Type}
```

Example 3 - DB2 Validate Log:

The validate log verifies the basic functions of a DB2 copy by checking the state of installation files, instance setup, and local database connections.

DB2 Validate Log Sample:

```
2014-08-14-23.59.02.038162", "VALIDATE", "AUTHENTICATION", 0, 0, "", "db2p20", "DB2P20", "", 0, 0, "LOCAL_APPLICATION", "db2audit", "",="/sap"
```

DB2 Validate Log Pattern:

```
{date:Date,yyyy-MM-dd-HH.mm.ss.SSSSSS} ,{text:Category},{text:Audit event},{text:Event correlator},{text:Event status},{text:Database Name},{text:User ID},{text:Authorization ID},{text:Execution ID},{text:Origin Node Number},{text:Coordinator Node Number},{text:Application Name},{text:Authentication Type}
```

Links

Template applying instructions:

1. Download the templates - Oracle - Template, DB2 - Templates
Frament: 2. Import the templates (see Importing a Template)
3. Apply the templates on multiple logs (see Applying a Template on Multiple Logs)

FTP Server Logs

Synopsis
The page contains patterns examples of FTP Server Logs such as VSFTPD. The FTP server generates log files containing messages that record all types of events, including errors, warning messages, and access information.

Examples

Example 1 - VSFTPD Log:
VSFTPD, (or very secure FTP daemon), is an FTP server for Unix-like systems, including Linux. It is licensed under the GNU General Public License. It supports IPv6 and SSL.

VSFTPD Log Sample:
Tue Aug  5 09:41:06 2014 [pid 9411] CONNECT: Client "103.5.6.247"
Tue Aug  5 09:41:06 2014 [pid 9411] FTP response: Client "103.5.6.247", "220 Welcome to Trend Micro BA FTP service."
Tue Aug  5 09:41:06 2014 [pid 9411] FTP command: Client "103.5.6.247", "USER anonymous"

VSFTPD Log Pattern:
{date:Date,locale=en,EEE MMM d yyyy} [pid {text:PID}]{block,start,emptiness=true} [{text:User} hh:mm:ss {block,end,emptiness=true}]{text:Operation}: Client "{text:Client} {block,start,emptiness=true} {block,end,emptiness=true} {string:Message} {block,end,emptiness=true}

Links
Template applying instructions:
1. Download the template - VSFTPD - Template
2. Import the template (see Importing a Template)
3. Apply the template on multiple logs (see Applying a Template on Multiple Logs)

J2EE Application Servers Logs

Synopsis
The page contains patterns examples of J2EE Application Servers Logs such as WebLogic, WebSphere, Tomcat and JBoss. Each J2EE application server generates log files containing messages that record all types of events, including startup and shutdown information, errors, warning messages, and access information about HTTP requests.

Examples

Example 1 - WebLogic Server Log Sample:
####<Jan 23, 2013 9:49:12 AM IDT> <Info> <WebLogicServer> <serverwin> <> <Main Thread> <> <> <> <1184050152371> <BEA-000377>
<Starting WebLogic Server with BEA JRockit(R) Version R26.4.0-63_CR302700-72606-1.5.0_06-20061127-1108-win-ia32 from BEA Systems, Inc.>
####<Jan 23, 2013 9:49:12 AM IDT> <Info> <Management> <serverwin> <> <Main Thread> <> <> <> <1184050152746> <BEA-141107>
-Version: WebLogic Server 10.0 Wed May 9 18:10:27 EDT 2007 933139>
####<Jan 23, 2013 9:49:15 AM IDT> <Info> <WebLogicServer> <serverwin> <> <Main Thread> <> <> <> <1184050155058> <BEA-000215>
<Loaded License : C:\bea\license.bea>

Example 1 - WebLogic Server Log Pattern:
####<{date:Timestamp,locale=en,MMM dd, yyyy HH:mm:ss a z}> <{priority:Severity,Debug;Info;Warning;Error;Notice;Critical;Alert;Emergency}> <{text:Subsystem}> <{text:Machine Name}> <{text:Server Name}> <{text:Thread ID}> {block,start,emptiness=true}<{block,end,emptiness=true}<{text:User ID}>{block,start,emptiness=true}<{block,end,emptiness=true}<{text:Transaction ID}> <{string:Diagnostic Context ID}> <{string:Raw Time Value}> <{text:Message ID}> {string:Message}

Example 2 - WebLogic Access Log Sample:
10.0.0.61 - - [9/Jan/2013:09:50:01 +0300] "GET /index.jsp HTTP/1.1" 200 8306
10.0.0.61 - - [9/Jan/2013:09:50:08 +0300] "GET /ootb.css HTTP/1.1" 200 6114
10.0.0.61 - - [9/Jan/2013:09:50:08 +0300] "GET /images/splash_server_90_short.gif HTTP/1.1" 200 10659

Example 2 - WebLogic Access Log Pattern:
{text:Remote Host,Remote Host} {string:Remote Logical Username} {string:Remote User} 
{[date:Date,locale=en,dd/MMM/yyyy:HH:mm:ss z]} 
{[string:Method] [string:URL] [string:Protocol]"} {number:Status} {string:Bytes Sent}{eoe}

Example 3 - WebSphere HTTP Error Log Sample:
[Thu, 05 Jan 2013 06:29:58 GMT] [debug] [10.0.0.39:1853/10.0.0.61:9080] Connection persistence updated to true
[Thu, 05 Jan 2013 06:29:58 GMT] [debug] [10.0.0.39:1853/10.0.0.61:9080] Finished parsing the message

Example 3 - WebSphere HTTP Error Log Pattern:
{[date:Date,locale=en,EEE, dd MMM yyyy HH:mm:ss z]} 
{[priority:Severity,debug;info;warn;error;crit]} 
{[string:Remote Host,refIndex=2,(.*):.*]}{regexp:Remote Port,refIndex=2,.*:(.*)}{regexp:Server Host,refIndex=3,(.*):.*}{regexp:Server Port,refIndex=3,.*:(.*)} 
{string:Message}

Example 4 - WebSphere HTTP Access Log Sample:
10.0.0.39 - - [05/Jan/2013:09:23:18 +0300] "GET /logeye HTTP/1.1" 302 0
10.0.0.39 - - [05/Jan/2013:09:23:18 +0300] "GET /logeye/ HTTP/1.1" 304 0
10.0.0.39 - - [05/Jan/2013:09:23:18 +0300] "GET /logeye/root.html HTTP/1.1" 304 0

Example 4 - WebSphere HTTP Access Log Pattern:
{string:Remote Host} {string:Remote Logical Username} {string:Remote User} 
{[date:Date,locale=en,dd/MMM/yyyy:HH:mm:ss z]} 
{[string:Method] [string:URL] [string:Protocol]"} {number:Status} {string:Bytes Sent}

Example 5 - WebSphere System Err Log Sample:

Example 5 - WebSphere System Err Log Pattern:
{[date:Date,locale=en,MM/dd/yy HH:mm:ss:SSS z]} 
{[string:Message ID]} 
{[string:Source,charsLength=13]} 
{[string:Priority]} 
{[string:Message]}

Example 6 - WebSphere System Out Log Sample:
TRAS0017I: The startup trace state is *=info.
[01/15/13 9:18:53:672 IDT] 0000000a I UOW=null source=com.ibm.ejs.ras.ManagerAdmin org=IBM prod=WebSphere component=Application Server thread=[main]
TRAS0111I: The message IDs that are in use are deprecated
ADMN0015I: The administration service is initialized.

Example 6 - WebSphere System Out Log Pattern:
{[date:Date,locale=en,MM/dd/yy HH:mm:ss:SSS z]} 
{[string:ThreadId,charsLength=9]} 
{[string:Event Type]} 
UOW={string:UOW} source={string:Source} org={string:Organization} prod={string:Product} component={string:Component} thread={string:Thread} {[string:Message]}

Links

Template applying instructions:
1. Download the templates - WebSphere - Templates, WebLogic - Templates
2. Import the templates (see Importing a Template)
3. Apply the templates on multiple logs (see Applying a Template on Multiple Logs)

**Linux System Logs**

**Synopsis**

The page contains patterns examples of Linux System Logs such as authorization mechanisms, system daemons, system messages, and the all-encompassing system log itself, syslog. The Linux system provides vital information using various system log files. These log files are typically plain ASCII text in a standard log file format, and most of them sit in the traditional system log sub-directory /var/log.

System logs deal primarily with the functioning of the Linux system, not necessarily with additional applications added by users.

**Examples**

**Example 1 - Authorization Log:**

The Authorization Log tracks usage of authorization systems, the mechanisms for authorizing users which prompt for user passwords, such as the Plug-gable Authentication Module (PAM) system, the sudo command, remote logins to sshd and so on. The Authorization Log file may be accessed at /var/log/auth.log. This log is useful for learning about user logins and usage of the sudo command.

**Authorization Log Sample:**

Dec 22 06:25:09 pizza1 CRON[27336]: pam_unix(cron:session): session closed for user root
Dec 22 06:25:23 pizza1 sshd[32006]: Accepted password for xplg from 10.0.0.124 port 62880 ssh2
Dec 22 06:25:23 pizza1 sshd[32006]: pam_unix(sshd:session): session opened for user xplg by (uid=0)

**Authorization Log Pattern:**

```
{date:Date,locale=en,MMM dd HH:mm:ss} {text:Host} {text:Process Name}
{number:Process Id}: {text:Message}
```

**Example 2 - System Log:**

The System log typically contains the greatest deal of information by default about your Linux system. It is located at /var/log/syslog, and may contain information other logs do not. You should consult the System Log when you can't locate the desired log information in another log.

**System Log Sample:**

Jan 6 06:35:01 pizza1 CRON[29271]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Jan 6 06:39:05 pizza1 postfix/sendmail[4506]: fatal: open /etc/postfix/main.cf: No such file or directory
Jan 6 06:39:05 pizza1 CRON[14731]: (root) MAIL (mailed 1 byte of output; but got status 0x004b, #012)

**System Log Pattern:**

```
{date:Date,locale=en,MMM dd HH:mm:ss} {text:Host} {text:Process Name}
{number:Process Id}: {text:Message}
```

**Example 3 - Messages Log:**

The Messages log contains informational messages from applications and system facilities, and is available at /var/log/messages. This log is useful for examining message output from applications and system facilities including mail, cron, daemon, kern, auth, etc.

**Messages Log Sample:**

Aug 17 04:02:05 serverlinux syslog-ng[23102]: Configuration reload request received, reloading configuration;
Aug 17 04:02:06 serverlinux syslog-ng[23102]: Syslog connection failed; Id=’14’, server=’AF_INET(10.0.0.101:2000)’, error=’No route to host (113)’, time_reopen=’60’
Aug 17 04:02:22 serverlinux sshd(pam_unix)[27814]: session opened for user root by root(uid=0)

**Messages Log Pattern:**

```
{date:Date,locale=en,MMM dd HH:mm:ss} {text:Host} {text:Process Name}
{number:Process Id}: {text:Message}
```

**Links**

Template applying instructions:
1. Download the templates - Linux System - Templates
2. Import the templates (see Importing a Template)
3. Apply the templates on multiple logs (see Applying a Template on Multiple Logs)

Windows Event Logs

Synopsis

The page contains patterns examples of Windows Events Logs such as Application, Security and System.

Windows event log is a record of a computer's alerts and notifications. The Windows operating system classifies events by type. For example, an information event describes the successful completion of a task, such as installing an application. A warning event notifies the administrator of a potential problem, such as low disk space. An error message describes a significant problem that may result in a loss of functionality. A success audit event indicates the completion of an audited security event, such as an end user successfully logging on. A failure audit event describes an audited security event that did not complete successfully, such as an end user locking himself out by entering incorrect passwords.

Examples

Example 1 - Application Log Sample:

Information*;*1397756882000*;*Microsoft-Windows-User Profiles Service*;*None*;*1531*;*SYSTEM*;*37L4247F27-26*;*The User Profile Service has started successfully.

Success*;*1397756885000*;*WinMgmt*;*None*;*5615*;*37L4247F27-26*;*Message was not found: 5615

Success*;*1397756885000*;*WinMgmt*;*None*;*5617*;*37L4247F27-26*;*Message was not found: 5617

Example 1 - Application Log Pattern:

{priority:Type,Error;Warning;Information;Success;Audit Failure;Audit Success}*;*{timestamp:Date,MM/dd/yyyy HH:mm:ss}*;*{text:Source}*;*{text:Category}*;*{number:Event}*;*{text:User}*;*{text:Computer}*;*{string:Description}

Example 2 - Security Log Sample:

Audit Success*;*1409379094000*;*Microsoft-Windows-Security-Auditing*;*12544*;*4624*;*WINXPOLOG45QA6.xpolog.local*;*An account was successfully logged on.

Subject:

Security ID: S-1-0-0
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type: 3

Example 2 - Security Log Pattern:

{priority:Type,Error;Warning;Information;Success;Audit Failure;Audit Success}*;*{timestamp:Date,MM/dd/yyyy HH:mm:ss}*;*{text:Source}*;*{text:Category}*;*{number:Event}*;*{text:User}*;*{text:Computer}*;*{string:Description}

Example 3 - System Log Sample:

Information*;*1290311759000*;*Service Control Manager*;*None*;*7036*;*37L4247F27-26*;*The Windows Event Log service entered the stopped state.

Information*;*1397756882000*;*EventLog*;*None*;*6011*;*37L4247F27-26*;*The NetBIOS name and DNS host name of this machine have been changed from 37L4247F27-26 to WIN-D2JU8NFHCP2.

Information*;*1397756882000*;*EventLog*;*None*;*6009*;*37L4247F27-26*;*Microsoft (R) Windows (R) 6.01. 7601 Service Pack 1 Multiprocessor Free.

Example 3 - System Log Pattern:

{priority:Type,Error;Warning;Information;Success;Audit Failure;Audit Success}*;*{timestamp:Date,MM/dd/yyyy HH:mm:ss}*;*{text:Source}*;*{text:Category}*;*{number:Event}*;*{text:User}*;*{text:Computer}*;*{string:Description}
Logstash XpoLog Integration

XpoLog’s architecture allows receiving data sent by logstash, using XpoLog’s logstash output.

There are options to push data over Syslog or over HTTP/S.

Adding Data from Logstash (HTTP/S)

Logstash XpoLog Integration

XpoLog’s architecture allows receiving data sent by logstash from JSON data objects. In order to do this, a HTTP/S listener account should be created in XpoLog for receiving the data on a specific network port, and the XpoLog logstash output should be sending data to this listener.

Technical Details

The logstash configuration file should look like the following:

```
input {
  file {
    path => "FULL_PATH_TO_LOGS_DIRECTORY/FILE"
    start_position => "beginning"
    sincedb_path => "SINCEDB_PATH"
  }
}

filter {
  grok {
    match => ["path","%(GREEDYDATA)%(DATA:parent)%(GREEDYDATA).log"]
    # Adding 3 fields to the JSON (optional).
    # xpologPath - '->' separated list of folders structure to place the log(s) in XpoLog Folders and Logs
    add_field => [ "xpologPath", "FOLDER_AND_LOGS_PATH_IN_XPOLOG" ]
    # xpologName - the name of the log that will be created in XpoLog
    add_field => [ "xpologName", "DEFAULT_NAME_OF_THE_LOG_IN_XPOLOG" ]
    # xpologType - the type of the log in XpoLog. XpoLog will automatically look for templates with the exact same type and, if
    # found, will apply the template's pattern on the received log
    add_field => [ "xpologType", "DEFAULT_TYPE_OF_THE_LOG_IN_XPOLOG" ]
  }
}

if [path] =~ "FILE_NAME_1" {
  # Modifying the parameters for specific file FILE_NAME_1 in the directory FULL_PATH_TO_LOGS_DIRECTORY
  mutate { replace => { xpologPath => "FOLDER_1->FOLDER_2" } }
  mutate { replace => { xpologType => "TYPE_1" } }
  mutate { replace => { xpologName => "NAME_1" } }
}
```
Adding Data from Logstash (Syslog)

Logstash XpoLog Integration

XpoLog’s architecture allows receiving data sent by logstash, using XpoLog’s logstash output. In order to do this, a Syslog listener account should be created in XpoLog for receiving the data on a specific network port, and the XpoLog logstash output should be sending data to this listener.

Technical Details

XpoLog’s logstash output is a Ruby file that implements the logstash output functionality. The data that is sent by the output to the XpoLog listener is stored in logs and is available for searching, monitoring and analysis.

Setup

Note that in order for XpoLog to receive information sent from logstash, you should have an XpoLog Syslog listener configured and running. For more information about setting up a Syslog listener, click [here](#)

1. Download XpoLog’s logstash output: `xpolog.rb`
2. Copy the `xpolog.rb` file you have downloaded to the `lib/logstash/outputs` directory, located under the logstash root directory
3. Configure the `xpolog` output according to the available configuration
4. Start XpoLog’s logstash output

XpoLog’s logstash output configuration

The following is an example of the structure of the `xpolog` output element.

```ruby
output {
  xpolog {
    host => "localhost"
    port => 514
    protocol => "udp"
    logname => "my-log"
    procid => "1"
    logparameters => {
      xpologPath => "Root->my-folder"
    }
  }
}
```

The following table describes the parameters of output element.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>host</strong></td>
<td>Mandatory</td>
<td>The name of the host to send the data to (the XpoLog host)</td>
<td>String</td>
</tr>
<tr>
<td><strong>port</strong></td>
<td>Mandatory</td>
<td>The network port on which the XpoLog Syslog listener is listening</td>
<td>Numeric</td>
</tr>
<tr>
<td><strong>protocol</strong></td>
<td>Optional</td>
<td>The network protocol to be used when sending data to the XpoLog Syslog listener. Optional values are udp or tcp. Default value is udp</td>
<td>String</td>
</tr>
<tr>
<td><strong>logname</strong></td>
<td>Optional</td>
<td>The name of the log that will be created in XpoLog. The value of this parameter will be concatenated to the name of the host sending the data, unless the logname parameter is preceded with #</td>
<td>String</td>
</tr>
<tr>
<td><strong>procid</strong></td>
<td>Optional</td>
<td>A parameter used to distinguish between different logstash processes that send data from the same machine to the same XpoLog Syslog listener</td>
<td>String</td>
</tr>
<tr>
<td><strong>logparameters</strong></td>
<td>Optional</td>
<td>A set of optional parameters</td>
<td>Hash</td>
</tr>
<tr>
<td><strong>logparameters/xpologPath</strong></td>
<td>Optional</td>
<td>The path, in XpoLog’s Folders and Logs tree, in which the log will be created</td>
<td>String</td>
</tr>
<tr>
<td><strong>logparameters/pattern</strong></td>
<td>Optional</td>
<td>The data pattern that will be applied on the log</td>
<td>String</td>
</tr>
</tbody>
</table>

### Defining a Log Collection Policy

For each log added to XpoLog, a Log Collection Policy must be used for defining how XpoLog server should collect the log information into its repository, and how long the logs should be archived. This can be a default Collection Policy or a previously defined Collection Policy. You can also define a new Collection Policy.

The Log Collection Policy criteria can be defined in the following tabs:

- **Members** – for selecting the logs that are collected into the XpoLog repository using this policy
- **Storage** – for defining where to store the log data, the maximum disk space that the policy can use for collecting data, how long to keep files in the storage to be available for searches before deleting them, and the email address of the administrator to notify when the maximum storage space is reached or if there is an error collecting data.
- **Collection Schedule** – for defining the frequency of bringing data into XpoLog
- **Archiving** – for defining the location of the archived data

### Storage: XpoLog ( Indexed) Data

is stored in a Binary, non readable format and cannot be read or decrypted only by XpoLog. In case data is being tampered, XpoLog immediately alerts on the issue.

### Archive: XpoLog archived Data

is stored in compressed flat files. XpoLog runs a standard checksum (SHA-1/MD5) on the archive repository. In case data is being tampered, XpoLog immediately alerts on the issue.

### To define a new Log Collection Policy:

1. In the XpoLog Manager main menu, select **Administration > Collection Policies.**
   - The Collection Policies page opens.
2. Click the **New Collection Policy** button.
   - The Add new collection policy page opens.
3. In **Name**, type the name of the Collection Policy.
4. In **Description**, type a short description of the Collection Policy.
5. Define the Collection Policy members. See Defining the Collection Policy Members section below.
6. Define the Collection Policy storage criteria. See Defining the Collection Policy Storage Criteria section below.
7. Define the archiving policy and security of the Collection Policy. See Defining Archiving below.
8. Click **Save**.
   - The Collection Policy is saved and can be used for adding logs and log directories.

### Defining the Collection Policy Members

In the Members tab, you can select the logs that are to use the Collection Policy.

**In the Collection Policies page, select the Members tab:**

1. In the page that appears, select the checkboxes of the logs that are to use this Collection Policy.

### Defining the Collection Policy Storage Criteria

In the Storage tab, you can define where to store the collected data and other storage criteria.

**In the Collection Policies page, select the Storage tab:**

1. **Storage Repository** - browse to the location where to store the collected data, it is recommended to use a fast storage for this location.
   - The default is the XpoLog internal data directory.
2. **Retention Policy** - in the Delete files older than, specify at what age files are to be removed from the repository.
3. **Email Notification** - specify a semicolon separated list of email addresses that an alert will be sent to on policy related failures.
4. **Data Encryption** - XpoLog stores its internal data in a proprietary, non-readable model, but not by default encryption is not active for maximal performance (recommended). By selecting an encryption algorithm, as of the next policy's execution data will be stored encrypted. Storing encrypted data causes an overhead when writing/reading data which may result in a performance decrease of data collection/index/search.

**Defining the Collection Schedule**

You can define the frequency of collecting data from the log: Daily, Weekly, Monthly, or Never. Depending on the frequency selected, parameters appear for specifying the collection schedule.

**In the Collection Policies page, select the Collection Schedule tab:**

1. **Set Frequency** - select the frequency of bringing data into the system: *Never, Daily, Weekly, or Monthly.*
   Set the parameters that appear, as relevant.
2. **Assigned Instance** - In case XpoLog is running in a clustered environment, with more than one processor node, this option allows to determine which of the processors will be responsible for the collection policy.
3. **Live Mode Collection Frequency** - activating Live Mode in the search console immediately executes collection from all relevant sources in order to fetch matching log records, in near real time, to the console.
   The frequency of collection while Live Mode is active is determined here. By default, the collection will run every 10 seconds as long as Live Mode is active in search.
   **Pay attention:** the frequency set here determines the collection frequency of logs which are part of the collection policy during Live Mode, and the load that may be seen on the sources while active. It is recommended that users will be guided to activate Live Mode on specific logs/folders/servers, and not on the entire environment, to avoid unnecessary load on multiple sources.

**Defining Archiving**

Data stored in an archive is for long-term storage of data, and unlike Storage data, is unavailable to the user for searching and viewing. However, archive data can be restored and added to XpoLog as a local log (note that it is a manual process).

Checksum algorithms for ensuring data integrity can be activated; supported types are SHA1 and MD5. The Checksum algorithm checks that there has been no data tampering. Execution of the checksum algorithm results in a signature, which is saved in a file location, so that the current signature can be compared with previous signatures. The Checksum result file location can be customized to any location that XpoLog can access (default is XpoLog internal repository.)

**In the Collection Policies page, select the Archiving tab:**

1. **Archive Repository** - select Local (recommended), Windows Network, Over SSH or AWS S3 Bucket. In **Archive Path**, browse to the location where to archive the collected data, it is not mandatory to use a fast storage for this location.
   **Note:** Local repository is recommended for large volumes of data, if you're not using Local then you'll be asked to select a connectivity account to the selected location.
2. **Archiving Policy**:
   a. Select the **Enable Archiving** checkbox to enable archiving collected logs; clear the checkbox to disable archiving.
   b. **Archive all data**, by default this option is selected. When initially enabled, the first archiving execution will archive ALL data which is currently stored in XpoLog - note that this may take a very long time in case the repository is large. If not selected, then archive will take place from the first time of execution going forward.
   c. In **Delete archive files older than**, select the age that logs are automatically deleted from the archive.
3. **Archiving Security** - In Checksum algorithm, select a checksum algorithm for securing your archived logs: *None, MD5, SHA1 or SHA-256.*

**Defining Data Forwarding**

XpoLog instances support forwarding logs data over a variety of protocols (Syslog UDP/TCP, HTTP/S, etc.) – the data can be received by either other XpoLog instances or any other supported device.

You can define predefined and generic data forwarders such as: **XpoLog Forwarder, Syslog Forwarder, HTTP/S Forwarder,** and **Generic Forwarder.** You can also define a couple of data forwarders that will run in parallel.

**In the Collection Policies page, select the Data Forwarding tab:**

1. In the page that appears, add new Data Forwarder. If this is the first time that XpoLog is configured to forward data then you will be asked to enter details that XpoLog can use to forward the requested data.
   Create the data forwarder and save it.

**Editing a Collection Policy**

You can modify the Name, Description, or any parameters in any of the tabs of a Collection Policy.
To modify a Collection Policy:

1. In the Collection Policies table, select the Collection Policy to modify.
2. Right-click the Collection Policy and from the menu that appears, click Edit OR
   Click the Edit button.
   The definition of the selected Collection Policy is displayed.
3. Modify the Collection Policy’s name, description, or any of the parameters in its tabs, as required. See Defining a Log Collection Policy on how to fill in the parameters.
4. Click Save.
   The collection policy is modified.

Duplicating a Collection Policy

You can base one Collection Policy on an existing policy, by duplicating the defined Collection Policy, giving it another name, and description, selecting the members for the policy, and modifying parameters in the tabs, as required.

To duplicate a Collection Policy:

1. In the Collection Policies table, select the Collection Policy to duplicate.
2. Right-click the Collection Policy and from the menu that appears, click Duplicate OR
   Click the Duplicate button.
   The Add new collection policy page is displayed. The name, description, and checkboxes of the members are cleared. The parameters in the other tabs are duplicated.
3. Type a Name and Description for the new collection policy, select its members, and modify any of the parameters in its other tabs, as required. See Defining a Log Collection Policy on how to fill in the parameters.
4. Click Save.
   The new collection policy is saved, and appears in the Collection Policies table.

Deleting a Collection Policy

You can delete a Collection Policy that is no longer in use by logs.

To delete a Collection Policy:

1. In the Collection Policies table, select the Collection Policy to delete.
2. Right-click the Collection Policy and from the menu that appears, click Delete OR
   Click the Delete button.
   A Confirmation of Deletion box appears.
3. Click Yes.
   The collection policy is deleted and removed from the Collection Policies table.

Scheduling the Archiving Task

By default, XpoLog archives the logs of all policies at 1 am, as archiving is a heavy task. You can reschedule the archiving for a different time.

To schedule archiving:

1. In the Collection Policies console, click the Schedule Archive Task
   A page opens for selecting the frequency and time of archiving.
2. Click Save.
   Scheduling is saved in the system. Archives will be run on this schedule.

Scheduling the Security Task

Checksum is a heavy task that should be run at off-peak hours. You can schedule the running of Checksum accordingly.

To schedule running Checksum:

1. In the Collection Policies console, click the Schedule Security Task button.
   A page opens for selecting the frequency and time of running Checksum.
2. Click Save.
   Scheduling is saved in the system. Checksum will be run on this schedule.

Syslog Forwarder

To send data over Syslog Forwarder:

1. Go to Manager > Administration > Collection Policies->Edit->Data Forwarding.
2. Add New Syslog Forwarder, for each Syslog Forwarder the following should be configured:
   a. Name: the name of the Syslog Forwarder
   b. Description: the description of the Syslog Forwarder
   c. Enabled: the Syslog forwarder is enabled by default. Uncheck for disabling.
   d. Host: the remote host to which data should be sent.
   e. Port: the port that will be used by the Syslog Forwarder to send data.
1. **Protocol**: the Syslog can forward data on either UDP or TCP

   g. **Advanced Settings**:
      
      - **Facility**:
        Select a unique facility value by which data should be sent.

      - **Severity**:
        Select a unique severity value by which data should be sent.

      - **Source ID**:
        The source ID of the data that are sent over the Syslog forwarder.

      - **Data Filter Query**:
        Enter a data filter query

3. Save the Syslog Forwarder.
4. Data sent from the Syslog Forwarder will be sent to the configured device.

**Note:** it is possible to configure multiple Syslog Forwarders in the same collection policy.

**XpoLog Forwarder**

To send data over **XpoLog Forwarder**:

1. Go to Manager > Administration > Collection Policies->Edit->Data Forwarding.
2. Add New **XpoLog Forwarder**, for each XpoLog Forwarder the following should be configured:
   a. **Name**: the name of the XpoLog Forwarder
   b. **Description**: the description of the XpoLog Forwarder
   c. **Enabled**: the XpoLog forwarder is enabled by default. Uncheck for disabling.
   d. **Remote Xplg**: the remote XpoLog account to which data should be send.
   e. **Token**: the token ID of the XpoLog Listener account to which data should be send.
   f. **Source ID**: the source ID of the data that are sent over the XpoLog forwarder.
   g. **Advanced Settings**:

      - **Data Filter Query**:
        Enter a data filter query

3. Save the XpoLog Forwarder.
4. Data sent from the XpoLog Forwarder will be sent to the configured remote XpoLog.

**Note:** it is possible to configure multiple XpoLog Forwarders in the same collection policy.

**HTTP/S Forwarder**

To send data over **HTTP/S Forwarder**:

1. Go to Manager > Administration > Collection Policies->Edit->Data Forwarding.
2. Add New **HTTP/S Forwarder**, for each HTTP/S Forwarder the following should be configured:
   a. **Name**: the name of the HTTP/S Forwarder
   b. **Description**: the description of the HTTP/S Forwarder
   c. **Enabled**: the HTTP/S forwarder is enabled by default. Uncheck for disabling.
   d. **URL**: the URL to which the forwarder should send data - including the IP address/Hostname, port, path and token
   e. **Method**: the method (POST/GET) of the HTTP/S forwarder by which data should be send.
   f. **Advanced Settings**:

      - **Data Filter Query**:
        Enter a data filter query

3. Save the HTTP/S Forwarder.
4. Data sent from the HTTP/S Forwarder will be sent to the configured device.

**Note:** it is possible to configure multiple HTTP/S Forwarders in the same collection policy.

**Apps Administration**

XpoLog Apps are logical containers of dashboards. Apps enable organizations to create and manage a rich variety of data visualizations for multiple teams, systems and environments in a convenient and logical way.

Each App may be identified by a different color, image and name and endow a set of characteristics to its associated dashboards and gadgets. Apps in XpoLog may be **Custom Apps** created by users and/or Out of the Box Apps from XpoLog Apps Market Place.
To enter the App console click the Apps tab. The available Apps are displayed.

Review the Out of the Box Applications delivered to you by XpoLog:

XpoLog allows to open multiple Apps/Dashboards in a single browser session. Mouse over the icon allows quick navigation between the open Apps/Dashboards:
Managing Apps

- To create a Custom App on your data see Adding a Custom App.
- To create an Out of the Box App from XpoLog Apps Marketplace see Adding an Out of the Box App.

The following icons which may be presented below an App, indicate an important configuration of this App:

- The icon \[\] indicates that one of the App's dashboards is set as the system home page
- The icon \[\] indicates that the App is scheduled to be exported
- The icon \[\] indicates that the App is running in offline mode.

XpoLog enables management of its Apps from menu entry of each App.

Mouse over an App and click the \[\] icon to display the menu options, as follows:

- **View** – For opening the App and get the list of available Dashboards under the App. See XpoLog Dashboards.
- **Close (optional)** – For closing an App if the App is opened (I.E. one of its dashboards is currently being displayed).
- **Edit** – For defining the general settings of an App - name, color/image identifier, generation interval, time frame, export settings, etc. (See App Settings)
- **Duplicate** – For duplicating an existing App and defining a new one on its basis.
- **Export Conf.** – For exporting an App configuration (all settings and dashboards) and allowing an import of its definition in another XpoLog. See Export/Import App Conf.
- **Delete** – For removing an existing App and all its dashboards.

Adding a Custom App

The following procedure describes how to add a new custom App to XpoLog.

To add a new App to XpoLog:

1. In the main screen, click the **Apps** tab on the top left. The Apps management console is displayed.
2. Click the 'Create APP' entry in the menu on the left of the main screen.
Adding an Out of The Box App

The following procedure describes how to add a new Out of the Box App to XpoLog.

To add a new Out of the Box App to XpoLog:

1. In the main screen, click the Apps tab on the top left.
   The Apps management console is displayed.

2. Click the 'Marketplace' entry in the menu on the left of the main screen.

   The Marketplace opens.

3. The Marketplace displays the available Apps that can be simply imported into XpoLog - mouse over an App and select preview to see more details about it:

4. Review the App information and details. Click deploy to add it to XpoLog:
Important: Each requires data preparations to ensure that requires logs are properly configured in XpoLog and visualized by the App. For more details please review the section - Preparing Data for Apps

5. The new App is deployed and available in the Apps main screen.
6. Mouse over the App and click the ! icon, then click the 'Edit' entry to display the App Settings or alternatively, click the new App to enter it and then click the 'Edit App' entry in the menu on the left.
7. Enter the new App to see its dashboards.

Removing an App
To remove an App from XpoLog:
1. In the main screen, click the Apps tab on the top left. The Apps management console is displayed.
2. Mouse over the App and click the ! icon, then click the 'Delete' entry and confirm the operation - the App and all its dashboard will be deleted.

App Settings
The App settings contains different settings on the App level. Unless changed individually, Dashboards and Gadgets inherit the Apps settings. There are two options to open the general settings of an App:
1. In the main Apps screen, mouse over an App and click the ! icon to displays the menu items and select Edit App.
2. Click an App to enter its Dashboards view, and click the Edit App on the left hand side.

App's general settings screen is opened.

General
The general settings section allows to configure Name, Description and color or image identifier to the App (if an image is used, it is recommended to use a square image and not a rectangle)
Time Settings

The time settings section allows to configure the following:

- **Time Range**: the default App time range which all dashboards and gadgets will display by default unless configured individually otherwise. Time Range which is set to Live determines a real time execution of the dashboards and gadgets under this App. Dashboards and gadgets will not be generated in the background, results will be calculated and displayed in real time only and while a dashboards is opened.

- **Generation Frequency**: the frequency that new data will be processed and displayed in the App's dashboards and gadgets. Generation frequency which is set to Never determines an offline mode of the App - dashboards and gadgets will be generated only on the exported time definition and/or on demand.

App Sources

The App sources enables a generic definition of the Apps logs/folders/servers sources which will be added to all used search queries in the dashboard's gadgets.

For example if the App's dashboards should refer to servers x, y, z then it is possible to specify this directly in each gadget's search query. Alternatively, it is possible to use generic queries in the gadgets and specify the list of sources in the App Sources section.

Using App Sources makes it very simple to duplicate, maintain and manage the list of sources that will be analyzed by the App's dashboards.

Export Settings

The export settings section determines if/what to export from this App.
- Exporting Frequency: a frequency, a specific time or several times in which the App's dashboards will be exported according to the Export to Email / Export to File definition.
- Dashboards: by default, all dashboards will be exported based on the export definition. It is possible to select only specific dashboards from the App's dashboards to be exported.
- Exporting:
  - The export mechanism supports an export of all selected dashboards as PDF and/or CSV files by email and/or by saving a file in the specified location.
  - Export To Email: the email settings that will be used when exporting the App's dashboards by email (for multiple recipients use a comma separated list).
  - Export To File: the format, location and retention settings that will be used when exporting the App's dashboards to files on the file system.

XpoLog Apps support definition of multiple export schedulers. Using more than one export scheduler allows configuration of a specific date range for each scheduled export. For example it is possible to configure on the same App an export scheduler once a week on the last week and another scheduler once a day on the last day - the result will be a daily export presenting the last day and a weekly export presenting the last week of the specified dashboards in this App.

Export / Import an App

Exporting an App Configuration

Exporting an App provides a zip file with the entire App's configuration to enable future import in another XpoLog. There are two options to export an App's configuration:

1. Mouse over an App and click the
Importing an App Configuration

Importing an App enables a fast creation of an App with its Dashboard's definition. To import an App:

In the main Apps screen, click the Import App Conf. on the left hand side, select the App's configuration zip file and click the Import App button.

A new App is created.

Preparing Data for Apps

Background

XpoLog Apps marketplace is a one stop shop for out of the box applications that will enable you to integrate your machine generated data into XpoLog, receive insights on logs and servers performance and data analysis automatically.

With XpoLog Apps Marketplace You have access to a broad selection of managed applications and devices like Load Balancing, Storage, Machines Images, Virtual servers, Web Servers, Audit servers, CDN and more.

Benefits

- Easily manage all your applications in a a one Data Analytics central container
- Search, Filter, Analyze and Report applications’ insights quickly
- Easy to use GUI dashboards to manage your system’s entities and objects

In order to setup and use XpoLog our of the box Apps you first need to add and prepare the log data from the system you plan to analyze. In order to make the out of the box apps work properly it is recommended to take the following steps:

1. Follow the add data for the target App steps, you can find the list of apps below.
2. Setup the log data according to the specification and then deploy the target app on the target data set that you have prepared.

Prepare Data for the following Out of the box Apps:

Web Servers

- Apache Httpd (Ver 2.2)
- Apache Httpd (Ver 2.4)
- Nginx (Ver 1.10)
- IIS (Ver 6)
- IIS (Ver 7)
IIS (Ver 8)

Load Balancers
- Apache Httpd (Ver 2.2)
- Apache Httpd (Ver 2.4)
- Nginx (Ver 1.10)
- Amazon EC2 ELB - Elastic Load Balancer
- Microsoft ISA
- F5

Technologies and Logging SDK
- Apache log4j (Ver 1.2)
- Apache log4j (Ver 2.0)

Operating Systems
- Windows
- Linux
- Amazon EC2 AMI Linux

Application Servers - J2EE
- Apache Tomcat (Ver 6)
- Apache Tomcat (Ver 7)
- Apache Tomcat (Ver 8)
- Apache Tomcat (Ver 9)
- JBoss (Ver 5)
- JBoss (Ver 6)
- WebSphere (Ver 9)
- WebLogic (Ver 11)

Amazon Web Services
- Amazon EC2 ELB - Elastic Load Balancer
- Amazon Cloudfront
- Amazon Linux AMI
- Amazon S3

Amazon Cloudfront

Background
Built in Amazon CloudFront dashboards and consoles to gain deep-level insights on your global content delivery network all across your cloud AMIs at once.

Steps

1. Add Log Data In XpoLog, When adding a log to XpoLog you can now set a Log Type (logtype). For Amazon Cloudfront set the following logtypes:
   a. AWS
   b. Cloudfront

2. The Cloudfront access log usually is placed in a S3 bucket with the name structure: <SITE_ID>.<DATE>.<UNIQUE_ID>.gz - in XpoLog it should be represented as {string}.{date,yyyy-MM-dd}-{string}.gz
   It is required to configure a S3 account for XpoLog to connect and read the required data from the S3 bucket.

3. Once all required information is set click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Amazon Cloudfront App. Use the following conversion table to build the XpoLog pattern out of the access log format.

Example
The Amazon Cloudfront access log format is:

date time x-edge-location sc-bytes c-ip cs-method cs-uri-stem sc-status cs(Host) cs-uri-query cs(Cookie)
x-edge-result-type x-edge-request-id x-host-header cs-protocol cs-bytes time-taken x-forwarded-for ssl-protocol ssl-cipher
x-edge-response-result-type cs-protocol-version

In XpoLog this pattern will be translated into:

```
```

for more information see below:

Amazon Cloudfront Access Log Format Conversion Table

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
<th>XpoLog Pattern</th>
<th>XpoLog ftype</th>
</tr>
</thead>
<tbody>
<tr>
<td>date time</td>
<td>Date and time of event</td>
<td>{date:Date,yyyy-MM-dd HH:mm:ss}</td>
<td></td>
</tr>
<tr>
<td>x-edge-location</td>
<td>The edge location that served the request</td>
<td>{text:x-edge-location,ftype=x-edge-location}</td>
<td>x-edge-location</td>
</tr>
<tr>
<td>sc-bytes</td>
<td>The total number of bytes that CloudFront served to the viewer in response to the request, including headers</td>
<td>{text:sc-bytes,ftype=bytesent}</td>
<td>bytesent</td>
</tr>
<tr>
<td>c-ip</td>
<td>The IP address of the viewer that made the request</td>
<td>{text:c-ip,ftype=remoteip}</td>
<td>remoteip</td>
</tr>
<tr>
<td>cs-method</td>
<td>HTTP access method: GET, HEAD, OPTIONS, PATCH, or PUT</td>
<td>{text:cs-method,ftype=reqmethod}</td>
<td>reqmethod</td>
</tr>
<tr>
<td>cs(Host)</td>
<td>The domain name of the CloudFront distribution</td>
<td>{text:cs(Host),ftype=hostname}</td>
<td>hostname</td>
</tr>
<tr>
<td>cs-uri-stem</td>
<td>The portion of the URI that identifies the path and object</td>
<td>{text:cs-uri-stem,ftype=requrl}</td>
<td>requrl</td>
</tr>
<tr>
<td>sc-status</td>
<td>Status code or which indicates that the viewer closed the connection (for example, closed the browser tab) before CloudFront could respond to a request.</td>
<td>{text:sc-status,ftype=respstatus}</td>
<td>respstatus</td>
</tr>
<tr>
<td>cs(Referer)</td>
<td>The name of the domain that originated the request. Common referrers include search engines, other websites that link directly to your objects, and your own website</td>
<td>{text:cs(Referer),ftype=referer}</td>
<td>referer</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Type</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>cs(User-Agent)</td>
<td>The value of the User-Agent header in the request. The header identifies the source of the request, such as the type of device and browser that submitted the request and, if the request came from a search engine, which search engine</td>
<td>useragent</td>
<td></td>
</tr>
<tr>
<td>cs-uri-query</td>
<td>The query string portion of the URI, if any. When a URI doesn’t contain a query string portion, the value of cs-uri-query is a hyphen (-)</td>
<td>querystring</td>
<td></td>
</tr>
<tr>
<td>cs(Cookie)</td>
<td>The cookie header in the request, including name-value pairs and the associated attributes. If you enable cookie logging, CloudFront logs the cookies in all requests regardless of which cookies you choose to forward to the origin: none, all, or a whitelist of cookie names. When a request doesn’t include a cookie header, the value of cs(Cookie) is a hyphen (-)</td>
<td>cookie</td>
<td></td>
</tr>
<tr>
<td>x-edge-result-type</td>
<td>How CloudFront classified the response after the last byte left the edge location</td>
<td>x-edge-result-type</td>
<td></td>
</tr>
<tr>
<td>x-edge-request-id</td>
<td>An encrypted string that uniquely identifies a request</td>
<td>x-edge-request-id</td>
<td></td>
</tr>
<tr>
<td>x-host-header</td>
<td>The value that the viewer included in the Host header for this request</td>
<td>x-host-header</td>
<td></td>
</tr>
<tr>
<td>cs-protocol</td>
<td>The protocol that the viewer specified in the request, either http or https</td>
<td>protocol</td>
<td></td>
</tr>
<tr>
<td>cs-bytes</td>
<td>The number of bytes of data that the viewer included in the request (client to server bytes), including headers</td>
<td>bytesreceived</td>
<td></td>
</tr>
<tr>
<td>time-taken</td>
<td>The number of seconds (to the thousandth of a second) between the time that a CloudFront edge server receives a viewer’s request and the time that CloudFront writes the last byte of the response to the edge server’s output queue as measured on the server</td>
<td>time-taken</td>
<td></td>
</tr>
</tbody>
</table>
x-forwarded-for
If the viewer used an HTTP proxy or a load balancer to send the request, the value of c-ip in field 5 is the IP address of the proxy or load balancer. In that case, x-forwarded-for is the IP address of the viewer that originated the request.

ssl-protocol
When cs-protocol in field 17 is https, the SSL protocol that the client and CloudFront negotiated for transmitting the request. When cs-protocol is http, the value for ssl-protocol is a hyphen (-).

ssl-cipher
When cs-protocol in field 17 is https, the SSL cipher that the client and CloudFront negotiated for encrypting the request. When cs-protocol is http, the value for ssl-cipher is a hyphen (-).

x-edge-response-result-type
How CloudFront classified the response just before returning the response to the viewer.

cs-protocol-version
the HTTP version that the viewer specified in the request.

Amazon ELB

Background
Built in Amazon Elastic load balancer dashboards and consoles to gain deep-level insights on your global content delivery network all across your cloud AMIs at once.

Steps

1. Add Log Data In XpoLog. When adding a log to XpoLog you can now set a Log Type (logtype). For Amazon Cloudfront set the following logtypes:
   a. AWS
   b. ELB

2. The Cloudfront access log usually is placed in a S3 bucket with the name structure: <SITE_ID>.<DATE>-<UNIQUE_ID>.gz - in XpoLog it should be represented as {string}.{date,yyyy-MM-dd}-{string}.gz
   It is required to configure a S3 account for XpoLog to connect and read the required data from the S3 bucket.

3. Once all required information is set click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Amazon Cloudfront App. Use the following conversion table to build the XpoLog pattern out of the access log format.

Example
The Amazon Cloudfront access log format is:

date time x-edge-location sc-bytes c-ip cs-method cs(Host) cs-uri-stem sc-status cs(Referer) cs(User-Agent) cs-uri-query cs(Cookie)
In XpoLog this pattern will be translated into:

```
```

for more information see below:

Amazon Cloudfront Access Log Format Conversion Table

logtype should be set to: AWS, Cloudfront

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
<th>XpoLog Pattern</th>
<th>XpoLog ftype</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>The type of request or connection. The possible values are as follows: HTTP, HTTP over SSL/TLS, HTTP/2 over SSL/TLS, WebSockets, WebSockets over SSL/TLS. Ignore any other values.</td>
<td>{date:Date,yyyy-MM-dd HH:mm:ss}</td>
<td>x-edge-location</td>
</tr>
<tr>
<td>timestamp</td>
<td>The time when the load balancer received the request from the client, in ISO 8601 format. For WebSockets, this is the time when the connection is closed.</td>
<td>{text:x-edge-location,ftype=x-edge-location}</td>
<td>x-edge-location</td>
</tr>
<tr>
<td>elb</td>
<td>The resource ID of the load balancer. If you are parsing access log entries, note that resources IDs can contain forward slashes (/).</td>
<td>{text:sc-bytes,ftype=bytesent}</td>
<td>bytesent</td>
</tr>
<tr>
<td>client:port</td>
<td>The IP address and port of the requesting client.</td>
<td>{text:c-ip,ftype=remoteip}</td>
<td>remoteip</td>
</tr>
<tr>
<td>target:port</td>
<td>The IP address and port of the target that processed this request. If the client didn't send a full request, the load balancer can't dispatch the request to a target, and this value is set to -1.</td>
<td>{text:cs-method,ftype=reqmethod}</td>
<td>reqmethod</td>
</tr>
<tr>
<td>request_processing_time</td>
<td>The total time elapsed, in seconds, from the time the load balancer received the request until the time it sent to a target. This value is set to -1 if the load balancer can't dispatch the request to a target.</td>
<td>{text:cs(Host),ftype=hostname}</td>
<td>hostname</td>
</tr>
<tr>
<td>target_processing_time</td>
<td>The total time elapsed, in seconds, from the time the load balancer sent the request to a target until the target started to send the response headers. This value is set to -1 if the load balancer can't dispatch the request to a target.</td>
<td>{text:cs-uri-stem,ftype=requrl}</td>
<td>requrl</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Type</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td></td>
</tr>
<tr>
<td>response_processing_time</td>
<td>The total time elapsed (in seconds) from the time the load balancer received the response header from the target until it started to send the response to the client. This includes both the queuing time at the load balancer and the connection acquisition time from the load balancer to the target. This value is set to (-1) if the load balancer can't send the request to a target. This can happen if the target closes the connection before the idle timeout or if the client sends a malformed request.</td>
<td>[text:sc-status,fctype=respstatus] respstatus</td>
<td></td>
</tr>
<tr>
<td>elb_status_code</td>
<td>The status code of the response from the load balancer.</td>
<td>[text:cs(Referer),fctype=referer] referer</td>
<td></td>
</tr>
<tr>
<td>target_status_code</td>
<td>The status code of the response from the target. This value is recorded only if a connection was established to the target and the request was sent to the target. The value is set to (-1) if the target does not send a response. Otherwise, the value is set to the target's status code.</td>
<td>[text:cs(User-Agent),fctype=useragent] useragent</td>
<td></td>
</tr>
<tr>
<td>received_bytes</td>
<td>The size of the request, in bytes, received from the client (requester). For HTTP requests, this includes the headers. For WebSockets, this is the total number of bytes received from the client on the connection.</td>
<td>[text:cs-uri-query,fctype=querystring] querystring</td>
<td></td>
</tr>
<tr>
<td>sent_bytes</td>
<td>The size of the response, in bytes, sent to the client (requester). For HTTP requests, this includes the headers. For WebSockets, this is the total number of bytes sent to the client on the connection.</td>
<td>[text:cs(Cookie),fctype=cookie] cookie</td>
<td></td>
</tr>
<tr>
<td>request</td>
<td>The request line from the client enclosed in double quotes and logged using the following format: HTTP method + protocol://host:port/uri + HTTP version.</td>
<td>[text:x-edge-result-type,fctype=x-edge-result-type] x-edge-result-type</td>
<td></td>
</tr>
<tr>
<td>user_agent</td>
<td>A User-Agent string that identifies the client that originated the request. The string consists of one or more product identifiers, product[/version]. If the string is longer than 8 KB, it is truncated.</td>
<td>[text:x-edge-request-id,fctype=x-edge-request-id] x-edge-request-id</td>
<td></td>
</tr>
<tr>
<td>ssl_cipher</td>
<td>[HTTPS listener] The SSL cipher. This value is recorded only if the incoming connection was established after a successful negotiation. Otherwise, the value is set to (-1).</td>
<td>[text:x-host-header,fctype=x-host-header] x-host-header</td>
<td></td>
</tr>
<tr>
<td>ssl_protocol</td>
<td>[HTTPS listener] The SSL protocol. This value is recorded only if the incoming connection was established after a successful negotiation. Otherwise, the value is set to (-1).</td>
<td>[text:cs-protocol,fctype=protocol] protocol</td>
<td></td>
</tr>
<tr>
<td>target_group_arn</td>
<td>The Amazon Resource Name (ARN) of the target group.</td>
<td>[text:cs-bytes,fctype=bytesreceived] bytesreceived</td>
<td></td>
</tr>
<tr>
<td>trace_id</td>
<td>The contents of the X-Amzn-Trace-Id header.</td>
<td>[text:time-taken,fctype=time-taken] time-taken</td>
<td></td>
</tr>
</tbody>
</table>

Amazon Linux AMI

Background

The AWS Linux AMI Servers logs analysis App automatically Collect - Read - Parse - Analyzes - Reports all machine generated log data of the server and presents a comprehensive set of graphs and reports to analyze machine generated data. Use a predefined set of dashboards and gadgets to visualize and address the system software, code written, and infrastructure during development, testing, and production. This Linux logs analysis App helps measure, troubleshoot, and optimize your servers integrity, stability and quality with the several visualization and investigation dashboards.

Steps:

1. The Amazon Linux App is running on messages/syslog, auth/secure, mail, kern and cron standard logs. When adding/editing the logs to XpoLog it is mandatory to apply the correct log type(s) to each of the logs:
   a. linux - all logs that the application will analyze must have linux as a log type
   b. linux-messages/linux-syslog - only the messages/syslog logs must also be configured to have linux-messages/linux-syslog as a log type
   c. linux-auth/linux-secure - only the auth/secure logs must also be configured to have linux-auth/linux-secure as a log type
   d. linux-cron - only the cron log must also be configured to have linux-cron as a log type
   e. linux-mail - only the mail log must also be configured to have linux-mail as a log type
   f. linux-kernel - only the kern log must also be configured to have linux-kernel as a log type
2. Once the required information is set, on each log click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Linux App. Use the following patterns for each of the logs:
   a. Linux messages/syslog log:
      \{date:Date,MMM dd HH:mm:ss\} \{text:source,ftype=source\} \{text:process name,ftype=process\} \{block,emptyness=true\} \{text:pid,ftype=pid\}:
      \{text:Message,ftype=message\} \{regexp:User,ftype=user;refName=message, [passed|failed] for (\^) from\}
   b. Linux auth/secure log:
      \{date:Date,MMM dd HH:mm:ss\} \{text:Source IP,ftype=source\} \{text:Process,ftype=process\}:
      \{text:pid,ftype=pid\}:
      \{text:Message,ftype=message\}
   c. Linux cron log:
      \{date:Date,MMM dd HH:mm:ss\} \{text:Server,ftype=server\} \{text:Process,ftype=process\}:
      \{text:pid,ftype=pid\}:
      \{text:Message,ftype=message\}
   d. Linux mail log:
      \{date:Date,MMM dd HH:mm:ss\} \{text:source\} \{text:process name,ftype=process\}:
      \{number:process id\}:
      \{text:Message,ftype=message\} \{regexp:session,refName=Message;ftype=session,^\w+:\}
      \{regexp:From,refName=Message;ftype=from,\s+from=(\[^,]+)\}
      \{regexp:To,refName=Message;ftype=to,\s+to=(\[^,]+)\}
      \{text:Message,ftype=message\}
   e. Linux kernel log:

Amazon S3

Background

Built in Amazon S3 dashboards and consoles to gain deep-level insights on your Elastic Load Balancer all across your cloud AMIs at once. DBAs, IT Admins, Sys Admins and DevOps – with rich premium visualizations like dashboards, gadgets and consoles XpoLog S3 features.

Steps

1. Add Log Data In XpoLog, When adding a log to XpoLog you can now set a Log Type (logtype). For AWS S3 set the following logtypes:
   a. AWS
   b. S3
   c. access
   d. w3c
   e. httpd
2. The S3 access log usually is placed in a bucket with the name structure: <Bucket>.<DATE>-<UNIQUE_ID>.gz - in XpoLog it should be represented as \{string\}.\{date,yyyy-MM-dd\}-\{string\}.gz
   It is required to configure a S3 account for XpoLog to connect and read the required data from the S3 bucket.
3. Once all required information is set click next and edit the log pattern, this step is crucial to the accuracy and deployment of the AWS S3 App. Use the following conversion table to build the XpoLog pattern out of the access log format.

Example

The AWS S3 access log format is:

```
bucket-owner bucket date-time remote-ip requester requester-id operation key request-uri http-status error-code bytes-sent object-size total-time turn-around-time referrer user-agnet version-id
```

In XpoLog this pattern will be translated into:

```
{text:Bucket Owner} \{text:Bucket,ftype=bucket;\} \{[date:Time,dd/MM/yyyy:HH:mm:ss z]} \{geoip:Remote IP,ftype=remoteip;type=;\}
{text:Requester} \{text:Request ID\} \{text:Operation\} \{text:Key\} \{choice:Request-Method,ftype=reqmethod;GET;POST\}
{text:Request-URI-FULL} \{regexp:Request-URI-Subject,ftype=requrl;refName=Request-URI-FULL,XPLG_PARAM((\^\w+)+)(([\^\w+]+)\w+)+)\}
{string:Request-Protocol,ftype=reqprotocol;} \{number:HTTP status,ftype=respstatus;\} \{text:Error Code,ftype=errorcode;\} \{number:Bytes Sent,ftype=bytesent;\} \{text:Object Size,ftype=objectsize;\} \{text:Total Time,ftype=totaltime;\} \{text:Turn-Around Time,ftype=turmaroundtime;\}
\{string:Referer,ftype=referer;\} \{string:User Agent,ftype=useragent;\} \{text:Version Id\}
```

for more information see below:
## AWS S3 Access Log Format Conversion Table

Log type should be set to: AWS, S3, access, w3c, httpd

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>XpoLog Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bucket Owner</td>
<td>The canonical user ID of the owner of the source bucket</td>
<td><code>{text:Bucket Owner}</code></td>
</tr>
<tr>
<td>Bucket</td>
<td>The name of the bucket that the request was processed against. If the system receives a malformed request and cannot determine the bucket, the request will not appear in any server access log</td>
<td><code>{text:Bucket,type=bucket;}</code></td>
</tr>
<tr>
<td>Time</td>
<td>The time at which the request was received</td>
<td><code>[[date:Time,dd/MMM/yyyy:HH:mm:ss z]]</code></td>
</tr>
<tr>
<td>Remote IP</td>
<td>The apparent Internet address of the requester. Intermediate proxies and firewalls might obscure the actual address of the machine making the request</td>
<td><code>{geoip:Remote IP,type=remoteip;}</code></td>
</tr>
<tr>
<td>Requester</td>
<td>The canonical user ID of the requester, or the string &quot;Anonymous&quot; for unauthenticated requests. If the requester was an IAM user, this field will return the requester’s IAM user name along with the AWS root account that the IAM user belongs to. This identifier is the same one used for access control purposes</td>
<td><code>{text:Requester}</code></td>
</tr>
<tr>
<td>Request ID</td>
<td>The request ID is a string generated by Amazon S3 to uniquely identify each request</td>
<td><code>{text:Request ID}</code></td>
</tr>
<tr>
<td>Operation</td>
<td>The operation listed here is declared as SOAP.operation, HTTP resource_type, or BATCH.DELETE.OBJECT.</td>
<td><code>{text:Operation}</code></td>
</tr>
<tr>
<td>Key</td>
<td>The &quot;key&quot; part of the request, URL encoded, or &quot;.&quot; if the operation does not take a key parameter.</td>
<td><code>{text:Key}</code></td>
</tr>
<tr>
<td>Request Method</td>
<td>HTTP request method name</td>
<td><code>{choice:Request-Method,type=reqmethod;,GET;POST}</code></td>
</tr>
<tr>
<td>Request-URI-Full</td>
<td>The full Request-URI part of the HTTP request message</td>
<td><code>{text:Request-URI-FULL}</code></td>
</tr>
<tr>
<td>Request-URI-Subject</td>
<td>The subject extracted from the URI (e.g. folder name of the file requested)</td>
<td>`{regexp:Request-URI-Subject,type=requrl;refName=Request-URI-FULL,XPLG_PARAM((.*?[^=]+)</td>
</tr>
<tr>
<td>Request Protocol</td>
<td>HTTP protocol used for the request in question</td>
<td><code>{string:Request-Protocol,type=reqprotocol;}</code></td>
</tr>
<tr>
<td>HTTP Status</td>
<td>The numeric HTTP status code of the GET portion of the copy operation</td>
<td><code>{number:HTTP status,type=respstatus;}</code></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Format</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Error Code</td>
<td>The Amazon S3 Error Code, of the GET portion of the copy operation or &quot;-&quot; if no error occurred</td>
<td>text:Error Code,ftype=errorcode;</td>
</tr>
<tr>
<td>Bytes Sent</td>
<td>The number of response bytes sent, excluding HTTP protocol overhead, or &quot;-&quot; if zero</td>
<td>number:Bytes Sent,ftype=bytesent;</td>
</tr>
<tr>
<td>Object Size</td>
<td>The total size of the object in question</td>
<td>text:Object Size,ftype=objectsize;</td>
</tr>
<tr>
<td>Total Time</td>
<td>The number of milliseconds the request was in flight from the server's perspective. This value is measured from the time your request is received to the time that the last byte of the response is sent. Measurements made from the client's perspective might be longer due to network latency</td>
<td>text:Total Time,ftype=totaltime;</td>
</tr>
<tr>
<td>Turn-Around Time</td>
<td>The number of milliseconds that Amazon S3 spent processing your request. This value is measured from the time the last byte of your request was received until the time the first byte of the response was sent</td>
<td>text:Turn-Around Time,ftype=turnaroundtime;</td>
</tr>
<tr>
<td>Referrer</td>
<td>The value of the HTTP Referrer header, if present. HTTP user-agents (e.g. browsers) typically set this header to the URL of the linking or embedding page when making a request</td>
<td>string:Referer,ftype=referer;</td>
</tr>
<tr>
<td>User-Agent</td>
<td>The value of the HTTP User-Agent header</td>
<td>string:User Agent,ftype=useragent;</td>
</tr>
<tr>
<td>Version ID</td>
<td>The version ID of the object being copied or &quot;-&quot; if the x-amz-copy-source header didn't specify a versionId parameter as part of the copy source</td>
<td>text:Version Id</td>
</tr>
</tbody>
</table>

**Background**

Apache HTTPD Log Analysis App is an Http server for Windows and Unix machines that automatically Collect - Read - Parse - Analyzes - Reports all machine generated log data of the server and presents a comprehensive automatic predefined set of Reports, Dashboards and Gadgets. Once you Setup and configure the Apache HTTPD App, you will be redirected to the dashboards where you will have graphs about: errors occurred, geographic data of users and requests, Browsers related analytics, Pages and hits analysis, resources and many statistics about your servers’ performance. You later use XpoLog built in Analytics features to zero in on errors and take actions to improve your system’s uptime. Apache HTTP server logs data can be viewed, filtered and searched via the main XpoLog console.

**Steps**

1. Add Log Data In XpoLog. When adding a log to XpoLog you can now select the Log Type (logtype) for Apache Httpd the are the following logtypes:
   a. httpd
   i. in addition select not only httpd but also the log type - access or error
2. Once all required information is set click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Apache Httpd App. Use the following conversion table to build the XpoLog pattern out of the access log format.

**Example**

In the Apache Httpd configuration file, usually httpd.conf by default, located under the conf/ directory (Linux "/etc/httpd/conf") search for the LogFormat directive:

```plaintext
LogFormat "%a %l %u %t "%r" %>s %b %D "%{Referer}i" "%{User-Agent}i"" combined
```
The following sequence is the log structure definition for the Httpd server:%

%a %l %u %t "%r" %>s %b %D "%{Referer}i" "%{User-Agent}i"

In XpoLog such pattern will be translated into:

```plaintext
{geoip:Client IP,ftype=remoteip:type=;}
{string:Remote Log Name,ftype=remotelog;}
[{date:Date,locale=en,dd/MM/yyyy:HH:mm:ss z}]
{choice:Method,ftype=reqmethod;,GET;POST}
{string:URL,ftype=requrl;}
{block,start,emptiness=true}?{string:Query,ftype=querystring;}
{string:reqprotocol,ftype=reqprotocol;}
{number:Status,ftype=respstatus;}
{number:BytesSent,ftype=bytesent;}
{number:TimeToProcessRequest,ftype=processrequestmilli;}
{string:Referer,ftype=referer;}
{string:UserAgent,ftype=useragent;}
```

for more information see below:

Apache Https Access Log Format Conversion Table

<table>
<thead>
<tr>
<th>Format String</th>
<th>Description</th>
<th>XpoLog Pattern</th>
<th>XpoLog ftype</th>
</tr>
</thead>
<tbody>
<tr>
<td>%a</td>
<td>Remote IP-address</td>
<td>{ip:RemoteIP,ftype=remoteip}</td>
<td>remoteip</td>
</tr>
<tr>
<td>%A</td>
<td>Local IP-address</td>
<td>{ip:LocalIP,ftype=localip}</td>
<td>localip</td>
</tr>
<tr>
<td>%b</td>
<td>Size of response in bytes, excluding HTTP headers.</td>
<td>{number:BytesSent,ftype=bytesent}</td>
<td>bytesent</td>
</tr>
<tr>
<td>%B</td>
<td>Size of response in bytes, excluding HTTP headers.</td>
<td>{text:BytesSent,ftype=bytesent}</td>
<td>bytesent</td>
</tr>
<tr>
<td>%{Foobar}C</td>
<td>The contents of cookie Foobar in the request sent to the server. Only version 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>cookies are fully supported.</td>
<td>{string:Cookie_&lt;FOOBAR&gt;}</td>
<td></td>
</tr>
<tr>
<td>%D</td>
<td>The time taken to serve the request, in micro-seconds.</td>
<td>{number:ResponseTimeMillis}</td>
<td></td>
</tr>
<tr>
<td>%{FOOBAR}e</td>
<td>The contents of the environment variable FOOBAR</td>
<td>{string:EnvVariable_&lt;FOOBAR&gt;}</td>
<td></td>
</tr>
<tr>
<td>%f</td>
<td>Filename</td>
<td>{text:FileName}</td>
<td></td>
</tr>
<tr>
<td>%h</td>
<td>Remote host</td>
<td>{text:Remotehost,ftype=remotehost}</td>
<td>remotestart</td>
</tr>
<tr>
<td>%H</td>
<td>The request protocol</td>
<td>{text:RequestProtocol,ftype=reqprotocol}</td>
<td>reqprotocol</td>
</tr>
<tr>
<td>%{Foobar}i</td>
<td>The contents of Foobar: header line(s) in the request sent to the server.</td>
<td>{text:&lt;FOOBAR&gt;}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Changes made by other modules (e.g. mod_headers)</td>
<td><a href="https://en.wikipedia.org/wiki/List_of_HTTP_header_fields">https://en.wikipedia.org/wiki/List_of_HTTP_header_fields</a> and so on it goes for the different headers.</td>
<td></td>
</tr>
<tr>
<td>%{Referer}i</td>
<td>[text:Referer,ftype=referer]</td>
<td></td>
<td>referer</td>
</tr>
<tr>
<td>%{User-agent}i</td>
<td>[text:User-agent,ftype=useragent]</td>
<td></td>
<td>useragent</td>
</tr>
<tr>
<td>%{X-Forwarded-For}i</td>
<td>[text: X-Forwarded-For,ftype=forwardforip] OR</td>
<td></td>
<td>forwardforip</td>
</tr>
<tr>
<td>%-k</td>
<td>Number of keepalive requests handled on this connection. Interesting if KeepAlive is being used, so that, for example, a '1' means the first keepalive request after the initial one, '2' the second, etc...; otherwise this is always 0 (indicating the initial request). Available in versions 2.2.11 and later.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%l</td>
<td>Remote logname (from identd, if supplied). This will return a dash unless mod_ident is present and IdentityCheck is set on.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%-m</td>
<td>The request method</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%Foobar-n</td>
<td>The contents of note Foobar from another module.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%Foobar-o</td>
<td>The contents of Foobar header line(s) in the reply.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%-p</td>
<td>The canonical port of the server serving the request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%format-p</td>
<td>The canonical port of the server serving the request or the server's actual port or the client's actual port. Valid formats are canonical, local, or remote.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%{format}p</td>
<td>The canonical port of the server serving the request or the server's actual port or the client's actual port. Valid formats are canonical, local, or remote.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%-P</td>
<td>The process ID of the child that serviced the request.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%format-P</td>
<td>The process ID or thread id of the child that serviced the request. Valid formats are pid, tid, and hextid. hextid requires APR 1.2.0 or higher.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%-q</td>
<td>The query string (prepended with a ? if a query string exists, otherwise an empty string)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%-r</td>
<td>First line of request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%-R</td>
<td>The handler generating the response (if any).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%-s</td>
<td>Status. For requests that got internally redirected, this is the status of the &quot;original&quot; request --- %&gt;s for the last.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%-t</td>
<td>Time the request was received (standard English format)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
\%t The time, in the form given by format, which should be in an extended `strftime(3)` format (potentially localized). If the format starts with `begin:` (default) the time is taken at the beginning of the request processing. If it starts with `end:` it is the time when the log entry gets written, close to the end of the request processing. In addition to the formats supported by `strftime(3)`, the following format tokens are supported:

<table>
<thead>
<tr>
<th>Format Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sec</td>
<td>Number of seconds since the Epoch</td>
</tr>
<tr>
<td>msec</td>
<td>Number of milliseconds since the Epoch</td>
</tr>
<tr>
<td>usec</td>
<td>Number of microseconds since the Epoch</td>
</tr>
<tr>
<td>msec_frac</td>
<td>Millisecond fraction</td>
</tr>
<tr>
<td>usec_frac</td>
<td>Microsecond fraction</td>
</tr>
</tbody>
</table>

These tokens can not be combined with each other or `strftime(3)` formatting in the same format string. You can use multiple %t tokens instead.

The extended `strftime(3)` tokens are available in 2.2.30 and later.

\%T The time taken to serve the request, in seconds.

\%(UNIT)T The time taken to serve the request, in a time unit given by UNIT. Valid units are ms for milliseconds, us for microseconds, and s for seconds. Using \%s gives the same result as \%T without any format; using \%d gives the same result as \%D. Combining \%T with a unit is available in 2.2.30 and later.

\%u Remote user (from auth; may be bogus if return status (\%s) is 401)

\%U The URL path requested, not including any query string.

\%V The server name according to the `UseCanonicalName` setting.

\%X Connection status when response is completed:

\x = connection aborted before the response completed.
\+ = connection may be kept alive after the response is sent.
\- = connection will be closed after the response is sent.

(This directive was used in late versions of Apache 1.3, but this conflicted with the historical `ssl` \%c syntax.)
Bytes received, including request and headers, cannot be zero. You need to enable `mod_logio` to use this.

Bytes sent, including headers, cannot be zero. You need to enable `mod_logio` to use this.

The contents of `VARNAME`: trailer line(s) in the request sent to the server.

The contents of `VARNAME`: trailer line(s) in the response sent from the server.

Apache log4j (Ver 1.2)

Background

The Log4j Analysis App presents a predefined set of dashboards and gadgets visualizing log4j logs. The Log4j analysis pack addresses the need to manage and debug Java applications and infrastructure during development, testing, and production. The App helps measure, troubleshoot, and optimize Java based applications with visualization and investigation dashboards.

Steps

1. Add Log Data In XpoLog, When adding a log to XpoLog you can now select the Log Type (logtype) for Apache log4j the are the following logtypes:
   a. `log4j`

2. Once all required information is set click next and edit the log pattern, this step is crucial to the accuracy and deployment of the App. Use the following conversion table to build the XpoLog pattern out of the log4j log format.

Example

In the Apache Log4J configuration file, can be either properties files, XML file, or in some case the log format was created programmatically for which you can manually create the pattern for the data.

```
```

The following sequence is the log structure definition for the log4j log `[%d] [%t] [%p] [%c] [%l] %m%n`

In XpoLog such pattern will be translated into:

for more information see below:

```
[[date:Date,locale=en,yyyy-MM-dd HH:mm:ss,SSS]] [[text:Thread,ftype=thread]]
[[priority:Priority,ftype=severity,:DEBUG;INFO;WARNING;ERROR;FATAL]] [[string:Class,ftype=class]]
[[string:Method,ftype=method]]((text:Source,ftype=sourcecode);{number:LineNumber,ftype=linenumber});{text:Message,ftype=message}
```

Apache Log4j Conversion Table

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%c</code></td>
<td>Used to output the category of the logging event. The category conversion specifier can be optionally followed by precision specifier, that is a decimal constant in brackets. If a precision specifier is given, then only the corresponding number of right most components of the category name will be printed. By default the category name is printed in full. For example, for the category name &quot;a.b.c&quot; the pattern <code>%c(2)</code> will output “b.c”.</td>
</tr>
<tr>
<td><code>{text:Class,ftype=class}</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%l</code></td>
<td></td>
</tr>
<tr>
<td>Conversion Specifier</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>%C</td>
<td>Used to output the fully qualified class name of the caller issuing the logging request. This conversion specifier can be optionally followed by a precision specifier. That is a decimal constant in brackets. If a precision specifier is given, then only the corresponding number of rightmost components of the class name will be printed. By default the class name is output in fully qualified form. For example, for the class name &quot;org.apache.xyz.SomeClass&quot;, the pattern %C{1} will output &quot;SomeClass&quot;.</td>
</tr>
<tr>
<td>%d</td>
<td>Used to output the date of the logging event. The date conversion specifier may be followed by a date format specifier enclosed between braces. For example, %d{HH:mm:ss,SSS} or %d{MMM yyyy HH:mm:ss,SSS}. If no date format specifier is given then ISO8601 format is assumed. The date format specifier admits the same syntax as the time pattern string of the SimpleDateFormat. Although part of the standard JDK, the performance of SimpleDateFormat is quite poor. For better results it is recommended to use the log4j date formatters. These can be specified using one of the strings &quot;ABSOLUTE&quot;, &quot;DATE&quot; and &quot;ISO8601&quot; for specifying AbsoluteTimeDateFormat, DateTimeDateFormat and ISO8601DateFormat. For example, %d{ISO8601} or %d(ABSOLUTE). These dedicated date formatters perform significantly better than SimpleDateFormat.</td>
</tr>
<tr>
<td>%f</td>
<td>Used to output the file name where the logging request was issued. Generating caller location information is extremely slow and should be avoided unless execution speed is not an issue.</td>
</tr>
<tr>
<td>%I</td>
<td>Used to output location information of the caller which generated the logging event. The location information depends on the JVM implementation but usually consists of the fully qualified name of the calling method followed by the callers source file name and line number between parentheses. The location information can be very useful. However, its generation is extremely slow and should be avoided unless execution speed is not an issue.</td>
</tr>
<tr>
<td>%l</td>
<td>Used to output the line number from where the logging request was issued. Generating caller location information is extremely slow and should be avoided unless execution speed is not an issue.</td>
</tr>
<tr>
<td>%m</td>
<td>Used to output the application supplied message associated with the logging event.</td>
</tr>
<tr>
<td>%M</td>
<td>Used to output the method name where the logging request was issued. Generating caller location information is extremely slow and should be avoided unless execution speed is not an issue.</td>
</tr>
<tr>
<td>Conversion Character</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>%n</td>
<td>Outputs the platform dependent line separator character or characters.</td>
</tr>
<tr>
<td></td>
<td>This conversion character offers practically the same performance as using</td>
</tr>
<tr>
<td></td>
<td>non-portable line separator strings such as &quot;\n&quot;, or &quot;\r\n&quot;. Thus, it is</td>
</tr>
<tr>
<td></td>
<td>the preferred way of specifying a line separator.</td>
</tr>
<tr>
<td>%p</td>
<td>Used to output the priority of the logging event.</td>
</tr>
<tr>
<td>%r</td>
<td>Used to output the number of milliseconds elapsed from the construction of</td>
</tr>
<tr>
<td></td>
<td>the layout until the creation of the logging event.</td>
</tr>
<tr>
<td>%t</td>
<td>Used to output the name of the thread that generated the logging event.</td>
</tr>
<tr>
<td>x</td>
<td>Used to output the NDC (nested diagnostic context) associated with the</td>
</tr>
<tr>
<td></td>
<td>thread that generated the logging event.</td>
</tr>
<tr>
<td>X</td>
<td>Used to output the MDC (mapped diagnostic context) associated with the</td>
</tr>
<tr>
<td></td>
<td>thread that generated the logging event.</td>
</tr>
<tr>
<td></td>
<td>The X conversion character must be followed by the key for the map placed</td>
</tr>
<tr>
<td></td>
<td>between braces, as in %X{clientNumber} where clientNumber is the key.</td>
</tr>
<tr>
<td></td>
<td>The value in the MDC corresponding to the key will be output.</td>
</tr>
<tr>
<td></td>
<td>See MDC class for more details.</td>
</tr>
<tr>
<td>%</td>
<td>The sequence %% outputs a single percent sign.</td>
</tr>
</tbody>
</table>

### Apache Log4j (Ver 2)

**Background**

The Log4j Analysis App presents a predefined set of dashboards and gadgets visualizing log4j logs. The Log4j analysis pack addresses the need to manage and debug Java applications and infrastructure during development, testing, and production. The App helps measure, troubleshoot, and optimize Java based applications with visualization and investigation dashboards.

**Steps**

1. **Add Log Data In XpoLog.** When adding a log to XpoLog you can now select the Log Type (logtype) for Apache log4j the are the following logtypes:
   a. **log4j**
2. Once all required information is set click next and edit the log pattern, this step is crucial to the accuracy and deployment of the App. Use the following conversion table to build the XpoLog pattern out of the log4j log format.

**Example**

In the Apache Log4J configuration file, can be either properties files, XML file, or in some case the log format was created programatically for which you can manually create the pattern for the data.

```log4j
```

The following sequence is the log structure definition for the log4j log
```
[\{date:Date,locale=en,yyyy-MM-dd HH:mm:ss,SSS\} [\{text:Thread,ftype=thread\}]
[\{priority:Priority,ftype=severity:,DEBUG;INFO;WARNING;ERROR;FATAL\} [\{string:Class,ftype=class\}]
[\{string:Method,ftype=method\}({\{text:Source,ftype=sourcecode}}:${\{number:LineNumber,ftype=linenumber\}})]
[\{string:Message,ftype=message\}]
```

Apache Log4j Conversion Table

logtype should be set to: **log4j**
<table>
<thead>
<tr>
<th>Name and Appears with</th>
<th>Description</th>
<th>XpoLog Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>%c{precision} %logger{precision}</td>
<td>Outputs the name of the logger that published the logging event. The logger conversion specifier can be optionally followed by a precision specifier, which consists of a decimal integer, or a pattern starting with a decimal integer. If a precision specifier is given and it is an integer value, then only the corresponding number of right most components of the logger name will be printed. If the precision contains other non-integer characters then the name will be abbreviated based on the pattern. If the precision integer is less than one the right-most token will still be printed in full. By default the logger name is printed in full.</td>
<td>{text:Logger,ftype=logger}</td>
</tr>
<tr>
<td>%C{precision} %class{precision}</td>
<td>Outputs the fully qualified class name of the caller issuing the logging request. This conversion specifier can be optionally followed by a precision specifier, that follows the same rules as the logger name converter. Generating the class name of the caller (location information) is an expensive operation and may impact performance. Use with caution.</td>
<td>{text:Class,ftype=class}</td>
</tr>
</tbody>
</table>
| %d{pattern} %date{pattern} | Outputs the date of the logging event. The date conversion specifier may be followed by a set of braces containing a date and time pattern string per SimpleDateFormat. The predefined formats are DEFAULT, ABSOLUTE, COMPACT, DATE, ISO8601, and ISO8601_BASIC. You can also use a set of braces containing a time zone id per java.util.TimeZone.getTimeZone. If no date format specifier is given then ISO8601 format is assumed. %d(UNIX) outputs the Unix time in seconds. %d(UNIX_MILLIS) outputs the UNIX time in milliseconds. The UNIX time is the difference, in seconds for UNIX and in milliseconds for UNIX_MILLIS, between the current time and midnight, January 1, 1970 UTC. While the time unit is milliseconds, the granularity depends on the operating system (Windows). This is an efficient way to output the event time because only a conversion from long to String takes place, there is no Date formatting involved. | {date:Date,<DATE_PATTERN>}
  (date:Date,locale=<?>,yyyyMMdd-HHmm:ss,SSS)
  Note: (use default locale)
  (date:Date,locale=<?>,<same pattern>)
  (date:Date,locale=<?>,yyyyMMdd-HHmm:ss,SSS)
  Note: (use default locale)
  Create the relevant date pattern for each option or use the pattern: Outputs the date of the logging event. The date conversion specifier may be followed by a set of braces containing a date and time pattern string per SimpleDateFormat. The predefined formats are DEFAULT, ABSOLUTE, COMPACT, DATE, ISO8601, and ISO8601_BASIC. You can also use a set of braces containing a time zone id per java.util.TimeZone.getTimeZone. If no date format specifier is given then ISO8601 format is assumed. |  |

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>%d(DEFAULT)</td>
<td>2012-11-02 14</td>
</tr>
<tr>
<td>%d(ISO8601)</td>
<td>2012-11-02T14</td>
</tr>
<tr>
<td>%d(ISO8601_BASIC)</td>
<td>20121102T1415:30:45</td>
</tr>
<tr>
<td>%d(Absolute)</td>
<td>14:34:02,781</td>
</tr>
<tr>
<td>%d(DATE)</td>
<td>02 Nov 2012 1</td>
</tr>
<tr>
<td>%d(COMPACT)</td>
<td>20121102143:45</td>
</tr>
<tr>
<td>%d(HHmm:ss,SSS)</td>
<td>14:34:02,781</td>
</tr>
<tr>
<td>%d(dd MMM yyyy HH:mm:ss,SSS)</td>
<td>02 Nov 2012 1</td>
</tr>
<tr>
<td>%d(HHmm:ss)GMT+0)</td>
<td>18:34:02</td>
</tr>
<tr>
<td>%d(UNIX)</td>
<td>1351866842</td>
</tr>
<tr>
<td>%d(UNIX_MILLIS)</td>
<td>13518668427</td>
</tr>
<tr>
<td>%d(UNIX)</td>
<td>Outputs the UNIX time in seconds. %d(UNIX_MILLIS) outputs the UNIX time in milliseconds. The UNIX time is the difference, in seconds for UNIX and in milliseconds for UNIX_MILLIS, between the current time and midnight, January 1, 1970 UTC. While the time unit is milliseconds, the granularity depends on the operating system (Windows). This is an efficient way to output the event time because only a conversion from long to String takes place, there is no Date formatting involved.</td>
</tr>
</tbody>
</table>
| %enc{pattern} | Escape newlines and HTML special characters in the specified pattern. | Create pattern according to the relevant encoding:
%enc[%m] = {string:Message,ftype=message}
%enc[%mdc{key}] = (string:Key) |
| %ex|exception|throwable | Outputs the Throwable trace bound to the LoggingEvent, by default this will output the full trace as one would normally find with a call to Throwable.printStackTrace().
You can follow the throwable conversion word with an option in the form %throwable(option).
%throwable[short] outputs the first line of the Throwable.
%throwable[short.className] outputs the name of the class where the exception occurred.
%throwable[short.methodName] outputs the method name where the exception occurred.
%throwable[short.fileName] outputs the name of the class where the exception occurred.
%throwable[short.lineNumber] outputs the line number where the exception occurred.
%throwable[short.message] outputs the message.
%throwable[short.localizedMessage] outputs the localized message.
%throwable[n] outputs the first n lines of the stack trace. Specifying %throwable(none) or %throwable(0) suppresses output of the exception. | {string:Throwable,ftype=throwable} |
<p>| %F | Outputs the file name where the logging request was issued | {text:Class,ftype=class} |
| %highlight{pattern}{style} | Adds ANSI colors to the result of the enclosed pattern based on the current event's logging level. | N/A |
| %K{key} | Outputs the entries in a MapMessage, if one is present in the event. The K conversion character can be followed by the key for the map placed between braces, as in %K{clientNumber} where clientNumber is the key. The value in the Map corresponding to the key will be output. If no additional sub-option is specified, then the entire contents of the Map key value pair set is output using a format {key1,val1},{key2,val2} | {text:Key} |
| %l | Outputs location information of the caller which generated the logging event. | {text:Method,ftype=method}({text:Class,ftype=class}:{number:LineNumber,ftype=linenumber}) |
| %L | Outputs the line number from where the logging request was issued. | {number:LineNumber,ftype=linenumber} |
| %m | Outputs the application supplied message associated with the logging event. | {string:Message,ftype=message} |
| %M | Outputs the method name where the logging request was issued. | {text:Method,ftype=method} |
| %marker | The name of the marker, if one is present. | {text:Marker,ftype=marker} |
| %n | Outputs the platform dependent line separator character or characters. | {eol} |</p>
<table>
<thead>
<tr>
<th><strong>Conversion</strong></th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%p</code></td>
<td>Outputs the level of the logging event. You provide a level name map in the form &quot;level=value, level=value&quot; where level is the name of the Level and value is the value that should be displayed instead of the name of the Level.</td>
<td>{priority:Priority, ALL; TRACE; DEBUG; INFO; WARN; ERROR; FATAL, ftype=severity}</td>
</tr>
<tr>
<td><code>%r</code></td>
<td>Outputs the number of milliseconds elapsed since the JVM was started until the creation of the logging event.</td>
<td>{number:LogSpeed, ftype=logprocesstimemilli}</td>
</tr>
<tr>
<td><code>%replace</code></td>
<td>Replaces occurrences of 'regex', a regular expression, with its replacement 'substitution' in the string resulting from evaluation of the pattern. For example, &quot;%replace(%msg){\s}&quot; will remove all spaces contained in the event message.</td>
<td>{string:&lt;PATTERN_NAME&gt;}</td>
</tr>
<tr>
<td><code>%s</code></td>
<td>Includes a sequence number that will be incremented in every event. The counter is a static variable so will only be unique within applications that share the same converter Class object.</td>
<td>{number:SequenceNumber, ftype=sequencenumber}</td>
</tr>
<tr>
<td><code>%sn</code></td>
<td>Outputs the thread that generated the logging event.</td>
<td>{text:Thread, ftype=thread}</td>
</tr>
<tr>
<td><code>%t</code></td>
<td>Outputs the Thread Context Stack (also known as the Nested Diagnostic Context or NDC) associated with the thread that generated the logging event.</td>
<td>{string:NDC}</td>
</tr>
<tr>
<td><code>%X</code></td>
<td>Outputs the Thread Context Map (also known as the Mapped Diagnostic Context or MDC) associated with the thread that generated the logging event.</td>
<td>{string:NDC.&lt;KEY&gt;}</td>
</tr>
<tr>
<td><code>%u</code></td>
<td>Includes either a random or a time-based UUID.</td>
<td>{text:UUID, ftype=uniqueid}</td>
</tr>
<tr>
<td><code>%x</code></td>
<td>The same as the %throwable conversion word but also includes class packaging information.</td>
<td>{string:NestedException, ftype=nestedexception}</td>
</tr>
</tbody>
</table>

For the example below:

```
(priority:Priority, ALL; TRACE; DEBUG; INFO; WARNING; ERROR; FATAL, ftype=severity)
```

For example:

```
%level{WARN=Warning, DEBUG=Debug, ERROR=Error, TRACE=Trace, INFO=Info}
```

Alternatively, for the compact-minded:

```
%level{WARN=W, DEBUG=D, ERROR=E, TRACE=T, INFO=I}
```

More succintly, for the same result as above, you can define the length of the level label:

```
%level{length=1}
```

If the length is greater than a level name length, the level name will be used.

You can combine the two kinds of options:

```
%level{ERROR=Error, length=2}
```

This give you the Error level name and all other level names of length 2.

Finally, you can output lower-case level names (the default is upper-case):

```
%level{lowerCase=true}
```

```
Outputs the number of milliseconds elapsed since the JVM was started until the creation of the logging event.

Replace occurrences of 'regex', a regular expression, with its replacement 'substitution' in the string resulting from evaluation of the pattern. For example, "%replace(%msg)\{\s\}" will remove all spaces contained in the event message.

The same as the %throwable conversion word but the stack trace is printed starting with the first exception that was thrown followed by each subsequent wrapping exception.

Includes a sequence number that will be incremented in every event. The counter is a static variable so will only be unique within applications that share the same converter Class object.

Outputs the thread that generated the logging event.

Outputs the Nested Diagnostic Context or NDC associated with the thread that generated the logging event.

Outputs the Mapped Diagnostic Context or MDC associated with the thread that generated the logging event.

Includes either a random or a time-based UUID.

The same as the %throwable conversion word but also includes class packaging information.

Include package information.
Apache Log4Net (Ver 2.0)

Background
The Apache Log4net Analysis App presents a predefined set of dashboards and gadgets visualizing Log4net logs. The Log4net analysis pack addresses the need to manage and debug Apache Log4net applications and infrastructure during development, testing, and production. This App helps measure, troubleshoot, and optimize Java based applications with visualization and investigation dashboards.

Steps
1. Add Log Data In XpoLog, When adding a log to XpoLog you can now select the Log Type (logtype) for Apache log4net with the following logtype:
   a. log4net
2. Once all required information is set click next and edit the log pattern, this step is crucial to the accuracy and deployment of the App. Use the following conversion table to build the XpoLog pattern out of the log4net log format.

Example
In the Apache Log4Net configuration file, can be either properties files, XML file, or in some case the log format was created pro-grammatically for which you can manually create the pattern for the data.

```xml
<appender name="A1" type="log4net.Appender.ConsoleAppender">
    <!-- A1 uses PatternLayout -->
    <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%timestamp \[%thread\] %-5level %logger %ndc - %message%newline" />
    </layout>
</appender>
```

The following sequence is the log structure definition for the log4net log `%timestamp \[%thread\] %-5level %logger %ndc - %message%newline` In XpoLog such pattern will be translated into:

for more information see below:

```
{date:Date,locale=en,yyyy-MM-dd HH:mm:ss,SSS} [{text:Thread,ftype=thread}]
{[priority:Priority,ftype=severity;,DEBUG;INFO;WARNING;ERROR;FATAL} {string:Logger,ftype=logger} {string:NDC,ftype=ndc} - {string:Message,ftype=message}
```

Apache Log4Net Conversion Table

<table>
<thead>
<tr>
<th>Name and Appears with</th>
<th>Description</th>
<th>XpoLog Pattern</th>
<th>ftype</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Equivalent to appdomain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>appdomain</td>
<td>Used to output the friendly name of the AppDomain where the logging event was generated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aspnet-cache</td>
<td>Used to output all cache items in the case of %aspnet-cache or just one named item if used as %aspnet-cache(key)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This pattern is not available for Compact Framework or Client Profile assemblies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aspnet-context</td>
<td>Used to output all context items in the case of %aspnet-context or just one named item if used as %aspnet-context(key)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This pattern is not available for Compact Framework or Client Profile assemblies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aspnet-request</td>
<td>Used to output all request parameters in the case of %aspnet-request or just one named param if used as %aspnet-request(key)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This pattern is not available for Compact Framework or Client Profile assemblies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aspnet-session</td>
<td>Used to output all session items in the case of %aspnet-session or just one named item if used as %aspnet-session(key)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This pattern is not available for Compact Framework or Client Profile assemblies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>Equivalent to logger</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Equivalent to type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pattern</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>class</td>
<td>Equivalent to type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td>Equivalent to date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date</td>
<td>Used to output the date of the logging event in the local time zone. To output the date in universal time use the <code>%utodate</code> pattern. The date conversion specifier may be followed by a date format specifier enclosed between braces. For example, <code>%date(HH:mm:ss,fff)</code> or <code>%date(dd MMM yyyy HH:mm:ss,fff)</code>. If no date format specifier is given then ISO8601 format is assumed (<code>Iso8601DateFormatter</code>). The date format specifier admits the same syntax as the time pattern string of the <code>ToString</code>. For better results it is recommended to use the log4net date formatters. These can be specified using one of the strings &quot;ABSOLUTE&quot;, &quot;DATE&quot; and &quot;ISO8601&quot; for specifying <code>AbsoluteTimeDateFormatter</code>, <code>DateTimeDateFormatter</code> and respectively <code>Iso8601DateFormatter</code>. For example, <code>%dateISO8601</code> or <code>%dateABSOLUTE</code>. These dedicated date formatters perform significantly better than <code>ToString</code>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exception</td>
<td>Used to output the exception passed in with the log message. If an exception object is stored in the logging event it will be rendered into the pattern output with a trailing newline. If there is no exception then nothing will be output and no trailing newline will be appended. It is typical to put a newline before the exception and to have the exception as the last data in the pattern.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>Equivalent to file</td>
<td></td>
<td></td>
</tr>
<tr>
<td>file</td>
<td>Used to output the file name where the logging request was issued.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WARNING Generating caller location information is extremely slow. Its use should be avoided unless execution speed is not an issue. See the note below on the availability of caller location information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>identity</td>
<td>Used to output the user name for the currently active user (Principal.Identity.Name).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WARNING Generating caller information is extremely slow. Its use should be avoided unless execution speed is not an issue. See the note below on the availability of caller location information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I</td>
<td>Equivalent to location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>Equivalent to line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>location</td>
<td>Used to output location information of the caller which generated the logging event. The location information depends on the CLI implementation but usually consists of the fully qualified name of the calling method followed by the callers source the file name and line number between parentheses. The location information can be very useful. However, its generation is extremely slow. Its use should be avoided unless execution speed is not an issue. See the note below on the availability of caller location information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>line</td>
<td>Used to output the level number from where the logging request was issued.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WARNING Generating caller location information is extremely slow. Its use should be avoided unless execution speed is not an issue. See the note below on the availability of caller location information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>logger</td>
<td>Used to output the logger of the logging event. The logger conversion specifier can be optionally followed by precision specifier, that is a decimal constant in brackets. If a precision specifier is given, then only the corresponding number of right most components of the logger name will be printed. By default the logger name is printed in full. For example, for the logger name &quot;a.b.c&quot; the pattern <code>%logger()</code> will output &quot;b.c&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>m</td>
<td>Equivalent to message</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>Equivalent to method</td>
<td></td>
<td></td>
</tr>
<tr>
<td>message</td>
<td>Used to output the application supplied message associated with the logging event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mdc</td>
<td>The MDC (old name for the ThreadContext.Properties) is now part of the combined event properties. This pattern is supported for compatibility but is equivalent to property.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>method</td>
<td>Used to output the method name where the logging request was issued.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WARNING Generating caller location information is extremely slow. Its use should be avoided unless execution speed is not an issue. See the note below on the availability of caller location information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identifier</td>
<td>Equivalent to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>n</td>
<td>newline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>newline</td>
<td>Outputs the platform dependent line separator character or characters. This conversion pattern offers the same performance as using non-portable line separator strings such as &quot;\n&quot;, or &quot;\r\n&quot;. Thus, it is the preferred way of specifying a line separator.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ndc</td>
<td>Used to output the NDC (nested diagnostic context) associated with the thread that generated the logging event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>p</td>
<td>Equivalent to level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>Equivalent to property</td>
<td></td>
<td></td>
</tr>
<tr>
<td>properties</td>
<td>Equivalent to property</td>
<td></td>
<td></td>
</tr>
<tr>
<td>property</td>
<td>Used to output the an event specific property. The key to lookup must be specified within braces and directly following the pattern specifier, e.g. <code>%property{user}</code> would include the value from the property that is keyed by the string 'user'. Each property value that is to be included in the log must be specified separately. Properties are added to events by loggers or appenders. By default the log4net:HostName property is set to the name of machine on which the event was originally logged. If no key is specified, e.g. <code>%property</code> then all the keys and their values are printed in a comma separated list. The properties of an event are combined from a number of different contexts. These are listed below in the order in which they are searched.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>r</td>
<td>Equivalent to timestamp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>stacktrace</td>
<td>Used to output the stack trace of the logging event. The stack trace level specifier may be enclosed between braces. For example, <code>%stacktrace{level}</code>. If no stack trace level specifier is given then 1 is assumed. Output uses the format: type3.MethodCall3 &gt; type2.MethodCall2 &gt; type1.MethodCall1 This pattern is not available for Compact Framework assemblies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>stacktracedetail</td>
<td>Used to output the stack trace of the logging event. The stack trace level specifier may be enclosed between braces. For example, <code>%stacktracedetail{level}</code>. If no stack trace level specifier is given then 1 is assumed. Output uses the format: type3.MethodCall3(type param,...) &gt; type2.MethodCall2(type param,...) &gt; type1.MethodCall1(type param,...) This pattern is not available for Compact Framework assemblies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>t</td>
<td>Equivalent to thread</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timestamp</td>
<td>Used to output the number of milliseconds elapsed since the start of the application until the creation of the logging event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>thread</td>
<td>Used to output the name of the thread that generated the logging event. Uses the thread number if no name is available.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>type</td>
<td>Used to output the fully qualified type name of the caller issuing the logging request. This conversion specifier can be optionally followed by precision specifier, that is a decimal constant in brackets. If a precision specifier is given, then only the corresponding number of right most components of the class name will be printed. By default the class name is output in fully qualified form. For example, for the class name &quot;log4net.Layout.PatternLayout&quot;, the pattern <code>%type{1}</code> will output &quot;PatternLayout&quot;. WARNING Generating the caller class information is slow. Thus, its use should be avoided unless execution speed is not an issue. See the note below on the availability of caller location information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>u</td>
<td>Equivalent to identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>username</td>
<td>Used to output the WindowsIdentity for the currently active user. WARNING Generating caller WindowsIdentity information is extremely slow. Its use should be avoided unless execution speed is not an issue.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
utcdate  Used to output the date of the logging event in universal time. The date conversion specifier may be followed by a date format specifier enclosed between braces. For example, %utcdate[HH:mm:ss,fff] or %utcdate[dd MMM yyyy HH:mm:ss,fff]. If no date format specifier is given then ISO8601 format is assumed (Iso8601dateFormat). The date format specifier admits the same syntax as the time pattern string of the ToString.

For better results it is recommended to use the log4net date formatters. These can be specified using one of the strings "ABSOLUTE", "DATE" and "ISO8601" for specifying AbsoluteTimeDateFormat, DateTimeDateFormat and respectively Iso8601dateFormat. For example, %utcdate[ISO8601] or %utcdate[ABSOLUTE].

These dedicated date formatters perform significantly better than ToString.

| w | Equivalent to username |
| x | Equivalent to ndc |
| X | Equivalent to mdc |
| % | The sequence %% outputs a single percent sign. |

Apache Tomcat (Ver 7+)

Tomcat server can be configured to use different type of logging systems, the server has default logging configuration and can be configured to use log4j. Tomcat can also create access logs based on the Access Log Valve.

**Tagging**

All Tomcat/Catalina logs are tagged by logtype - tomcat

In addition there are the following log types that must be assigned for the Tomcat App to be deployed on:

- Catalina out log or Console out log will be tagged by logtype - out
- Catalina Servlet or webapp log will be tagged by logtype - servlet
- Access logs will be tagged by logtype - access

Default logging configuration can be found under the conf directory (tomcat/conf) or *nix /etc/tomcat../conf/logging.properties file. Usually the access log will be defined in server.xml file under the conf directory.

**Default Log structure and configuration**

For log type out and servlet, those logs can be name by default catalina.out, and will be located under the logs directory. Use the following XpoLog pattern for those logs

```
{date:Date,dd-MMM-yyyy HH:mm:ss.SSS} {priority:Prioriryt,ftype=severity,ALL;FINEST;FINER;FINE;INFO;CONFIG;WARNING;SEVERE} [{text:thread,ftype=thread}] {text:Source,ftype=source} {string:Message,ftype=message}
```

**Custom Logging**

If the Tomcat server is configured to use external logging with log4j or other java.util framework than use XpoLog pattern wizard and definition to configure the log pattern correctly for the app to work.

Make sure that if you are using log4j wizard you will need to setup the log sources and manually apply the Tomcat/Catalina tags on them for the App to work correctly.

**References**

Tomcat 7

https://tomcat.apache.org/tomcat-7.0-doc/logging.html

Access Logs: https://tomcat.apache.org/tomcat-7.0-doc/config/valve.html#Access_Legging

Tomcat 8


Tomcat 9


**Log4J**

If the Server is using the log4j library for logging please follow the steps documented in adding logs from log4j 1.2 or log4j 2.*
Tomcat Access Logs Configuration

1. Add Log Data In XpoLog, When adding a log to XpoLog you can now select the Log Type (logtype) for Apache Tomcat Access with the following logtypes:
   a. tomcat
      i. in addition select the log type - access

Tomcat access logs are created with the AccessLogValve or with ExtendedAccessLogValve implementation.

For the configuration look into the server `<TOMCAT-HOME/conf/server.xml>` / (Linux `/etc/tomcat/conf/server.xml`) or other webapp configuration files and search for the following:

```xml
<Engine name="Catalina" defaultHost="localhost">
  <Host name="localhost" ...>
    <!-- Access log processes all example.
    Documentation at: /docs/config/valve.html
    Note: The pattern used is equivalent to using pattern="common"
    <Valve className="org.apache.catalina.valves.AccessLogValve">
      directory="logs"
      prefix="localhost_access_log."
      suffix=".txt"
      pattern="%h %l %u %t "%r" %s %b"
    </Valve>
  </Host>
</Engine>
```

The pattern field may defined also as below:

The shorthand pattern `pattern="common"` corresponds to the Common Log Format defined by `%h %l %u %t "%r" %s %b`

The shorthand pattern `pattern="combined"` appends the values of the Referer and User-Agent headers, each in double quotes, to the common pattern.

In XpoLog such pattern (combined) will be translated into:

```
{ip:Client IP,ftype=remoteip;type=;}
{string:Remote Log Name,ftype=remotelog;}
{{date:Date,locale=en,dd/MMM/yyyy:HH:mm:ss z}}
{choice:Method,ftype=reqmethod;GET;POST}
{string:URL,ftype=requrl;}
{string:Query,ftype=querystring;}
{string:reqprotocol,ftype=reqprotocol;}
{number:Status,ftype=respstatus;}
{number:Bytes Sent,ftype=bytesent;}
```

In XpoLog such pattern (common) will be translated into:

```
{ip:Client IP,ftype=remoteip;type=;}
{string:Remote Log Name,ftype=remotelog;}
{{date:Date,locale=en,dd/MMM/yyyy:HH:mm:ss z}}
{choice:Method,ftype=reqmethod;GET;POST}
{string:URL,ftype=requrl;}
{string:Query,ftype=querystring;}
{string:reqprotocol,ftype=reqprotocol;}
{number:Status,ftype=respstatus;}
{number:Bytes Sent,ftype=bytesent;}
```

**XpoLog Pattern Wizard**

When configuring access logs for Tomcat in the XpoLog pattern wizard, paste the pattern directive value into the wizard in order to generate the correct XpoLog pattern for our example you will need to paste: `%h %l %u %t "%r" %s %b`

Note: If the pattern value is common or combined simply past them into the wizard and XpoLog will build the right pattern as well.

### Apache Tomcat Access Log Format Conversion Table both for AccessLogValve and for ExtendedAccessLogValve

<table>
<thead>
<tr>
<th>Format String</th>
<th>Description</th>
<th>XpoLog Pattern</th>
<th>XpoLog ftype</th>
</tr>
</thead>
<tbody>
<tr>
<td>tomcat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%a</td>
<td>Remote IP-address</td>
<td>{ip:RemoteIP,ftype=remoteip}</td>
<td>remoteip</td>
</tr>
<tr>
<td>%A</td>
<td>Local IP-address</td>
<td>{ip:LocalIP,ftype=localip}</td>
<td>localip</td>
</tr>
<tr>
<td>%B</td>
<td>Size of response in bytes, excluding HTTP headers.</td>
<td>{number:BytesSent,ftype=bytesent}</td>
<td>bytesent</td>
</tr>
<tr>
<td>%b</td>
<td>Bytes sent, excluding HTTP headers, or '-' if zero</td>
<td>{text:BytesSent,ftype=bytesent}</td>
<td>bytesent</td>
</tr>
<tr>
<td>%c</td>
<td>The contents of cookie Foobar in the request sent to the server. Only version 0 cookies are fully supported.</td>
<td>{string:Cookie_&lt;FOOBAR&gt;}</td>
<td>Replace &lt;FOOBAR&gt; with cookie name</td>
</tr>
<tr>
<td>%d</td>
<td>The time taken to serve the request, in microseconds.</td>
<td>{number:ResponseTimeMicroSecs,ftype=responsetime}</td>
<td>responsetime</td>
</tr>
<tr>
<td>%f</td>
<td>Time taken to commit the response, in millis</td>
<td>{number:ResponseTimeMillisecs,ftype=responsetimemillis}</td>
<td>responsetimemillis</td>
</tr>
<tr>
<td>%h</td>
<td>Remote host name (or IP address if enableLookups for the connector is false)</td>
<td>{text:Remotehost,ftype=remotehost}</td>
<td>remotehost</td>
</tr>
<tr>
<td>%H</td>
<td>The request protocol</td>
<td>{text:RequestProtocol,ftype=reqprotocol}</td>
<td>reqprotocol</td>
</tr>
<tr>
<td>%i</td>
<td>The contents of Foobar header line(s) in the request sent to the server. Changes made by other modules (e.g. mod_headers) affect this. If you're interested in what the request header was prior to when most modules would have modified it, use mod_setenvif to copy the header into an internal environment variable and log that value with the %</td>
<td>VARNAME</td>
<td>c described above.</td>
</tr>
<tr>
<td>%j</td>
<td>Referer</td>
<td>{text:Referer,ftype=referer}</td>
<td>referer</td>
</tr>
<tr>
<td>%l</td>
<td>Remote logical username from identd (always returns '-')</td>
<td>{text:logicalname,ftype=logicalname}</td>
<td>logicalname</td>
</tr>
<tr>
<td>%m</td>
<td>The request method</td>
<td>{text:RequestMethod,ftype=reqmethod}</td>
<td>reqmethod</td>
</tr>
<tr>
<td>%o</td>
<td>write value of outgoing header with name xxx</td>
<td>{string:&lt;FOOBAR&gt;}</td>
<td></td>
</tr>
<tr>
<td>%p</td>
<td>The canonical local port of the server serving the request</td>
<td>{number:ServerPort,ftype=serverport}</td>
<td>serverport</td>
</tr>
<tr>
<td>%q</td>
<td>The query string (prepended with a ? if a query string exists, otherwise an empty string)</td>
<td>{text:QueryString,ftype=querystring}</td>
<td>querystring</td>
</tr>
</tbody>
</table>
**%r**  First line of the request (method and request URI)  
{text:FirstLine,ftype=reqfirstline}  
TBD - might be parsed to multiple value and types

**%s**  Status. For requests that got internally redirected, this is the status of the "original" request --- %s for the last.  
{number:ResponseStatus,ftype=respstatus}  
For requests that got internally redirected, this is the status of the "original" request --- %s for the last.

**%S**  User session ID  
{text:UserSessionId,ftype=sessionid}

**%t**  Time the request was received (standard english format)  
{date:Date,locale=en,dd/MMM/yyyy:HH:mm:ss z}

**{%format}t**  The time, in the form given by format, which should be in an extended `strftime(3)` format (potentially localized). If the format starts with `begin:` (default) the time is taken at the beginning of the request processing. If it starts with `end:` it is the time when the log entry gets written, close to the end of the request processing. In addition to the formats supported by `strftime(3)`, the following format tokens are supported:

<table>
<thead>
<tr>
<th>Format Token</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sec</td>
<td>number of seconds since the Epoch</td>
</tr>
<tr>
<td>msec</td>
<td>number of milliseconds since the Epoch</td>
</tr>
<tr>
<td>usec</td>
<td>number of microseconds since the Epoch</td>
</tr>
<tr>
<td>msec_frac</td>
<td>millisecond fraction</td>
</tr>
<tr>
<td>usec_frac</td>
<td>microsecond fraction</td>
</tr>
</tbody>
</table>

These tokens can not be combined with each other or `strftime(3)` formatting in the same format string. You can use multiple `{%format}t` tokens instead.

The extended `strftime(3)` tokens are available in 2.2.30 and later.

**%T**  The time taken to serve the request, in seconds.  
{number:ResponseTimeSecs,ftype=processrequestsec}

**%u**  Remote user that was authenticated (if any), else '-'  
{text:User,ftype=remoteuser}  
Remote user (from auth; may be bogus if return status ( %s ) is 401)

**%U**  The URL path requested, not including any query string.  
{text:RequestURL,ftype=requrl}  
The URL path requested, not including any query string.

**%v**  Local server name  
{text:ServerName,ftype=servername}

The ExtendedAccessLogValve conversion table below:

<table>
<thead>
<tr>
<th>Format String</th>
<th>Description</th>
<th>XpoLog Pattern</th>
<th>XpoLog ftype</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>Bytes sent, excluding HTTP headers, or '-' if zero</td>
<td>{text:BytesSent,ftype=bytesent}</td>
<td>bytesent</td>
</tr>
<tr>
<td>c-dns</td>
<td>Remote host name (or IP address if enableLocups for the connector is false)</td>
<td>{ip:RemoteIP,ftype=remoteip}</td>
<td>remoteip</td>
</tr>
<tr>
<td>c-ip</td>
<td>Remote IP address</td>
<td>{ip:RemoteIP,ftype=remoteip}</td>
<td>remoteip</td>
</tr>
<tr>
<td>cs-method</td>
<td>Request method (GET, POST, etc.)</td>
<td>{text:RequestMethod,ftype=reqmethod}</td>
<td>reqmethod</td>
</tr>
<tr>
<td>cs-uri</td>
<td>Request URI</td>
<td>{text:FirstLine,ftype=reqfirstline}</td>
<td>reqfirstline</td>
</tr>
</tbody>
</table>

TBD - might be parsed to multiple value and types
Linux

Background

The Linux Servers logs analysis App automatically Collect - Read - Parse - Analyzes - Reports all machine generated log data of the server and presents a comprehensive set of graphs and reports to analyze machine generated data. Use a predefined set of dashboards and gadgets to visualize and address the system software, code written, and infrastructure during development, testing, and production. This Linux logs analysis App helps measure, troubleshoot, and optimize your servers integrity, stability and quality with the several visualization and investigation dashboards.

Steps:

1. The Linux App is running on messages/syslog, auth/secure, mail, kern and cron standard logs. When adding/editing the logs to XpoLog it is mandatory to apply the correct log type(s) to each of the logs:
   a. **linux** - all logs that the application will analyze must have **linux** as a log type
   b. **linux-messages/linux-syslog** - only the messages/syslog logs must also be configured to have **linux-messages/linux-syslog** as a log type
   c. **linux-auth/linux-secure** - only the auth/secure logs must also be configured to have **linux-auth/linux-secure** as a log type
   d. **linux-cron** - only the cron log must also be configured to have **linux-cron** as a log type
   e. **linux-mail** - only the mail log must also be configured to have **linux-mail** as a log type
   f. **linux-kernel** - only the kern log must also be configured to have **linux-kernel** as a log type

2. Once the required information is set, on each log click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Linux App. Use the following patterns for each of the logs:
   a. Linux messages/syslog log:
      ```
      {date:Date,MMM dd HH:mm:ss} {text:source,ftype=source} {text:process name,ftype=process;}{block:start,emptiness=true}{(text:pid,ftype=pid)}{block:end,emptiness=true};
      {text:Message,ftype=message;}{regexp:User,ftype=user;refName=message,[passed|failed] for (.*) from}
      ```
   b. Linux auth/secure log:
      ```
      {date:Date,MMM dd HH:mm:ss} {text:SourceIP,ftype=source}{text:process,ftype=process}{block:start,emptiness=true}{(text:pid,ftype=pid)}{block:end,emptiness=true};
      ```
   c. Linux cron log:
      ```
      {date:Date,MMM dd HH:mm:ss} {text:Server,ftype=server}{text:process,ftype=process}{block:start,emptiness=true}{(text:pid,ftype=pid)}{block:end,emptiness=true};
      ```
   d. Linux mail log:
      ```
      {date:Date,MMM dd HH:mm:ss} {text:source} {text:process name,ftype=process;}{block:start,emptiness=true}{(number:process id)}{block:end,emptiness=true};
      {regexp:session,refName=Message;ftype=session,^\(w+\):\{regexp:From,refName=Message;ftype=from,\s+from=([^,]+)\}\{regexp:To,refName=Message;ftype=to,\s+to=([^,]+)\}{text:Message,ftype=message;}}
      ```
Microsoft IIS (Ver 6)

Background

The Microsoft IIS Server logs analysis App automatically Collect - Read - Parse - Analyzes - Reports all web machine generated log data of the server and presents a comprehensive set of graphs and reports to analyze machine generated data. Use a predefined set of dashboards and gadgets to visualize and address the system software, code written, and infrastructure during development, testing, and production. This Microsoft IIS logs analysis App helps measure, troubleshoot, and optimize your servers integrity, stability and quality with visualization and investigation dashboards.

Steps

1. Add Log Data In XpoLog, When adding a log to XpoLog you can now select the Log Type (logtype) for Microsoft IIS these are the following logtypes:
   a. iis
      i. in addition select not only iis but also you will need to select the log type - access or error

2. Once all required information is set click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Analytic App. Use the following conversion table in order to build XpoLog pattern out of the access log format.

Example

In the header of IIS access logs , or on the IIS configuration file locate the format specification strings that configure the logged fields for example:

```plaintext
#Fields: date time s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs-version cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken
```

The following sequence is the log structure definition: date time s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs-version cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken

In XpoLog such pattern will be translated into:

```plaintext
{date:Date,yyyy-MM-dd HH:mm:ss} {text:SiteName,ftype=sitename} {text:ServerName,ftype=servername} {geoip:ServerIP,ftype=localip} {text:RequestMethod,ftype=reqmethod} {text:RequestURL,ftype=requir} {text:QueryString,ftype=querystring} {number:ServerPort,ftype=serverport} {text:username,ftype=remoteuser} {geoip:ClientIP,ftype=remoteip} {text:ProtocolVer,ftype=protocolversion} {text:User-agent,ftype=useragent} {text:Cookie,ftype=cookie} {text:Referer,ftype=referer} {text:HostName,ftype=hostname} {number:ResponseStatus,ftype=respstatus} {number:SubStatus,ftype=ressubstatus} {text:Win32Status,ftype=win32status} {number:BytesSent,ftype=bytesent} {number:BytesSent,ftype=bytesreceived} {number:ResponseTimeSecs,ftype=processrequestmilli}{eoe}
```

for more information see below the format Conversion Table

<table>
<thead>
<tr>
<th>Format String</th>
<th>Appear as</th>
<th>Description</th>
<th>XpoLog Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date + Time</td>
<td>date time</td>
<td>The date on which the activity occurred.</td>
<td>{date,yyyy-MM-dd HH:mm:ss}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The time, in coordinated universal time (UTC), at which the activity occurred.</td>
<td></td>
</tr>
<tr>
<td>Client IP Address</td>
<td>c-ip</td>
<td>The IP address of the client that made the request.</td>
<td>{geoip:ClientIP,ftype=remoteip} remoteip</td>
</tr>
<tr>
<td>User Name</td>
<td>cs-username</td>
<td>The name of the authenticated user who accessed your server. Anonymous users are indicated by a hyphen.</td>
<td>{text:username,ftype=remoteuser} remoteuser</td>
</tr>
<tr>
<td>Service Name and Instance Number</td>
<td>s-sitename</td>
<td>The Internet service name and instance number that was running on the client.</td>
<td>{text:SiteName,ftype=sitename} sitename</td>
</tr>
<tr>
<td>Server Name</td>
<td>s-computename</td>
<td>The name of the server on which the log file entry was generated.</td>
<td>{text:ServerName,ftype=servername} servername</td>
</tr>
</tbody>
</table>
### Server IP Address
- **s-ip**: The IP address of the server on which the log file entry was generated.

### Server Port
- **s-port**: The server port number that is configured for the service.

### Method
- **cs-method**: The requested action, for example, a GET method.

### URI Stem
- **cs-uri-stem**: The target of the action, for example, **Default.htm**.

### URI Query
- **cs-uri-query**: The query, if any, that the client was trying to perform. A Universal Resource Identifier (URI) query is necessary only for dynamic pages.

### HTTP Status
- **sc-status**: The HTTP status code.

### Win32 Status
- **sc-win32-status**: The Windows status code.

### Bytes Sent
- **sc-bytes**: The number of bytes that the server sent.

### Bytes Received
- **cs-bytes**: The number of bytes that the server received.

### Time Taken
- **time-taken**: The length of time that the action took, in milliseconds.

### Protocol Version
- **cs-version**: The protocol version — HTTP or FTP — that the client used.

### Host
- **cs-host**: The host header name, if any.

### User Agent
- **cs(User-Agent)**: The browser type that the client used.

### Cookie
- **cs(Cookie)**: The content of the cookie sent or received, if any.

### Referrer
- **cs(Referrer)**: The site that the user last visited. This site provided a link to the current site.

### Protocol Substatus
- **sc-substatus**: The substatus error code.

---

### Microsoft IIS (Ver 7)

#### Background

The Microsoft IIS Server logs analysis App automatically Collect - Read - Parse - Analyzes - Reports all web machine generated log data of the server and presents a comprehensive set of graphs and reports to analyze machine generated data. Use a predefined set of dashboards and gadgets to visualize and address the system software, code written, and infrastructure during development, testing, and production. This Microsoft IIS logs analysis App helps measure, troubleshoot, and optimize your servers integrity, stability and quality with visualization and investigation dashboards.

#### Steps

1. **Add Log Data In XpoLog**, When adding a log to XpoLog you can now select the Log Type (logtype) for Microsoft IIS these are the following logtypes:
   a. **iis**
   
   i. in addition select not only iis but also you will need to select the log type - access or error

2. Once all required information is set click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Analytic App. Use the following conversion table in order to build XpoLog pattern out of the access log format.

#### Example

In the header of IIS access logs, or on the IIS configuration file locate the format specification strings that configure the logged fields for example:

```
#Fields: date time s-sitename s-computernumber s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs-version cs(User-Agent)
```
The following sequence is the log structure definition: date time s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs-version cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken

In XpoLog such pattern will be translated into:

```
{date:Date,yyyy-MM-dd HH:mm:ss} {text:SiteName,ftype=sitename} {text:ServerName,ftype=servername} {geoip:ServerIP,ftype=localip} {text:RequestMethod,ftype=reqmethod} {text:RequestURL,ftype=requrl} {text:QueryString,ftype=querystring} {number:ServerPort,ftype=serverport} {text:username,ftype=remoteuser} {geoip:ClientIP,ftype=remoteip} {text:ProtocolVer,ftype=protocolversion} {text:User-agent,ftype=useragent} {text:Cookie,ftype=cookie} {text:Referer,ftype=referer} {text:HostName,ftype=hostname} {number:ResponseStatus,ftype=respstatus} {number:SubStatus,ftype=ressubstatus} {text:Win32Status,ftype=win32status} {number:BytesSent,ftype=bytesent} {number:BytesSent,ftype=bytesreceived} {number:ResponseTimeSecs,ftype=processrequestmilli}
```

for more information see below the format Conversion Table

<table>
<thead>
<tr>
<th>Format String</th>
<th>Apear as</th>
<th>Description</th>
<th>XpoLog Pattern</th>
<th>ftype</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date + Time</td>
<td>date time</td>
<td>The date on which the activity occurred.</td>
<td>{date,yyyy-MM-dd HH:mm:ss}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The time, in coordinated universal time (UTC), at which the activity occurred.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client IP Address</td>
<td>c-ip</td>
<td>The IP address of the client that made the request.</td>
<td>{ip:ClientIP,ftype=remoteip}</td>
<td>remoteip</td>
</tr>
<tr>
<td>User Name</td>
<td>cs-username</td>
<td>The name of the authenticated user who accessed your server. Anonymous users are indicated by a hyphen.</td>
<td>{text:username,ftype=remoteuser}</td>
<td>remoteuser</td>
</tr>
<tr>
<td>Service Name and Instance Number</td>
<td>s-sitename</td>
<td>The Internet service name and instance number that was running on the client.</td>
<td>{text:SiteName,ftype=sitename}</td>
<td>sitename</td>
</tr>
<tr>
<td>Server Name</td>
<td>s-computername</td>
<td>The name of the server on which the log file entry was generated.</td>
<td>{string:ServerName,ftype=servername}</td>
<td>servername</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>s-ip</td>
<td>The IP address of the server on which the log file entry was generated.</td>
<td>{ip:ServerIP,ftype=localip}</td>
<td>localip</td>
</tr>
<tr>
<td>Server Port</td>
<td>s-port</td>
<td>The server port number that is configured for the service.</td>
<td>{number:ServerPort,ftype=serverport}</td>
<td>serverport</td>
</tr>
<tr>
<td>Method</td>
<td>cs-method</td>
<td>The requested action, for example, a GET method.</td>
<td>{text:RequestMethod,ftype=reqmethod}</td>
<td>reqmethod</td>
</tr>
<tr>
<td>URI Stem</td>
<td>cs-uri-stem</td>
<td>The target of the action, for example, Default.htm.</td>
<td>{text:RequestURL,ftype=requrl}</td>
<td>requrl</td>
</tr>
<tr>
<td>URI Query</td>
<td>cs-uri-query</td>
<td>The query, if any, that the client was trying to perform. A Universal Resource Identifier (URI) query is necessary only for dynamic pages.</td>
<td>{text:QueryString,ftype=querystring}</td>
<td>querystring</td>
</tr>
<tr>
<td>HTTP Status</td>
<td>sc-status</td>
<td>The HTTP status code.</td>
<td>{number:ResponseStatus,ftype=respstatus}</td>
<td>respstatus</td>
</tr>
<tr>
<td>Win32 Status</td>
<td>sc-win32-status</td>
<td>The Windows status code.</td>
<td>{text:Win32Status,ftype=win32status}</td>
<td>win32status</td>
</tr>
<tr>
<td>Bytes Sent</td>
<td>sc-bytes</td>
<td>The number of bytes that the server sent.</td>
<td>{number:BytesSent,ftype=bytesent}</td>
<td>bytesent</td>
</tr>
<tr>
<td>Bytes Received</td>
<td>cs-bytes</td>
<td>The number of bytes that the server received.</td>
<td>{number:BytesSent,ftype=bytesreceived}</td>
<td>bytesreceived</td>
</tr>
<tr>
<td>Time Taken</td>
<td>time-taken</td>
<td>The length of time that the action took, in milliseconds.</td>
<td>{number:ResponseTimeSecs,ftype=processrequestmilli}</td>
<td>processrequestmilli</td>
</tr>
<tr>
<td>Protocol Version</td>
<td>cs-version</td>
<td>The protocol version —HTTP or FTP —that the client used.</td>
<td>{text:ProtocolVer,ftype=protocolversion}</td>
<td>protocolversion</td>
</tr>
<tr>
<td>Host</td>
<td>cs-host</td>
<td>The host header name, if any.</td>
<td>{text:HostName,ftype=hostname}</td>
<td>hostname</td>
</tr>
<tr>
<td>User Agent</td>
<td>cs(User-Agent)</td>
<td>The browser type that the client used.</td>
<td>{text:User-agent,ftype=useragent}</td>
<td>useragent</td>
</tr>
</tbody>
</table>
Microsoft Windows

Background

The Microsoft Windows Servers logs analysis App automatically Collect - Read - Parse - Analyzes - Reports all machine generated log data of the server and presents a comprehensive set of graphs and reports to analyze machine generated data. Use a predefined set of dashboards and gadgets to visualize and address the system software, code written, and infrastructure during development, testing, and production. This Windows logs analysis App helps measure, troubleshoot, and optimize your servers integrity, stability and quality with the several visualization and investigation dashboards.

Steps:

1. The Microsoft Windows App is running on Application, Security and System standard event logs (*.evtx).
   When adding/editing the logs to XpoLog it is mandatory to apply the correct log type(s) to each of the logs:
   a. windows - all logs that the application will analyze must have windows as a log type
   b. windows-application - only the Application log must also be configured to have windows-application as a log type
   c. windows-security - only the Security log must also be configured to have windows-security as a log type
   d. windows-system - only the System log must also be configured to have windows-system as a log type

2. Once the required information is set, on each log click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Microsoft Windows App. Use the following patterns for each of the logs:
   a. Windows Application event log:
      {priority:Type,ftype=type,Error;Warning;Information;Success;Audit Failure;Audit Success}[*];{timestamp:Date,MM/dd/yyyy HH:mm:ss}{regexp:Account Name,refName=Description;ftype=account name,Account Name:\s+\(S+.\)\)*{regexp:Account Domain,refName=Description;ftype=domain,Account Domain:\s+\(S+.\)\)*{text:Source,ftype=source}*{text:Category,ftype=category}*{number:Event,ftype=event}*{text:User,ftype=user}*{text:Computer,ftype=computer}*{string:Description,ftype=description}
   b. Windows Security event log:
      {priority:Type,ftype=type,Error;Warning;Information;Success;Audit Failure;Audit Success}[*];{timestamp:Date,MM/dd/yyyy HH:mm:ss}{regexp:Account Name,refName=Description;ftype=account name,Account Name:\s+\(S+.\)\)*{regexp:Account Domain,refName=Description;ftype=domain,Account Domain:\s+\(S+.\)\)*{text:Source,ftype=source}*{text:Category,ftype=category}*{number:Event,ftype=event}{map:Event Description,ftype=event description,refIndex=6,file:knowledge/repository/system/win/map/winEventsMap.prop}{map:Category Description,ftype=category description,refIndex=6,file:knowledge/repository/system/win/map/winEventsCategoryMap.prop}{map:Sub Category,ftype=sub category,refIndex=6,file:knowledge/repository/system/win/map/winEventsSubCategoryMap.prop}{map:User,ftype=user}{regexp:Logon ID,refName=description;ftype=logon id,Logon ID:\s+\(S+.\)\)*{text:Computer,ftype=computer}*{string:Description,ftype=description}
   c. Windows System event log:
      {priority:Type,ftype=type,Error;Warning;Information;Success;Audit Failure;Audit Success}[*];{timestamp:Date,MM/dd/yyyy HH:mm:ss}{regexp:Account Name,refName=Description;ftype=account name,Account Name:\s+\(S+.\)\)*{regexp:Account Domain,refName=Description;ftype=domain,Account Domain:\s+\(S+.\)\)*{text:Source,ftype=source}*{text:Category,ftype=category}*{number:Event,ftype=event}*{text:User,ftype=user}*{text:Computer,ftype=computer}*{string:Description,ftype=description}

NGINX (Ver 1.10+)

Background

The NGINX server logs analysis App automatically Collect - Read - Parse - Analyzes - Reports all machine's generated log data of the server and
presents a comprehensive set of graphs and reports to analyze machine generated data. Use a predefined set of dashboards and gadgets to visualize and address the system software, code written, and infrastructure during development, testing, and production. This NGINX server logs analysis App helps you measure, troubleshoot, and optimize your servers integrity, stability and quality with visualization and investigation dashboards.

**Steps**

1. Add Log Data In XpoLog. When adding a log to XpoLog you can now select the Log Type (logtype) for NGINX with the following logtypes:
   a. nginx
   i. in addition select not only httpd but also the log type - access or error
   ii. see error log definition at the bottom of this page
2. Once all required information is set click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Analytic App. Use the following conversion table to build the XpoLog pattern.

**Example**

In the NGINX configuration file, usually nginx.conf by default, located under the conf/ directory (Linux "NGINX ROOT DIR/conf/nginx.conf") search for the ______ directive:

Information from NGINX site:

"NGINX writes information about client requests in the access log right after the request is processed. By default, the access log is located at logs/access.log, and the information is written to the log in the predefined combined format. To override the default setting, use the log_format directive to change the format of logged messages, as well as the access_log directive to specify the location of the log and its format. The log format is defined using variables.

The following examples define the log format that extends the predefined combined format with the value indicating the ratio of gzip compression of the response. The format is then applied to a virtual server that enables compression.

```bash
access_log path [format [buffer=size] [gzip[=level]] [flush=time] [if=condition]]; access_log off; Default: access_log logs/access.log combined;

log_format combined '$remote_addr - $remote_user [$time_local] '
   '"$request" $status $body_bytes_sent ' 
   '"$http_referer" "$http_user_agent"';
```

In XpoLog such pattern will be translated into:

```
{geoip:RemoteIP,ftype=remoteip} - {text:User,ftype=remoteuser} [{date:Date,dd/MM/yyyy:HH:mm:ss z}]
"{text:RequestMethod,ftype=reqmethod} {text:RequestURL,ftype=requrl} {text:RequestProtocol,ftype=reqprotocol}"
{number:ResponseStatus,ftype=respstatus} {number:BytesSent,ftype=bytesent} "{text:Referer,ftype=referer}"
"{text:User-agent,ftype=useragent}"{eoe}
```

for more information see below:

**Apache Https Access Log Format Conversion Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Appears as</th>
<th>Description</th>
<th>XpoLog Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>$arg_{name}</td>
<td></td>
<td>argument name in the request line</td>
<td></td>
</tr>
<tr>
<td>$args</td>
<td></td>
<td>arguments in the request line</td>
<td>[text:QueryString,ftype=querystring]</td>
</tr>
<tr>
<td>$binary_{remote_addr}</td>
<td></td>
<td>client address in a binary form, value’s length is always 4 bytes for IPv4 addresses or 16 bytes for IPv6 addresses</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Type</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>$body_bytes_sent</td>
<td>number of bytes sent to a client, not counting the response header; this variable is compatible with the &quot;%B&quot; parameter of the mod_log_config Apache module</td>
<td>{number:BytesSent,type=bytesent}</td>
<td></td>
</tr>
<tr>
<td>$bytes_sent</td>
<td>number of bytes sent to a client (1.3.8, 1.2.5)</td>
<td>{number:TotalBytesWHeadersSent,type=resp}</td>
<td></td>
</tr>
<tr>
<td>$connection</td>
<td>connection serial number (1.3.8, 1.2.5)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$connection_requests</td>
<td>current number of requests made through a connection (1.3.8, 1.2.5)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$content_length</td>
<td>“Content-Length” request header field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$content_type</td>
<td>“Content-Type” request header field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$cookie_name</td>
<td>the name cookie</td>
<td>{string:CookieName}</td>
<td></td>
</tr>
<tr>
<td>$document_root</td>
<td>root or alias directive’s value for the current request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$document_uri</td>
<td>same as $uri</td>
<td>{text:RequestURL,type=requrl}</td>
<td></td>
</tr>
<tr>
<td>$host</td>
<td>in this order of precedence: host name from the request line, or host name from the “Host” request header field, or the server name matching a request</td>
<td>{text:ServerName,type=servername}</td>
<td></td>
</tr>
<tr>
<td>$hostname</td>
<td>host name</td>
<td>{text:Remotehost,type=remotehost}</td>
<td></td>
</tr>
<tr>
<td>$http_name</td>
<td>arbitrary request header field; the last part of a variable name is the field name converted to lower case with dashes replaced by underscores</td>
<td>{text:&lt;name&gt;_,type=&lt;NAME&gt;}</td>
<td></td>
</tr>
<tr>
<td>$https</td>
<td>“on” if connection operates in SSL mode, or an empty string otherwise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$is_args</td>
<td>“?” if a request line has arguments, or an empty string otherwise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$limit_rate</td>
<td>setting this variable enables response rate limiting; see limit_rate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$msec</td>
<td>current time in seconds with the milliseconds resolution (1.3.9, 1.2.6)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$nginx_version</td>
<td>nginx version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$pid</td>
<td>PID of the worker process [text:ProcessID,ftype=processid]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$pipe</td>
<td>&quot;p&quot; if request was pipelined, &quot;.&quot; otherwise (1.3.12, 1.2.7)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$proxy_protocol_addr</td>
<td>client address from the PROXY protocol header, or an empty string otherwise (1.5.12)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The PROXY protocol must be previously enabled by setting the proxy_protocol parameter in the listen directive.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$proxy_protocol_port</td>
<td>client port from the PROXY protocol header, or an empty string otherwise (1.11.0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The PROXY protocol must be previously enabled by setting the proxy_protocol parameter in the listen directive.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$query_string</td>
<td>same as $args [text:QueryString,ftype=querystring]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$realpath_root</td>
<td>an absolute pathname corresponding to the root or alias directive's value for the current request, with all symbolic links resolved to real paths</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$remote_addr</td>
<td>client address [ip:RemoteIP,ftype=remoteip]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$remote_port</td>
<td>client port [number:RemotePort,ftype=remoteport]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$remote_user</td>
<td>user name supplied with the Basic authentication [text:User,ftype=remoteuser]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$request</td>
<td>full original request line [text:RequestMethod,ftype=reqmethod]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[text:RequestURL,ftype=requrl]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[text:RequestProtocol,ftype=reqprotocol]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>$request_body</code></td>
<td>request body</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The variable’s value is made available in locations processed by the <code>proxy_pass</code>, <code>fastcgi_pass</code>, <code>uwsgi_pass</code>, and <code>scgi_pass</code> directives when the request body was read to a memory buffer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>$request_body_file</code></td>
<td>name of a temporary file with the request body</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>At the end of processing, the file needs to be removed. To always write the request body to a file, <code>client_body_in_file_only</code> needs to be enabled. When the name of a temporary file is passed in a proxied request or in a request to a FastCGI/uwsgi/SCGI server, passing the request body should be disabled by the <code>proxy_pass_request_body off</code>, <code>fastcgi_pass_request_body off</code>, <code>uwsgi_pass_request_body off</code>, or <code>scgi_pass_request_body off</code> directives, respectively.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>$request_completion</code></td>
<td>“OK” if a request has completed, or an empty string otherwise</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>$request_filename</code></td>
<td>file path for the current request, based on the <code>root</code> or <code>alias</code> directives, and the request URI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>$request_id</code></td>
<td>unique request identifier generated from 16 random bytes, in hexadecimal (1.11.0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>$request_length</code></td>
<td>request length (including request line, header, and request body) (1.3.12, 1.2.7)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>$request_method</code></td>
<td>request method, usually “GET” or “POST”</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>$request_time</code></td>
<td>request processing time in seconds with a milliseconds resolution (1.3.9, 1.2.6); time elapsed since the first bytes were read from the client</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>$request_uri</code></td>
<td>full original request URI (with arguments)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>$scheme</code></td>
<td>request scheme, “http” or “https”</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
$sent_http_name

arbitrary response header field; the last part of a variable name is the field name converted to lower case with dashes replaced by underscores

$server_addr

an address of the server which accepted a request

Computing a value of this variable usually requires one system call. To avoid a system call, the listendirectives must specify addresses and use the bind parameter.

(ip:LocalIP,ftype=localip)

$server_name

name of the server which accepted a request

[text:ServerName,ftype=servername)

$server_port

port of the server which accepted a request

[number:ServerPort,ftype=serverport)

$server_protocol

request protocol, usually "HTTP/1.0", "HTTP/1.1", or "HTTP/2.0"

[text:RequestProtocol,ftype=reqprotocol)

$status

response status (1.3.2, 1.2.2)

[number:ResponseStatus,ftype=respstatus]

$tcpinfo_rtt, $tcpinfo_rttvar, $tcpinfo_snd_cwnd, $tcpinfo_rcv_space

information about the client TCP connection; available on systems that support the TCP_INFO socket option

$time_iso8601

local time in the ISO 8601 standard format (1.3.12, 1.2.7)

$time_local

local time in the Common Log Format (1.3.12, 1.2.7)

[date:Date,dd/MMM/yyyy:HH:mm:ss z]

$uri

current URI in request, normalized

The value of $uri may change during request processing, e.g. when doing internal redirects, or when using index files.

[text:RequestURL,ftype=requrl]

$http_user_agent

[text:User-agent,ftype=useragent]

$http_referer

[text:Referer,ftype=referer]

Error Log

Look for the error_log logs/error.log warn; directive the nginx configuration file.
With PID and TID being the logging process and thread id and CID a number identifying a (probably proxied) connection, probably a counter. The *CID part is optional.

debug, info, notice, warn, error, crit, alert, or emerg.

Default XpoLog Pattern:

```
{date:Date,yyyy/MM/dd:mm:ss} [{priority:Level,ftype=severity,debug;info;notice;warn;error;crit;alert;emerg}] {text:PID,ftype=processid}#{text:TID,ftype=threadid}: {text:CID,ftype=connectionid} {string:Message,ftype=message}
```

WebSphere (Ver 6.0+)

Background

The WebSphere Server logs analysis App automatically Collect - Read - Parse - Analyzes - Reports all WebSphere machine generated log data of the server and presents a comprehensive set of graphs and reports to analyze machine generated data. Use a predefined set of dashboards and gadgets to visualize and address the system software, code written, and infrastructure during development, testing, and production. This WebSphere logs analysis App helps measure, troubleshoot, and optimize your servers integrity, stability and quality with visualization and investigation dashboards.

Steps

1. Add Log Data In XpoLog, When adding a log to XpoLog you can now set a Log Type (logtype). For WebSphere set the following logtypes for each log:
   a. System out - was,was-server,was-systemout
   b. System err - was,was-server,was-systemerr
   c. Server start - was,was-server,was-server-start
   d. Server stop - was,was-server,was-server-stop
   e. Native out - was,was-server,was-nativeout
   f. Http error - was,was-server,http-error
   g. Http access - was,was-server,access,w3c

2. In the WebSphere server configuration file, usually server.xml by default, located under the [SERVER_DIR]/config/.../[SERVER_NAME] directory. Search for the following parameters:
   a. System out - outputStreamRedirect
   b. System err - errorStreamRedirect
   c. Server start - outputStreamRedirect
   d. Server stop - outputStreamRedirect
   e. Native out - ioRedirect
   f. Http error - enableErrorLogging
   g. Http access - enableAccessLogging

3. Once the required information is set, on each log click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Linux App. Use the following patterns for each of the logs:
   a. System out - Basic Information - [{date:Date,locale=en,MM/dd/yy HH:mm:ss:mm:ss z}] {text:Thread ID,charsLength=8;ftype=threadid;} {text:Short Name,charsLength=13;ftype=shortname;} {map:Event Type,ftype=severity;,F=FATAL;E=ERROR;W=WARNING;A=AUdit;I=INFO;C=CONFIGURATION;D=DETAIL;O=SYSTEM OUTPUT;R=SYSTEM ERROR;Z=UNKNOWN} {block,start,emptiness=true} {text:Class,ftype=class;stopPattern=^com\.ibm\.[\w\.]\+\(\w\\)+\(\w\)+\(\w\)+;}{text:Method,ftype=method;}{block,end,emptiness=true} {regexp:messagecode,refName=Message;ftype=messagecode,^\s*(\[A-Z\][A-Z]\d\d\d\d[EWI]):}{string:Message,ftype=message;}
   b. System out - Advanced Information - [{date:Date,locale=en,MM/dd/yy HH:mm:ss:mm:ss z}] {text:Thread ID,charsLength=8;ftype=threadid;} {text:Short Name,charsLength=13;ftype=shortname;} {map:Event Type,ftype=severity;,F=FATAL;E=ERROR;W=WARNING;A=AUdit;I=INFO;C=CONFIGURATION;D=DETAIL;O=SYSTEM OUTPUT;R=SYSTEM ERROR;Z=UNKNOWN} UOW={text:UOW,ftype=uow;} source={text:Source,ftype=source;}{block,start,emptiness=true} class={text:Class,ftype=class;}{method=(text:Method,ftype=method;){block,end,emptiness=true} org=(text:Organization,ftype=organization;){block,end,emptiness=true} prod=(text:Product,ftype=product;){block,end,emptiness=true} component=(text:Component,ftype=component;){block,end,emptiness=true} thread=(text:Thread Name,ftype=thread;){block,end,emptiness=true} {regexp:messagecode,refName=Message;ftype=messagecode,^\s*(\[A-Z\][A-Z]\d\d\d\d[EWI]):}{string:Message,ftype=message;}
   c. System err - [{date:Date,locale=en,MM/dd/yy HH:mm:ss:mm:ss z}] {text:Thread ID,charsLength=8;ftype=threadid;} {text:Short Name,charsLength=13;ftype=shortname;} {map:Event Type,ftype=severity;,F=FATAL;E=ERROR;W=WARNING;A=AUdit;I=INFO;C=CONFIGURATION;D=DETAIL;O=SYSTEM OUTPUT;R=SYSTEM ERROR;Z=UNKNOWN} {string:Message,ftype=message;}
   d. System start - [{date:Date,locale=en,MM/dd/yy HH:mm:ss:mm:ss z}] {text:Thread ID,charsLength=8;ftype=threadid;} {text:Short Name,charsLength=13;ftype=shortname;} {map:Event Type,ftype=severity;,F=FATAL;E=ERROR;W=WARNING;A=AUdit;I=INFO;C=CONFIGURATION;D=DETAIL;O=SYSTEM OUTPUT;R=SYSTEM ERROR;Z=UNKNOWN} {string:Message,ftype=message;}

YYYY/MM/DD HH:MM:SS [LEVEL] PID#TID: *CID MESSAGE
OUTPUT: R=SYSTEM ERROR; Z=UNKNOWN

System stop - [[date:Date, locale=en, MM/dd/yy HH:mm:ss:SSS z]] [text:Thread ID, charsLength=8; ftype=threadid;] [text:Short Name, charsLength=13; ftype=shortname;] [map:Event Type, ftype=severity; F=FATAL; E=ERROR; W=WARNING; A=Audit; I=INFO; C=CONFIGURATION; D=DETAIL; O=SYSTEM OUTPUT; R=SYSTEM ERROR; Z=UNKNOWN] (block, start, emptiness=true)

Native out - [[date:Date, locale=en, MM/dd/yy HH:mm:ss:SSS z]] [text:Thread ID, charsLength=8; ftype=threadid;] [text:Short Name, charsLength=13; ftype=shortname;] [map:Event Type, ftype=severity; F=FATAL; E=ERROR; W=WARNING; A=Audit; I=INFO; C=CONFIGURATION; D=DETAIL; O=SYSTEM OUTPUT; R=SYSTEM ERROR; Z=UNKNOWN] (block, start, emptiness=true)

Http erro - [[date:Date, locale=en, EEE, dd MMM yyyy HH:mm:ss z]] [priority:Severity, ftype=severity; DEBUG; INFO; WARN; ERROR; CRITICAL] [[geoip:Client IP, stopPattern=^\[\d+.:]+(:\d+)/; ftype=remoteip; type=country:region:city;] {text:Remote Port, ftype=remoteport;}] [text:Server Host, stopPattern=^\[\d+.:]+(:\d+); ftype=localip;] [text:Server Port, ftype=localport;] [string:Message, ftype=message;]

Http access - Basic Format - [geoip:Client IP, ftype=remoteip; type=;] [string:Remote Logical Username, ftype=remoteuser;] [string:Remote User, ftype=remoteuser;] [[date:Date, locale=en, dd/MMM/yyyy:HH:mm:ss z]] "{choice:Method, ftype=reqmethod; GET;POST} {string:URL, ftype=requrl;} {string:Query, ftype=querystring;} {string:reqprotocol, ftype=reqprotocol;}" {number:Status, ftype=respstatus;} {number:Bytes Sent, ftype=bytesent;}

Http access - Combined Format - [geoip:Client IP, ftype=remoteip; type=;] [string:Remote Logical Username, ftype=remoteuser;] [string:Remote User, ftype=remoteuser;] [[date:Date, locale=en, dd/MMM/yyyy:HH:mm:ss z]] "{choice:Method, ftype=reqmethod; GET;POST} {string:URL, ftype=requrl;} {block, start, emptiness=true} {string:Query, ftype=querystring;} {string:reqprotocol, ftype=reqprotocol;}" {number:Status, ftype=respstatus;} {number:Bytes Sent, ftype=bytesent;} "{string:Referer, ftype=referer;}" "{string:User Agent, ftype=useragent;}" "{string:Cookie, ftype=cookie;}"
<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>A Fatal message.</td>
</tr>
<tr>
<td>E</td>
<td>An Error message.</td>
</tr>
<tr>
<td>W</td>
<td>A Warning message.</td>
</tr>
<tr>
<td>A</td>
<td>An Audit message.</td>
</tr>
<tr>
<td>I</td>
<td>An Informational message.</td>
</tr>
<tr>
<td>C</td>
<td>An Configuration message.</td>
</tr>
<tr>
<td>D</td>
<td>A Detail message.</td>
</tr>
<tr>
<td>O</td>
<td>A message that was written directly to System.out by the user application or internal components.</td>
</tr>
<tr>
<td>R</td>
<td>A message that was written directly to System.err by the user application or internal components.</td>
</tr>
<tr>
<td>Z</td>
<td>A placeholder to indicate the type was not recognized.</td>
</tr>
</tbody>
</table>

### Managing Dashboards

An XpoLog Center Dashboard is a portal that contains gadgets. Multiple dashboards may be defined under an App context. The gadgets in the dashboards are used to display visual or textual information from the logs that exist in the XpoLog environment.

Each gadget displays the data that the user requested to view in the gadget’s definition. For example, three gadgets can be displayed in a dashboard for displaying search results, transactions list, and Analytics summary. Gadgets simplify and expedite performing searches and operations on the log file. For example, instead of going each time to the Search engine and running a search, you can define gadgets for viewing these search results in different visual manners.

XpoLog has an engine that enables customizing multiple dashboards, each for a different purpose. For example, you can define four dashboards – for application problems, performance problems, network issues, and security.

Each dashboard can contain multiple gadgets, with each gadget displayed in one of the available visualizations: Line chart, Bar chart, Column chart, Pie chart, Data table, Events list, etc. The gadgets can be organized within the dashboard in any of several predefined layouts. Also, any gadget can be dragged and dropped to a preferred location on the dashboard page.

To create a Dashboard see [Adding a Dashboard](#).

To see existing dashboards open the Apps console and click the App in which you wish to add/modify a dashboard.

The following icons which may be presented below a dashboard, indicate an important configuration of this dashboard:
The icon 📊 indicates that the dashboard is set as the system home page.
The icon 📈 indicates that the dashboard is scheduled to be exported.
The icon 📈 indicates that the dashboard is scheduled to be exported as part of its parent App's configuration. See App Settings.
The icon 🌐 indicates that the dashboard is running in an offline mode.

XpoLog enables management of a dashboard from menu entry of each dashboard. Mouse over a dashboard and click the icon to display the menu options, as follows:

- **View** – For opening the dashboard.
- **Close (optional)** – For closing a dashboard if it is open (I.E. currently being displayed).
- **Edit** – For defining the general settings of a dashboard - name, description, generation interval, time frame, export settings, etc. (See Dashboard Settings)
- **Duplicate** – For duplicating an existing dashboard and defining a new one on its basis.
- **Copy To** – For copying an existing dashboard to another App and defining a new one on its basis.
- **Move To** – For copying an existing dashboard to another App, without leaving the dashboard in the current App, and defining a new one on its basis.
- **Export Conf.** – For exporting a dashboard's configuration (all settings) and allow an import of its definition in another XpoLog (See Export / Import a Dashboard).
- **Delete** – For removing an existing dashboard.

Click a dashboard to enter its view and gadgets administration options.

### Adding a Dashboard

To add a new Dashboard to XpoLog:

1. In the main screen, click the Apps tab on the top left. The Apps management console is displayed. Select an App or create one then click it to enter.
2. Click the 'Add New Dashboard' entry in the menu on the left or the 'Add New Dashboard' icon in the main screen. Name the new Dashboard - a new dashboard is created.
3. Click the dashboard and add gadgets that visualizes data from the environment, or alternatively, load the dashboard by clicking the new dashboard and then select the 'Add Gadget' from the icon on the top right hand side of the Dashboard toolbar. See Managing Gadgets.
4. To edit a dashboard, mouse over the dashboard and click the icon, then click the 'Edit' entry to display the Dashboard Settings or alternatively, load the dashboard by clicking the new dashboard and then select the 'Edit Dashboard' from the icon on the top right hand side of the Dashboard toolbar.

### Removing a Dashboard

To remove a Dashboard from XpoLog:

1. In the main screen, click the Apps tab on the top left. The Apps management console is displayed. Select an App and click it to enter.
2. Mouse over the dashboard and click the icon, then click the 'Delete' entry and confirm the operation - the Dashboard will be deleted.

### Dashboard Settings

The dashboard settings contain different settings on the dashboard level. Unless changed individually, Gadgets inherit the dashboard's settings. There are several options to open the general settings of a dashboard:

1. In the dashboards screen, mouse over a dashboard and click the icon to displays the menu items and select Edit Dashboard.
2. Click a dashboard to load it and then select the 'Edit Dashboard' from the icon on the top right hand side of the Dashboard toolbar.

Dashboard's general settings screen is opened.

**General**

The general settings section allows to configure the Name and Description of a dashboard

**Time Settings**

The time settings section allows to configure the following:

- **Time Range**: the default dashboard time range which all gadgets will display by default unless configured individually otherwise. Time Range which is set to **Live** determines a real time execution of the dashboard - gadgets will not be generated in the background, results will be calculated and displayed in real time only and while the dashboards is opened.
- **Generation Frequency**: the frequency that new data will be processed and displayed in the gadgets. Generation frequency which is set to **Never** determines an offline mode of the dashboard - gadgets will be generated only on the exported time definition and/or on demand.

**Dashboard Sources**

The dashboard sources enables a generic definition of the dashboard's logs/folder/servers sources which will be added to all used search queries in the gadgets. For example if the dashboard should refer to servers x, y, z then it is possible to specify this directly in each gadget's search query. Alternatively, it is possible to use generic queries in the gadgets and specify the list of sources in the Dashboard Sources section.

Using Dashboard Sources makes it very simple to duplicate, maintain and manage the list of sources that will be analyzed by the dashboard.

**User Inputs**

Users Inputs provide an interface for users to supply values that effect gadgets search terms and displayed results based on their selection. Typically, the inputs are displayed in a checkbox, text area, dropdown menus or radio buttons.

The forms allow users to visually make selections which impact the underlying searches and focus only on points of interest while viewing dashboard's results.

There are 2 aspects the should be configured in order to use Inputs -

- **General Definition** (Dashboard's Settings section)
  In the Dashboard Settings section the general settings of the inputs are configured - type of input, input key, label, etc.
Based on these definitions the user inputs form at the top of a dashboard will be built and displayed.

- **Searches Definition** (Gadget's underlying searches)

  It is also mandatory to use inputs keys within the gadgets underlying searches so in case a user uses an input the correspondent gadget will be updated based on the selection.

### Export Settings

The export settings section determines if/when to export this dashboard.

- **Exporting Frequency**: a frequency, a specific time or several times in which the dashboard will be exported according the Export to Email / Export to File definition.
- **Exporting**:
  - The export mechanism supports an export of all selected dashboards as PDF and/or CSV files by email and/or by saving a file in the specified location.
    - Export To Email: the email settings that will be used when exporting the dashboard by email (for multiple recipients use a comma separated list).
    - Export To File: the format, location and retention settings that will be used when exporting the dashboard to files on the file system.

![Dashboard Export Settings](image)

Note: no images are exported in a CSV formatted file.

- XpoLog dashboards support definition of multiple export schedulers. Using more than one export scheduler allows a configuration of a specific date range and specified user inputs for each scheduled export. For example it is possible to configure on the same dashboard an export scheduler once a week on the last week in a daily granularity (per day view) and another scheduler once a day on the last day on an hourly granularity (per hour view) - the result will be a daily export presenting the last day on an hourly basis and a weekly export presenting the last week on a daily basis.

### User Inputs - General Definition

Users Inputs provide an interface for users to supply values that effect gadgets search terms and displayed results based on their selection. Typically, the inputs are displayed in a checkbox, text area, dropdown menus or radio buttons.

The forms allow users to visually make selections which impact the underlying searches and focus only on points of interest while viewing dashboard's results.
Configuring User Inputs:
The first part to configure inputs is done in the Dashboard's Settings section. Edit the Dashboard and you'll find a User Inputs section.

In the User Inputs section, Administrators define the list of Inputs to be available while viewing a dashboard. Each input has several settings:

- **General Settings:**
  - **Input Key** - The key is the unique identifier of an input in which is used in the underlying search within a gadget. Upon selection of a value in the input form in the dashboard, the selected value will be integrated in the query or queries that contains this key.

- **Display Settings:**
  - **Title** - The title of the input that is displayed in the inputs form above this input.
  - **Description** - The input's description.
  - **Visible** - Determines whether this input is displayed in the inputs form or not.
  - **Break Line** - Determines whether this input starts a new line in the inputs form or not.
  - **Advanced** - Determines if this input should be presented in the main inputs form (default) or should be displayed only in the advanced section of the inputs form.

- **Input Settings:**
  - **Input Type:**
    - **Text**
      - **Default Value** - The value that will be used by default (leave empty for empty default).
      - **Placeholder** - Text that will be displayed within the input text area to imply the user what the optional values are.
- **List**
  - Multiple Selection - Determines whether it is possible to select more than one value of the list or not
  - Show as Drop Down - Determines whether the list should be displayed as an horizontal values list or as a dropdown menu
  - List Type - Determines the type of list of this input:
    - Static - A static list of values entered by the administrator
    - Query Based - A dynamic list which is a result of a search query
    - Sources Based - A dynamic list of sources available in XpoLog (Logs, Folders, AppTags, Servers)
    - Predefined - Upload a key=value type of file which contains a list of values that will be displayed in the input

- **Checkbox**
  - Checked by Default - Allow a true/false type of input
  - Checkbox Label - The label to be displayed next to the checkbox

After completing the configuration and saving it, the configured inputs will be displayed at the upper part of the dashboard. However, using the inputs will have no effect at this point until the second part of configuring the gadgets underlying searches to use the inputs is completed.

**User Inputs - Searches Definition**

Users Inputs provide an interface for users to supply values that affect gadgets search terms and displayed results based on their selection. Typically, the inputs are displayed in a checkbox, text area, dropdown menus or radio buttons.

The forms allow users to visually make selections which impact the underlying searches and focus only on points of interest while viewing dashboard’s results.

Searches in the Gadgets within a dashboard

After the inputs are defined in the dashboard settings it is mandatory to configure the searches of the gadgets to use them in order to update a gadget’s result upon an input selection.

The syntax which is used in the search queries is \[XI:INPUT\_KEY\] - this value will be replaced by XpoLog when a user makes a selection in the inputs forms and clicks Apply, INPUT\_KEY stands for the input key configured in the dashboard settings inputs section.

For example:

1. In the dashboard settings create a Granularity input with a key 'interval'. Set it as a list of static values (1 second, 1 minute, 1 hour (default), etc.) and save:
1. In the dashboard itself you will see a drop down menu with the values of the Granularity input (with the default selected).

Note, at this point the gadget will not react to selections made on the input as the input key is not combined with the search query yet:

2. In the dashboard itself you will see a drop down menu with the values of the Granularity input (with the default selected).

Note, at this point the gadget will not react to selections made on the input as the input key is not combined with the search query yet:

3. Edit the gadget and combine the interval XpoLog Input as part of the query and save:


```
* | count | interval [X:interval] | display count as events over time
```

Notice the [X:interval] which will be used when a selection of the input's value will be made.

4. A selection of Granularity 'Minutes' and applying will display a different view of the gadget:

![Image of the gadget with different view](image)

**User Inputs - Example**

The following example demonstrates the step to add sources, granularity and search term to a gadget using User Inputs:

1. **Step I: Sources Input**

   The following input retrieves a list of logs defined in XpoLog under the 'XpoLog System Log' folder to be selected and combined in the search:
**Input Key:**

| sources |

*Used to reference the input's value from a search query*

**Display Settings**

| Title: | Log Sources |
| Description: | |

| Visible: | Show this input in the inputs panel |
| Break Line: | Place this input in a new line in the inputs panel |
| Advanced: | Show this input only in the advanced inputs panel |

**Input Settings**

| Input Type: | List |
| Multiple Selection: | Allow selection of multiple list entries |
| Show as Drop Down: | When list contains more than 3 entries |
| List Type: | Sources Based |
| Sources Type: | Logs |
| Sources Query: | * in folder.xpolog system logs |

**Result in Dashboard:**

[Dashboard Screen Screenshot]

**Query Used:**
```
* in [XI:sources] count | interval 1 hour | display count as events over time
```

Upon selection the query will run only on the selected log(s).

2. **Step II: Granularity Input**

The following input displays a list of granularity options to be selected and combined in the search:
(Note if a default is not selected, the gadget will wait to a selection to display the result)

Enter Title: Granularity

Description:

Visible: ✔ Show this input in the inputs panel

Break Line: □ Place this input in a new line in the inputs panel

Advanced: □ Show this input only in the advanced inputs panel

**Input Settings**

Input Type: List

Multiple Selection: □ Allow selection of multiple list entries

Show as Drop Down: Always

List Type: Static

<table>
<thead>
<tr>
<th>Value</th>
<th>Label</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 minute</td>
<td>Minutes</td>
<td></td>
</tr>
<tr>
<td>1 hour</td>
<td>Hours</td>
<td></td>
</tr>
<tr>
<td>1 day</td>
<td>Days</td>
<td></td>
</tr>
</tbody>
</table>

Result in Dashboard:
Query Used:

* in [XI:sources] | count | interval [XI:interval] | display count as events over time

Upon selection of sources the query will run only on the selected log(s) and upon selection of granularity the result will be displayed in the specified granularity.

3. Step III: Search Term Input

The following input displays a search term to be combined in the search if entered:
(Note if a default is not specified, the gadget will use * as the search term)

Input Key:

Search

Used to reference the input's value from a search query

Display Settings

Title:

Search

Description:

Bounding Box

Visible:

Show this input in the inputs panel

Break Line:

Place this input in a new line in the inputs panel

Advanced:

Show this input only in the advanced inputs panel

Input Settings

Input Type:

Text

Default Value:

Enter Search Here...
Result in Dashboard:

Query Used:

\([XI:\text{search}]) in [XI:\text{sources}] \mid \text{count} \lor \text{interval} [XI:\text{interval}] \lor \text{display count as events over time}\)

Upon entering a search term it will be used in the query, upon selection of sources the query will run only on the selected log(s) and upon selection of granularity the result will be displayed in the specified granularity.

Result:

The dashboard will now be loaded with the default values and will display the list of User Inputs to provide users with the ability to modify parameters and reload dashboard based on their selection.

For example - here's a view of the same dashboard on the last 1 hour, on a specific log (xpologlog) in Minutes interval and searching for only 'error or fail*' in that logs:

Dashboards Options

You can manage a Dashboard in XpoLog by using the options accessible by clicking the icon on the top right hand side of the Dashboard toolbar.

Available dashboard options are:

- **Add Gadget** – For adding a gadget to the dashboard. See Managing Gadgets in Administrator's Guide.
- **Edit Dashboard** – For Editing the general settings of a dashboards. See Dashboard Settings in the Administrator's Guide.
- **Save Layout** – If the Dashboard's layout was modified, click this option to save it as the default layout of this dashboard.
- **Reset Layout** – For resetting a layout back to its default in the current display.
- **Export to PDF** – For exporting the dashboard to a PDF file (see Exporting the Dashboard to a PDF/CSV).
- **Export to CSV** – For exporting the dashboard to a CSV file (see Exporting the Dashboard to a PDF/CSV).
Setting a Dashboard as Homepage

You can set a dashboard to appear on the homepage of XpoLog Center.

To set a dashboard as homepage:

1. Open the dashboard that you want to set as homepage, and click the
   icon on the top right hand side of the Dashboard toolbar.
2. Click the Set as Home Page.
   The Set Home Page dialog box opens.
3. Select the Default home page checkbox, and then click Save.
   The dashboard is set as the XpoLog homepage.

Note: each user may define a specific dashboard to be the home page. The system Administrator should define the dashboard which will be the default home page of XpoLog.

Export / Import a Dashboard

Exporting a Dashboard Configuration

Exporting a dashboard creates a zip file with the entire dashboard's configuration to enable future import in another XpoLog.

In the dashboards console under an App, mouse over a dashboard and click the
icon to displays the menu items and select Export Conf.

A zip file of the dashboard's configuration is created.

Importing a dashboard Configuration

Importing a dashboard enables a fast creation of a dashboard with its definition. To import a dashboard:

In the main Apps screen, click the App to which the dashboard should be imported to, on the left hand side, click the ‘Import Dashboard Conf.’, select the dashboard's configuration zip file and click the Import Dashboard button.

A new dashboard is created.

Managing Gadgets

Gadgets are the data visualization units which are displayed in dashboards. Multiple gadgets can be added to a single dashboard to visualize data in many forms and shapes such as line chart, area chart, bar chart, column chart, pie chart, events list or table, analytics summary, transactions list and more.

Adding a gadget is done from within a dashboard. After clicking a dashboard to load it, select the ‘Add Gadget’ from the
icon on the top right hand side of the Dashboard toolbar.

The Add a Gadget administration console opens:
Click one of the Visual Types to filter the list of available gadgets to that specific type or type the name in the search box to filter the list. By clicking the image of the selected type, the gadget’s administration screen will appear for defining the gadget.

To add a gadget to a dashboard:

1. Create a dashboard or load an existing dashboard to which you want to add a gadget, and select the ‘Add Gadget’ from the icon on the top right hand side of the Dashboard toolbar.
   The Select Gadget page opens, displaying the available gadget types.
2. Click a gadget type.
   A page opens for defining the information for the new gadget. Fill in the fields of the selected gadget type:

   - For a Line Chart gadget, see Adding a Line Chart Gadget
   - For a Pie Chart gadget, see Adding a Pie Chart Gadget
   - For a Column Chart gadget, see Adding a Column Chart Gadget
   - For a Bar Chart gadget, see Adding a Bar Chart Gadget
   - For an Area gadget, see Adding an Area Gadget
   - For a Scatter gadget, see Adding a Scatter Chart Gadget
   - For a Gauges gadget, see Adding a Gauge Gadget
   - For a Table gadget, see Adding a Table Gadget
   - For an Events gadget, see Adding an Events Gadget
   - For a Map gadget, see Adding a Map Gadget
   - For a Transactions gadget, see Adding a Transactions Gadget
   - For an Analytics gadget, see Adding an Analytics Gadget
Gadget Definition Principles

The definition screen of gadgets may slightly change based on the gadget type that was selected, however the principles of the definition are similar.

Below is an example of a 3D Pie Chart gadget definition screen that details the required information for generating the result:

- **Title** - enter a title for the gadget
- **Search Query** - enter the simple / complex search query that will be used by this gadget
- **Group By** - the result will be aggregated based on this selection (this option is disabled if entering a complex search query)
- **Time Range** - the time range that this gadget will generate its result on (by default gadgets inherit their parent dashboard's time range definition)
- **Max Number of Results** - specify the max number of results to be displayed
- **More Settings**
  - **Pie Type** - specify the pie type (in case of a pie - regular pie, donut or semi circle donut)
  - **3D** - specify if the selected type should be presented in 3D or 2D

**Note**: at any given time it is possible to click the 'Change gadget type' and select a different type using the used definitions.
Results Example:

Adding a Line Chart Gadget

Displays a line/spline chart showing a count over time or label of log events matching a given simple/complex Search query; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down. To add a Line Chart Gadget:

1. In Title, type a name for the gadget.
2. In Search Query, type the search query to run, based on the Search simple/complex syntax.
3. In Time Range, select the time frame following which the gadget display is to be refreshed.
4. In X-Axis, select the type of X-Axis to be displayed: Time or Label.
5. In Group By, select the grouping dimension of the result: None, Log, Application, or Server.
6. If available, click on More Settings in order to specify specific visualization options for this gadget.
7. Click the Save button.
   The gadget is saved in the dashboard.

Note: in the settings of some of the line charts gadgets it is possible to add plot bands which highlights a certain line in a selected color or paints an area.
Results Example:

Adding an Area Chart Gadget
Displays an area chart showing a count over time or label of log events matching a given simple/complex Search query; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down.

To add an Area Chart Gadget:

1. In **Title**, type a name for the gadget.
2. In **Search Query**, type the search query to run, based on the Search simple/complex search syntax.
3. In **Time Range**, select the time frame following which the gadget display is to be refreshed.
4. In **X-Axis**, select the type of X-Axis to be displayed: Time or Label.
5. In **Group By**, select the grouping dimension of the result: None, Log, Application, or Server.
6. If available, click on **More Settings** in order to specify specific visualization options for this gadget.
7. Click the **Save** button.
   
   The gadget is saved in the dashboard.

Results Examples:
Adding a Column Chart Gadget

Displays a column/stacked column chart showing a count over time or label of log events matching a given simple/complex Search query; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Column Chart Gadget:

1. In Title, type a name for the gadget.
2. In Search Query, type the search query to run, based on the Search simple/complex syntax.
3. In Time Range, select the time frame following which the gadget display is to be refreshed.
4. In X-Axis, select the type of X-Axis to be displayed: Time or Label.
5. In Group By, select the grouping dimension of the result: None, Log, Application, or Server.
6. In Max Number of Results, select the maximum number of events to be returned.
7. If available, click on More Settings in order to specify specific visualization options for this gadget.
8. Click the Save button.

The gadget is saved in the dashboard.

Results Examples:
Adding a Bar Chart Gadget

Displays a bar/stacked bar chart showing a count over time or label of log events matching a given simple/complex Search query; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Bar Chart Gadget:

1. In Title, type a name for the gadget.
2. In Search Query, type the search query to run, based on the Search simple/complex syntax.
3. In Time Range, select the time frame following which the gadget display is to be refreshed.
4. In X-Axis, select the type of X-Axis to be displayed: Time or Label.
5. In Group By, select the grouping dimension of the result: None, Log, Application, or Server.
6. In Max Number of Results, select the maximum number of events to be returned.
7. If available, click on More Settings in order to specify specific visualization options for this gadget.
8. Click the Save button.

The gadget is saved in the dashboard.

Results Examples:
Adding a Stacked Grouped Column Chart

Displays a stacked grouped column chart showing a count over time of log events matching a given simple/complex which are associated to another group; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Stacked Grouped Column Chart Gadget:

1. In Title, type a name for the gadget.
2. In Search Query, type the search query to run, based on the Search simple/complex syntax. This gadget requires 2 group by values one which will be used as the base category and the other which will be displayed as a stack on top of it.
3. In Time Range, select the time frame following which the gadget display is to be refreshed.
4. In X-Axis, the type of X-Axis will be Time.
5. In Group By, select the grouping dimension of the result: None, Log, Application, or Server.
6. In Category Fields, enter one of the groups names (used in the query 'group by') to be used as the base category.
7. If available, click on More Settings in order to specify specific visualization options for this gadget.
8. Click the Save button.

The gadget is saved in the dashboard.

Results Examples:

Adding a Pie Chart Gadget

Displays a pie/donut chart showing a count over time or label of log events matching a given simple/complex Search query; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Pie Chart Gadget:

1. In Title, type a name for the gadget.
2. In Search Query, type the search query to run, based on the Search simple/complex syntax.
3. In Group By, select the grouping dimension of the result: Log, Application, or Server.
4. In **Time Range**, select the time frame following which the gadget display is to be refreshed.
5. In **Max Number of Results**, select the maximum number of events to be returned.
6. If available, click on **More Settings** in order to specify specific visualization options for this gadget.
7. Click the **Save** button.

The gadget is saved in the dashboard.

**Results Examples:**

---

**Adding a Scatter Chart Gadget**

Displays a scatter chart showing a count over time or label of log events matching a given simple/complex Search query, grouped by log, application, or server; gadget has a [View in Search](#) link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Scatter Chart Gadget:

1. In **Title**, type a name for the gadget.
2. In **Search Query**, type the search query to run, based on the Search simple/complex search syntax.
3. In **Time Range**, select the time frame following which the gadget display is to be refreshed.
4. In **X-Axis**, select the type of X-Axis to be displayed: **Time** or **Label**.
5. In **Group By**, select the grouping dimension of the result: **None**, **Log**, **Application**, or **Server**.
6. If available, click on **More Settings** in order to specify specific visualization options for this gadget.
7. Click the **Save** button.

The gadget is saved in the dashboard.

**Results Examples:**

---

![3D Pie Chart](image)

**3D Pie Chart**

- [View in Search](#)

![3D Donut Chart](image)

**3D Donut Chart**

- [View in Search](#)

![3D Semi Circle Donut Chart](image)

**3D Semi Circle Donut Chart**

- [View in Search](#)
Adding a Heat Map Gadget

Displays a Heat Map chart showing a count over time or label of log events matching a given simple/complex Search query; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Line Chart Gadget:

1. In Title, type a name for the gadget.
2. In Search Query, type the search query to run, based on the Search simple/complex syntax.
3. In Time Range, select the time frame following which the gadget display is to be refreshed.
4. In X-Axis, select the type of X-Axis to be displayed: Time or Label.
5. In Group By, select the grouping dimension of the result: None, Log, Application, or Server (available if a simple search query is used).
6. If available, click on More Settings in order to specify specific visualization options for this gadget:
   a. Set Color Labeling Theme - 2 colors / 3 colors and distribution of the results in the Heat Map.
   b. Category Fields: if X-Axis is set to display label, enter the category in which will populate the X-Axis.
7. Click the Save button.
   The gadget is saved in the dashboard.

Adding a Gauge Gadget

Displays a gauge showing a result of a given simple/complex Search query; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Gauge Chart Gadget (Speedometer/VU Meter/Solid):

1. In Title, type a name for the gadget.
2. In Search Query, type the search query to run, based on the Search simple/complex syntax.
3. In Time Range, select the time frame following which the gadget display is to be refreshed.
4. Click on **More Settings** in order to specify specific min and max values for this gadget, label and plot bands colors for the different level between min and max.
5. Click the **Save** button.
   The gadget is saved in the dashboard.

Results Examples:

Adding a Table Gadget
Displays a search result table showing a count of log events matching a given simple/complex Search query, grouped by log, application, or server; gadget has a **View in Search** link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Table Gadget:

1. In **Title**, type a name for the gadget.
2. In **Search Query**, type the search query to run, based on the Search simple/complex syntax.
3. In **Display Columns**, type the names of the columns to be displayed separated by commas, or leave blank to display all columns.
4. In **Time Range**, select the time frame following which the gadget display is to be refreshed.
5. In **Group By**, select the grouping dimension of the result: **None**, **Log**, **Application**, or **Server**.
6. In **Max Number of Results**, select the maximum number of events to be returned.
7. Click the **Save** button.
   The gadget is saved in the dashboard.

Result Example:
Adding an Events Gadget

Displays a search result events showing log events matching a given Search query; gadget has a View in Search link that can be clicked to navigate to the XpoSearch search engine to perform a drill-down.

To add an Events Gadget:
1. In **Title**, type a name for the gadget.
2. In **Search Query**, type the search query to run, based on the Search simple/complex syntax.
3. In **Display Columns**, type the names of the columns to be displayed separated by commas, or leave blank to display all columns.
4. In **Time Range**, select the time frame following which the gadget display is to be refreshed.
5. In **Max Number of Events**, select the maximum number of events to be returned.
6. Click the **Save** button.

The gadget is saved in the dashboard.

Result Example:

Adding a Map Gadget

Displays a Geo IP map of the result of a given search, grouped by countries or cities; used to find the city or country of an IP address in a log record; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Map Gadget:
1. In **Title**, type a name for the gadget.
2. In **Search Query**, type the search query to run, based on the XpoSearch simple/complex search syntax.
3. In **Time Range**, select the time frame following which the gadget display is to be refreshed.
4. In **Group Type**, select the type of chart to be displayed: **Countries** or **Cities**.
5. In Max Number of Events, select the maximum number of events to be returned.
6. Click the Save button.
   The gadget is saved in the dashboard.

Result Examples:

Adding a Google Map

Displays a Geo IP map of the result of a given search based on Google Maps, grouped by countries or cities; used to find the city or country of an IP address in a log record; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Google Map Gadget:

1. In Title, type a name for the gadget.
2. In Search Query, type the search query to run, based on the XpoSearch simple/complex search syntax.
3. In Time Range, select the time frame following which the gadget display is to be refreshed.
4. In Group Type, select the type of chart to be displayed: Countries or Cities.
5. If available, click on More Settings in order to specify specific visualization options for this gadget:
   a. Map Center - by Data or by Specific location (determines the initial view when first loaded).
   b. Visualization - type of visualization to be displayed in the gadget.
   c. Set Color Theme - Heat Map style based on value, or one color.
   d. Set Color Labeling Theme - 2 colors / 3 colors and distribution of the results in the Map.
6. Click the Save button.
   The gadget is saved in the dashboard.

Note: Google Maps require internet connection - view and export by users requires connection only on the client side, scheduled export requires connection from the server.

Result Examples:
Adding a Transactions Gadget

Displays transactions list matching a given search; gadget has a View in Search link that can be clicked to navigate to the Search Console to perform a drill-down.

To add a Transactions Gadget:

1. In Title, type a name for the gadget.
2. In Search Query, type the search query to run, based on the XpoSearch simple/complex search syntax.
3. In Time Range, select the time frame following which the gadget display is to be refreshed.
4. In Max Number of Transactions, select the maximum number of transactions to be returned.
5. Click the Save button.

The gadget is saved in the dashboard.

Result Example:

Adding an Analytics Gadget

Displays log top problems and server problems detected by Analytics; gadget has a View in Analytics link that can be clicked to navigate to the Analytics Console to perform a drill-down.

To add an Analytics Gadget:

1. In Title, type a name for the gadget.
2. In **Time Range**, select the time frame following which the gadget display is to be refreshed.
3. Specify the **Data Sources** to be included in the Analytics view (server/folder/application/logs).
4. Click the **Save** button.
   The gadget is saved in the dashboard.

Result Examples:

![Analytics Problems Over Time](image)

![Analytics Log Problems](image)

**Search Administration**

By default, all the logs in XpoLog are being indexed. The indexing process enables extremely fast search on the log data and is highly recommended.

If you do wish to disable indexing on selected logs, it is possible under XpoLog Search > Administration.

**Note:** Logs which are not indexed will not be available for search in the Search console, their data will be collected and available in the Log Viewer only.

**Analytics Administration**

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 knowledgebase, 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 activated, **Servers Metrics Analysis** displays the CPU, memory, and disk problems on the source servers from which the logs originated. The problems definition for metrics can be easily customized to meet the environmental constraints.

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.

**Analytics Settings**

Under the Analytics Settings section (Analytics > Administration > Settings) the following options are available:

1. **General**
   - Customize the Analytics console default view:
     - **View By:** presenting the analysis based on Folders and Logs, Applications, or Server.
     - **View Type:** Total - presenting an analysis which summarizes the number of log events and problems that were scanned on each time slot. Risk - presenting an analysis which summarizes the severities of problems that were scanned on each time slot.
     - **Group By:** presenting an aggregated analysis of all logs (Summary View) or per each Folder/Application/Server independently (Split).
     - **Hierarchy Type:** presenting an analysis in the defined hierarchy of Folders/Applications/Servers (Hierarchical) or simply list each log independently (Flat).
     - **Show Metrics:** check this to present the metrics (CPU/Memory/Disk) measurements in the console (see below how to activate metrics measurements).
     - **Dates Range:** the default time frame that the Analytics console will load when first entering it.

   **Note:** the above settings determine the default view of the Analytics console when first entering it. The view may be easily changed by users while viewing the Analytics User Interface.

2. **Problems Management**
   - All Severity changes that were to automatically detected problems by users are centralized in this tab. System Administrators may customize or reset these changes as required.

3. **Metrics**
   - The Analytics console can measure servers metrics and present it side by side to the logs analysis. The Analytics measures metrics from servers over SSH and over the Windows network. Metrics information (CPU/Memory/Disk) is stored for as long as needed and presents historical view of servers CPU/Memory/Disk levels over time.
   - The control of the metrics sampling interval and problems definition of metrics analysis can be found under the Metrics tab.

   **Note:** In order to define a specific metrics policy (sampling interval and problems definition) to a server, you may override the global definition by going to: Analytics > Administration > Logs, select servers view and then right click the server you wish to edit and click the metrics link.

**Troubleshooting Analytics Metrics**

To verify the status of the capability of XpoLog to measure CPU/Memory/Disk Space (Metrics) of a remote server in XpoLog’s Analytics go to 'Analytics -> Administration -> Logs' and select 'View by Servers', click a server/right click a server and click "Verify Connection" to check the connectivity and get a metrics measurements validation.

**Windows machines:**

1) **RPC server is unavailable / Access is denied**
   - Problem description: Cannot access the RPC server on a remote computer.
   - Probable cause: This can be caused by the Windows Firewall service and Distributed Component Object Model (DCOM).
   - Solution: To allow connection to the remote computer:
     a. Make sure that the used host name is valid and that the server is running.
     b. Ensure that the user account that XpoLog uses is an administrator on the remote computer.
   - If the XpoLog user account is not an administrator on the remote computer, the user account has Remote Enable permission on the remote computer, then the user must also be given DCOM Remote Launch and Remote Activation privileges on the remote computer by running Dcomcnfg.exe at the command prompt.
   - c. Allow for remote administration on the remote computer.
   - You can use either the Group Policy editor (Gpedit.msc) or a script to enable the Windows Firewall: Allow remote administration exception, or use a NETSH firewall command at the command prompt to allow for remote administration on the remote computer.
   - The following command enables this feature:
     netsh firewall set service RemoteAdmin enable

   If you would rather use the Group Policy editor than the NETSH commands above, use the following steps in the Group Policy editor (Gpedit.msc) to enable "Allow Remote Administration" on the remote computer.
- Under the Local Computer Policy heading, double-click Computer Configuration.
- Double-click Administrative Templates, Network, Network Connections, and then Windows Firewall.
- If the computer is in the domain, then double-click Domain Profile; otherwise, double-click Standard Profile.
- Click Windows Firewall: Allow remote administration exception.
- On the Action menu, select Properties.
- Click Enable, and then click OK.

2) CScript is not recognized
- Problem description: The dynamic link library (DLL) VBScript.DLL is not properly installed on your computer.
- Probable cause: It is likely this file (VBScript.DLL) is missing
- Solution: run "regsvr32 VBScript" in a Command Prompt.

UNIX machines:

1) Command not found
- Problem description: One or more of the following commands executed on the machine could not be found - "date", "top", "df", "free"
- Solution: Ensure permissions are given to the user XpoLog is using for these commands. If required, install the command/s or the missing package or consult with your system administrator.

2) Account is missing
- Problem description: Failed to find the account associated with a host.
- Solution: Make sure that the account associated with this the host is defined properly:
  Go to 'Analytics -> Administration -> Logs' and select 'View by Servers'
  Select the server and click 'Verify Connection'. If the verification fails, click 'Edit Server' and select the 'Metrics' tab.
  Make sure the 'Connection Details' is set. If not, click 'new' and enter new connection details.
  Click 'Save' in the account page to save the newly defined account and then 'Save' in the server's edit window to save the server definitions.

3) Date command / format is missing
- Problem description: Failed to get date from the host.
- Solution: Contact your XpoLog administrator or XpoLog Support to verify XpoLog's configuration.

4) Failed to fetch
- Problem description: The metrics data (cpu, memory or disk space) could not be fetched
- Solution: Contact your XpoLog administrator or XpoLog Support to verify XpoLog's configuration.

5) Server type is unknown
- Problem description: May be caused when a server has a "NA" as the server type (like a server that has been created through a database account)
- Solution: Edit the server and set a proper connectivity account so that XpoLog can use to measure metrics, save it and verify that the connection is valid.

For more information please contact [XpoLog Support](mailto:).

**Changing a Severity of a Problem**

The Analytics engine presents two types of problems Predefined and Auto-Detected.

- **Predefined problems** are saved searches that a severity was assigned on, to change the severity please see [Editing a Saved Search](#).
- **Auto-Detected problems** are problems which were automatically detected by the Analytics engine. In the Analytics console at the bottom part 'Most Severe Problems' there's a menu on the right hand side next to each problem which allows a customization of the problem:
  - Change a severity of a problem
  - Exclude a problem from the future analyses (note: if you select this option, it will be used on future analyses and will not be removed from the existing analysis)

To see all changes that were made on Analytics problems see [Analytics Settings](#).

**Managing Analytics Members**

By default, all the logs are being analyzed by the Analytics engine. It is possible to customized which logs will be analyzed and which will be disabled under Analytics > Administration > Logs:

- Select the view type - Folders and Logs, Applications, or Server
- Select the Folder/Log/Application/Server and click the Enable / Disable button

Note: for Servers view, in case servers metrics is enabled in the system, you will be asked to enable/disable both Logs analysis originated from the selected server and the server metrics.

**Monitors Administration**

XpoLog comes with a built-in monitoring engine that enables you to monitor logs data and get alerts when defined criteria is met. The monitors
console presents all defined monitors, their last execution time, and their last status (failure = matching events were detected in the last execution and alerts were sent, success = matching events were not found in the last execution and alerts were not sent).

Alert Types
The monitors can be automated, and send alerts in various forms:

- Email - sends an email alerts to a list of users (make sure you have configured the required mail settings in XpoLog).
  - Email Alert Advanced options
    - Data Attachment: it is possible to add to the email alert the following:
      - Append event to end of email body: add to the email body the latest log event that triggered the alert in the current execution
      - Attach a dashboard: attach to the email one of the existing Dashboards
      - Attach matched events as: attach to the email all the records which triggered the alert in the current execution as a files from one of the selected types CSV / Tab Delimited / XML
    - Check to zip the attached file: in case 'Attach matched events as' is checked - determine whether the attachment will be zipped or not.
  - From Email Address: it is possible to customize the 'From' email address (by default the system email address will be used).
- SNMP Traps - sends a SNMP trap (make sure you have configured the required SNMP account in XpoLog).
- JMS Messages - sends a JMS message (make sure you have configured the required JMS account in XpoLog).
- Custom Scripting - open mechanism which executes any script as part of the monitor's failure.
  - Custom Scripting Details: it is possible to export all the records which triggered the alert in the current execution to a file (Program/Script path=CMD echo "export").
  - Custom Scripting Alert Advanced options:
    - Export Data: it is possible to export all the records which triggered the alert in the current execution to a file (it is also possible to export only selected fields under the Custom type) from one of the available types.
- REST API Call: it is possible to open a URL (POST/GET/PUT/DELETE) call and send information which was detected in the monitor execution.

NOTE: XpoLog can add additional information to the alerts from the logs and monitors which are executed such as log name, monitor name, log column content, etc. It is also possible to add selected log fields to monitor alerts by placing the following placeholders (case sensitive):

- [SEARCH_QUERY] = By default, the search query used in the search monitor is presented in the alert's subject. Occasionally, the search query may be long so it is possible to include this placeholder in the email body which will be replaced upon execution with the query.
- [END_OF_SUBJECT] = Used in the end of the message subject in case there is a need to exclude the search query from the subject.
- [COLUMN_NAME] = the name of the column which its content will be included
- [MONITOR_ID] = the unique id of the monitor
- [MONITOR_NAME] = the name of the monitor
- [MONITOR_STATUS] = the monitor status: 1 = failure, 0 = success
- [LOG_ID] = the log name that the included event is originated from
- [LOG_NAME] = the log name that the included event is originated from
- [HOST_NAME] = the host name that the included event is originated from
- [APPS_ID] = the application(s) name(s) that the included event is originated from
- [FOLDER_NAME] = the parent folder name that the included event is originated from

Defining a Search Monitor
XpoLog search monitor runs automatically by the system at scheduled intervals and execute a search query as its monitoring rule. The search monitor can be defined directly from the search console as well.

The following is a step by step flow to add a search monitor with alerts:

1. From The Monitors console (Manager > Log Actions > Monitors) - select Add Search Monitor.
2. Name the Monitor, and add the search query (simple or complex) you wish the monitor to execute.
3. Alerts - Add new Alert. If this is the first time XpoLog is configured to send alerts then you will be asked to enter details that XpoLog can use to send the requested alert. Create the alert and save it.
4. Schedule - configure the frequency that you wish for this monitor - based on the configured frequency the monitor will scan the log.
   - Never will turn off the scheduler and will not execute the monitor
   - Daily will run every day based on time interval (Repeat Every) or at a specific hour (Daily At)
   - Weekly - will run on the specified day(s) based on time interval (Repeat Every) or at a specific hour (Daily At)
   - Monthly - will run on the specified month(s) on a given day based on time interval (Repeat Every) or at a specific hour (Daily At)
5. Save it. It will run automatically based on the frequency you configured and it is also possible to execute a monitor manually if needed by selecting the monitor and click the execute button.

Note:
On each execution, the monitor scans only new records and not the entire log.

### Advanced section:

- Scan log from last scan point - determines whether the monitor will scan only new records in the log on each execution or the entire log either way. By default this option is selected.
- Failure - determines the fail criteria of a monitor. By default if a single record was found matched to the configured rule, it will be considered as a failure and the alerts will be triggered.
- Once failed, execute failure actions only after - after a failure, alerts will be sent again only after a specified number of additional failure without a success between.
- Once failed, execute failure actions for - by default the monitor executes the alerts on the latest record that was matched per each execution. This is the recommended option - the last event only. None of the events - no alerts will be sent, the first event only - a single alert on the first record that was matched per each execution, each event - the alerts will be triggered on each log record that was matched per each execution (not recommended since the number of records that may be found matched is not limited and the alert will be sent per each one).

In case each event is selected, it is recommended to limit the total number of alerts that may be sent per each execution (Maximum number of alerts to send).
- Positive Alerts - execute a positive alert as an indication that a specified time has passed since last failure.

### Defining a Log Monitor

XpoLog log monitor runs automatically by the system at scheduled intervals on a selected log and filter rule(s).

The following is a step by step flow to add a monitor with alerts on a log:

1. From The Monitors console (Manager > Log Actions > Monitors) - select Add Log Monitor.
2. Name the Monitor, and select the log that you wish to monitor from the existing logs in XpoLog, or define a new log.
3. Rules - select the rule(s) you wish to monitor from the existing rules on the selected log or define new rules (rules can be also regular expressions).
4. Alerts - Add new Alert. If this is the first time XpoLog is configured to send alerts then you will be asked to enter details that XpoLog can use to send the requested alert. Create the alert and save it.
5. Schedule - configure the frequency that you wish for this monitor - based on the configured frequency the monitor will scan the log.
6. Save it. It will run automatically based on the frequency you configured and it is also possible to execute a monitor manually if needed by selecting the monitor and click the execute button.

### Note:

- On each execution, the monitor scans only new records and not the entire log.
- It is also possible to configure the alerts to include the entire result or selected information from the matched log events:
  - Under the Advanced Section of the email alert you can attach data:
    - Append event to end of email body - matched log events will be included in the email body.
    - Attach matched events as a compressed Tab Delimited / CSV / XML file.
  - It is possible to add selected log fields to monitor alerts by placing the following place holders:
    - [COLUMN_NAME] = the name of the column which its content will be included
    - [MONITOR_ID] = the unique id of the monitor
    - [MONITOR_NAME] = the name of the monitor
    - [MONITOR_STATUS] = the monitor status : 1 = failure , 0 = success
    - [LOG_NAME] = the log name that the included event is originated from
    - [LOG_ID] = the log name that the included event is originated from
    - [MERGE_SOURCE_NAME] = the log name which triggers the alert will be included (relevant for merged logs)

### Advanced section:

- Scan log from last scan point - determines whether the monitor will scan only new records in the log on each execution or the entire log either way. By default this option is selected.
- Failure - determines the fail criteria of a monitor. By default if a single record was found matched to the configured rule, it will be considered as a failure and the alerts will be triggered.
- Once failed, execute failure actions only after - after a failure, alerts will be sent again only after a specified number of additional failure without a success between.
- Once failed, execute failure actions for - by default the monitor executes the alerts on the latest record that was matched per each execution. This is the recommended option - the last event only. None of the events - no alerts will be sent, the first event only - a single alert on the first record that was matched per each execution, each event - the alerts will be triggered on each log record that was matched per each execution (not recommended since the number of records that may be found matched is not limited and the alert will be sent per each one).

In case each event is selected, it is recommended to limit the total number of alerts that may be sent per each execution (Maximum number of alerts to send).
- Positive Alerts - execute a positive alert as an indication that a specified time has passed since last failure.
number of additional failure without a success between.

- Once failed, execute failure actions for - by default the monitor executes the alerts on the latest record that was matched per each execution. This is the recommended option - the last event only. None of the events - no alerts will be sent, the first event only - a single alert on the first record that was matched per each execution, each event - the alerts will be triggered on each log record that was matched per each execution (not recommended since the number of records that may be found matched is not limited and the alert will be sent per each one).

In case each event is selected, it is recommended to limit the total number of alerts that may be sent per each execution (Maximum number of alerts to send).

- Positive Alerts - execute a positive alert as an indication that a specified time has passed since last failure.

**Defining Monitors Group**

XpoLog monitor group is an entity containing multiple monitors which can be executed as a group.

The following is a step by step flow to add a monitor group:

1. From The Monitors console (Manager > Log Actions > Monitors) - select Add New Group.
2. Name the Monitor, and select the monitors that you wish to include as part of this group.
3. Alerts - Add new Alert. If this is the first time XpoLog is configured to send alerts then you will be asked to enter details that XpoLog can use to send the requested alert. Create the alert and save it.
4. Schedule - configure the frequency that you wish for this monitor - based on the configured frequency the monitor will scan the log.
5. Save it. It will run automatically based on the frequency you configured and it is also possible to execute a monitor manually if needed by selecting the monitor and click the execute button.

**Advanced section:**

- Failure - determines the fail criteria of a monitor. By default if a single monitor from the group members will fail, it will be considered as a group failure and the alerts will be triggered.
- Once failed, execute failure actions only after - after a failure, alerts will be sent again only after a specified number of additional failure without a success between.
- Positive Alerts - execute a positive alert as an indication that a specified time has passed since last failure.

**Management Console for Cloud Accounts**

Address Book is used for adding accounts for connecting to sources of logs. Logs or log directories from these sources can then be added to XpoLog. Some of the account types that can be added are dedicated to one source, such as SSH, which is connected to one machine that can have many logs. However, there are also three cloud accounts that can be added – **Google App Engine**, **Amazon Web Services**, and **Hadoop**. These accounts, which are encased in a cloud, manage many applications that have many logs. For these cloud accounts that can access large quantities of data in many logs, XpoLog provides separate Console Management for integration to cloud (big data). Based on these cloud accounts, data can be added to XpoLog from the clouds accessed through these accounts.

To integrate to the cloud:

1. In XpoLog Manager, in the menu, select **Administration > Cloud**.
   The Cloud and Big Data Configuration Management console opens for managing the cloud accounts.

**AppTags**

The implementation of AppTag is optional in XpoLog Center, and is used mainly for data enrichment.

An AppTag is a logical tagging of different elements that exist in XpoLog Center. The AppTag definition includes a set of static parameters that describe the application, and a set of the members that compose the application, such as folders, logs, accounts, dashboards, or anything else that is configured in XpoLog.

The AppTags console enables administrators to enrich the data with logical groupings by defining the AppTags that participate in the log. These AppTags can include data from multiple logs or servers. The AppTags console presents all the AppTags defined in XpoLog and enables administrators to create new ones, and modify and delete existing AppTags.

The implementation of AppTags has the following advantages:

- Search can be run at the AppTag level. For example: **error in AppTag.<appl name>**
- In Analytics, can see analysis according to AppTags (I.E. Applications).
- Security can be managed at the AppTag/application level. Users who enter the application under an AppTag context can only view the members under that AppTag definition.
Adding an AppTag

To add an AppTag:

1. In the Administration menu, select AppTags.
   The AppTags console is displayed. AppTags defined in XpoLog Manager are listed.
2. In the AppTags console, click the New AppTag button.
   The Add AppTag console is displayed.
3. In Name, type a name for the new AppTag.
4. In Description, type a description of the new AppTag (optional).
5. Available tabs:
   a. Members tab, and select the members of the application (see Mapping Sources by AppTag).
   b. Security tab (displayed only if security is active), set the view and edit permissions of users/groups related to the AppTag.
   c. Localization tab (displayed only if security is active and if the Apply AppTags time zone is selected under Advanced General Settings), set the set the specific time of the AppTag.
6. Click the Save button.
   The new AppTag is saved in XpoLog Center.

Mapping Sources by AppTag

When adding an AppTag to the system, you should associate with the AppTag all members, i.e. system elements connected to the AppTag. This association enables managing a minienvironment in the system. Only those selected members will be available to users who are authorized to use the AppTag.

To associate members with an AppTag:

1. In the Add AppTag console, click the Members tab.
2. Click a member type, and then select the checkboxes of the members to associate with the AppTag.
3. Repeat step 2 for all member types, as required.
4. Click Save.
   The members are associated with the AppTag.

Editing an AppTag

You can modify the name, description, and/or members of an AppTag.

To modify an AppTag:

1. In the Administration menu, select AppTags.
   The AppTags console is displayed. AppTags defined in XpoLog Manager are listed.
2. Select an AppTag, and then click the Edit button.
   The Edit AppTag console is displayed.
3. Modify the Name, Description, or the members of the AppTag (see Adding an AppTag).
4. Click the Save button.
   The AppTag is updated in XpoLog Center.

Removing an AppTag

You can remove from XpoLog an AppTag and its members, or an AppTag only.

To remove an AppTag from XpoLog:

1. In the Administration menu, select AppTags.
   The AppTags console is displayed. AppTags defined in XpoLog Manager are listed.
2. Select an AppTag, and then click the Delete button.
   The Delete confirmation box is displayed.
3. Select one of the following: AppTag and members or AppTag only.
   Depending on your selection, the selected AppTag and its members, or the AppTag only are deleted from XpoLog.

Address Book

Address Book displays a listing of all the connectivity accounts that are available in XpoLog for connecting to remote data sources. These accounts contain information regarding remote protocol connections, databases, and emails. This information includes the account’s name and description, and specific information pertaining to the specific account type, such as host address, port, username, and password in the case of an SSH account, or the email address in the case of an email account. These accounts are required for adding a log from a remote source, such as a database log, as well as for a variety of other operations, such as exporting logs and modules and defining SQL queries on previously defined logs.

In Address Book, you can create and manage the connectivity accounts, including modifying, enabling, disabling, and removing account(s).

Creating an Account

XpoLog enables creating the following types of accounts: Amazon Web Services, Database, Email, Google App Engine, Hadoop, JMS, Remote XpoLog, SNMP, SSH, and Windows Authentication. The following sections describe how to create each of these accounts.
To create an account:

1. In the Log Manager toolbar, click **Tools > Address Book**. A list of all accounts is displayed. Buttons are provided for creating a new account, and enabling, disabling, editing, deleting, or verifying an account.
2. In Address Book, click **New Account**. A list of available account types is displayed.
3. Select the option button of the type of account that you want to create, and then click the **Continue** button. The configuration page for the selected account type is displayed.
4. Configure the account. See the sections below for the configuration procedures of the various account types.
5. Click **Save**. The new account is saved in Address Book.

**Note:** After saving the account in Address Book, it is recommended to click the **Verify** button to ensure that XpoLog can establish a valid connection to the newly created account.

**Configuring an Amazon Web Services Account**

An Amazon Web Services (AWS) account enables you to access data stored in files and folders in the Amazon server.

The following are required to use any service on Amazon Web Services:

- **Access Key ID** – the username; an alphanumeric text string that uniquely identifies the user who owns the account. No two accounts can have the same AWS Access Key ID.
- **Secret Access Key** – plays the role of a password. It is secret, as it should be known to the owner only.

The following procedure describes how to configure the parameters of an Amazon Web Services account.

To configure an Amazon Web Services account:

1. In **Name**, type the name of the new account.
3. In **Access Key ID**, type the identification name for signing into AWS.
4. In **Secret Access Key**, type the password for signing into AWS.
5. In **Default Region**, select the geographical area where you want to access data.

**Configuring a Database Account**

The following procedure describes how to configure the parameters of a database account.

**Note:** Not all fields apply to all database types.

To configure a database account:

1. In the Database Types page, select a database type and click the **Create Account** button OR Double-click the database type.
2. In **Name**, type the name of the new database account. The default is the database type.
4. In **Host Address**, type the address of the machine on which the database is installed. Default: localhost.
5. In **Port**, type the port number on which the database accepts connections.
6. In **Database Name**, type the name of the database to connect to.
7. In **Username** and **Password**, type the username and password (optional) required for connecting to the database.
8. In **Connection string params**, type the names of the parameters that should be passed upon connection. Optional.

Creating a Data Source

If you choose to add a Data Source (and not define a database account), you should specify the following configuration details: Name: the name of the data source. Description (optional): the description of the data source. JNDI Name: the JNDI name of the data source. Environment Properties (optional) Database Type: select the type of database the data source will work against (choose 'other' for an unknown database).· Click the 'Save' button to save the new account.· Verify the account the ensure XpoLog can establish a valid connection.

**Configuring an Email Account**

The following procedure describes how to configure the parameters of an Email account.

To configure an Email account:

1. In **Name**, type the name of the new account.
3. In **Email Address**, type one or multiple email addresses used by the account. Separate multiple email addresses with a semicolon.

**Configuring a Google App Engine Account**
The following procedure describes how to configure the parameters of a Google App Engine account.

To configure a Google App Engine account:

1. In **Name**, type the name of the new account.
3. In **Email** and **Password**, type the email address and password required to sign on to the Google App Engine account.

### Configuring a Hadoop Account

The following procedure describes how to configure the parameters of a Hadoop account.

**Note:** Only connections to Hadoop version 0.20.203.0 and later are supported.

To configure a Hadoop account:

1. In **Name**, type the name of the new account.
3. In **Host Address**, type the the host name / IP address of the Hadoop environment.
4. In **Port**, type the port number on which the remote host accepts Hadoop connections.

### Configuring a JMS Account

The following procedure describes how to configure the parameters of a JMS account.

To configure a JMS account:

1. In **Name**, type the name of the new account.
3. In **JNDI Context**, type the the full JNDI context.
4. In **JNDI Provider URL**, type the URL to be used to access the JNDI provider.
5. In **Username** and **Password**, type the username and password required for connecting to the JNDI provider. Optional.
6. In **JMS Topic Factory**, type the JNDI name of the JMS topic factory.
7. In **JMS Queue Factory**, type the JNDI name of the JMS queue factory.

### Configuring a Remote XpoLog Account

The following procedure describes how to configure a Remote XpoLog account for communicating to a remote instance of XpoLog over HTTP/S. It is mandatory that the respective HTTP/S ports will be opened to enable the communication.

To configure a Remote XpoLog account:

1. In **Name**, type the name of the new account.
3. In **Host Address**, type the host name / IP address of the remote XpoLog.
4. In **Protocol**, select whether the remote XpoLog listens on HTTP or HTTPS.
5. In **URL Context**, type the context under which the remote XpoLog is deployed (optional). Default: `logeye`.
6. In **Port**, type the number of the port on which the remote XpoLog listens. Default: 30303 for HTTP; 30443 for HTTPS
7. In **Username** and **Password**, type the username and password required to log in to the remote XpoLog, in case security is activated on the remote XpoLog. Optional.
8. Check the enabled check-box if you wish this account to be enabled or un-check it to disable it. Disabled accounts will not allow the communication to the remote XpoLog instance.
9. **Account Type:**
   a. **Proxy** - use this type if the remote XpoLog instance is processing the logs remotely and the current XpoLog instance should only send queries to it and receive the results. In this mode the data itself will not be collected to the current XpoLog instance but will be available for searches and view.
   b. **Agent** - use this type if the remote XpoLog instance is used as an agent, I.E. the remote XpoLog instance is used to allow access to the remote environment and all the logs that will be added from the remote XpoLog instance will be collected by the current XpoLog instance. Usually, when this mode is selected the remote XpoLog instance should also be set to ‘Agent Mode’ to reduce its footprint to minimum on the remote server.

### Advanced Remote XpoLog Account Settings

Advanced Settings enable you to configure configuration synchronization. When activated, the configuration synchronization makes sure that for each log that exists in the remote instance, a remote log will be created in the local instance. Note that deleting a log in the remote instance will not delete the remote log in the local instance.

To configure advanced settings:

- **Click Advanced Settings.**
  The Advanced Settings section opens, with the Synchronize Configuration subsection.

#### Network Settings

In Network Settings, you can configure the following:

- **Compress Traffic** – You can determine whether the traffic against the host will be compressed or not. By default, the traffic is compressed.
To configure network settings:

1. Click **Network Settings**.
   The Network Settings section opens.
2. Select the **Compress Traffic** checkbox.

Synchronize Configuration

In Synchronize Configuration, you can configure the following:

- **Enable remote configuration synchronization** – You can enable the remote synchronization in order to create a remote log in the local instance for each new log that is created in the remote instance.
- **Parent Folder** – Specify the parent folder of new logs.
- **Remote Time Zone** – Specify the time zone of new logs.
- **Collection Policy** – Specify the collection policy of new logs.

To configure synchronize configuration:

1. Click **Synchronize Configuration**.
   The Synchronize Configuration section opens.
2. Select the **Enable remote configuration synchronization** checkbox.
3. Specify the parent folder of new logs:
   a. Select the **Use default parent folder** option in order to place the new logs under a folder named after the account.
   b. Select the **Use a specific parent folder** option in order to select a specific parent folder for the new logs.
4. Specify the time zone of new logs.
5. Specify the collection policy of new logs.

**Configuring an SNMP Account**

The following procedure describes how to configure an SNMP account.

To configure an SNMP account:

1. In **Name**, type the name of the new account.
3. In **Host**, type the host name/IP address of the remote host.
4. In **Port**, type the port number on which the remote host accepts SNMP traps.
5. In **Version**, select the version of SNMP to be used.
6. In **Protocol**, select the protocol to be used.
7. Select the **Use Proxy** checkbox to use the proxy; otherwise, leave cleared. Optional.

**Configuring an SSH Account**

The following procedure describes how to configure an SSH account.

SSH accounts can be enabled or disabled. If disabled, all related activity using the SSH account is suspended in XpoLog.

To configure an SSH account:

1. In **Name**, type the name of the new account.
3. In **Host Address**, type the host name/IP address of the remote host.
4. In **Port**, type the port number on which the remote host accepts SSH connections. Default: 22
5. In **Username** and **Password**, type the username and password required for connecting to the remote host.
6. Select the **Enabled** checkbox to enable the account; otherwise, to disable, leave cleared. Optional.
7. Configure advanced settings, as required. See Advanced SSH Account Settings section below.

**Advanced SSH Account Settings**

Advanced Settings enable you to configure advanced general settings and customize the account policy.

To configure advanced settings:

- **Click Advanced Settings**.
  The Advanced Settings section opens, with the General Settings and Account Policy subsections.

**General Settings**

In General Settings, you can configure the following:

- **Private Key Path** – In cases where a private key is used to authenticate with the specified host (when the private key path is configured - the password for connecting to the remote host is optional).
- **SCP** – The default file transfer protocol is SFTP (SSH File Transfer Protocol). However, if the remote host does not support SFTP for file transfer, you can use SCP (Secure Copy Protocol).
- **Administrator Email Address** – The email address of the system administrator to be notified when an SSH policy is breached.

To configure general settings:

1. Click **General Settings**.
   The General Settings section opens.
In Private Key Path, if private key authentication is used, type the path to the private key that XpoLog can use.

3. Select the SCP checkbox if the remote host does not support SFTP for file transfer.

4. In Administrator Email Address, type the email address of the system administrator to be notified upon connection failure.

Account Policy

In Account Policy, you can customize a specific account policy, instead of using the default policy for the SSH account, as configured in the Connection Policy tab of the Settings > General page.

To customize the account policy:

1. Click Account Policy.
   The Account Policy section opens.
2. Select the Define a Custom Policy option, and configure the custom policy’s settings. For a full explanation of the settings, see Settings > General, the Connection Policy tab.

Configuring a Windows Authentication Account

The following procedure describes how to configure the parameters of a Windows Authentication account.

To configure a Windows Authentication account:

1. In Name, type the name of the new account.
2. In Description, type a short description of the new account. Optional.
3. In Domain, type the name of the domain in which the user is defined.
4. In Username and Password, type the username and password (optional) for connecting to the Windows Authentication account.

Configuring an Amazon Web Services (AWS) S3 Bucket Account

The following procedure describes how to configure the parameters of an AWS S3 Bucket account.

To configure a AWS S3 Bucket account:

1. In Name, type the name of the new account.
2. In Description, type a short description of the new account. Optional.
3. In Access Key, type the access key of the AWS S3.
4. In Secret Key and Password, type the secret key of the AWS S3.

Disclaimer: Xpolog stores all passwords using industry standard algorithms.

Editing an Account

You can modify the settings of any account.

To edit an account:

1. In the Address Book, select an account from the list of accounts, and click the Edit button.
   The settings of the account are displayed.
2. Modify the parameters of the account, as required. See a detailed explanation of the parameters for each type of account in Address Book.
3. Click Save.
   The account settings are updated in the system.

Enabling/Disabling an Account

You can enable a disabled SSH/Remote XpoLog account, or disable an enabled SSH/Remote XpoLog account.

To enable a disabled account:

- In the Address Book, select an account from the list of accounts, and click the Enable button.
  The account becomes enabled.

To disable an enabled account:

- In the Address Book, select an account from the list of accounts, and click the Disable button.
  The account becomes disabled.

Removing an Account

You can remove from the XpoLog address book an account that you no longer require.

To remove an account:
1. In Address Book, select an account, and then click the **Delete** button.
   A Delete confirmation box is displayed.
2. Click **OK**.
   The account is deleted from the Address Book.

### Verifying an Account

You can verify any account in the system.
To verify an account:

1. In the Address Book, select an account from the list of accounts, and click the **Verify** button.
   The Account Verification dialog box opens, and verification begins.
2. When verification is complete, click the **OK** button.

### Templates

A Template is a complete configuration set for a certain log type: its definition includes the log data pattern, filters, and metadata. Usage of templates accelerates and automates the configuration process of logs added to or updated in XpoLog.

Administrators can perform the following actions related to templates:

- View templates (see **Viewing XpoLog Templates**)
- Save a log as a template (see **Saving a Log as a Template**)
- Create a log based on a template (see **Creating a Log Based On a Template**)
- Apply a template on multiple logs (see **Applying a Template on Multiple Logs**)
- Import a template from another XpoLog system (see **Importing a Template**)
- Export a template to another XpoLog system (see **Exporting a Template**)
- Delete a template from the system (see **Deleting a Template**)

### Viewing XpoLog Templates

You can view a listing of all templates defined in XpoLog.
To view the XpoLog templates:

- In XpoLog Manager, select the **Configuration > Templates** menu item.

  The Templates console opens, displaying an alphabetically sorted list of templates. The first letters of the template names in the list are highlighted in the Filtering Area above the list.

### Quickly Navigating to a Template

The Filtering Area above the lists of templates enables quick navigation to a template beginning with a specific letter. The letters which begin the template names in the list are highlighted in the Filtering Area. This is a convenient feature in systems that have many templates.
To quickly navigate to a template:

- Click a highlighted letter above one of the template groups.
  The template names beginning with that letter are displayed.

### Saving a Log as a Template

You can save any log in the system that is opened in the Log Viewer, as a template. The file structure, patterns, and customization (if it exists) of the log are all saved in the template. This template is then available for applying on other logs in XpoLog.
To save a log as a template:

1. In XpoLog Manager left pane, in the Folders and Logs tree, select any log in the system.
   The log records are displayed in the Log Viewer.
2. Select the **Configuration > Save as Template** menu item.
   The Save Template page is displayed.
   **Note:** A log must be selected before selecting **Configuration > Save as Template. Otherwise, an error occurs.**
3. Select one of the following:
   a. **Overwrite an existing template:**
      i. Select an existing template from the templates’ list.
      **Note:** the template will be overwritten by the configuration of the log that is currently being saved as the template. The template's **Name** and **Description** will remain as before.
   b. **Create a new template:**
      i. Type a **Name** for the template
      ii. Type a **Description** for the template
      iii. Type a **Unique Identifier** for the template - it is mainly used when XpoLog receive data with a 'Type' - then it applied the template's configuration automatically on the received data if the template's Unique Identifier matches the received type (in XpoLog Listeners for example).
4. Click **Save**.
   The Templates page opens, displaying the new template name on the templates list.
Templates Advanced Configuration:

1. Include template while running wizard
   Determines whether to match this template to detected logs during the add logs directory process
2. Use template's validation while running wizard
   If checked, the data from the log file will be matched to the template's pattern in addition to matching the log file name
   If not checked, only log file name will be matched to the template
3. Ignore file's name expression
   If checked, the log file name in the template will be ignored and the template will be matched to the log file by either searching for a text in the header of the file, or applying an expression that will "replace" the log file's name

Creating a Log Based On a Template

You can create a log from any template defined in XpoLog.
To create a log based on a template:

1. Open the list of templates in the system (see Viewing XpoLog Templates).
2. In the Templates list, click the Create Log link to the right of the template from which you want to create a log.
   The Edit Log page opens, with all the details of the template, besides for its name.
3. In Log Name, type a name for the new log.
4. If necessary, click Next to edit the configuration of the newly created log.
5. Click Save.
   The log configuration is saved, and the log name appears under the Folders and Logs tree in the left navigation pane of the Log Viewer.

Applying a Template on Multiple Logs

You can update the configuration of multiple logs that exist in XpoLog, based on a single template. For example, you can add a column to 10 logs of the same type residing in your XpoLog system, by creating or updating a single template, and applying it on all the logs. For logs having log names with common characters, this can be done by specifying in the log name, the common characters of the logs' log names, and an asterisk as placeholder for uncommon characters in the log names. For example, to apply a template on logs with log names beginning with access, you can enter the log name access*. Alternately, and especially when the log names do not contain common characters, you can select the checkbox of each log name on which to apply the template.
To apply a template on multiple logs:

1. Open the list of templates in the system (see Viewing XpoLog Templates).
2. Click apply template on logs near the template that you want to apply on multiple logs.
   The Specify Template Target Logs page appears, for specifying the logs on which to apply the template.
3. Do one of the following:
   - Select the Specify log name option, and in Log Name, type the name of the log or a name that can represent a group of logs (for example, access*).
   - Select the Select folders and logs option, open the Folders and Logs tree to show the relevant logs, and select the checkboxes of the logs on which to apply the selected template.
4. Click the Apply button.
   The configuration of the selected logs is updated according to the selected template.

Importing a Template

Templates can be imported from another XpoLog system. The names of imported templates appear in the list of templates on the Templates page.
To import a template:

1. In XpoLog Manager, select the Configuration > Import Templates menu item.
   The Import Templates page opens.
2. In Path, browse to the template archive file, and select the template '<name>.zip' file or type the Network URL to import, and then click the next link.
   The template is imported into XpoLog, and the Templates page opens, displaying its name in the templates list.

Exporting a Template

Templates can be exported as a Zip file to a template archive file, from where they can be imported to another XpoLog system.
To export a template:

1. In XpoLog Manager, select the Configuration > Export Templates menu item.
   The Export Templates page opens.
2. Select the checkboxes of the templates to export, and then click the export link.
3. Download and save the '<name>.zip' file in a template archive file.

Deleting a Template

You can delete from XpoLog a template, provided that logs in the system are not based on this template.
To delete a template from XpoLog:

1. Open the list of templates in the system (see Viewing XpoLog Templates).
2. Click Delete near the template that you want to delete.
   Operation Verification page requests confirmation of the template removal.
3. Click OK.
   The template is removed from XpoLog and no longer appears on the list.

Tasks

Tasks are operations that can be activated by XpoLog in a scheduled or manual manner. The Tasks console presents all the tasks that are available in XpoLog, and enables creating, duplicating, modifying, executing, and removing tasks.

To open the Tasks console:

- In the XpoLog Manager menu, select Tools > Tasks.
  The Tasks console opens.

Adding a Task

The following types of tasks can be added to XpoLog:

- Add Logs Directory – see Adding an Add Logs Directory Task
- Batch Execution – see Adding a Batch Execution Task
- Collection to Database – see Adding a Collection to Database Task
- Email – see Adding an Email Task
- JMS Message – see Adding a JMS Message Task
- SNMP Trap – see Adding an SNMP Trap Task
- SSH Execution – see Adding an SSH Execution Task
- URL – see Adding a URL Task

Adding a Batch Execution Task

A Batch Execution task executes a script or program according to the defined configuration – name of the program or script, arguments, environment variables, and working directory.

To add a Batch Execution task:

1. Open the Tasks console (see Tasks), and click the New Task button
   OR
   In the XpoLog Manager homepage, under More Actions, click Add Task.
2. In the page that opens, select the Batch Execution option, and then click Continue.
   The Batch Execution Task page opens.
3. In Name, type the name of the new task.
4. In Description, type a description of the new task; optional.
5. In Program/Script Path, type the name of the program/script to be executed by the task.
6. In Arguments, type the arguments needed for the program/script to run, separated by spaces.
7. In Environment Variables, type the environment variables needed for the program/script to run; optional.
8. In Working Directory, type the name of the directory from which the program/script should be run; optional.
9. In Output Target File, type the path to the file where output of the program/script execution is to be written; optional.
10. Select the Add Optional Params checkbox to include in the output file the date, account name, host name, and username.
11. To automate task execution, open the Schedule tab, and configure the scheduler as described in Scheduling a Task.
12. Click Save.
   The Batch Execution task is saved.

Adding a Collection to Database Task

A Collection to Database task exports data from an XpoLog log into a specified database.

To add a Collection to Database task:

1. Open the Tasks console (see Tasks), and click the New Task button
   OR
   In the XpoLog Manager homepage, under More Actions, click Add Task.
2. In the page that opens, select the Collection to Database option, and then click Continue.
   The Collection to Database Task page opens.
3. In Name, type the name of the new task.
4. In Description, type a description of the new task; optional.
5. In Log, click Select log, and in the Select Log to Collect window that opens, select a log to export to a database.
6. In Data Filter Query, type a query to filter out events that do not satisfy the above query.
7. In Connection Details, select the Database account to use, or click New to define a new Database account (see Creating an Account).
8. Enter the table name into which data is to be exported. Under 'database advanced settings', you can see the CREATE TABLE and INSERT statements that will be used.
9. To automate task execution, open the Schedule tab, and configure the scheduler as described in Scheduling a Task.
10. Click Save.
    The Collection to Database task is saved.
Adding a JMS Message Task

A JMS message task sends a JMS message using a JMS account. You can automate task execution by configuring a scheduler on it. XpoLog will run the task based on the scheduler configuration.

To add a JMS Message task:

1. Open the Tasks console (see Tasks), and click the New Task button
   OR
   In the XpoLog Manager homepage, under More Actions, click Add Task.
2. In the page that opens, select the JMS Message option, and then click Continue.
   The JMS Message Task page opens.
3. In Name, type the name of the new task.
4. In Description, type a description of the new task; optional.
5. In Connection Details, select the JMS account to use, or click New to define a new JMS account (see Creating an Account).
6. In JMS message, type the JMS message to send.
7. In JMS Topic name, type the name of the JMS topic that the message should be written to; optional if JMS Queue name is specified.
8. In JMS Queue name, type the name of the JMS queue that the message should be written to; optional if JMS Topic name is specified.
9. To automate task execution, open the Schedule tab, and configure the scheduler as described in Scheduling a Task.
10. Click Save.
    The task is saved and appears in the Tasks console in the Tasks list.

Adding a LogSync Task

The LogSync task enables synchronizing a single or multiple logs directories from remote XpoLog to another XpoLog, and automating their execution using a scheduler. This feature should be used when you want to create an image of a directory or multiple directories content (logs and/or binaries) on another XpoLog.

Configuration of a LogSync task requires specifying a connectivity account to the remote XpoLog machine created, see Creating an Account - Remote XpoLog.

Configuration of a LogSync task for synchronizing multiple single log directory or multiple logs directories to XpoLog requires specifying the path to an XML-based LogSync Configuration file, which contains the configuration for the synchronization from multiple servers and/or directories to XpoLog. For a detailed explanation on creating the XML-Based LogSyncConfiguration file, see below.

To add a LogSync task:

1. Open the Tasks console (see Tasks), and click the New Task button
   OR
   In the XpoLog Manager homepage, under More Actions, click Add Task.
2. In the page that opens, select the LogSync option, and then click Continue.
   The LogSync Task page opens.
3. In Name, type the name of the new task.
4. In Description, type a description of the new task; optional.
5. Under Details tab:
   a. Use a synchronization configuration file, and in Configuration file path, type the full path name to the LogSync configuration file or browse to it.
   b. Create Configuration, while synchronization takes place, XpoLog can also create configuration on all the logs which were synchronized under the Folders and Logs panel so all logs will be available for view and search in the XpoLog console. Check the 'create configuration' check-box if you wish to automatically add logs to XpoLog, and select/create a parent folder under which all synchronized logs from this task will be placed.
6. To automate task execution, open the Schedule tab, and configure the scheduler as described in Scheduling a Task.
7. Click Save.
   The Add LogSync task is saved.

Note:
When right clicking the LogSync task the following options are available:

1. Execute - Run the task.
2. Edit - Edit the task.
3. Duplicate - Duplicate the task.
4. Delete - Delete the task.
5. Force Log Sync (All) - Force the LogSync task to re-sync all files that were deleted from the repository but still exist on the remote sources related to this task. The re-sync will take place during the next task execution.
6. Force Log Sync (Checksum mismatch) - Force the LogSync task to re-sync only files that a checksum mismatch was found between repository to source. The re-sync of these files will take place during the next task execution.
7. Reconstruct Configuration (displayed only if 'Create Configuration' is defined in the task) - Force the LogSync task to re-create missing Folders and Logs configuration, based on the structure of the repository. The reconstruction will take place during the next task execution.

Execution:
- In case you are running XpoLog cluster with more than one processor, an option will be presented to determine which of the processors is assigned on the execution of the LogSync task.
LogSync XML Based Configuration

```xml
<SyncLogsConfiguration>
  <SyncLogsRepository repositoryDirectory="C:\xplgshare\logSyncTest" timeToKeep="7" />
  <SyncLogsNode repositoryDirectory="profiler">
    <Remote>
      <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="XPOLOG Profiler"/>
    </Remote>
    <SyncLogsDirectory syncDirectory="C:\logSyncTest\zip3">
    </SyncLogsDirectory>
  </SyncLogsNode>
  <SyncLogsNode repositoryDirectory="2" key="MY_KEY">
    <Remote>
      <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="XPOLOG Profiler"/>
    </Remote>
    <SyncLogsDirectory syncDirectory="C:\logSyncTest\logs\Zip1">
    </SyncLogsDirectory>
  </SyncLogsNode>
</SyncLogsConfiguration>
```

The following table describes the general structure of SyncLogsConfiguration.

<table>
<thead>
<tr>
<th>Tag Path</th>
<th>Mandatory/Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SyncLogsConfiguration</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>SyncLogsConfiguration/SyncLogsRepository</td>
<td>Mandatory</td>
<td>The repository tag</td>
</tr>
<tr>
<td>SyncLogsConfiguration/SyncLogsNode</td>
<td>Mandatory</td>
<td>A single log synchronizatoin node configuration</td>
</tr>
<tr>
<td>SyncLogsConfiguration/SyncLogsNode/Remote</td>
<td>Mandatory</td>
<td>Contains the Remote XpoLog Account details to which with the directories will be synched.</td>
</tr>
<tr>
<td>SyncLogsConfiguration/SyncLogsNode/Remote/Account</td>
<td>Mandatory</td>
<td>Mandatory as XpoLog should connect to a Remote XpoLog server (See: Creating an Account)</td>
</tr>
<tr>
<td>SyncLogsConfiguration/SyncLogsNode/SyncLogsDirectory</td>
<td>Mandatory</td>
<td>Configure the remote path to synch with the local XpoLog</td>
</tr>
</tbody>
</table>

XML Reference

**SyncLogsRepository Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>repositoryDirectory</td>
<td>Mandatory</td>
<td>The name of the root folder that will be synced with he content of the remote sync log directories.</td>
<td>String</td>
</tr>
<tr>
<td>timeToKeep</td>
<td>Optional</td>
<td>Time to keep the synched data on the repository</td>
<td>String</td>
</tr>
</tbody>
</table>

Example

```xml
<SyncLogsRepository repositoryDirectory="C:\xplgshare\logSyncTest" timeToKeep="7" />
```

**Checksum Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>algorithm</td>
<td>Mandatory</td>
<td>The algorithm to use to calculate the checksum</td>
<td>MD5/SHA-1</td>
</tr>
<tr>
<td>enabled</td>
<td>Optional</td>
<td>Determines whether to activate checksum</td>
<td>true/false</td>
</tr>
<tr>
<td>interval</td>
<td>Mandatory</td>
<td>The frequency that checksum will be calculated</td>
<td>m=minutes h=hours d=days</td>
</tr>
</tbody>
</table>
retryAttempts | Mandatory | The number of times that XpoLog will try to re-synchronize a file in case of a checksum validation failure before alerting | number
mailRecipients | Optional | The list of recipients that will be alerted in case of a checksum validation failure | semicolon separated list of email addresses

* The Checksum definition can be placed inside a specific SyncLogNode tag to be applied on that specific node, or inside the SyncLogsConfiguration tag to be applied globally on all nodes

Example:

```xml
<Checksum interval="2m" algorithm="MD5" mailRecipients="ops@xpolog.com" enabled="true" retryAttempts="1" />
```

**SyncLogNode Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>repositoryDirectory</td>
<td>Mandatory</td>
<td>The name of the folder within the repository to which remote directory from this node will be synced into</td>
<td>String - path</td>
</tr>
<tr>
<td>key</td>
<td>Optional</td>
<td>The SyncLogNode unique key</td>
<td></td>
</tr>
</tbody>
</table>

Example

```xml
<SyncLogsNode repositoryDirectory="profiler" />
```

**Account Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>classKey</td>
<td>Mandatory</td>
<td>The account class to use</td>
<td>String</td>
</tr>
<tr>
<td>name</td>
<td>Mandatory</td>
<td>The Remote XpoLog account name/ID to use</td>
<td>String (case sensitive)</td>
</tr>
</tbody>
</table>

**Remote Account Example**

```xml
<Remote>
<Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="XPOLOG Profiler"/>
</Remote>
```

**SyncLogsDirectory Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>syncDirectory</td>
<td>Mandatory</td>
<td>The directory on the remote XpoLog Node that will be synchronized into the SyncLogNode repository directory</td>
<td>String - path</td>
</tr>
<tr>
<td>repositoryDirectory</td>
<td>Optional</td>
<td>The name of the folder within the repository to which remote directory from this node will be synced into</td>
<td>String</td>
</tr>
<tr>
<td>directoriesToInclude</td>
<td>Optional</td>
<td>Define which directories to include in the log sync scan:</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using wildcard: Apps* - include all directories whose name starts with Apps Using a regular expression: regexp:\d\d\d\d-\d\d-\d\d - include all directories whose name is a date, for example 2013-11-26</td>
<td></td>
</tr>
<tr>
<td>directoriesToExclude</td>
<td>Optional</td>
<td>Define which directories to exclude from the log sync scan:</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using wildcard: Apps* - exclude all directories whose name starts with Apps Using a regular expression: regexp:\d\d\d\d-\d\d-\d\d - exclude all directories whose name is a date, for example 2013-11-26</td>
<td></td>
</tr>
<tr>
<td>filesToInclude</td>
<td>Optional</td>
<td>Define which files to include in the log sync scan:</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using wildcard: <em>.log,</em>.txt - include all files whose name ends with .log or .txt Using a regular expression: regexp:\w+.log - include all files whose name is constructed of word characters only and ends with .log, for example helloWorld.log</td>
<td></td>
</tr>
<tr>
<td>filesToExclude</td>
<td>Optional</td>
<td>Define which files to exclude in the log sync scan:</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using wildcard: *.zip,.gz - exclude all files whose name ends with .zip or .gz Using a regular expression: regexp:\w+.tar.gz - exclude all files whose name is constructed of word characters only and ends with .tar.gz, for example helloWorld.tar.gz</td>
<td></td>
</tr>
<tr>
<td><strong>subdirsScanLevel</strong></td>
<td>Optional</td>
<td>Number of sub-folder depth to scan</td>
<td>Number</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------</td>
<td>-----------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>timeInterval/timeIntervalUnit</strong></td>
<td>Optional</td>
<td>The task will synchronize only files with last updated time that is within the specified time interval</td>
<td>years, months, weeks, days, hours, mins</td>
</tr>
</tbody>
</table>

**Examples**

```xml
<SyncLogsConfiguration>
  <SyncLogsRepository repositoryDirectory="/home/LOGS_REPOSITORY/" timeToKeep="7" />
  <Checksum interval="2m" algorithm="MD5" mailRecipients="ops@xpolog.com" enabled="true" retryAttempts="1" />
  <SyncLogsNode repositoryDirectory="Tent">
    <Remote>
      <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="Tent"/>
    </Remote>
    <SyncLogsDirectory syncDirectory="C:\configurations\4.5_Build\log" directoriesToInclude="regexp:\d\d\d\d-\d\d-\d\d" directoriesToExclude="temp" filesToInclude="" filesToExclude="" subdirsScanLevel="">
    </SyncLogsDirectory>
  </SyncLogsNode>

  <SyncLogsNode repositoryDirectory="RedHat">
    <Remote>
      <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="RedHat"/>
    </Remote>
    <Checksum interval="2m" algorithm="SHA-1" mailRecipients="ops@xpolog.com" enabled="true" retryAttempts="1" />
    <SyncLogsDirectory repositoryDirectory="/root/xpolog45/log" directoriesToInclude="" directoriesToExclude="dump" filesToInclude="" filesToExclude="" subdirsScanLevel="">
    </SyncLogsDirectory>
  </SyncLogsNode>

  <SyncLogsDirectory repositoryDirectory="/var/log/" directoriesToInclude="" directoriesToExclude="" filesToInclude="" filesToExclude="" subdirsScanLevel="" timeInterval="1" timeIntervalUnit="days" >
    </SyncLogsDirectory>
  </SyncLogsNode>
</SyncLogsConfiguration>
```

**Configuration Parameters on synchronized Logs**

The configuration parameters are relevant only if the **Create Configuration** option is selected. XpoLog will scan the repository to add all relevant logs.

It is possible to add `<scanConfiguration>` tag either globally (above all `<SyncLogsNode>` tag) or individually by placing it internally in a `<SyncLogsNode>`.

**Using Proxy XpoLog for Log Synchronization**

It is possible to use a remote XpoLog as a proxy to synchronize logs from remote agents which are managed by a remote XpoLog and not directly by the current XpoLog that executes the task.

- To do so add the account(s) of the remote XpoLog before the ‘SyncLogsNode’ tags.
  The following example will synchronize logs from the directory ‘C:\logs\’ on the ‘Agent 1’ machine, where ‘Agent 1’ is not a direct agent of the current XpoLog, but an agent connected to ‘Remote XpoLog Master1’ and ‘Remote XpoLog Master2’:

```xml
<SyncLogsConfiguration>
  <SyncLogsRepository repositoryDirectory="/home/LOGS_REPOSITORY/" timeToKeep="7" />
  <Checksum interval="2m" algorithm="MD5" mailRecipients="ops@xpolog.com" enabled="true" retryAttempts="1" />
  <ProxyRemote>
    <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="Remote XpoLog Master1"/>
    <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="Remote XpoLog Master2"/>
  </ProxyRemote>
  <SyncLogsNode repositoryDirectory="/Agent 1">
    <Remote>
      <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="Agent 1"/>
    </Remote>
    <SyncLogsDirectory syncDirectory="/C:\logs/" directoriesToInclude="" directoriesToExclude="dump" filesToInclude="" filesToExclude="" subdirsScanLevel="">
    </SyncLogsDirectory>
  </SyncLogsNode>
</SyncLogsConfiguration>
```
• It is also possible to define the `<ProxyRemote>` inside an individual `<SynchLogNode>`:

The following example will synchronize logs from the directory 'C:\logs' on the 'Agent 1' machine, where 'Agent 1' is not a direct agent of the current XpoLog, but an agent connected to 'Remote XpoLog Master1' and 'Remote XpoLog Master2'. In addition, it will synchronize logs from the directory '/root/xpolog45/log' on the 'Agent 2' machine, where 'Agent 2' is a direct agent of the current XpoLog (no proxy has been defined for it):

```xml
<SyncLogsConfiguration>
  <SyncLogsRepository repositoryDirectory="/home/LOGS_REPOSITORY/" timeToKeep="7" />
  <Checksum interval="2m" algorithm="MD5" mailRecipients="ops@xpolog.com" enabled="true" retryAttempts="1" />
  <SyncLogsNode repositoryDirectory="Agent 1">
    <ProxyRemote>
      <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="Remote XpoLog Master1"/>
      <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="Remote XpoLog Master2"/>
    </ProxyRemote>
    <Remote>
      <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="Agent 1"/>
    </Remote>
    <SyncLogsDirectory syncDirectory="C:\logs" directoriesToInclude="" directoriesToExclude="dump" filesToInclude="" filesToExclude="" subdirsScanLevel="">
      </SyncLogsDirectory>
  </SyncLogsNode>
  <SyncLogsNode repositoryDirectory="Agent 2">
    <Remote>
      <Account classKey="xpolog.eye.media.remote.RemoteXplgAccount" name="Agent 2"/>
    </Remote>
    <SyncLogsDirectory repositoryDirectory="xpolog-logs" syncDirectory="/root/xpolog45/log" directoriesToInclude="" directoriesToExclude="" filesToInclude="" filesToExclude="" subdirsScanLevel="">
      </SyncLogsDirectory>
  </SyncLogsNode>
</SyncLogsConfiguration>
```

### Adding an Add Logs Directory Task

The Add Logs Directory task enables scanning a single or multiple logs directories to XpoLog, and automating their execution using a scheduler. This feature should be used, as opposed to the Administration > Add Logs Directory menu item, when you want to add multiple logs directories (as opposed to a single log directory), or to automate the execution of a single or multiple log directories (as opposed to manual execution).

Configuration of an Add Logs Directory task for adding a single logs directory to XpoLog is similar to the configuration of the Administration > Add Logs Directory feature; it requires specifying the path to the logs directory. For a logs directory that resides on a remote machine (SSH or Windows Network), it also requires specifying a connectivity account to the remote machine.

Configuration of an Add Logs Directory task for adding multiple logs directory to XpoLog requires specifying the path to an XML-based Scanner Configuration file, which contains the configuration for the addition of multiple logs from multiple servers and/or directories to XpoLog. For a detailed explanation on creating the XML-Based Scanner Configuration file, see Creating an XML-Based Scanner Configuration File.

To add an Add Logs Directory task:

1. Open the Tasks console (see Tasks), and click the New Task button
   OR
   In the XpoLog Manager homepage, under More Actions, click Add Task.
2. In the page that opens, select the Add Logs Directory option, and then click Continue.
   The Add Logs Directory Task page opens.
3. In Name, type the name of the new task.
4. In Description, type a description of the new task; optional.
5. In Parent Folder, click select and select the folder under which the new folders and logs are to be added.
6. Under Configuration, if the tasks configuration is specified in an external file, select the Use a scanner configuration file option, and in Configuration file path, either type the full path name to the scanner configuration file or browse to it, or click on Upload File to upload the external file. Otherwise, select the Scan a specific directory option, and proceed as described in the Scanning a Single Logs Directory section below.
7. Optionally, configure Advanced Settings (see Configuring Advanced Settings).
8. To automate task execution, open the Schedule tab, and configure the scheduler as described in Scheduling a Task.
9. Click Save.
   The Add Logs Directory task is saved.

### Scanning a Single Logs Directory

The Scan a Specific Directory option is used for bringing in a single logs directory from any of the following locations:

- **Local** – The logs directory is on the same machine as XpoLog Center.
- **Windows Network** – The logs directory is on a remote Windows machine.
- **Over SSH** – The logs directory is on a remote UNIX machine (with SSH connecting protocol).

Adding a **Windows Network** or **Over SSH** logs directory requires connecting to their server using a connectivity account.

To scan a single logs directory:

1. In **Location Type**, select the location of the log directory to add: Local, Windows Network, or Over SSH.
2. For a Windows Network or Over SSH location, in **Connection Details**, select the authentication account required to connect to the server where the selected directory resides, or click the new link to add an authentication account to the system (see Address Book).
3. In **Directory Path**, type the path to the directory that contains the log files
   OR
   Click Browse and in the System Files Browser (of the local, Windows Network, or Over SSH machine) that opens, expand the folders to get to the desired directory, and then click **Select** to display the path to the logs directory in **Directory Path**.
4. In **Collection Policy**, select a predefined collection policy.

---

**Creating an XML-Based Scanner Configuration File**

You can create an XML file to build an environment for scanning many servers, and per server, scanning many directories. The path to this XML file is placed in the Add Logs Directories Task, for adding multiple directories to XpoLog, and automating addition of directories.

**DirectoryScanner XML General Structure**

The following is the XML code of DirectoryScanner.

```xml
<DirectoryScanner>
  <ScannerNode name="NAME_OF_FOLDER_IN_XPOLOG">
    <Account name="ACCOUNT NAME" ... /> <!-- OPTIONAL -->
  </ScannerNode>
  <ScanDirectories>
    <ScanDirectory scanPath="DIRECTORY_PATH_ON_SOURCE">
      <ScanConfiguration>
        <!-- OPTIONAL CONF PARAMETERS (ScanFileFilter, ScanConfApplications) -->
      </ScanConfiguration>
    </ScanDirectory>
  </ScanDirectories>
</DirectoryScanner>
```

The following table describes the general structure of DirectoryScanner.

<table>
<thead>
<tr>
<th>Tag Path</th>
<th>Mandatory/Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirectoryScanner</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>DirectoryScanner/ScannerNode</td>
<td>Mandatory</td>
<td>The root folder that will be placed above its scanned directories.</td>
</tr>
<tr>
<td>DirectoryScanner/Account</td>
<td>Optional</td>
<td>Mandatory if XpoLog should connect to a remote server - Windows / UNIX (Creating an Account)</td>
</tr>
<tr>
<td>DirectoryScanner/ScanDirectories</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>DirectoryScanner/ScanDirectories/ScanDirectory</td>
<td>Mandatory</td>
<td>Contains the scanPath</td>
</tr>
<tr>
<td>DirectoryScanner/ScanDirectories/ScanDirectory/ScanConfiguration</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>DirectoryScanner/ScanDirectories/ScanDirectory/ScanConfiguration/ScanFileFilter</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>DirectoryScanner/ScanDirectories/ScanDirectory/ScanConfiguration/ScanConfApplications</td>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>
**XML Reference**

ScannerNode Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Mandatory</td>
<td>The name of the root folder that will be placed above its scanned directories.</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Leave the name empty to create all sub-directories under the parent folder with their original name from the source server.</td>
<td></td>
</tr>
</tbody>
</table>

Example

```
<ScannerNode name=""/>
```

Account Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Mandatory</td>
<td>The account name</td>
<td>String</td>
</tr>
<tr>
<td>useEncrypt</td>
<td>Mandatory</td>
<td>Indicates whether or not account password will be encrypted</td>
<td>Boolean</td>
</tr>
<tr>
<td>isPublicKey</td>
<td>Mandatory (SSH Only)</td>
<td>If authentication is done by private key, should be FALSE. If user/password are used, it should be TRUE, and a path should be specified under privateKeyPath (see the following parameter).</td>
<td>Boolean</td>
</tr>
<tr>
<td>privateKeyPath</td>
<td>Optional (SSH Only)</td>
<td>The path to the key, if authentication is done by private key</td>
<td>Boolean</td>
</tr>
<tr>
<td>isSystemAccount</td>
<td></td>
<td>Indicates whether or not account is a system account</td>
<td>Boolean</td>
</tr>
<tr>
<td>isScriptAPI</td>
<td></td>
<td>Indicates whether or not account is Script API</td>
<td>Boolean</td>
</tr>
<tr>
<td>isSSH</td>
<td></td>
<td>Indicates whether or not account is SSH</td>
<td>Boolean</td>
</tr>
<tr>
<td>isEditable</td>
<td></td>
<td>Indicates whether or not account can be edited in the XpoLog Address Book</td>
<td>Boolean</td>
</tr>
<tr>
<td>isCertificate</td>
<td></td>
<td>Indicates whether or not the account uses a certificate</td>
<td>Boolean</td>
</tr>
<tr>
<td>description</td>
<td>Optional</td>
<td>Description of the account</td>
<td></td>
</tr>
<tr>
<td>classKey</td>
<td>Mandatory</td>
<td>Windows: xpolog.eye.media.auth.win.WinAuthenticationAccount</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSH: xpolog.eye.media.telsh.TelnetAccount</td>
<td></td>
</tr>
<tr>
<td>certificateID</td>
<td>Optional</td>
<td>The ID of the certificate, if account uses a certificate (see isCertificate).</td>
<td>String</td>
</tr>
<tr>
<td>UserName</td>
<td>Mandatory</td>
<td>The username that the account uses to connect</td>
<td>String</td>
</tr>
<tr>
<td>isDefault</td>
<td></td>
<td></td>
<td>Boolean</td>
</tr>
<tr>
<td>Port</td>
<td>Mandatory (SSH Only)</td>
<td>The port that will be used to establish the connection to the remote data source</td>
<td>Numeric</td>
</tr>
<tr>
<td>TYPE_SCP_SFTP</td>
<td>Optional (SSH Only)</td>
<td>Indicates if the SSH account will use SCP or SFTP (default) protocol</td>
<td>String</td>
</tr>
<tr>
<td>Password</td>
<td>Optional</td>
<td>The password that the account uses to connect. Optional only if SSH account uses Public/Private key</td>
<td>String</td>
</tr>
<tr>
<td>NetAddress</td>
<td>Mandatory</td>
<td>The IP/hostname of the remote data source used in the account</td>
<td>String</td>
</tr>
</tbody>
</table>

**Note 1:** If a remote data source is scanned then an account to that source should be specified (it can be verified after execution under XpoLog > Tools > Address Book). In case an account for a specified machine already exists, XpoLog will automatically use it.

**Note 2:** In case XpoLog is running on a Windows machine, it is recommended to configure a service account on the Windows services panel and then all Windows network logs can be scanned as local without specifying an account in the ScannerNode (path may be \<server-name><drive-name>$...).

Windows Account Example

```
<Account name="ACCOUNT NAME" useEncrypt="false" isSystemAccount="false" isEditable="true" description="" classKey="xpolog.eye.media.auth.win.WinAuthenticationAccount" Password="PASSWORD" user="USERNAME" isDefault="false"/>
```

SSH Account Example

```
<Account name="ACCOUNT NAME" useEncrypt="false" privateKeyPath="" isSystemAccount="false" isScriptApi="false" isSSH="true" isPublicKey="false" isEditable="true" isCertificate="false" description="" classKey="xpolog.eye.media.telsh.TelnetAccount" certificateId="" UserName="USERNAME" TYPE_SCP_SFTP="SFTP" Port="22" Password="PASSWORD" NetAddress="IP"/>
```
Note: you should not use an id parameter in the account line in the scanner XML. In case an account already exists in XpoLog then based on the NetAdress and Name it will be matched and re-used. In case the account does not exist it will be created during the scanner execution.

ScanDirectory Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanPath</td>
<td>Mandatory</td>
<td>The full path to the directory that is to be scanned</td>
<td>Path</td>
</tr>
</tbody>
</table>

Examples

<ScanDirectory scanPath="C:\logs"/> (Windows Local)

<ScanDirectory scanPath="\qaserver\C:\logs\"/> (Windows Network)

<ScanDirectory scanPath="/opt/application/logs/"/> (UNIX Local / Over SSH)

ScanConfiguration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>condenseLogsTree</td>
<td>Optional</td>
<td>A &quot;true&quot; value indicates that folders containing only one sub-folder and without logs, will be omitted from the Folders and Logs tree.</td>
<td>Boolean</td>
</tr>
<tr>
<td>directoriesToHide</td>
<td>Optional</td>
<td>A comma separated list of name expressions of folders that will not be added to the Folders and Logs tree; their sub-folders/logs will be added.</td>
<td></td>
</tr>
<tr>
<td>fileSuffixesToIgnore</td>
<td>Optional</td>
<td>Unite logs with different suffixes into one log type (advanced)</td>
<td></td>
</tr>
<tr>
<td>numberOfThreads</td>
<td>Optional</td>
<td>The number of threads to be used as part of the scanning operation</td>
<td>Integer</td>
</tr>
<tr>
<td>removeEmptyNodes</td>
<td>Optional</td>
<td>In case there are no matching files under one of the Folders and Logs members, remove it from the Folders and Logs tree.</td>
<td>Boolean</td>
</tr>
<tr>
<td>subdirsScanLevel</td>
<td>Optional</td>
<td>The number of sub-directories to scan from the given directory. Default is unlimited; any number can be specified.</td>
<td>Integer or &quot;Unlimited&quot;</td>
</tr>
<tr>
<td>scanMethod</td>
<td>Optional</td>
<td>0 = Use existing configuration (file names and content) and automatic matching. 1 = Use existing configuration (file names and content). 2 = Use existing configuration (file names only).</td>
<td>0, 1, or 2</td>
</tr>
<tr>
<td>namePatternLogic</td>
<td>Optional</td>
<td>0 = Capture each file separately (without name pattern). 1 = Unite files with a similar names (apply name pattern automatically). 2 = Unite files with a similar suffix (apply name pattern only at the end of the file name).</td>
<td>0, 1, or 2</td>
</tr>
<tr>
<td>filesToInclude</td>
<td>Optional</td>
<td>Define which files to include in the log scan: Using wildcard: &quot;.<em>.log&quot;, &quot;.</em>.txt&quot; - include all files whose name ends with .log or .txt Using a regular expression: regexp:^[wW].log - include all files whose name is constructed of word characters only and ends with .log, for example helloWorld.log</td>
<td></td>
</tr>
<tr>
<td>filesToExclude</td>
<td>Optional</td>
<td>Define which files to exclude in the log scan: Using wildcard: &quot;.<em>.zip&quot;, &quot;.</em>.gz&quot; - exclude all files whose name ends with .zip or .gz Using a regular expression: regexp:^[wW].tar.gz - exclude all files whose name is constructed of word characters only and ends with .tar.gz, for example helloWorld.tar.gz</td>
<td></td>
</tr>
<tr>
<td>directoriesToExclude</td>
<td>Optional</td>
<td>Define which directories to exclude from the log scan: Using wildcard: &quot;<em>Apps</em>&quot; - exclude all directories whose name starts with Apps Using a regular expression: regexp:^\d\d\d\d-\d\d-\d\d$ - exclude all directories whose name is a date, for example 2013-11-26</td>
<td></td>
</tr>
<tr>
<td>directoriesToInclude</td>
<td>Optional</td>
<td>Define which directories to include in the log scan: Using wildcard: &quot;<em>Apps</em>&quot; - include all directories whose name starts with Apps Using a regular expression: regexp:^\d\d\d\d-\d\d-\d\d$ - include all directories whose name is a date, for example 2013-11-26</td>
<td></td>
</tr>
<tr>
<td>templatesToUse</td>
<td>Optional</td>
<td>The scan task will add only logs which were matched to one of the comma separated list of specified templates.</td>
<td>String</td>
</tr>
<tr>
<td>namePatternToApply</td>
<td>Optional</td>
<td>Automatically name the matched logs based on the given name pattern. Allowed identifiers are: [PARENT_FOLDER n] - the name of n-th parent folder of the log [CHILD_FOLDER n] - the name of n-th child folder of the root folder [APPLICATION] - the name of the log's application [SERVER] - the name of the log's server [LOG] - the current name of the log</td>
<td>String</td>
</tr>
</tbody>
</table>
timeZone | Optional | Set the specified time zone on all matched logs | String
---|---|---|---
onlineLogsApplication | Optional | Comma separated list of application name(s) that the online logs will be tagged to once created | String
assignedCollectionPolicy | Optional | The policy name of the collection policy that will be applied on the logs once created; If the parameter does not exist - the default policy will be automatically applied | String
fileSuffixesToIgnore | Optional | Regular expression used to ignore part of the files names to define a name pattern | String
enableLogsIndex* | Optional | True – Online logs that are added under Folders and Logs will be indexed. False – Disable indexing. | Boolean
enableLogsAnalytics* | Optional | True – Online logs that are added under Folders and Logs will be analyzed by Analytics. False – Disable Analytics. | Boolean
addCollectors* | Optional | True – All the logs that are added by the scanner task will be collected; default policy will be applied, unless a specific policy is specified. False – Disables logs collection. | Boolean
enableCollectedLogsAnalytics* | Optional | True – enables Analytics analysis on collected logs. Online logs state will be taken from the collection policy; relevant only when addCollectors="true". False – Enables Analytics analysis on collected log. | Boolean
enableCollectedLogsIndex* | Optional | True – enables indexing of collected logs. The online logs state will be taken from the collection policy; relevant only when addCollectors="true". False – Disables indexing of collected logs. | Boolean
collectedLogsApplication* | Optional | Comma separated list of application name(s) that the collected logs will be tagged to once created; relevant only when addCollectors="true". | String

* Properties relevant only to versions 4.4 and below

Example

<ScanConfiguration condenseLogsTree="false" directoriesToInclude="log,home" numberOfThreads="3" assignedCollectionPolicy="live" filesToInclude="*.log"/>

ScanFileFilter Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeInterval/timeIntervalUnit</td>
<td>Optional</td>
<td>The scan will only add log files with last updated time that is within the specified time interval per log type.</td>
<td>years, months, weeks, days, hours, mins</td>
</tr>
<tr>
<td>maxNumberOfFiles</td>
<td>Optional</td>
<td>The maximum number of log files that are added per log type.</td>
<td>Integer</td>
</tr>
</tbody>
</table>

Examples

<ScanFileFilter timeInterval="3" timeIntervalUnit="months"/>

<ScanFileFilter maxNumberOfFiles="2"/>

ScanConfApplications Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>applicationNamePattern</td>
<td>Optional</td>
<td>The pattern that is used to extract the application name. An application will be created as part of the scan process.</td>
<td></td>
</tr>
<tr>
<td>applicationGroupNamePattern</td>
<td>Optional</td>
<td>The pattern that is used to extract the application group name. An application will be created as part of the scan process that all its sub-application are tagged to.</td>
<td></td>
</tr>
</tbody>
</table>

Example

<ScanConfApplications applicationNamePattern="/\w+-\(\w+\).*" applicationGroupNamePattern="/\(\w+-\w+\).*"/>

Templates:

Please use the following examples as templates and modify accordingly (multiple directories per host can be defined by adding more <scanDirectory> entries / multiple hosts can be defined by adding multiple <scannerNode> entries:

Example 1 (scanner_example_Windows_logs_account_on_xpolog_service): scanner_example_Windows_logs_account_on_xpolog_service.xml

Example 2 (scanner_example_Windows_logs_using_windows_network_account): scanner_example_Windows_logs_using_windows_network_account.xml
Adding an Email Task

An Email task sends an email alert to preconfigured addresses. For example, you can configure a Keep Alive email task that sends an email every hour to show that XpoLog is up and running. You can automate task execution by configuring a scheduler on it. XpoLog then runs the task based on the scheduler configuration.

You can send a log as an attachment to the email alert, in either of the following export formats:

- Together with its configuration, thus enabling future import into XpoLog
- Transformed into an XML, CSV, or Tab delimited file.

A common use case of Email Task is testing the mail settings of XpoLog, the steps of adding an email test are the same as the steps below, the only difference there is no need of step #11, just Save and Execute the task afterwards and check if an email was received properly. In case an email was not received, an indication of error may be found at XpoLog system log.

**Note:** Ensure that your SMTP server is configured in XpoLog before creating Email Tasks and sending emails (see Settings).

To add an email task:

1. Open the Tasks console (see Tasks), and click the New Task button
   OR
   In the XpoLog Manager homepage, under More Actions, click Add Task.
2. In the page that opens, select the Email option, and then click Continue. The Email Task page opens.
3. In Name, type the name of the new task.
4. In Description, type a description of the new task; optional.
5. Open the Details tab.
6. In From, type the account from which the email will be sent.
7. In To, type the account to which the email will be sent.
8. In Subject, type the subject of the email.
9. In Body, type the body of the email; optional.
10. In Data Export Format, select one of the following for the format of the email attachment:
    - Send an email alert without any data attached.
    - Attach the log together with its configuration, to enable future import.
    - Transform the data and attach to mail as XML, CSV or TAB Delimited.
11. To automate task execution, open the Schedule tab, and configure the scheduler as described in Scheduling a Task.
12. Click Save. The Email task is saved.

Adding an SNMP Trap Task

An SNMP Trap task generates an SNMP trap.

To add an SNMP Trap task:

1. Open the Tasks console (see Tasks), and click the New Task button
   OR
   In the XpoLog Manager homepage, under More Actions, click Add Task.
2. In the page that opens, select the SNMP Trap option, and then click Continue. The SNMP Trap Task page opens.
3. In Name, type the name of the new task.
4. In Description, type a description of the new task; optional.
5. In Connection Details, select the SNMP account to use, or click New to define a new SNMP account (see Creating an Account).
6. In SNMP Trap OID, type the OID of the SNMP trap; mandatory only for SNMP version 2 account.
7. In SNMP Community, type the name of the target community; optional; default is Public.
8. Specify the SNMP trap variables. See the Specifying SNMP Trap Variables section below.
9. To automate task execution, open the Schedule tab, and configure the scheduler as described in Scheduling a Task.
10. Click Save. The task is saved and appears in the Tasks console in the Tasks list.

Specifying SNMP Trap Variables

You can add SNMP trap variables to the SNMP trap. You can either add a predefined SNMP, or customize a new variable of one of the following available types:

- Trap Time – the time of the SNMP trap
- Log Time – the time of the event
- Time – the value of a date column from the event
- **Text** – free text or the value of any column from the event. Specify the column name in square brackets.
- **Unsigned Integer** – the value of a number column from the event
- **Status** – the status of the event
- **IP Address, Integer 32, Unsigned Integer 32, Counter 32, Counter 64, Gauge 32, SMI Address, TCP Address, Time ticks, UDP Address** – the value of a column from the event. Choose the type matching the data in the event, i.e. `Integer 32` for a numeric value and `IP Address` for an IP address.

To add an SNMP trap variable:

1. In the SNMP Trap Task Details tab, click **Add new variables**.
2. Select the **Select a predefined variable** option, and in the adjacent dropdown list, select the variable.
   OR
   Select the **Create a custom variable** option, and customize the following details for the new variable:
   - In **OID**, type the OID of the variable.
   - In **Name**, type the name of the variable.
   - In **Description**, type a description of the variable.
   - In **Type**, select the type of the variable.
   - In **Message**, type the message to be sent in the trap. Optionally, include in this dynamic field placeholders for data from the log. The available placeholders are determined by the variable type, as follows:
     - For a **Trap Time** variable, specify the date format in the Message column, or leave empty for default date format (MM/dd/yyyy HH:mm:ss).
     - For a **Log Time** variable, specify the date format in the Message column, or leave empty for default date format (MM/dd/yyyy HH:mm:ss).
     - For a **Status** variable, specify the status of the event.
     - For other variables, specify the column name in square brackets.
3. Click **Add**.
   The new variable is added to the Existing Variables list.

Adding an SSH Execution Task

An SSH Execution task opens an SSH connection to a remote machine and executes a command or set of commands.

To add an SSH Execution task:

1. Open the Tasks console (see **Tasks**), and click the **New Task** button
   OR
   In the XpoLog Manager homepage, under **More Actions**, click **Add Task**.
2. In the page that opens, select the **SSH Execution** option, and then click **Continue**.
   The SSH Execution Task page opens.
3. In **Name**, type the name of the new task.
4. In **Description**, type a description of the new task; optional.
5. In **Connection Details**, select the account of the SSH host on which the program/script is to be executed, or click **New** to define a new SSH account (see **Creating an Account**).
6. In **Program/Script Path**, type the name of the program/script to be executed by the task.
7. In **Arguments**, type the arguments needed for the program/script to run, separated by spaces; optional.
8. In **Environment Variables**, type the environment variables needed for the program/script to run; optional.
9. In **Output Target File**, type the path to the file where output of the program/script execution is to be written; optional.
10. Select the **Add Optional Params** checkbox to include in the output file the date, account name, host name and username.
11. To automate task execution, open the **Schedule** tab, and configure the scheduler as described in **Scheduling a Task**.
12. Click **Save**.
   The SSH Execution task is saved.

Adding a URL Task

A URL task opens a URL to a remote Web server and parameters can be passed as part of the URL to that remote server.

To add a URL task:

1. Open the Tasks console (see **Tasks**), and click the **New Task** button
   OR
   In the XpoLog Manager homepage, under **More Actions**, click **Add Task**.
2. In the page that opens, select the **URL** option, and then click **Continue**.
   The URL Task page opens.
3. In **Name**, type the name of the new task.
4. In **Description**, type a description of the new task; optional.
5. In **Connection Details**, select the HTTP account in which the program/script is to be executed, or click **New** to define a new HTTP account (see **Creating an Account**).
6. To automate task execution, open the **Schedule** tab, and configure the scheduler as described in **Scheduling a Task**.
7. Click **Save**.
   The task is saved and appears in the Tasks console in the Tasks list.

Scheduling a Task

Each task is made up of its definition and scheduler. You can schedule a task to automatically run on a daily, weekly, or monthly basis.
Tasks that are only to be manually operated do not have to be scheduled (the default).

**Scheduling Daily Running of a Task**

You can configure a scheduler to run a task at a set time every day, or at a specified frequency during the day – either throughout the day, beginning at a certain hour, ending at a certain hour, or in a specified time interval.

To schedule daily running of a task:

1. In **Set Frequency**, select **Daily**. Parameters are displayed for setting the time(s) to run the task.
2. Select one of the following two options:
   - **Repeat every** – In the adjacent textbox, type the frequency of running the task and select the appropriate unit of time. For example, 2 Hours. Optionally, select the **Start at** checkbox to schedule running the task from a set hour, and in the dropdown list, select that hour. Optionally, select the **Stop at** checkbox to schedule running the task until a set hour, and in the dropdown list, select that hour.
   - **Daily at** – Select the exact time (HH:MM:SS) of running the task every day.

**Scheduling Weekly Running of a Task**

You can configure a scheduler to run a task on set day(s) every week, and at a set time or frequency on those days.

To schedule weekly running of a task:

1. In **Set Frequency**, select **Weekly**. Parameters are displayed for setting the day(s) of the week, and the time(s) on those days to run the task.
2. Select the checkboxes of the days on which you want the task to automatically run.
3. Define the time(s) to run the task during those days (see step 2 of the **Scheduling Daily Running of a Task** section).

**Scheduling Monthly Running of a Task**

You can configure a scheduler to run a task on specific months or every month, on a specific day on those months or every day of those specified months, and at specific hours or frequencies on those specified days.

To schedule monthly running of a task:

1. In **Set Frequency**, select **Monthly**. Parameters are displayed for selecting the month(s), day of the month, and time(s) on those days to run the task.
2. Select the checkboxes of the months on which you want the task to automatically run.
3. In the dropdown list, select **Every Day** (the default) or a specific day of the month.
4. Define the time(s) to run the task during those days (see step 2 of the **Scheduling Daily Running of a Task** section).

**Disabling Scheduling**

You can disable scheduling of a task. Such tasks will only be able to run when manually operated.

To disable scheduling:

- In **Set Frequency**, select **Never**.

**Deleting a Task**

You can delete a task that you no longer want to run in the system.

To delete a Task:

1. Open the Tasks console (see **Tasks**), and either
   - Right-click a task and in the menu that appears, click **Delete**
   - OR
   - Select a task from the Tasks list, and click the **Delete** button.
   - The delete confirmation box opens.
2. Click **Yes**.
   - The task is deleted from the system, and is removed from the Tasks list.

**Duplicating a Task**

You can create a new task based on an existing task, by duplicating an existing task, giving it another name, and description, and modifying parameters in the tabs, as required.

To duplicate a Task:

1. Open the Tasks console (see **Tasks**), and either
   - Right-click a task and in the menu that appears, click **Duplicate**
   - OR
   - Select a task from the Tasks list, and click the **Duplicate** button.
   - The Add Logs Directories Task opens. The parameters in the Details and Schedule tabs are configured as in the duplicated task.
2. In **Name**, type the name of the new task.
3. In **Description**, type a description of the new task; optional.
4. Modify **Details** and/or **Schedule** tab parameters, as required.
5. Click **Save**.
The task is saved.

**Editing a Task**

You can edit a task.

To edit a task:

1. Open the Tasks console (see Tasks), and either
   Right-click a task and in the menu that appears, click **Edit**
   OR
   Select a task from the Tasks list, and click the **Edit** button.
   The Add Logs Directories Task opens.

2. Modify **Name**, **Description**, and the parameters in the **Details** and/or **Schedule** tab parameters, as required.

3. Click **Save**.
   The task is updated.

**Filtering the Tasks Console**

You can filter the Tasks Console by task name, type, and/or description, by typing characters in the corresponding textboxes under the **Name**, **Type**, and/or **Description** columns.

**Manually Executing a Task**

You can manually execute a task, regardless of whether it is automated.

To execute a task:

- Open the Tasks console (see Tasks), and either
  Right-click a task and in the menu that appears, click **Execute**
  OR
  Select a task from the Tasks list, and click the **Execute** button.
  The task is executed.

**Settings**

**Installing and Updating Your XpoLog License**

Users require a valid product license to run XpoLog. An XpoLog license is dedicated per installation server, meaning that you require a unique license for each server on which XpoLog runs. A license must be updated when it expires or when you want to change license settings, such as increasing the data volume handled by XpoLog. From the Settings>License menu item, you can view your license settings, update your license, or generate a server key for a new license.

**Generating a Server Key**

A unique license must be applied on each deployment of XpoLog. This requires generating a server key and sending it to XpoLog. XpoLog then creates and sends to you a license file, which you can install on the server.

**To generate a server key**

1. In the XpoLog Manager menu, select **Settings > License**.
   The XpoLog Center License page opens.
2. Click **generate server key**.
   A server key is generated for the server. Note that in case running XpoLog as a cluster the entire cluster console is generated on any of the nodes (it is not needed to generate a key per node).
3. Copy-paste the the server key in an email to XpoLog requesting a license for the deployment, and then click **OK** to close the Server Key box.

**Installing a License**

You can install a license onto your server from the License page, by either uploading the license file into XpoLog or copying the text of the license file into the License File textbox.

**To install a license:**

1. In the XpoLog Manager menu, select **Settings > License**.
   The XpoLog Center License page opens.
2. In the **Update License** section, in **License File**, click **Browse** to select the path to the license file that you want to upload.
   Alternatively, in **License Text**, paste the complete license text.
3. Click **save**.
   The license is updated.

**Configuring General Settings**

- **Saving XpoLog Configuration**
- **Configuring Mail Settings**
Configuring Connection Policies
Configuring Advanced General Settings

Configuring General Security Settings

In the Security tab of the General settings page in XpoLog Manager, you can configure the following security settings:

- **Activate security** – By default, security is not activated in XpoLog, and you are not required to log in with a username and password. You can activate XpoLog's security mechanism by selecting this option, so that you are redirected to XpoLog's login page, and will be required to enter a username and password (default: admin, admin) in order to access XpoLog. In addition, a new Security item will be added to the XpoLog Manager menu.

- **session time out** – By default, a session shuts down after 30 minutes of no use. You can set a different length of time for the time out.

- **Login URL** – the URL to which users will be redirected for login.

The Security tab also provides several different predefined authentication types:

- **XpoLog Realm** – Usernames and passwords are managed internally by XpoLog. Any user that logs in can change their username and password in User General Settings in the Security menu.

- **LDAP** – Active Directory

- **Siteminder**

- **WebSeal**

- **Remote User**

**Note:** In case your company uses a different authentication type, contact our support team for further assistance.

To configure security settings:

1. In the General Settings console, open the **Security** tab.
2. Select the **Activate Security** checkbox to require login to XpoLog with a username and password.
3. In **Session time out**, select the number of minutes of inactivity before XpoLog closes. Default: 30 minutes
4. In **Login URL**, if your organization has an external mechanism that it wants to use for validating login, type the URL; otherwise, leave the default URL.
5. Under **Authentication**, in the **Available Types** list, select a type, and then click **Add**. The selected type appears in the **Selected Types** list. For LDAP, SiteMinder, and WebSeal, click the configuration link to the right of Selected Types, and complete the settings page that appears. For details on LDAP authentication configuration, see **Set up user authentication with LDAP**.

   **Note:** You can remove a type from the Selected Types list by selecting it and clicking **Remove**.

6. Click **Save**.

   The Security settings are saved.

   If you activated security (in step 2), the login page appears, requiring you to enter username and password. Once you log in, a Security tab appears in the menu.

**Set up user authentication with LDAP**

This section describes how to use Active Directory for authenticating users with the LDAP server.

The LDAP settings include:

- **General**
  - **initial context factory**
  - **Provider URL** – the connection URL to the LDAP server (you can use several URLs to multiple LDAP servers separated by a space).

- **Manager Settings** (optional)
  - **Manager Path** – the manager DN for searching users
  - **Manager password** – the manager’s password

- **Search Settings**
  - **Root path** – the path for starting to search users.

  In case there's a need to search user's information from multiple domains, it is required to enter [ALL DOMAINS] in root path of the LDAP configuration

  - **Search filter** – how to search the users in the LDAP directory; the {0} is replaced with username.

  - **User path** – full path of the user DN; the {0} is replaced with username. For example:

    `uid={0},ou=people,dc=xplg`

  - **Unique id attribute** – optional; which attribute of the user will be provided as the unique id of the user.

  - **Display name attribute** – optional; which attribute of the user will be provided as the display name of
the user.

- Further Settings
  - Group id pattern
  - Groups attribute

To configure Active Directory authentication:

1. In Provider URL, type the URL to the active directory server – ldap://ACTIVEDIRECTORYSERVER:389/ (for several LDAP servers enter a space separated list of URLs)
2. In Search Filter, type sAMAccountName={0}. {0} is replaced with the username.
3. In User path, type USER_DOMAIN\{0}, where USER_DOMAIN is the domain of your users.
4. In Unique id attribute, type sAMAccountName.
5. In Display name attribute, type displayName.
6. In Groups attribute, type memberOf.
7. Click save. The LDAP configuration is saved.

Use single sign-on (SSO) with XpoLog

This section describes how to configure XpoLog to work with your SSO solution for validating users authentication. Configuring XpoLog to work with SSO requires that XpoLog instance which is accessed via SSO is secured behind an HTTP proxy or web agent. The HTTP proxy you configure is then responsible for handling authentication and is the only entity capable of communicating with XpoLog. Active Directory

XpoLog expects that your user authentication is handled by a web proxy. The web proxy server must be configured to authenticate against the external authentication system (for example AD). Once a user has been authenticated by the proxy, the proxy must insert the authenticated user's username as a REMOTE_USER header in all HTTP requests forwarded to XpoLog.

XpoLog accepts incoming HTTP requests which include a REMOTE_USER header from a trusted proxy. If the user in the REMOTE_USER header is not currently authenticated by XpoLog, an authentication request is made to XpoLog via a trusted authentication endpoint the XpoLog process provides. If REMOTE_USER is not provided in every request, the REMOTE_USER is assumed to not be authenticated and will receive a XpoLog login screen.

Note: If your proxy uses some other remote user header name besides REMOTE_USER, you can change the name of the header as described below:

The settings include:

- General
  - User header key - key used by the trusted authentication endpoint on authenticated users in the HTTP header (comma separated list. For example: REMOTE_USER)
    XpoLog uses the header key(s) to validate the user's authentication and to retrieve information regarding the user. If more than one key is provided, XpoLog will use the keys one by one to try and retrieve the information.
  - Protected URLs - a list of the trusted authentication endpoint(s) which XpoLog will allow authentication from (comma separated list, wild card supported).
    Click save. The SSO configuration is saved.

Set up a proxy server

XpoLog SSO implementation supports most proxy servers. The proxy server must handle its own authentication and must insert the authorized username into a REMOTE_USER (or equivalent) header for all HTTP requests it forwards to XpoLog.

Site Minder

XpoLog's integration to SiteMinder supports a scenario where there are SiteMinder's web agents in-front of XpoLog. Users are performing the login operation directly against the SiteMinder, and then being redirected to XpoLog. XpoLog is validating the user's authentication and retrieving the information from SiteMinder.

The SiteMinder settings include:

- General
  - User header key - key used by the SiteMinder on authenticated users in case where information can be retrieved from the HTTP header (comma separated list. For example: HTTP_SM_USER, HTTP_UID)
    XpoLog uses the header key(s) to validate the user's authentication and to retrieve information regarding the user. If more than one key is provided, XpoLog will use the keys one by one to try and retrieve the information.
- **Client cookie name** - cookie name used by the SiteMinder on authenticated users in case where information can be retrieved from a cookie (for example: SMSESSION). XpoLog uses the cookie name to validate the user's authentication and to retrieve information regarding the user.
- **Protected URLs** - a list of the protected SiteMinder web agents URLs which XpoLog will allow authentication from (comma separated list, wild card supported).
- **Group header key** - key used by the SiteMinder, used in order to retrieve from the HTTP header information regarding the authenticated user's group(s). XpoLog is using the header key(s) to retrieve information regarding the user's group(s). If more than one key is provided, XpoLog will use the keys one by one to try and retrieve the information.
- **Group id pattern** - used if a specific value should be retrieved from the authenticated user's group.
- **User HTTP request key** - key used by the SiteMinder on authenticated users in case where information can be retrieved directly from the HTTP request (comma separated list. For example: HTTP_SM_USER, HTTP_UID). XpoLog is using the request key(s) to validate the user's authentication and to retrieve information regarding the user. If more than one key is provided, XpoLog will use the keys one by one to try and retrieve the information.

Click **save**. The SiteMinder configuration is saved.

### Configuring Mail Settings

In order for XpoLog to send emails, you must allocate an SMTP mail server and configure it.

To configure mail settings:

1. In the General Settings console, open the **Mail** tab.
2. In **SMTP Host**, type the SMTP host address that XpoLog is to use to send emails.
3. In **SMTP Port**, type the port that the given SMTP host is listening on.
4. In **System Email Address**, type the default/system ‘From’ email address that is to be used when sending emails.
5. In **Administrator Email Address**, type the email address of XpoLog’s administrator, where system notifications such as disk space, violation messages, and more, are to be sent.
6. If the SMTP requires authentication, select the **Use SMTP Authentication** checkbox. In this case, provide **SMTP Username** and **SMTP Password**, and indicate whether or not to use TLS/SSL.
7. To test that the mail settings are correct and usable, click the **Test Mail Settings** link, enter a valid email address to which a test message should be sent, and click the **Send Message** button. If an error message appears, fix the relevant setting based on the error message and run another test.
8. Click the **Save** button.

The mail settings are saved.

### Use Case: GMAIL as SMTP server in XpoLog

In order to use your GMAIL as the mail server that XpoLog uses to send emails, please use the following settings:

1. In the General Settings console, open the **Mail** tab
2. In **SMTP Host**, type smtp.gmail.com
3. In **SMTP Port**, type 465
4. **System Email Address** - typically this is the default/system ‘From’ email address that is to be used when sending emails from XpoLog. However, when using GMAIL the ‘From’ email address will always be the email address of the GMAIL account you're using in these settings. GMAIL does not allow a custom email address to be used as the ‘From’ email address.
5. In **Administrator Email Address**, type the email address of XpoLog’s administrator, where system notifications such as disk space, violation messages, and more, are to be sent.
6. Check the **Use SMTP Authentication** check-box.
7. Provide **SMTP Username** and **SMTP Password** (your GMAIL user and password)
8. Check the **Use TLS/SSL** check-box
9. Click the **Save** button.

The GMAIL settings are saved.

### Configuring Connection Policies

In the Connection Policies tab of the general settings, you can configure the default SSH account connection policy that is to be applied on any SSH account in XpoLog. This determines the default behavior of SSH activity between XpoLog and remote UNIX machines.

To configure connection policies:

1. In the General Settings console, open the **Connection Policies** tab.
2. In **Connection pool timeout interval**, type the allowed period of connections inactivity before a pool is closed, selecting **minutes** or **hours** as the unit of time. Type 1 and select **Minutes** to close the pool as soon as possible. Default: **5 minutes**.
3. In **User session timeout interval**, type the allowed period of user inactivity before a log is closed, selecting **minutes** or **hours** as the unit of time. Leave blank for unlimited inactivity period. Default: unlimited.
4. In **Number of connections allowed to remote machine**, type the allowed number of connections to a remote machine (default: unlimited). Leave blank for an unlimited number of connections.
5. In **Number of sessions allowed per connection**, type the number of sessions that can be opened using the same connection. Default: 7
6. In **Number of pooled sessions allowed**, type the number of sessions that can be pooled. Leave blank to disable session pooling.
   
   **Note:** Session pool is required only if there is a relatively high number of log types on a single remote server (>50) - in that case if there will not be enough allowed sessions to manage all logs from the server in parallel a pool will optimize the process. Furthermore, some machines may block connectivity from XpoLog when sessions will constantly be opened from XpoLog for collecting data, in such cases pool is recommended. For most common cases this is not required.
7. **Click Save.**
   
   The Connection Policies settings are saved.

**Recommendation:** In general XpoLog requires 3 sessions to process a single log type from a remote server. I.E. a limitation of 10 connections (7 sessions each) will be sufficient to process about 25 log types from a remote server which should be sufficient for most cases.

**Configuring Advanced General Settings**

In the XpoLog Manager General settings Advanced tab, you can:

- **Specify the business hours and non business hours** - Define if XpoLog should distinguish between business and non-business hours and specify the desired hours.
- **Upload custom functions** – Import a JAR of custom functions defined by the XpoLog team.
- **User Time Zone Mode** – set the policy that XpoLog uses to apply time zone for users entering the system from different locations.

**To configure advanced settings:**

1. In the General Settings console, open the **Advanced** tab.
2. Under **Business Hours** enable/disable whether XpoLog should distinguish between business and non-business hours and specify the desired hours. This is used by XpoLog mainly for data monitoring.
3. Under **Custom Functions**, click here to upload the report functions JAR to XpoLog Center.
4. Under **User Time Zone Mode**, there are 3 options that can be used:
   a. Apply the system time zone (default) - XpoLog instances have a global, cross-system, time zone. By default the global time zone is taken from the machine that XpoLog is running on – this time zone is the baseline and all dates and times selections/interpretations are done based on it (user interface always refers to the system time zone – last hour selection is interpreted to the last hour of the system time zone). Each log source, by default, gets the system time zone. I.E. XpoLog assumes that the log data is written in the same time zone. A log source specific time zone may be defined in the log regional settings configuration and, in case different than the system time zone, XpoLog will interpret the log records timestamps to the system time zone.
   b. Apply dynamic time zone - By selecting this option, XpoLog will try to automatically retrieve a the user's specific time zone, from the user client, on log in. If the retrieved time zone of the user is different than the system time zone, the user will automatically see all dates and times selections/interpretations to the retrieved time zone and not as the system time zone. Note: Even if this option is selected, all scheduled / system tasks will be executed based on the system time zone.
   c. Apply AppTags time zone - By selecting this option, an option to configure a specific time zone per AppTag will be available. Each AppTag will have its own designated time zone configured and if a user is allowed to see a specific AppTag's data then that AppTag's time zone will be automatically applied, regardless of the user's location. If a user is allowed to see multiple AppTag's with the same time zone then that time zone will be applied, if the user is allowed to see more than one AppTag with different time zones then the system time zone will be automatically used instead. Note: Even if this option is selected, all scheduled / system tasks will be executed based on the system time zone.

**Saving XpoLog Configuration**

In the General Settings tab, you can do the following:

- **Save the entire configuration used by XpoLog.**
- **Change the ports used by XpoLog for HTTP/HTTPS.**

**Saving the XpoLog Configuration**

It is recommended to save in a directory, the entire configuration that XpoLog uses. This directory should be external to the installation directory, and XpoLog should be granted full permissions on it. See Post Installation Recommendations for full explanation.

In cases where more than one XpoLog instance shares the same configuration, you also have the option of specifying that XpoLog run in Cluster mode, so that the XpoLog instances are aware of each other. See XpoLog...
Cluster Installation for full explanation.

To save the entire XpoLog configuration:

1. In the XpoLog General Settings console, open the General tab.
2. Select the Use external configuration directory checkbox, and in Configuration full path, type the absolute path to a directory that XpoLog can use to store and manage its configuration and analysis. Example: C:/XpoLogConfig/.
3. If you want XpoLog to run in cluster mode, select the Cluster mode check-box. This is required only if XpoLog is installed in a cluster with multiple instances.
4. If you want XpoLog to run as agent where ALL system activities are disabled select the Agent Mode check-box. Mainly used for Remote XpoLog in Agent mode or LogSync.
5. Click Save.
6. The XpoLog configuration is saved in the specified directory.
7. Restart XpoLog.

Changing the HTTP/HTTPS Ports

The default HTTP port is 30303; default HTTPS port is 30443. You can change the ports used by XpoLog for HTTP/HTTPS.

To change the HTTP/HTTPS port:

1. In the XpoLog General Settings General tab, in HTTP port, type the port to be used by XpoLog for HTTP, and/or in HTTPS port, type the port to be used by XpoLog for HTTPS.
2. Click Save.
   The ports configuration is saved.

Disabling HTTP/HTTPS Access to XpoLog

To disable the HTTP/HTTPS access to XpoLog it is required to edit the servlet container configuration that XpoLog uses (standalone installations only, if XpoLog is deployed on a different application server then it has to be done on the application server level):

1. Stop XpoLog
2. Go to XPOLOG_INSTALLATION_DIRECTORY/ServletContainer/conf/ and edit the file server.xml
3. Follow these:
   a. To disable HTTP comment the line:
   
      ```
      <!--
      <Connector protocol="HTTP/1.1" acceptCount="100" connectionTimeout="50000" disableUploadTimeout="true"
      enableLookups="false" maxHttpHeaderSize="8192" maxPostSize="0" maxSpareThreads="75" maxThreads="150"
      minSpareThreads="25" port="30303" redirectPort="30443" xpolog="http"/>
      -->
      ```
   b. To disable HTTPS comment the line:
   
      ```
      <!--
      <Connector acceptCount="100" clientAuth="false" protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"
      compressableMimeTypes="text/html,text/xml" compression="on" compressionMinSize="2048" debug="0"
      disableUploadTimeout="true" enableLookups="false" keystoreFile="${catalina.home}/.keystore" maxHttpHeaderSize="8192"
      maxPostSize="0" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" noCompressionUserAgents="gozilla,
      traviata" port="30443" scheme="https" secure="true" sslProtocol="TLS" xpolog="ssl"/>
      -->
      ```
   4. Save the modification and restart XpoLog.
   Note: XpoLog will not be accessible on the disabled protocol and port (also consider modifying XpoLog agents account URLs if required).

HTTPS Certificate in XpoLog

XpoLog is not shipped with a certificate. These could leave you vulnerable, because the default certificate is the same in every XpoLog download. Data encryption (HTTPS) can be easily used in XpoLog. Keep in mind that encryption with the default certificate is not fully secure and you’re encouraged to create and replace it with your organization’s trusted CA certificate.

For better security, replace the default certificates with certificates signed by a trusted CA. We strongly recommend using CA certs (note that a self-signed certificate is considered untrusted by users’ browsers).

XpoLog standalone installation runs on a Tomcat, for more information about installing a certificate please refer to [https://tomcat.apache.org/tomcat-8.0-doc/ssl-howto.html](https://tomcat.apache.org/tomcat-8.0-doc/ssl-howto.html)

Configuring SNMP Settings

In order for XpoLog to send SNMP Traps (mainly from System Status Console), you must allocate an SNMP server and configure it.
View the XpoLog management information base (MIB) here

To configure SNMP settings:

1. In the General Settings console, open the SNMP tab.
2. In SNMP Host, type the SNMP host address that XpoLog is to use to send traps to.
3. In SNMP Port, type the port that the given SNMP host is listening on.
4. In Version, select Version 1 or Version 2 based on your SNMP server.
5. check Proxy if needed (Default: un-checked).
6. Click the Save button.

The SNMP settings are saved.

XpoLog Alert MIB

Mib Link

Download mib file

Mib source

```plaintext
-- XpoLog Center System Event MIB
-- SNMP V2 Version

XPOLOG-CENTER-SYSTEM-ALERT-MIB

DEFINITIONS ::= BEGIN

IMPORTS
enterprises FROM SNMPv2-SMI
MODULE-IDENTITY FROM SNMPv2-SMI
DisplayString FROM SNMPv2-TC
OBJECT-TYPE FROM SNMPv2-SMI
NOTIFICATION-TYPE FROM SNMPv2-SMI;

---------------------------------------------------------------------------
--
-- XpoLog Module Identity
--
---------------------------------------------------------------------------

xpoLogMIB MODULE-IDENTITY
LAST-UPDATED "201508010000Z"
ORGANIZATION "XpoLog Ltd."
CONTACT-INFO "XpoLog Ltd. http://www.xpolog.com"
DESCRIPTION "SNMPV2 MIB Module for XpoLog Center System Alerts."
REVISION "201508010000Z"
DESCRIPTION "XpoLog Center System Alerts MIB"
::= { enterprises 45222 }

---------------------------------------------------------------------------
--
-- XpoLog Center Tree Structure
--
---------------------------------------------------------------------------

xpoLog OBJECT IDENTIFIER ::= { enterprises 45222 }
products OBJECT IDENTIFIER ::= { xpoLog 1 }
xpoLogCenter OBJECT IDENTIFIER ::= { products 1 }
xpoLogCenterSystemAlert OBJECT IDENTIFIER ::= { xpoLogCenter 1 }

---------------------------------------------------------------------------
--
-- XpoLog Center System Alert objects and structures
--
---------------------------------------------------------------------------

xpoLogCenterSystemAlertKey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The System Alert key."
::= { xpoLogCenterSystemAlert 1 }
```
Configuring Connectivity to a Bug Tracking System

XpoLog provides integration to two common bug tracking systems: Bugzilla by Mozilla and JIRA by Atlassian. You can configure the connectivity details to an available Bugzilla or JIRA bug tracking system that you have in your organization. This enables you to publish events in your log viewer to the bug tracking system that XpoLog is connected to.

To connect XpoLog to a bug tracking system:

1. In the XpoLog Manager menu, select Settings > Bug Tracking System.
   The Bug Tracking Systems page opens, displaying a list of bug tracking systems with connectivity configured in XpoLog.
2. Click the **New Bug Tracking System** button.
3. In the page that appears, select the bug tracking system to add: **Bugzilla** or **JIRA**, and then click **Continue**.
   For Bugzilla, continue as in *Configuring Connectivity to Bugzilla*.
   For JIRA, continue as in *Configuring Connectivity to JIRA*.

   **Note:** Following configuration of a bug tracking system, it is recommended to verify its connectivity. See [Verifying Bug Tracking System Connectivity](#).

### Configuring Connectivity to Bugzilla

To configure connectivity to Bugzilla:

1. In **Name**, type a name for the Bugzilla system that you are connecting to XpoLog; mandatory. Default: **Bugzilla**
2. In **Description**, type a short description of the Bugzilla system to which you are connecting XpoLog; optional.
3. In **Bugzilla URL**, type the URL of the Bugzilla bug tracking system. For example: http://BUGZILLA_HOST:8080/bugzilla; mandatory.
   4. Click **Save**.
   The new bug tracking system appears in the table in the Bug Tracking Systems page.

### Configuring Connectivity to JIRA

To configure connectivity to JIRA:

1. In **Name**, type a name for the JIRA system that you are connecting to XpoLog; mandatory. Default: **JIRA**
2. In **Description**, type a short description of the JIRA system to which you are connecting XpoLog; optional.
3. In **JIRA URL**, type the URL of the JIRA bug tracking system. For example: http://JIRA_HOST:8080; mandatory.
4. In **Port Name**, type the name of the JIRA web service port; mandatory. Default: JirasoapserviceV2
   5. Click **Save**.
   The new bug tracking system appears in the table in the Bug Tracking Systems page.

### Editing Bug Tracking System

You can modify the configuration of a bug tracking system, including its name, description, URL, or port (for JIRA) of a bug tracking system.

To modify a bug tracking system:

1. In the Bug Tracking Systems page, highlight a system in the table, and then click the **Edit** button.
   The details of the bug tracking system are displayed.
2. Modify the parameter values, as required. See *Configuring Connectivity to a Bug Tracking System*.
3. Click **Save**.
   The Bug Tracking Systems page is displayed, with the modified bug tracking system configuration updated in the table.

### Removing a Bug Tracking System

You can remove from XpoLog a bug tracking system that you no longer require.

To remove a bug tracking system from XpoLog:

1. In the Bug Tracking Systems page, highlight a bug tracking system, and then click the **Delete** button.
   A Delete Confirmation box is displayed, requesting confirmation of removal.
2. Click **Yes**.
   The bug tracking system is removed from the table on the Bug Tracking Systems page.

### Verifying Bug Tracking System Connectivity

You can verify the connectivity of any bug tracking system defined in XpoLog.

To verify connectivity:

1. In the Bug Tracking Systems page, highlight a bug tracking system in the table, and then click the **Verify** button.
   The Bug Tracking System Verification box opens. It either informs of successful connectivity, or lists (in red) problems with connectivity, and suggested recommendations.
2. In the Bug Tracking System Verification box, click **OK**.
   The Bug Tracking System Verification box closes.

### Adding Environment Tables

In the XpoLog Environment Settings page, you can define tables with variables that can be used throughout the XpoLog system. You can refer to this environment table in any field by enclosing it in brace brackets and preceding it with a $ sign, as follows: `$(table name:value:key:key name)`.

The advantage of using environment tables is that when the value of the variable changes, you only have to change it in the Environment Settings page, instead of every place that it appears in the XpoLog system. For example, you can add an environment table that contains the path to a
logs folder, so that for every log that you add, you only need to put the environment variable’s name in the Path field, and not the full path. This way, if the path to the log folder changes, you only need to edit the environment variable’s value in one place - on the XpoLog Environment Settings page, thus ensuring that all the logs remain functional.

For example, if the logs are located under the directory "/opt/logs", you can save an environment variable for that location using the name logs.home. When you add logs to XpoLog, you can type $[logs.home] in the log path, instead of the actual path. If the logs directory is transferred elsewhere, you can simply update the environment variable with the new path. All the logs which use $[logs.home] will automatically have the updated value.

Another example, if you have reports that should be generated based on 2 shifts (day shift and night shift), you can save an environment table called “Shifts” in which you will have 2 keys, 1of2 with the value 8-20 and 2of2 with the value 20-8. When you run searches in the XpoLog Search Engine, you can type $[shifts.time:key:1of2] or $[shifts.time:key:2of2] in the search query, instead of the actual time value.

If the value of the shifts is changed, you can simply update the environment table with the new time value. All the queries which use $[shifts.time:key:1of2] or $[shifts.time:key:2of2] will automatically use the updated value.

To add an environment table:
1. In the XpoLog Manager menu, select Settings > Environment Tables.
   The XpoLog environment settings page opens.
2. Click new environment table.
3. In the name and value fields that appear, type the name of the environment table and its value, and then click save.

Removing an Environment Table

You can remove any environment table that you no longer require in the system.

To remove an environment table:
1. In the XpoLog environment settings page, click the remove link adjacent to each environment table that you want to delete.
2. Click save.
   The environment tables are removed from the system.

Viewing the Audit Log

XpoLog contains a comprehensive audit mechanism, which lists in a log every operation that users perform in XpoLog from login until logout.

From the Settings > Audit menu item in the XpoLog Log Viewer, you can run audit filtering of users’ activities.

The available filters are:

- **Time Frames** – for specifying the time frame of the audit view
- **Audit Types** – for specifying the types of actions to view
- **General** – for viewing a specific user’s audit (User Name) or a general term, such as action type, component name, or action description (General)

**Note:** Although not recommended, you can view the audit log on all data, without filtering.

To run audit filtering:
1. In the XpoLog Manager menu, select Settings > Audit.
   The System Audit page opens.
2. Filter the Audit log by time frame, audit type, user name, or general term (see following sections for details).
3. Click generate.
   The filtered audit log view is displayed in the Log Viewer.

**Filtering by Time Frame**

You can filter the audit log to show records from before or after a specific date, or between two specific dates. Alternately, you can show records from a time relative to the current time: from the last minutes, hours, or days; from the previous days, weeks, or months; or from a specified number of days or hours ago for the duration of a specific number of days of hours.

To show records from a specific time period:

- Select the Dates limit option, and do one of the following:
  - Show audit records from a specific date – Select the show records that arrive after checkbox, and click calendar to select a date from the calendar. Default: todays’ date.
  - Show audit records until a specific date – Select the show records that arrive before checkbox, and click calendar to select a date from the calendar. Default: todays’ date.
  - Show audit records between two dates – Select the show records that arrive after and the show records that arrive before checkboxes, and click calendar to select the range of dates from the calendar. Default: todays’ date.

To show records from a time period relative to the current date:

- Select the show records option, and select one of the following options from the dropdown box:
  - Select from – Show records from a specific number of hours or days, for a specific number of hours or days.
  - Select from the last, and input the number of days, hours, or minutes – Show most recent records, as specified.
  - Select from the previous, and input the number of days, weeks, or months – Show previous records, as specified.
Filtering by Audit Type

You can filter the audit log view to show any or all of the following actions performed by users:

- Logins/Logouts
- View system components
- Change system components

**Note:** At least one audit type should be selected.

To filter by audit type:

- In the **Audit Types** section, select the checkboxes of the type of actions to include in the audit view: Logins/Logouts, View system components, or Change system components.

General Filtering

You can filter the audit log view to show operations performed by a specific user, and/or that include a specific term.

To filter by user name or general term:

1. In the **General** section, in **User Name**, type a user name to generate an audit view of a specific user, or leave empty for audit view of all users.
2. In **General**, type a specific term to include in the audit view only operations including this term.

Viewing XpoLog Version and System Patches

The **Settings > About** console displays the following:

- **Version Information:** Includes the version of XpoLog Center installed on your computer, as well as the latest version available. If your version is not the latest, you can download the latest version at [www.xpolog.com](http://www.xpolog.com)
- **Support Information:** Includes a link to the XpoLog Center support portal
- **Patches:** Lists patches that have been made to the system, including their build, date of deployment, and description.

From this console, you can:

- Access the XpoLog Center Support Portal, where you can manage system logs, and view detailed system information.
- Export a system report.
- Publish a patch to local and remote XpoLogs.

To view version and patch information:

- In the XpoLog Manager menu, select **Settings > About**.
  The About XpoLog Center page opens.

Accessing the Support Portal

The XpoLog Center Support Portal includes two tabs:

- **Systems Logs** – includes detailed information on XpoLog logs
- **System Information** – includes detailed system information, XpoLog information, basic information, and license information

To access the support portal:

- In the About XpoLog Center console, click **Open XpoLog Center Support Portal**.
  The Support portal opens.

Accessing the XpoLog Support Portal

From the About XpoLog Center page, you can access the XpoLog Center Support Portal, where you can manage system logs and view detailed system information.

To open the XpoLog Support portal:

- In the About XpoLog Center page, under **Support Information**, click **Open XpoLog Center Support Portal**.
  The Support portal opens. In the **System Logs** tab, you can manage logs; in the **System Information** tab, you can see detailed information on the system.

Exporting the System Support Report

You can export a report of system support information to an XML file.

To export a system support report:

1. In the About XpoLog Center page, click the **Export System Report** link.
   Support information is prepared for the report. This may take a few moments.
2. When the report is prepared, save the XML file.
Installing the Latest Trial Version

The About XpoLog Center console shows the installed XpoLog version, as well as the latest available version. If you do not have the latest version, you can install our free 30-day trial version.

To install the latest trial version:

- In the About XpoLog Center console, click XpoLog Website.
  The XpoLog Center website opens in a separate window, from where you can download the trial version.

Publishing a Patch

You can distribute a patch to all XpoLog cluster nodes and remote XpoLog nodes that exist in your enterprise from a single location.

To publish a patch:

1. In the About XpoLog Center page (Manager > Settings > About), click publish patch.
   The Publish Patch page appears.
2. In Path, click Browse to select the XpoLog patch zip file to be published.
3. Select the nodes which you want to publish the patch to:
   - Current Node: the current XpoLog which the browser is now opened on
   - Cluster Nodes: the nodes which are part of the cluster that the browser is now opened on (appears only if a cluster is active).
   - Enterprise Nodes: select the remote nodes to which you want to publish the patch. You can click select all to select all nodes (appears only if there are any remote enterprise accounts).
4. Click run.

The patch is applied on all the selected XpoLog nodes.

Log Viewer Settings

The Log Viewer Settings allows system administrators to configure a few parameters that impact the Viewer’s behavior:

Log Viewer Records Per Page

Log viewer records per page: a comma separated list of numbers which will be available in the viewer when opening a log. Default values are 25, 50, 100, 250, 500 and may be modified here.
Note that using high number of records per page may impact browser performance.

Default number of records per page: The default number log records which will be presented when opening a log in the viewer. This value should be one of the available options of the ‘log viewer records per page’ list above.

Default Log Search Settings

Default Search: When checked - a search and filter result will be presented from the beginning of the logs (Note: when unchecked the result that will be presented is on current view from current location).

Default Tail Settings

Tail refresh rate: you can set the refresh rate of tailing (in seconds). Note: when activating the tail on log viewer XpoLog is loading the new records, if available, according to the specified refresh rate.

Tail number of records view: while tailing XpoLog will accumulate the selected number of records in log viewer. Note: after the view will reach the selected number of records, XpoLog will restart the accumulation in a new page.

Search Context Menu

Context menu may be used when right-clicking a log column value in the log viewer (under the option ‘Search’). By using the placeholder [LOG_COL_DATA] you can use the right-clicked value in an external site.
For example an internal organization site that can identify information from the logs, XpoLog Search engine, Google, etc.

Sort Folders and Logs Alphabetically

By default, Folders and Logs that are created in XpoLog are sorted by creation. If you wish to apply an alphabetical sorting of the entire tree, follow these steps:

1. Open a browser to XpoLog, login if required.
2. Go to Manager > Settings > About, click the Open XpoLog Center Support Portal link - a new browser/tab will be opened displaying the support console.
3. Select Advanced Settings at the top of the screen select box.
4. Search for the property ‘module.sortMembersAlphabetically’ (set to false by default).
5. Right click > Edit it and enter true as the custom value.
6. Save and restart XpoLog.

The Folders and Logs tree will be displayed sorted alphabetically.

Security

The Security menu is displayed in the XpoLog Manager menu, only if security has been activated in the General Settings Security tab (see Configuring General Security Settings).

Using the Security mechanism of XpoLog, Administrators do the following:

- Create groups, which are composed of users or groups that have the same permissions and tasks in the system, and manage them (see Managing Groups).
- Create policies that define permissions that can be assigned to the various groups or users for performing activities in the system, and manage them (see Managing Policies).
- Create Users and associate them with groups and assign to them a policy, and manage them (see Managing Users).
- Change their password or display name (see Changing Your Password or Display Name).

If your organization uses an internal XpoLog realm to authenticate Users, Administrators can do all of the above. However, if your organization uses an external XpoLog realm for assigning usernames and passwords to users and for authentication, Administrators can only create Groups and Policies.

Changing Your Password or Display Name

In the Security > User General Settings page, you can change your password and display name (used whenever the user is displayed, as in administration or in the welcome message).

Note: The default user name and password of the Administrator are: admin

To change your password or display name:

1. In the XpoLog Manager menu, click Security > User General Settings.
   The User General Settings console opens.
2. In Old Password, type your current password.
3. In New Password, type your new password, and retype it in Confirm Password.
4. In Display Name, type the name to appear whenever your name is displayed in XpoLog.
5. Click Save.
   Your new settings are saved throughout the system.

Note regarding passwords encryption and decryption

All the encryption and decryption of passwords in XpoLog are based on JCE (Java Cryptography Extension). The default encryption/decryption is using "DES" algorithm with SUN JCE Provider that uses ECB as the default mode and PKCS5 Padding (this is configurable in XpoLog).

Available encryption algorithms:

- DES: 56 bits
- Triple DES: 112 bits
Apply Permissions on a Folder or Log

A policy is assigned to each user/group of XpoLog to define the permissions of that user/group members in the system. The policy includes permissions for viewing and editing logs and folders and applying different operations in the system. In addition, for a specific log/folder/application, XpoLog enables Administrators to edit the permissions granted to a user/group, so that the log/folder/application will be exposed to them or not.

It lets the Administrator choose one of the following to define the permissions of users on the folder/log:

- **Use parent permissions** – the folder/log inherits permissions from its parent folder.
- **Use application permissions** – the folder/log has the permissions defined in the application which the folder/log is tagged to.
- **Use specified permissions** – the folder/log has the permissions that you assign on this page.

To edit permissions of a folder or log:

1. In the XpoLog menu, click **Administration > Folders and Logs**, select a folder or log, and then click the **Permissions** button.
   Alternately, in the Log Viewer left pane, under the **Folders and Logs** menu, right-click a log, and click **Edit Permissions**. The Permissions console opens.
2. Select one of the following options:
   - **Use parent permissions**
   - **Use specified permissions**
3. Under **Edit Group Members**, in the **Available Members** list, select a member that you want to be able to view and edit the folder/log, and click **Add**.
   The member is moved to the **Selected Members** list.
4. Repeat step 3 for each user/group that is to be permitted to view and edit the folder/log. **Note:** You can remove a user/group from the **Selected Members** list by selecting it and clicking **Remove**. It then returns to the **Available Members** list.
5. Under **View Group Members**, in the **Available Members** list, select a member that you want to be able to view only the folder/log, and click **Add**.
   The group is moved to the **Selected Members** list.
6. Repeat step 5 for each user/group that is to be permitted to view only the folder/log. **Note:** You can remove a group from the **Selected Members** list by selecting it and clicking **Remove**. It then returns to the **Available Members** list.
7. Click **Apply**.
   The permissions are applied on the selected folder/log.

**LDAP/AD Authentication**

In case the authentication of users is done against an LDAP or Active Directory (see **LDAP/AD Authentication**) it is possible to assign permissions on groups which are defined in the organizational LDAP/AD.

Add groups in XpoLog - XpoLog>Security>Groups, for each new group set its name to be the exact name as it is in the LDAP/AD server, no need to change anything inside it will be done automatically. Set the relevant policy from the policies list to the created group. In case no policy will be selected; the default policy will be applied to the authenticated user which is associated to this group.

Specify on each Folder/Log/Application which group is allowed to view it as described above (make sure the All group is removed from the top Folders and Logs and other Folders/Logs).

When a user will sign in to XpoLog ( authenticating against the LDAP/AD) XpoLog will match the groups retrieved from the LDAP/AD and will look to a matched group which is defined internally - in case such a match exists the user will be enforced with the group's policy and permissions (based on the group's policy) automatically.

XpoLog audit (audit log) the list of groups that the authenticated user is associated to in the LDAP/AD server. After a user signs in, you can check the list of groups in the audit log in order to create matching groups internally in XpoLog.

**Managing Users**

**Note:** Users can be managed in XpoLog, only if an internal XpoLog realm is being used to define and authenticate users.

From the **Security > Users** console, Administrators can:
- View a listing of all users in XpoLog, and filter the list to display users from a specific group.
- Create a user.
- Modify or view a user's settings and lock a user.
- Unlock a user.
- Remove a user from XpoLog.

An XpoLog user must be assigned to at least one group. This way, permissions can be assigned to the user at a group level, as opposed to at a user level.

Viewing and Filtering XpoLog Users

In the Security > Users console, Administrators can view a listing of all users defined in XpoLog, or in a specific group.

The Users list can be filtered to display users from a specific group. This is especially useful when there are many users defined in the system, and you want to quickly find the user so that you can view or modify its settings, or delete it.

Viewing XpoLog Users

To view users defined in XpoLog:

- In XpoLog Manager, click Security > Users.
  The Users console opens, listing all the users that are defined in XpoLog.

Filtering Users Display

To filter the users display:

- In the Users console, select from the Groups drop-down list, a group.
  The users from the selected group are displayed under Group Users.

Adding a New User

In the Users Settings console, Administrators can add new users to XpoLog.

For each new user, the Administrator can:

- Assign a username and password.
- Associate the user with a user group that is defined in the system. Associating a user with a group enables giving permissions to a user at a group level, instead of at a user level.
- Select the user groups that are to be under the new user's administration.
- Set the policy used by the user – either the policy of the groups that the the user is associated with or another policy.

Note: At least one associated group must be selected for a new User.

To add a new User to XpoLog:

1. In the XpoLog Manager menu, click Security > Users.
   The Users console opens.
2. In the Users console, click Add User.
   The Users Settings console opens.
3. In Username, type a username for identifying the new user.
4. In Password, type a password for the new user, and in Confirm Password, retype the password.
5. In Display Name, type the name to be displayed across the system for this user.
6. Under Associated Groups List, in Available Groups, select a group that you want the user to be associated with, and click Add.
   The group is moved to the Associated Groups list.
7. Repeat step 6 for each group that you want the user to be associated with.
   Note: You can remove a group from the Associated Groups list by selecting it and clicking Remove. It then returns to the Available Groups list.
8. Under Administered Groups List, in Available Groups, select the group that you want the user to administer, and click Add.
   The group is moved to the Administered Groups list.
9. Repeat step 8 for each group that you want the user to administer.
   Note: You can remove a group from the Administered Groups list by selecting it and clicking Remove. It then returns to the Available Groups list.
10. Under Policy Settings, select either of the following options:
    Use the Policy of the selected groups
**Use the following Policy:** in the adjacent drop-down list, select one of the policies that is defined in the system.

11. Click **Save**.  
The Operation Done page appears with the message: "Users operation ended successfully".

12. Click **ok**.  
The Users console opens with the new User on the list.

---

**Modifying/Viewing XpoLog User Settings**

1. From the Security > Users console, Administrators can view or modify the settings of any XpoLog User, with the exception of their Username and Password. An administrator can also lock a user.

**Viewing User Settings**

Administrators can view the settings of any user.

To view user settings:

1. In the XpoLog Manager menu, click **Security > Users**.  
The Users console opens.
2. In the Users console, optionally filter the Users display, by selecting in **Groups**, a group.  
The users of the selected group are displayed on the console.
3. Click the **Edit** link adjacent to the group.  
The User Settings console opens, displaying the settings of the selected user.
4. Click **Cancel**.  
The Users console opens, displaying all the users in the system.

**Modifying User Settings**

Administrators can modify the following user settings:

- **Display Name of the user**
- **Groups to which the user is associated**
- **Groups that this user administers**
- **Policy used by the user**

To modify a user’s settings:

1. In the XpoLog Manager menu, click **Security > Users**.  
The Users console opens.
2. In the Users console, optionally filter the Users display, by selecting in **Groups**, a group.  
The users of the selected group are displayed on the console.
3. Under **Group Users**, click **Edit** on the row of the User whose settings you want to modify.  
The User Settings console opens.
4. Modify the **Display Name**, and the selected **User Groups, Administered Groups**, and **Policy**, as required. See **Adding a New User** for details.
5. To lock the user, select the **Lock Out** checkbox.
6. Click **Save**.
7. Operation Done page appears, with message: "User operation ended successfully."
8. Click **ok**.  
The Users console opens, displaying all the users in the system.
If the user has been locked, the Unlock link appears on the user row.

---

Removing a User from XpoLog
From the Users console, Administrators can delete from the system an XpoLog user.

**Note:** You cannot remove an Administrator user.

To remove a user from XpoLog:

1. In the XpoLog Manager menu, click **Security > Users**.
   - The Users console opens.
2. Under **Group Users**, click **delete** on the row of the user that you want to delete.
   - The Operation Verification page appears, asking you to confirm the user removal.
3. Click **ok**.
   - The Operation Done page appears, with the message: “User removal ended successfully.”
4. Click **ok**.
   - The Users console appears, with the deleted user removed from the list.

**Unlocking a User**

Users who have unsuccessfully logged in to XpoLog five times, are automatically locked. Also, administrators can choose to lock users (See *Modifying/Viewing XpoLog User Settings*.)

In the Security > Users console, locked users have an Unlock link on their row. Administrators can unlock users who have been locked.

**To unlock a user:**

1. In the XpoLog Manager menu, click **Security > Users**.
   - The Users console opens.
2. Under **Group Users**, click **Unlock** on the row of the User that you want to unlock.
   - Operation Done page appears, with message: “User unlock ended successfully.”
3. Click **ok**.
   - The Users console opens, displaying all the users in the system. The Unlock link no longer appears on the user row.

**Managing Groups**

From the Security > Groups console, Administrators can:

- View a listing of all groups in XpoLog, and filter the list to display a specific group.
- Create a group.
- Modify or view a group's settings.
- Remove a group from XpoLog.

Groups can be composed of users and/or other groups defined in the system.

An XpoLog user must be associated with (i.e. belong to) at least one group. **This way, permissions can be assigned to users at a group level, as opposed to at a user level.**

**Note:** An XpoLog system has at a minimum an Administrators group and an All group.

**Viewing and Filtering XpoLog Groups**

In the Security > Groups console, Administrators can view a listing of all groups defined in XpoLog.

The Groups list can be filtered to display a specific group. This is especially useful when there are many groups defined in the system, and you want to quickly find the group so that you can view or modify its settings, or delete it.

**Viewing XpoLog Groups**

To view groups defined in XpoLog:

- In XpoLog Manager, click **Security > Groups**.
  - The Groups console opens, listing all the groups that are defined in XpoLog.

**Filtering Groups Display**

To filter the groups display:

- In the Groups console, select from the Groups drop-down list, a group.
  - The selected group is displayed under **Group Members**.

**Creating a New Group**

From the Security > Groups console, Administrators can create new groups in XpoLog.

To create an XpoLog group:

1. In the Groups console, click **Add Group**.
   - The Group Settings console opens.
2. In **Group name**, type a name to identify the new group.
3. In **Display Name**, type the name that is to be displayed across the system.
4. In **Description**, type a description of the new group; optional.
5. Under **Groups List**, in **Available Groups**, select a group to associate with this group, and click **Add**.
   The selected group is moved to the **Associated Groups** list.
6. Repeat step 5 for all groups to associate with the new group.
   **Note:** You can disassociate a group from the new group, by selecting it in the **Associated Groups** list, and clicking **Remove** to return it to the **Available Groups** list.
7. Under **Administered Groups List**, in **Available Groups**, select the group that this group is to administer, and click **Add**.
   The selected group is moved to the **Administered Groups** list.
8. Repeat step 7 for all groups that this new group is to administer.
   **Note:** You can remove an administered group from the new group, by selecting it in the **Administered Groups** list, and clicking **Remove** to return it to the **Available Groups** list.
9. Under **Group Members**, in **Available Members**, select a group or user that is to be a member of the new group, and click **Add**.
   The selected group or user is moved to the **Selected Members** list.
10. Repeat step 9 for all members to add to this new Group.
    **Note:** You can remove a member from the group, by selecting it in the **Selected Members** list, and clicking **Remove** to return it to the **Available Members** list.
11. Under **Policy Settings**, select one of the following:
    **Use the policy of the selected groups**
    **Use the following Policy**, and in the adjacent drop-down box, select the Policy to use for the new group.
12. Click **Save**.
    The Operation done page appears, with the message:“Group operation ended successfully”.
13. Click **ok**.
    The Groups console opens, with the newly added group under the **Groups members** list.

**Modifying/Viewing Group Settings**

From the **Security > Groups** console, Administrators can view or modify a group's settings.

The settings of all groups, with the exception of the All and Administrators groups, can be modified. These groups can only be viewed.

**Viewing Group Settings**

From the Security > Groups console, Administrators can view the settings of any group.

To view group settings:

1. In the XpoLog Manager menu, click **Security >Groups**.
   The Groups console opens.
2. In the Groups console, optionally filter the Groups display, by selecting in **Groups**, a group to view.
   The selected group is displayed on the console.
3. To view the settings of the All or Administrators group, click the **View** link adjacent to the group.
   To view the settings of any other group, click the **edit** link adjacent to the group.
   The Group Settings console opens, displaying the settings of the selected group.
4. Click **Cancel**.
   The Groups console opens, displaying all the groups in the system.

**Modifying Group Settings**

From the Groups console, Administrators can view or modify the settings of an XpoLog group, with the exception of the Group Name.

The modifiable settings include:

- **Display Name of the group**
- **Description of the group**
- **Groups to which the group is associated**
- **Groups that this group administers**
- **Group members**
- **Group administrators**
- **Policy used by the group**

**Note:** You cannot modify the settings of the All and Administrators groups.

To modify a Group's settings:

1. In the XpoLog Manager menu, click **Security >Groups**.
   The Groups console opens.
2. In the Groups console, optionally filter the Groups display, by selecting in **Groups**, a group.
   The selected group is displayed on the console.
3. Under **Groups Members**, click **edit** on the row of the group whose settings you want to modify.
   The Group Settings console opens.
4. Modify the **Display Name, Description**, and the **Associated Groups, Administered Groups, Group Members, Group**
Removing a Group from XpoLog

From the Groups console, Administrators can delete from the system, an XpoLog group that is no longer relevant, provided that it is not being used.

Note: You cannot remove the Administrators or All group.

To remove a Group from XpoLog:

1. In the XpoLog Manager menu, click **Security > Groups**.
   The Groups console opens.
2. In the Groups console, optionally filter the Groups display, by selecting in **Groups**, a group.
   The selected group is displayed on the console.
3. Under **Groups Members**, click **delete** on the row of the group that you want to delete.
   The Operation Verification page appears, asking you to confirm the group removal.
4. Click **ok**.
   The Operation Done page appears, with the message: “Groups removal ended successfully.”
5. Click **ok**.
   The Groups console opens, with all groups, but not the deleted group, displayed on the list.

Managing Policies

Each user and group defined in XpoLog is assigned a policy that defines the permissions that the user/group has in XpoLog, i.e. a set of activities (functionalities) that users of the policy can perform in the system.

A policy can be set to grant permission to perform all actions in the system, or specific actions. A policy can also give View Only permission, and not permit performing any actions in XpoLog.

From the Security > Policies console, Administrators can:

- View a listing of all policies in XpoLog.
- Create a policy.
- Modify or view a policy's settings.
- Remove a policy from XpoLog.

Although a policy defines the permissions that a user has in the system, XpoLog enables the Administrator to customize permissions for individual folders and logs in XpoLog (see **Apply Permissions on a Folder or Log**).

Viewing Policies

In the Security > Policies console, Administrators can view a listing of all policies defined in XpoLog.

To view policies defined in XpoLog:

- In XpoLog Manager, click **Security > Policies**.
  The Policies console opens, listing all the policies that are defined in XpoLog.

Creating a New Policy

From the Security > Policies console, Administrators can create new policies in XpoLog.

A policy defines the actions that a user or group that is assigned this policy, can perform. All actions of a specific component (categories) (such as Analytics, Monitors, Search, and more), or specific actions can be permitted under a specific policy. Selecting a parent component automatically permits all the components underneath it.

Defining a policy without selecting any permissions defines a View Only permission for folders and logs, and no permission for all other components in XpoLog.

To create a policy:

1. In the Policies console, click **Add Policy**.
   The Policy Settings console opens.
2. In **Policy name**, type a name to identify the new policy.
3. In **Display Name**, type the name that is to be displayed across the system.
4. In **Description**, type a description of the new policy; optional.
5. Under **Permissions List**, select the checkboxes of components or actions that are permitted to users of this policy
6. Click **Save**.
The Operation done page appears, with the message: "Policies operation ended successfully".

7. Click ok.
The Policies console opens, with the newly added policy under the Policies list.

Modifying/Viewing Policy Settings

From the Security > Policies console, Administrators can view or modify a policy's settings.
The settings of all policies, with the exception of the Administrations policy, can be modified. This policy can only be viewed.

Viewing Policy Settings

From the Security > Policies console, Administrators can view the settings of any policy.

To view policy settings:

1. In the XpoLog Manager menu, click Security > Policies.
The Policies console opens.
2. To view the settings of the Administrations policy, click the View link adjacent to the policy.
   To view the settings of any other group, click the Edit link adjacent to the policy.
   The Policy Settings console opens, displaying the settings of the selected policy.
3. Click Cancel.
The Policies console opens, displaying all the policies in the system.

Modifying Policy Settings

From the Policies console, Administrators can view or modify the settings of an XpoLog policy, with the exception of the Policy name.
The modifiable settings include:

- Display Name of the policy
- Description of the policy
- Actions with permissions

Note: You cannot modify the settings of the Administrations policy.

To modify a Policy's settings:

1. In the XpoLog Manager menu, click Security > Policies.
The Policies console opens.
2. Under Policies, click edit on the row of the group whose settings you want to modify.
The Policy Settings console opens.
3. Modify the Display Name, Description, and the selected actions in the Permissions list. See Creating a New Policy for details.
4. Click Save.
   Operation Done page appears, with message: "Policies operation ended successfully."
5. Click ok.
The Policies console opens, displaying all the policies in the system.

Removing a Policy from XpoLog

From the Policies console, Administrators can delete from the system, an XpoLog policy that is no longer being used.

Note: You cannot remove the Administrations policy.

To remove a Policy from XpoLog:

1. In the XpoLog Manager menu, click Security > Policies.
The Policies console opens.
2. Under Policies, click delete on the row of the policy that you want to delete.
The Operation Verification page appears, asking you to confirm the policy removal.
3. Click ok.
The Operation Done page appears, with the message: "Policy removal ended successfully."
4. Click ok.
The Policies console opens, with all policies, but not the deleted policy, displayed on the list.

Importing/Exporting a Log

From the Tools menu in XpoLog Manager, you can export a log from XpoLog or import a log into XpoLog.

Exporting a Log

From the Tools > Export Log menu item, you can export any log that is displayed in the XpoLog Log Viewer, together with its configuration or only its data. For a complete explanation, see Exporting a Log in the User Guide.
Importing a Log

From the Tools > Import Log menu item in XpoLog Manager, you can import into XpoLog any log that has previously been exported from XpoLog (your system or another system) together with its configuration.

Note: It is only possible to import logs that were created with XpoLog version 2.2 and later.

To import a log into XpoLog:

1. In the XpoLog Manager menu, select **Tools > Import Log**.
   The Import Log page is displayed.
2. In **Path**, type or browse to the XpoLog archive file location of the zipped log file to import.
3. Click the **Next** button.
4. In the Parent Folder Selection page that appears, in **Parent Folder**, click the **select** link to select a parent folder for this log from the list of available folders, or create a new folder under which to place the log.
5. Click the **Next** button.
   The log is imported into the selected location, and a message notifies you of such.
6. Click **OK**.
   The Log Viewer opens, displaying the imported log records.

XpoLog API / SDK

- XpoLog API provides a URL-based querying of XpoLog to retrieve information from XpoLog.
- XpoLog SDK provides a set of commands that enables remote configuration of different XpoLog properties without accessing the GUI.

XpoLog API

**General**

XpoLog exposes a URL based API to the users. The API exposes a set of HTTP/S calls that can be used to retrieve information from XpoLog:

- **URL that returns events from XpoLog Search in XML/CSV format**
- **URL that returns a Dashboards latest result in PDF format**
- **URL to open Search console on an executed search query**
- **URL to open a specific log in the Log Viewer**
- **URL to enter XpoLog under specific Folder(s) context**
- **URL to enter XpoLog under specific AppTag(s) context**
- **URL that returns Collected Data Information**

**Security**

In case security is activated in XpoLog (login is required) then using the URL based API will require passing user's credentials in order to login into the system prior to executing the API command.

It is required to pass the username and password in the URL to XpoLog in order to get the command executed.

Add to each link at the end:

```
&autoLogin=true&username=[USER_NAME]&password=[PASSWORD]
```

[USER_NAME] = the user name which the API will use to login

[PASSWORD] = the password of the user name
1. http://[MACHINE_NAME]:[XPOLOG_PORT]/logeye/view/api/widgetAPI.jsp?widgetId=searchAPI&searchQuery=[see item 2]&fixedInterval=[see item 3]&startTimeFullStr=[see item 4]&endTimeFullStr=[see item 4]&maxNumOfRecords=[see item 5]&resultFormat=[see item 6]&paginate=[see item 7]&maxRecordsPerPage=[see item 8]

2. searchQuery=a query as used in XpoSearch console

3. fixedInterval=optional values are: last15Minutes, last30Minutes, last60Minutes, last3Hours, last12Hours, last24Hours, last7Days, last14Days, last1Months, last6Months, currentDay, previousDay, currentWeek, previousWeek, allData

   IMPORTANT: when using fixedInterval only values from the above list can be provided as is. Optional; if fixedInterval is used then startTimeFullStr and endTimeFullStr should not be used.

4. startTimeFullStr=the start time full string, formatted according to the XpoLog system format; default format is MM/dd/yyyy HH:mm:ss

   endTimeFullStr=the end time full string, formatted according to the XpoLog system format; default format is MM/dd/yyyy HH:mm:ss

   Optional; used only if fixedInterval is missing; if used, both values are mandatory.

5. maxNumOfRecords=the maximal number of records to return in the result; if missing, the default value is taken from the widgets.searchAPI.maxNumOfRecords XpoLog system property (default is 100 but may be modified)

6. resultFormat=the format in which the result will be returned. Optional values xml/csv (case sensitive)

7. paginate=activate pagination; optional values true/false

8. maxRecordsPerPage=the maximal number of results per page; If missing, the default value is 100 records per page.

The following is the XML structure of the API execution response:

```xml
<APIResult>
  <Status state="OK">
    <Url>[URL_TO_RESULT_FILE]</Url>
    <Message/>
  </Status>
  <Data/>
</APIResult>
```

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APIResult</td>
<td>General document root tag</td>
</tr>
<tr>
<td>Status</td>
<td>The state of the API execution. Optional values OK/Fail</td>
</tr>
<tr>
<td>Url</td>
<td>Exists only when the status is OK. The URL to a file containing the API execution result.</td>
</tr>
<tr>
<td>Message</td>
<td>Exists only when the status is Fail.</td>
</tr>
<tr>
<td>Data</td>
<td>Contains the API execution result. Note: When the result format is CSV, the content of the &lt;Data&gt; tag will be wrapped with CDATA. Note: If the execution result is larger than the system-configured limit, the &lt;Data&gt; tag will not contain the execution result. Instead, the content of the &lt;Url&gt; tag should be used to access the execution result file.</td>
</tr>
</tbody>
</table>

**Examples**

(You need to change machine/port/logs names, ids / folder names, ids / application names, ids if used to be relevant to your environment)

- Returns records matching the search query “error or fail” in logs that their names start with “log4j” in the specified time frame. Result is limited to maximum 1000 log records in csv format:

  `http://localhost:30303/logeye/view/api/widgetAPI.jsp?widgetId=searchAPI&searchQuery=error or fail* in log.log4j*&startTimeFullStr=01/01/2014 00:00:00&endTimeFullStr=02/02/2014 00:00:00&maxNumOfRecords=1000&resultFormat=csv`

- Returns records matching the search query “error or exception in in all logs in the last 7 days’ time frame. Result is limited to maximum 1000 log records in xml format:

  `http://localhost:30303/logeye/view/api/widgetAPI.jsp?widgetId=searchAPI&searchQuery=error or exception&fixedInterval=last7Days&maxNumOfRecords=1000&resultFormat=xml`

- Returns the complex search query “* in app.Windows Event Logs | count | group by event’ result in the last 7 days’ time frame. Result is limited
to maximum 1000 entries in csv format. In this example the URL also contains a username and password (admin/admin) that will perform a login to XpoLog in order to be able to execute the search query:

ount%20%20group%20by%20event&fixedInterval=last7Days&maxNumOfRecords=1000&resultFormat=csv&autoLogin=true&username=admin
$password=admin

**URL that returns a Dashboard’s latest result in PDF format**

1. http://[MACHINE_NAME]:[XPOLOG_PORT]/logeye/view/api/dashboardAPI.jsp?action=export&appName= [see item 2]&viewName= [see item 3]
2. appName=a name of an existing App in XpoLog (case insensitive).
3. viewName=a name of an existing Dashboard in XpoLog (case insensitive).

**Examples**

(You need to change machine/port/logs names, ids / folder names, ids / application names, ids if used to be relevant to your environment)

- Returns the Dashboard “Dashboard-1” in PDF format

http://localhost:30303/logeye/view/api/dashboardAPI.jsp?action=export&appName=App-1&viewName=Dashboard-1

**URL to open Search console on an executed search query**

1. http://[MACHINE_NAME]:[XPOLOG_PORT]/logeye/search/view/loadSearchModel.jsp?searchQuery= [see item 2]&fixedInterval= [see item 3]&startTimeFullStr= [see item 4]&endTimeFullStr= [see item 4]
2. searchQuery=a query as used in XpoSearch console
3. fixedInterval=optional values are: last15Minutes, last30Minutes, last60Minutes, last3Hours, last12Hours, last24Hours, last7Days, last14Days, last1Months, last6Months, currentDay, previousDay, currentWeek, previousWeek, allData
   IMPORTANT: when using fixedInterval only values from the above list can be provided as is. Optional; if fixedInterval is used then startTimeFullStr and endTimeFullStr should not be used.
4. startTimeFullStr=the start time full string, formatted according to the XpoLog system format; default format is MM/dd/yyyy HH:mm:ss
   endTimeFullStr=the end time full string, formatted according to the XpoLog system format; default format is MM/dd/yyyy HH:mm:ss
   Optional; used only if fixedInterval is missing; if used, both values are mandatory.

**Examples**

(You need to change machine/port/logs names, ids / folder names, ids / application names, ids if used to be relevant to your environment)

- Presents Search console after execution of the search query “error” in the specified time frame:

http://localhost:30303/logeye/search/view/loadSearchModel.jsp?searchQuery=error&startTimeFullStr=01/01/2014
00:00:00&endTimeFullStr=02/02/2014 00:00:00

- Presents Search console after execution of the search query “error” in the specified time frame (last 7 days):

http://localhost:30303/logeye/search/view/loadSearchModel.jsp?searchQuery=error&fixedInterval=last7Days

**URL to open a specific log in the Log Viewer**

1. http://[MACHINE_NAME]:[XPOLOG_PORT]/logeye/view/api/logViewAPI.jsp?logId= [see in item 2]&searchQuery= [see item 3]&logFilter
   Name= [see item 4]&filterName= [see item 5]&filterId= [see item 6]&startTimeFullStr= [see item 7]&endTimeFullStr= [see item 8]&opdire
   ct= [see item 9]&expandLogViewer= [see item 10]
2. logId=one or more log ids, separated by comma (mandatory parameter)
3. searchQuery=a term to filter the log by (similar syntax to XpoSearch)
4. logFilterName=the name to be given to the filter defined in item c; if missing, the name of the filter will be ‘external filter’
5. filterName=the name of an existing filter that should be activate on the log; used only if the searchQuery parameter is missing
6. filterId=the id of an existing filter that should be activate on the log; used only if the searchQuery parameter is missing or if the filterName parameter is missing or does not match an existing filter’s name
7. startTimeFullStr=the start time full string, formatted according to the XpoLog system format; default format is MM/dd/yyyy HH:mm:ss
8. endTimeFullStr=the end time full string, formatted according to the XpoLog system format; default format is MM/dd/yyyy HH:mm:ss
9. opdirect=start will display the first records of the result; last will display the last records. Default is start.
10. expandLogViewer=true will present the log in the viewer without the folder and logs and the menu presented. Default is false.

* Contact XpoLog Support to find out how to retrieve applications/folders/logs/filters IDs.

Examples
(You need to change machine/port/logs names, ids / folder names, ids / application names, ids if used to be relevant to your environment)

- Enter the viewer on the log Application_1235558747694 filtered on records that contain ‘error or information’ (the name of the temporary filter is set to be testQuery):
  http://localhost:30303/logeye/view/api/logViewAPI.jsp?logId=Application_1235558747694&searchQuery=error or information&logFilterName=testQuery

- Enter the viewer on the log Application_1235558747694 with an existing filter named ‘error’ activated (the last matching events will be presented):
  http://localhost:30303/logeye/view/api/logViewAPI.jsp?logId=Application_1235558747694&filterName=error&opdirect=last

- Enter the viewer on a merge of the logs Application_1235558747694 and Security_1235558747851 filtered on records in the specified time frame (the name of the filter is set to be testTimeFilter):
  http://localhost:30303/logeye/view/api/logViewAPI.jsp?logId=Application_1235558747694&filterName=testTimeFilter&startTimeFullStr=01/01/2014 00:00:00&endTimeFullStr=02/01/2014 00:00:00

- Enter the viewer on the log Application_1235558747694 with the filter ‘error’ activated but also filtered on records in the specified time frame (the name of the temporary filter is set to be testFilterAndTime and the last matching events will be presented). Log viewer will be expanded (the folders and logs tree and the top menus will not be presented):
  http://localhost:30303/logeye/view/api/logViewAPI.jsp?logId=Application_1235558747694&filterName=error&opdirect=last&startTimeFullStr=05/01/2012 00:00:00&endTimeFullStr=05/03/2012 00:00:00&expandLogViewer=true

URL to enter XpoLog under specific Folder(s) context
1. http://[MACHINE_NAME]:[XPOLOG_PORT]/logeye/componentAction.jsp?selectedCompId=XpoLog&forward=root.jsp?folderId=[see item 2]&mainPage=view/mainView.jsp
2. folderId=a comma separated list of folder ids (mandatory parameter)

* Contact XpoLog Support to find out how to retrieve applications/folders/logs/filters IDs.

Examples
(You need to change machine/port/logs names, ids / folder names, ids / application names, ids if used to be relevant to your environment)

- Enter into XpoLog directly to view the folder with ID 1271697039748 under the Folders and Logs tree:
URL to enter XpoLog under specific AppTag(s) context

1. http://[MACHINE_NAME]:[XPOLOG_PORT]/logeye/componentAction.jsp?selectedCompId=XpoLog&forward=root.jsp?applicationId=[see item 2]&mainPage=view/mainView.jsp
2. applicationId=a comma separated list of AppTags ids (if an empty application id is provided, it will reset any AppTag context).

* Contact XpoLog Support to find out how to retrieve AppTags/Folders/Logs/filters IDs.

Examples

(You need to change machine/port/logs names, ids / folder names, ids / application names, ids if used to be relevant to your environment)

- Enter into XpoLog with under the AppTag app1 context:
  http://localhost:30303/logeye/componentAction.jsp?selectedCompId=XpoLog&forward=root.jsp?applicationId=app1&mainPage=view/mainView.jsp

- Enter into XpoLog with under the AppTags app1,app2 context:
  http://localhost:30303/logeye/componentAction.jsp?selectedCompId=XpoLog&forward=root.jsp?applicationId=app1,app2&mainPage=view/mainView.jsp

URL that returns Collected Data Information

1. http://[MACHINE_NAME]:[XPOLOG_PORT]/logeye/message/messageJsonApi.jsp?api=collectedDataInfo&type=[see item 2]&timeFrame=[see item 3]&detailsLevel=[see item 4]&maxNumberOfResults=[see item 5]
2. type = fixed string values: AppTags / Folders (default = Folders)
3. timeFrame = fixed string values: last15Minutes, last30Minutes, last60Minutes, last3Hours, last12Hours, last24Hours, last7Days, last14Days, last1Months, last6Months, currentDay, previousDay, currentWeek, previousWeek, allData (default = last24Hours)
4. detailsLevel = fixed string values: Basic, Detailed

a. Basic – returns a JSON specifying: AppTag/Folder based on specified type with AppTag/Folder name, number of defined log and number of collected logs.

Examples:

http://localhost:30303/logeye/message/messageJsonApi.jsp?api=collectedDataInfo&type=Folders&timeFrame=last24Hours&detailsLevel=Basic&autoLogin=true&username=admin&password=admin

Result JSON:

6.1.0.9, "collectedLogs":0}, "totalLogs":1, "Folders": "CloudXpLog", "collectedLogs":0}]}

http://localhost:3003/logeye/message/message.JsonApi.jsp?api=collectedDataInfo&type=AppTags&timeFrame=last24Hours&detailsLevel=Basic&autoLogin=true&username=admin&password=admin

Result JSON:

{"data":{"collectionData":{"totalLogs":1, "collectedLogs":0, "AppTags": "Tomcat 5.0.28"}, "totalLogs":22, "collectedLogs":0, "AppTags": "PrudentialA"}, "totalLogs":1, "collectedLogs":0, "AppTags": "XplgWiki"}, {"totalLogs":4, "collectedLogs":3, "AppTags": "Tomcat"}, {"totalLogs":11, "collectedLogs":0, "AppTags": "LogLooud"}, {"totalLogs":11, "collectedLogs":0, "AppTags": "DASTLab"}, {"totalLogs":10, "collectedLogs":0, "AppTags": "Example AppTag"}, {"totalLogs":9, "collectedLogs":0, "AppTags": "XpLog"}, {"totalLogs":2, "collectedLogs":1, "AppTags": "Website"}, {"totalLogs":1, "collectedLogs":0, "AppTags": "Lab_LoadTest"}, {"totalLogs":1, "collectedLogs":0, "AppTags": "Audit"}, {"totalLogs":24, "collectedLogs":0, "AppTags": "AppInTech_LoadIab"}, {"totalLogs":19, "collectedLogs":8, "AppTags": "Linux"}, {"totalLogs":5, "collectedLogs":0, "AppTags": "Linux OS"}, {"totalLogs":7, "collectedLogs":0, "AppTags": "Weblogic 10.0"}, {"totalLogs":10, "collectedLogs":0, "AppTags": "VOLoadTesting"}, {"totalLogs":2, "collectedLogs":0, "AppTags": "Log4J"}, {"totalLogs":1, "collectedLogs":0, "AppTags": "JET-XPLG"}, {"totalLogs":9, "collectedLogs":0, "AppTags": "ID"}}

b. Detailed – returns a JSON specifying: AppTag/Folder based on specified type, number of defined logs, number of collected logs and a list of uncollected logs with their sizes in bytes (comma separated full Folders path in XpoLog Folders and Logs tree).

Examples:

http://localhost:3003/logeye/message/message.JsonApi.jsp?api=collectedDataInfo&type=Folders&timeFrame=last24Hours&detailsLevel=Detailed&maxNumberOfResults=10&autoLogin=true&username=admin&password=admin

Result JSON:

{"data":{"collectionData":{"totalLogs":1, "Folders": "JS.Logloud", "collectedLogs":0, "unCollectedLogsData": [{"path": "JS.Logloud,JS_Logloud","dataSize": 250}]}}, "totalLogs":1, "Folders": "AWS ELB", "collectedLogs":0, "unCollectedLogsData": [{"path": "AWS ELB,elasticloadbalancing","dataSize": 3161841}]}}, {"totalLogs":9, "Folders": "Demo,Tomcat,TX_EXAMPLE", "collectedLogs":0, "unCollectedLogsData": [{"path": "Demo,Tomcat,TX_EXAMPLE,IMPACS_BookingInterface-IMPACS_LoanBooking_ReqRep","dataSize": 1482923}]}], {"totalLogs":9, "Folders": "Demo,Tomcat,TX_EXAMPLE,ICV_Customer_Interface--ICV_Customer_Search_Response","dataSize": 865204}]

http://localhost:3003/logeye/message/message.JsonApi.jsp?api=collectedDataInfo&type=Folders&timeFrame=last24Hours&detailsLevel=Detailed&maxNumberOfResults=10&autoLogin=true&username=admin&password=admin

Result JSON:

{"data":{"collectionData":{"totalLogs":1, "collectedLogs":0, "unCollectedLogsData": [{"path": "Demo,Tomcat,TX_EXAMPLE,NESS-LPNameRequesttoNESS","dataSize": 6681574}]}}, "totalLogs":2, "Folders": "Demo,MySQL","collectedLogs":0, "unCollectedLogsData": [{"path": "Demo,MySQL,mysqld-instance-1","dataSize": 184975}]}]

http://localhost:3003/logeye/message/message.JsonApi.jsp?api=collectedDataInfo&type=Folders&timeFrame=last24Hours&detailsLevel=Detailed&maxNumberOfResults=10&autoLogin=true&username=admin&password=admin

Result JSON:

{"data":{"collectionData":{"totalLogs":1, "collectedLogs":0, "unCollectedLogsData": [{"path": "Tomcat 5.0.28,localhost_log","dataSize": 103891}]}}, }
XpoLog SDK

General

XpoLog SDK provides a set of commands that enables remote configuration of different XpoLog properties without accessing the GUI.

The following commands are available.

Connection

Settings

- Ports (HTTP, SSL, SHUTDOWN and AJP)
- Enable/Disable Security
- Enable/Disable Agent Mode

Security

- Add/Edit user

Accounts Management

- Add/Edit/Remove/Enable/Disable remote XpoLog account
- Add/Edit/Remove/Enable/Disable SSH account
- Add/Edit/Remove/Enable/Disable AWS S3 account

Tasks Management

5. `maxNumberOfResults` = number, max number of results to return. Relevant only when ‘Detailed’ type is specified (default = 100)
- Add/Edit/Execute Add Logs Directory task
- Add/Edit/Execute LogSync task

**Folders and Logs Management**
- Add Log
- Add Folder
- Remove existing folder/log

**AppTags**
- Apply a Time Zone for AppTags

**Restart**

**Apply License**

**Apply Patch**

**Requirements**
- XpoLog Client Jar ([download here](#))
- XpoLog keystore file - mandatory when using HTTPS, extract the zip at the same directory of the xpologClient.jar file and ensure a file .keystore exists in the location after extraction ([download here](#))
- JAVA on client machine that executes the commands
- Connectivity (HTTP/S) between the client machine that executes the commands to the XpoLog server

**Syntax**

**Connection**

In order to execute remote commands it is first required to provide connection parameters to the XpoLog instance:

**Connection Parameters**

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>xpologURL</td>
<td>The URL to the XpoLog instance</td>
<td>URL, Mandatory</td>
</tr>
<tr>
<td>user</td>
<td>Authentication user name</td>
<td>Text, Optional</td>
</tr>
<tr>
<td>password</td>
<td>Authentication password</td>
<td>Text, Optional</td>
</tr>
</tbody>
</table>

Example of base command to connect to a remote XpoLog:

```
```

When using scripts, it is recommended to set the above as parameters, as they should be used on any command which is being executed:

**Windows:**

```
set JAVA_RUN=java -cp xpologClient.jar com.xpolog.sdk.client.XpoLogSDKClient
set XPOLOG_CONN=-xpologURL http://<xpolog-machine>:<xpolog-port>/logeye -user USER_NAME -password PASSWORD
```

**Linux:**

```
JAVA_RUN="java -cp xpologClient.jar com.xpolog.sdk.client.XpoLogSDKClient"
XPOLOG_CONN="-xpologURL http://<xpolog-machine>:<xpolog-port>/logeye -user USER_NAME -password PASSWORD"
```

After a connection is established the following command may be executed against the connected XpoLog instance:
**General Settings and Security Commands**

### Settings Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be settings</td>
<td>&quot;settings&quot;</td>
</tr>
<tr>
<td>httpPort</td>
<td>The HTTP port XpoLog is listening on</td>
<td>Number</td>
</tr>
<tr>
<td>sslPort</td>
<td>The SSL port XpoLog is listening on</td>
<td>Number</td>
</tr>
<tr>
<td>shutdownPort</td>
<td>The server’s shutdown port</td>
<td>Number</td>
</tr>
<tr>
<td>ajpPort</td>
<td>The server’s ajp port</td>
<td>Number</td>
</tr>
<tr>
<td>agentMode</td>
<td>Enable/Disable agent mode</td>
<td>true/false</td>
</tr>
<tr>
<td>activateSecurity</td>
<td>Enable/Disable security</td>
<td>true/false</td>
</tr>
<tr>
<td>activateSystemTimeZone</td>
<td>Set the XpoLog's user Time Zone Mode to System (Default)</td>
<td>true/false</td>
</tr>
<tr>
<td>activateDynamicTimeZone</td>
<td>Set the XpoLog's user Time Zone Mode to Dynamic</td>
<td>true/false</td>
</tr>
<tr>
<td>activateAppTagsTimeZone</td>
<td>Set the XpoLog's user Time Zone Mode to per AppTags</td>
<td>true/false</td>
</tr>
</tbody>
</table>

Example of configuring ports:

```
%JAVA_RUN% %XPOLOG_CONN% -api settings -httpPort 30304 -sslPort 30444 -ajpPort 8010 -shutdownPort 8096 -agentMode true -activateSecurity true
```

Example of changing system time zone mode:

```
%JAVA_RUN% %XPOLOG_CONN% -api settings -activateAppTagsTimeZone true
```

### Security Users Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be securityUsers</td>
<td>&quot;securityUsers&quot;</td>
</tr>
<tr>
<td>name</td>
<td>The user name of the user</td>
<td>Text</td>
</tr>
<tr>
<td>userPassword</td>
<td>The user password</td>
<td>Text</td>
</tr>
<tr>
<td>displayName</td>
<td>The display name of the user</td>
<td>Text</td>
</tr>
<tr>
<td>override</td>
<td>Override an existing user (Default: false)</td>
<td>true/false</td>
</tr>
<tr>
<td>userPolicy</td>
<td>The policy name to associate to this user</td>
<td>Text</td>
</tr>
<tr>
<td>selectedGroupsList</td>
<td>The names of the selected groups to associate with this user</td>
<td>Text List (separate by ;)</td>
</tr>
</tbody>
</table>

Example of adding a new user and setting its properties:

```
%JAVA_RUN% %XPOLOG_CONN% -api securityUsers -name testUser -userPassword testPassword -displayName "TEST USER" -override true -userPolicy test -selectedGroupsList testgroup;All
```

### Accounts Management

#### Remove Account

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Description</td>
<td>Values</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>api</td>
<td>The API type to use – must be removeAccount</td>
<td>&quot;removeAccount&quot;</td>
</tr>
<tr>
<td>name</td>
<td>The name of the account to be removed</td>
<td>Text</td>
</tr>
</tbody>
</table>

Example of removing an account:

```
%JAVA_RUN% %XPOLOG_CONN% -api removeAccount -name "ACCOUNT_NAME"
```

## Disable/Enable Account

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be enableAccount</td>
<td>&quot;enableAccount&quot;</td>
</tr>
<tr>
<td>name</td>
<td>The name of the account to be removed</td>
<td>Text</td>
</tr>
<tr>
<td>enabled</td>
<td>Enable/Disable the account</td>
<td>true/false</td>
</tr>
</tbody>
</table>

Example of disabling an account:

```
%JAVA_RUN% %XPOLOG_CONN% -api enableAccount -name "ACCOUNT_NAME" -enabled false
```

## Add SSH Account Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be addSSHAccount</td>
<td>&quot;addSSHAccount&quot;</td>
</tr>
<tr>
<td>name</td>
<td>The name of the account</td>
<td>Text</td>
</tr>
<tr>
<td>description</td>
<td>The description of the account</td>
<td>Text</td>
</tr>
<tr>
<td>hostName</td>
<td>Host Name</td>
<td>Text</td>
</tr>
<tr>
<td>conType</td>
<td>The connection type (Default: SFTP)</td>
<td>SFTP/SCP</td>
</tr>
<tr>
<td>port</td>
<td>The port to be used in the account (Default: 22)</td>
<td>Number</td>
</tr>
<tr>
<td>override</td>
<td>Override an existing account (Default: false)</td>
<td>true/false</td>
</tr>
<tr>
<td>enabled</td>
<td>Enable/Disable the account</td>
<td>true/false</td>
</tr>
<tr>
<td>privateKeyPath</td>
<td>Full Path to Key</td>
<td>Text</td>
</tr>
<tr>
<td>username</td>
<td>Authentication user name</td>
<td>Text</td>
</tr>
<tr>
<td>userPassword</td>
<td>Authentication password</td>
<td>Text</td>
</tr>
</tbody>
</table>

Example for adding an SSH account:

```
%JAVA_RUN% %XPOLOG_CONN% -api addSSHAccount -name "ACCOUNT_NAME" -hostName MACHINE_IP -conType SFTP -port 22 -override true -enabled true -privateKeyPath "" -username USER_NAME -userPassword PASSWORD
```

## Add Remote XpoLog Account Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be addRemoteXpoLogAccount</td>
<td>&quot;addRemoteXpoLogAccount&quot;</td>
</tr>
<tr>
<td>name</td>
<td>The name of the account</td>
<td>Text</td>
</tr>
<tr>
<td>description</td>
<td>The description of the account</td>
<td>Text</td>
</tr>
<tr>
<td>hostName</td>
<td>Host Name</td>
<td>Text</td>
</tr>
<tr>
<td>conType</td>
<td>The connection type (Default: HTTP)</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td>override</td>
<td>Override an existing account (Default: false)</td>
<td>true/false</td>
</tr>
<tr>
<td>enabled</td>
<td>Enable/Disable the account</td>
<td>true/false</td>
</tr>
<tr>
<td>isCollected</td>
<td>False – Proxy mode, True – Agent Mode (Default: true)</td>
<td>true/false</td>
</tr>
</tbody>
</table>
Example of adding a remote XpoLog account:

```
%JAVA_RUN% %XPOLOG_CONN% -addRemoteXpoLogAccount -name "ACCOUNT_NAME" -hostName MACHINE_IP -conType HTTP -port 30303 -context logeye -override true -enabled true -isCollected true -username admin -userPassword admin
```

### Add AWS S3 Account Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
</table>
| api                  | The API type to use – must be addExternalAccount | "addExternalAccount" | Mandatory
| name                 | The name of the account          | Text           | Mandatory
| description          | The description of the account   | Text           | Optional
| externalMediaType    | The type of the account          | s3             | Mandatory (lowercase only)
| ema_custom_accessKey | The AWS S3 access key            | Text           | Mandatory
| ema_custom_secretKey | The AWS S3 secret key            | Text           | Mandatory
| override             | Override an existing account     | true/false     | Optional
| enabled              | Enable/Disable the account       | true/false     | Optional

Example for adding an SSH account:

```
%JAVA_RUN% %XPOLOG_CONN% -addExternalAccount -externalMediaType "s3" -name "ACCOUNT_NAME" -description "ACCOUNT_DESCRIPTION" -override true -ema_custom_accessKey "ACCOUNT_ACCESS_KEY" -ema_custom_secretKey "ACCOUNT_SECRET_KEY"
```

### Tasks Management

#### Execute Task Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
</table>
| api     | The API type to use – must be executeTask        | "executeTask"  | Mandatory
| name    | The name of the task (case sensitive)            | Text           | Mandatory

Example for executing a task:

```
%JAVA_RUN% %XPOLOG_CONN% -executeTask -name "TASK_NAME"
```

### Execution of a Logs Directory Task (Scanner)

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be executeScanTask</td>
<td>&quot;executeScanTask&quot;</td>
</tr>
<tr>
<td>name</td>
<td>The name of the task to be presented in XpoLog logs / Activity console while running (recommended)</td>
<td>Text</td>
</tr>
<tr>
<td>id</td>
<td>The id of the task - used to avoid re-creation of logs which were already created by a SDK command (recommended)</td>
<td>Text</td>
</tr>
<tr>
<td>parentFolderPath</td>
<td>Determines under which folder to create/update logs that are created by the SDK command (Default: Folders and Logs). Folder is created if does not exist</td>
<td>ROOT = Top Folder (Folders and Logs) Use ‘-&gt;’ in the path between folders</td>
</tr>
<tr>
<td>accountName</td>
<td>The connectivity account to use if the scan is not local</td>
<td>Text</td>
</tr>
<tr>
<td>scanPath</td>
<td>The full path to scan (local or on the remote source after connection is established)</td>
<td>Text</td>
</tr>
</tbody>
</table>
### Add Logs Directory Task (Scanner)

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be executeScanTask</td>
<td>“addScanTask”</td>
</tr>
<tr>
<td>name</td>
<td>The name of the task to be presented in XpoLog logs / Activity console while running (recommended)</td>
<td>Text</td>
</tr>
<tr>
<td>id</td>
<td>The id of the task - used to avoid re-creation of logs which were already created by a SDK command (recommended)</td>
<td>Text</td>
</tr>
<tr>
<td>parentFolderPath</td>
<td>Determines under which folder to create/update logs that are created by the SDK command (Default: Folders and Logs). Folder is created if does not exist</td>
<td>ROOT = Top Folder (Folders and Logs) Use ‘-&gt;’ in the path between folders</td>
</tr>
<tr>
<td>accountName</td>
<td>The connectivity account to use if the scan is not local</td>
<td>Text</td>
</tr>
<tr>
<td>scanPath</td>
<td>The full path to scan (local or on the remote source after connection is established)</td>
<td>Text</td>
</tr>
<tr>
<td>directoriesToInclude</td>
<td>The SDK supports all the ‘ScanConfiguration’ parameters Use -PARAM_NAME PARAM_VALUE in the command</td>
<td>Text</td>
</tr>
<tr>
<td>filesToExclude</td>
<td>Unix cron expression format</td>
<td>cron expression format</td>
</tr>
<tr>
<td>override</td>
<td>Override an existing task (Default: false)</td>
<td>true/false</td>
</tr>
</tbody>
</table>

#### Example of executing a scan directory operation:

```bash
%JAVA_RUN% %XPOLOG_CONN% -api executeScanTask -name "SCANNER_SDK" -id "SCAN12345" -parentFolderPath "ROOT->NEW_PARENT_FOLDER" -accountName ACCOUNT_NAME -scanPath ”/var/log” -scanMethod 0 -timeZone GMT -directoriesToInclude "DIR1,DIR2" -filesToExclude ”*.zip,*.gzip,*.tar”
```

### Add Log Sync Task Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be addSyncLogTask</td>
<td>“addSyncLogTask”</td>
</tr>
<tr>
<td>name</td>
<td>The name of the task</td>
<td>Text</td>
</tr>
<tr>
<td>configFilePath</td>
<td>The absolute path to the LogSync configuration file to be used by this task</td>
<td>Text</td>
</tr>
<tr>
<td>createConfiguration</td>
<td>Determines whether to create Folders and Logs configuration from the synched logs (Default: false)</td>
<td>true/false</td>
</tr>
<tr>
<td>parentFolderPath</td>
<td>The parent folder path of this task’s result. Folder and Logs is the default path. Use ‘-&gt;’ in the path between folders</td>
<td>Optional</td>
</tr>
<tr>
<td>cron</td>
<td>Unix cron expression format</td>
<td>cron expression format</td>
</tr>
<tr>
<td>assignedNode</td>
<td>The name of the XpoLog node to be assigned on this task</td>
<td>Text</td>
</tr>
<tr>
<td>override</td>
<td>Override an existing task (Default: false)</td>
<td>true/false</td>
</tr>
</tbody>
</table>

#### Example of adding a scan directory task:

```bash
%JAVA_RUN% %XPOLOG_CONN% -api addScanTask -name "SCANNER_SDK" -id "SCAN12345" -parentFolderPath "ROOT->NEW_PARENT_FOLDER" -accountName ACCOUNT_NAME -scanPath ”/var/log” -scanMethod 0 -timeZone GMT -directoriesToInclude "DIR1,DIR2" -filesToExclude ”*.zip,*.gzip,*.tar” -cron "0/10 * * * * ? *"
```

#### Example of adding a Log Sync task:

```bash
%JAVA_RUN% %XPOLOG_CONN% -api addSyncLogTask -name "New Log Sync Test" -configFilePath C:\dev\syncLogsTest.xml -override true -cron "0/10 * * * * ? *"
```
## Folders and Logs Management

### Add Log

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be addLog</td>
<td>&quot;addLog&quot;</td>
</tr>
<tr>
<td>logName</td>
<td>The name of the log to be created</td>
<td>Text</td>
</tr>
<tr>
<td>logId</td>
<td>The unique ID of a log in XpoLog that can be modified. In case logId is used, it is mandatory to use override true, since it is an edit mode of an existing log in XpoLog - all the parameters that will be passed in this command will override and update an existing log.</td>
<td>Text</td>
</tr>
<tr>
<td>logPath</td>
<td>The full path to the log under the Folders and Log Tree (excluding the log name)</td>
<td>ROOT = Top Folder (Folders and Logs) Use '-' in the path between folders</td>
</tr>
<tr>
<td>filesPath</td>
<td>The full path to the files on the source (name pattern may be used)</td>
<td>Text</td>
</tr>
<tr>
<td>collectionPolicy</td>
<td>The exact name of the collection policy to be assigned on the log (if doesn't exist, the command will be ignored)</td>
<td>Text</td>
</tr>
<tr>
<td>accountName</td>
<td>The name of the account to be used if needed (SSH or Win Account)</td>
<td>Text</td>
</tr>
<tr>
<td>patterns</td>
<td>A list of patterns that will be applied on the log that is added (separated by XPLG_SDK_SEP)</td>
<td>Text</td>
</tr>
<tr>
<td>appTags</td>
<td>A comma separated list of appTags that the added log will be tagged to</td>
<td>Text</td>
</tr>
<tr>
<td>timezone</td>
<td>The timezone definition of the added log</td>
<td>Text (a value from JAVA time zone list)</td>
</tr>
<tr>
<td>charset</td>
<td>The charset definition of the added log</td>
<td>Text (a value from JAVA charset list)</td>
</tr>
<tr>
<td>template</td>
<td>The name of the template to be used</td>
<td>Text</td>
</tr>
<tr>
<td>dataFilterQuery</td>
<td>The dataFilterQuery to be applied on the specified - see Advanced Log Settings for more information. (pass an empty filter to clear an existing filter)</td>
<td>Text</td>
</tr>
<tr>
<td>override</td>
<td>Overwrite an existing log configuration (Default: false)</td>
<td>true/false</td>
</tr>
</tbody>
</table>

Example for adding a log over SSH using an existing account (for direct access simple remove the -accountName parameter):

```
%JAVA_RUN% %XPOLOG_CONN% -api addLog -logName "LOG_NAME" -logPath "ROOT->FOLDER_1->FOLDER_2" -filesPath "c:\LogFiles\messages\{string}\{date:Date,dd/MM/yyyy HH:mm:ss.SSSSSS}\{text:priority}\{string:message}\{XPLG_SDK_SEP}\{date:Date,dd/MM/yyyy HH:mm:ss.SSS}\{text:priority}\{string:message}\{string}" -patterns "{date:Date,dd/MM/yyyy HH:mm:ss.SSS}\{text:priority}\{string:message}\{string}" -appTags "APP_TAG_NAME_1,APP_TAG_NAME_2"
```

Example for adding an empty folder:

```
%JAVA_RUN% %XPOLOG_CONN% -api addFolder -folderPath "ROOT->FOLDER_1->FOLDER_2->FOLDER_NAME_TO_BE_ADDED"
```
### Remove Folder

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be removeMember</td>
<td>“removeMember”</td>
<td>Mandatory</td>
</tr>
<tr>
<td>folderPath</td>
<td>The full path to the folder to be removed</td>
<td>ROOT = Top Folder (Folders and Logs) Use ‘-&gt;’ in the path between folders</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

Example for removing a folder (and all its contents):

```bash
%JAVA_RUN% %XPOLOG_CONN% -api removeMember -folderPath "ROOT->FOLDER_1->FOLDER_2->FOLDER_NAME_TO_BE_REMOVED"
```

### Remove Log

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be removeMember</td>
<td>“removeMember”</td>
<td>Mandatory</td>
</tr>
<tr>
<td>logPath</td>
<td>The full path to the log to be removed</td>
<td>ROOT = Top Folder (Folders and Logs) Use ‘-&gt;’ in the path between folders</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

Example for removing a folder (and all its contents):

```bash
%JAVA_RUN% %XPOLOG_CONN% -api removeMember -folderPath "ROOT->FOLDER_1->FOLDER_2->LOG_NAME_TO_BE_REMOVED"
```

### License Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be license</td>
<td>“license”</td>
<td>Mandatory</td>
</tr>
<tr>
<td>files</td>
<td>The path (relative to execution location or absolute path) to the license file which will be updated</td>
<td>Text</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

Example of applying a license:

```bash
%JAVA_RUN% %XPOLOG_CONN% -api license -files license.lic
```

### AppTags Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be settings</td>
<td>“settings”</td>
<td>Mandatory</td>
</tr>
<tr>
<td>appTags</td>
<td>A comma separated list of AppTags names (exactly as defined in XpoLog)</td>
<td>Text</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>(The time zone will be applied only if the general User Time Zone Mode in XpoLog is set to ‘AppTags’)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZone</td>
<td>A single time zone from JAVA available time zones</td>
<td>Text</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>(The time zone should be exactly as appears in the time zones list, in case XpoLog will not be able to find that given value, default system time zone will be applied automatically. Use “Default” to apply the time zone to the system default time zone)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example of applying a time zone on an AppTag:

```bash
%JAVA_RUN% %XPOLOG_CONN% -api settings -timeZone "America/New_York" -appTags "APPTAG1, APPTAG2"
```

### Restart Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Publish Patch Task Parameters

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>api</td>
<td>The API type to use – must be addPatch</td>
<td>“addPatch”</td>
</tr>
<tr>
<td>files</td>
<td>The path (relative to execution location or absolute path) to the patch file</td>
<td>Text</td>
</tr>
<tr>
<td>type</td>
<td>Patch type – must be “api”</td>
<td>“api”</td>
</tr>
</tbody>
</table>

**Example of applying a patch:**

`%JAVA_RUN% %XPOLOG_CONN% -api addPatch -type api -files patch.zip`

**Comments:**

1. Any value which contains the space character should be wrapped with “quotes”. For example if the display name of a user is TEST USER then it should wrapped with quotes as:
   ```
   ... -displayName "TEST USER" ...
   ```
2. General Script Example: [download here](#)

**Common Use Case:**

1. **Important:** In all examples above we have used `%JAVA_RUN% %XPOLOG_CONN%` which is suitable to Windows environments. For Linux, the SDK should use `$JAVA_RUN $XPOLOG_CONN`
2. **Automatically Add Servers to XpoLog:**
   Automating the process of adding new servers to XpoLog, mainly in dynamic environments such as clouds where servers are constantly added and removed. The SDK provides full support so when a new machine is added, simply be a couple of commands the new server is added to XpoLog and the required logs are be collected and available for the users. See Script Example: [download here](#)
3. **Automatically Remove / Disable Servers in XpoLog:**
   a. Disable Server but keep data that was already collected
      If a server is removed from the environment but you wish to keep the data that was already collected by XpoLog from that server, simply disable the account of that specific server so XpoLog will not try to connect to it but will keep the data based on the retention policy. See Script Example: [download here](#)
   b. Remove Server and data that was collected from it
      If a server is removed from the environment and you wish to remove it from XpoLog including all data then simply remove the account of that server and the folder which contains all its logs. See Script Example: [download here](#)

### Batch Configuration

A batch configuration allows performing a set of changes on the log configuration; its set of changes includes the Log Type and the Field Type. Usage of Batch Configuration accelerates and automates the configuration process of logs added to or updated in XpoLog.

Administrators can perform the following actions related to batch configuration:

- View Log Type/Field Type (see Viewing XpoLog Batch Configuration)
- Add a new Log Type/Field Type (see Adding a new batch Configuration)
- Apply a Log Type/Field Type on multiple logs (see Applying a Batch Configuration on Multiple Logs)

### Adding a New Batch Configuration

You can define a new XpoLog batch configuration.

To add a new XpoLog batch configuration:

- In XpoLog Manager, select the **Tools > Batch Configuration** menu item.
  The **Batch Configuration** console opens, displaying an alphabetically sorted list of batch types. The first letters of the type names in the list are highlighted in the Filtering Area above the list.
Quickly Adding a Log Type on Multiple Logs

The Filtering Area above the lists of log types enables quick navigation to a log type beginning with a specific letter. The letters which begin the template names in the list are highlighted in the Filtering Area. This is a convenient feature in systems that have many batch types.

To quickly apply a log type:

- In Filter List, write the first letters of the source and then the first letters of the log type
- Click on Apply
- Click on New
- In the field box, write the name of the Log Type
- Check the required logs in the tree
- Click on Save.

Quickly Adding a Field Type on Multiple Logs

The Filtering Area above the lists of field types enables quick navigation to a field type beginning with a specific letter. The letters which begin the template names in the list are highlighted in the Filtering Area. This is a convenient feature in systems that have many batch types.

To quickly apply a field type:

- In Filter List, write the first letters of the source and then the first letters of the field type
- Click on Apply
- Click on New
- In the field box, write the name of the Field Type
- Check the required fields in the tree
- Click on Save.

Applying a Batch Configuration on Multiple Logs

You can apply the batch configuration on multiple logs.

To apply the XpoLog batch configuration on multiple logs:

- In XpoLog Manager, select the Tools > Batch Configuration menu item.
  The Batch Configuration console opens, displaying an alphabetically sorted list of batch types. The first letters of the type names in the list are highlighted in the Filtering Area above the list.

Quickly Applying a Log Type on Multiple Logs

The Filtering Area above the lists of log types enables quick navigation to a log type beginning with a specific letter. The letters which begin the template names in the list are highlighted in the Filtering Area. This is a convenient feature in systems that have many batch types.

To quickly apply a log type:

- In Filter List, write the first letters of the source and then the first letters of the log type
- Click on Apply
- Click on the required Log Type
- Check the logs to be applied
- Click on Save

Quickly Applying a Field Type on Multiple Logs

The Filtering Area above the lists of field types enables quick navigation to a field type beginning with a specific letter. The letters which begin the template names in the list are highlighted in the Filtering Area. This is a convenient feature in systems that have many batch types.

To quickly apply a field type:

- In Filter List, write the first letters of the source and then the first letters of the field type
- Click on Apply
- Click on the required Field Type
- Check the fields to be applied
- Click on Save

Viewing XpoLog Batch Configuration

You can view a listing of all batch configuration defined in XpoLog.

To view the XpoLog batch configuration:

- In XpoLog Manager, select the Tools > Batch Configuration menu item.
  The Batch Configuration console opens, displaying an alphabetically sorted list of batch types. The first letters of the type names in the list are highlighted in the Filtering Area above the list.

Quickly Navigating to a Log Type
The Filtering Area above the lists of log types enables quick navigation to a log type beginning with a specific letter. The letters which begin the template names in the list are highlighted in the Filtering Area. This is a convenient feature in systems that have many batch types. To quickly navigate to a log type:

- In Filter List, write the first letters of the source and then the first letters of the log type
- Click on Apply

**Quickly Navigating to a Field Type**

The Filtering Area above the lists of field types enables quick navigation to a field type beginning with a specific letter. The letters which begin the template names in the list are highlighted in the Filtering Area. This is a convenient feature in systems that have many batch types. To quickly navigate to a field type:

- In Filter List, write the first letters of the source and then the first letters of the field type
- Click on Apply

**Geo Redundancy**

XpoLog contains a mechanism that replicates configuration between a Primary and a Secondary sites in order to keep them synchronized for disaster recovery purposes.

The Geo-redundancy mechanism is designed to create a replication of selected XpoLog's configuration between a primary geographical location and a secondary geographical location that XpoLog instance/cluster runs on. In the event of a complete regional outage or disaster in your primary location, if users are redirected to the secondary site, the entire set of configuration will be available identically to the primary site.

XpoLog does not replicate raw data between sites or copies over the configuration files independently. Organizations that wish to activate and use the Geo-redundancy mechanism should have in place a process that copies the raw data to be processed on both sites, and the zipped configuration files created by the Geo-redundancy mechanism on each site to their designated locations on the other site.

The high level logic of the Geo-redundancy mechanism is as follows:

Each site contains an 'Inbox' and 'Outbox' directories. Based on the configured synchronization schedule, XpoLog creates a zipped configuration file which is placed in the site's 'Outbox' directory, and checks if there is a new file in the site's 'Inbox' directory and merges its contents to its local configuration. It is the organization's responsibility on both sites to copy the contents of each site's 'Inbox' directory to the other site's 'Outbox' directory keeping the files last modified time.

**Geo-redundancy Configuration**

On each XpoLog instance/cluster there are 2 files in which determine the synchronization schedule and contents:

- `/.../XPOLOG_CONF/conf/general/configMerge.xml`
  This file determine the contents of configuration that will be included in the sync process between sites.
  - InputsInfo
    - filesToKeep - determines how many files XpoLog should keep in its 'Inbox' directory.
    - Includes - the list of local configuration directories that will be included in the zipped configuration files that is created. By default, all user oriented configuration (available in the GUI) are included:
      - `/.../XPOLOG_CONF/conf/general/addressbook.xml` - connectivity accounts from the address book.
      - `/.../XPOLOG_CONF/conf/logsconf/*` and `/.../XPOLOG_CONF/conf/modules/*` - Folders and Logs.
      - `/.../XPOLOG_CONF/conf/metadata/*` - appTags.
      - `/.../XPOLOG_CONF/conf/verifiers/*` - monitors.
      - `/.../XPOLOG_CONF/conf/usersenv/*` - saved searches and user's specifics.
      - `/.../XPOLOG_CONF/conf/system/system.xml` - collection policies.
  - Excludes - specify directories to exclude from the above list.
  - BinaryIncludes - handle binary configuration data. Currently relevant only to user's specifics and user's defined templates.
  - OutputsInfo
    - filesToKeep - determines how many files XpoLog should keep in its 'Outbox' directory.

- `/.../XPOLOG_CONF/conf/general/configMerge.user.xml`
  This file determine the schedule and 'Inbox'/'Outbox' directories location.
  - ScheduleOp - the scheduler settings which determines the frequency of executing synchronization. The only change should be the cron expression.
  - Note: commenting the ScheduleOp object pauses the synchronization process (node(s) restart is required).
  - InputsInfo
    - path - the absolute path to the site's 'Inbox' directory.
  - OutputsInfo
    - path - the absolute path to the site's 'Outbox' directory

**Geo-redundancy Activation**
Activation of Geo-redundancy is divided to 2 steps. There is a need to run an initial replication (baseline) so both sites will be synchronized, afterwards the on going synchronization process takes place.

It is mandatory to go through the baseline process and validate it prior to activating the on going sync in order to a valid synchronization process and to avoid configuration duplications.

1. Geo-redundancy baseline creation
   a. Prerequisite:
      i. Primary site contains configuration and Secondary site is empty from all configuration.
      ii. Disable Geo-redundancy on both sites.
      iii. Stop XpoLog instance/cluster on both sites.
   b. Manually copy the directories /files that are part of the sync from the Primary site to the Secondary site (override existing):
      i. /.../XPOLOG_CONF/conf/general/addressbook.xml
      iii. /.../XPOLOG_CONF/conf/metadata/
      iv. /.../XPOLOG_CONF/conf/verifiers/
      v. /.../XPOLOG_CONF/conf/usersenv/
      vi. /.../XPOLOG_CONF/conf/ui/apps/deploy/
      vii. /.../XPOLOG_CONF/conf/ext/templates/user/
      viii. /.../XPOLOG_CONF/conf/verifiers/
   c. StartXpoLog instance/cluster on both site and validate that all the configuration is available and identical.

2. On going synchronization first activation
   a. Prerequisite:
      i. Baseline procedure complete and validated.
   b. Ensure the files /.../XPOLOG_CONF/conf/general/configMerge.xml and /.../XPOLOG_CONF/conf/general/configMerge.user.xml are properly configured on each site with the correct local path of each site to its ‘Inbox’ and ‘Outbox’ directories, scheduler, sync contents, etc.
   c. Ensure on each site that its ‘Inbox’ and ‘Outbox’ directories are available and empty.
   d. Enable Geo-redundancy on both sites.
   e. Ensure there’s a process in place that copies:
      i. Raw data from Primary site to Secondary site to the required location.
      ii. Each site’s contents of ‘Outbox’ to the other site’s ‘Inbox’ and vice versa (keeping files last modified time).

3. Once the procedure is completed and active, all changes that will be made on any of the sites will be synced to other site.
   Configuration changes of the same object in XpoLog should take place on one site only and the Geo-redundancy mechanism will sync and merge them in the other site (keep in mind: if the same object is modified on both sites, the last change will be applied based on the file’s last modified time).

Important:

User Guide
Starting XpoLog

Launching XpoLog

XpoLog can be installed on a Windows or Linux/Solaris machine, or deployed as a Web application (see Installation). After installation or deployment, XpoLog runs automatically.

For subsequent uses of XpoLog, launch XpoLog as follows:

- Under Windows or Linux/Solaris, in your browser, navigate to http://MACHINE_NAME:30303 or https://MACHINE_NAME:30443

Consult the system administrator to ensure the default ports presented above were not changed.

Logging In

If security is not activated in your organization (the default), launching XpoLog Center from your browser automatically starts XpoLog.

If security is activated in your organization, you are required to enter your credentials (username and password).

Default credentials are admin/admin and may be changed immediately after first time login.

To log into XpoLog Center:

1. Navigate to the XpoLog Center address in your browser (http://localhost:30303).
2. If security is activated in your organization, in the login page that appears, type your Username and Password, and then click OK. The XpoLog Center homepage is presented. See XpoLog Homepage for a description of the homepage elements.
Logging Out

A Logout button appears at the right side of the main menu on any XpoLog page of organizations where security is activated, i.e. where username and password were required to log into XpoLog. In this case, clicking the **Logout** button logs you out of XpoLog Center.

XpoLog Homepage

Upon accessing XpoLog Center, the XpoLog homepage is displayed.

The homepage can also be accessed from any XpoLog console, by clicking the **XpoLog** logo on the top left side of the screen.

The main elements of the XpoLog homepage are described in the following table:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab Bar</td>
<td>On the left side, <strong>Apps</strong>, <strong>Search</strong>, and <strong>Analytics</strong> tabs. On the right side, the <strong>Manager</strong> tab:</td>
</tr>
<tr>
<td><strong>Apps</strong> tab</td>
<td>Clicking this tab opens the Apps console (see XpoLog Apps).</td>
</tr>
<tr>
<td><strong>Search</strong> tab</td>
<td>Clicking this tab opens the Search console (see XpoLog Search).</td>
</tr>
<tr>
<td><strong>Analytics</strong> tab</td>
<td>Clicking this tab opens the Analytics console (see XpoLog Analytics).</td>
</tr>
<tr>
<td><strong>Manager</strong> tab</td>
<td>(right hand side): Clicking this tab opens the Manager's console (see XpoLog Manager).</td>
</tr>
<tr>
<td><strong>XpoLog</strong> logo</td>
<td>- return to homepage</td>
</tr>
<tr>
<td>Notification Bar</td>
<td>A notification area with a red background, which includes important system notifications is displayed if necessary. For example cases of insufficient storage, license expiration, slowness, etc.</td>
</tr>
<tr>
<td>Main Pane</td>
<td>Displays the dashboard that the system administrator configured to be displayed on the homepage. Each XpoLog user can define the dashboard that appears on their homepage. See set a dashboard as the system home page</td>
</tr>
<tr>
<td>Quick Start Div</td>
<td>During an evaluation period, a ‘Quick Start’ div is displayed with different shortcuts to key operations in XpoLog:</td>
</tr>
</tbody>
</table>

XpoLog Apps

An XpoLog App is a container that contains one or more dashboards. Each dashboard in the App is used to display visual or textual information from the logs that exist in the XpoLog environment.

- Apps and Dashboards simplify and expedite analysis of an Application or Environment. The Dashboards provide live visualization of the data to quickly expose and understand faults and outages.
- XpoLog has an engine that enables customizing multiple dashboards. For example, four dashboards can be defined under an App one for displaying application problems, performance problems, network issues, and security.

Click the Apps tab to open the Apps console.
XpoLog Custom Apps - create any application and dashboard on your data using XpoLog visualization tools.

XpoLog Apps Marketplace - select out of the box applications, a predefined set of dashboards, made for you by XpoLog team for a quick and easy deployment of known system applications.
Click the App that you wish to view its Dashboards. You can filter the list of available Apps by typing the name of the App in the search area or sort the displayed Apps list by name, recently viewed or most viewed by simply clicking the desired option on the left menu.

XpoLog allows to open multiple Apps/Dashboards in a single browser session. Mouse over the icon allows quick navigation between the open Apps/Dashboards:

### Accessing the XpoLog Apps Console

To access the Apps console:

- In the Tab Bar, click the Apps tab.
  
  The Apps console opens, displaying the available Apps. See XpoLog Apps.

---

**XpoLog Dashboards**
An XpoLog Center Dashboard is a portal that contains gadgets. Multiple dashboards may be defined under an App context. Each gadget in the dashboard is used to display visual or textual information from the logs that exist in the XpoLog environment.

Each gadget displays the data that the user requested to view in the gadget's definition. For example, three gadgets can be displayed in a dashboard for displaying search results, filtered logs and Analytics summary. Gadgets simplify and expedite performing searches and operations on the log file. For example, instead of going each time to the XpoSearch search engine and running a search, you can define gadgets for viewing these search results in different visual manners.

XpoLog has an engine that enables customizing multiple dashboards, each for a different purpose. For example, you can define four dashboards – for application problems, performance problems, network issues, and security.

Each dashboard can contain multiple gadgets, with each gadget displayed in one of the available visualizations: Line Chart, Bar Chart, Column Chart, Pie Chart, Data Table, Events List, etc. The gadgets can be organized within the dashboard in any of several predefined layouts. Also, any gadget can be dragged and dropped to a preferred location on the dashboard page.

Each dashboard contains a header bar with the name of the dashboard and different actions on the dashboard (see Dashboard Options). Its gadgets are arranged in the main pane in the layout selected in the dashboard definition.

To view a dashboard:

1. Click the relevant App under the XpoLog Apps console.
   You can filter the list of available dashboards by typing the name of the dashboard in the search area

   or sort the displayed dashboards list by name, recently viewed or most viewed by simply clicking the desired option on the left menu.

   A summary of the defined dashboards under the selected App is displayed:

   ![Dashboard Options](image)

2. Click the desired Dashboard to view it.
   The selected dashboard is opened. All its gadgets are displayed:

   ![Dashboard View](image)

While viewing a dashboard it is possible to filter a dashboard view or change its time frame on demand.
Dashboard Options

While viewing a dashboard it is possible to filter the view result and/or change the time frame.

- Change a Dashboard Time Frame - For changing the default time frame of all gadgets in a dashboard. See Change Dashboard Time Frame.
- Filter Dashboard Result - For adding a constraint to the gadget's queries on demand to filter the displayed result. See Filter Dashboard Result.
- Use Dashboard Inputs form (if available) - Use a visual form to select values that will reload the dashboard based on the selections. See Dashboard Inputs.

You can manage a Dashboard in XpoLog by using the options accessible by clicking the icon on the top right hand side of the Dashboard toolbar.

Available dashboard options are:

- **Add Gadget** – For adding a gadget to the dashboard. See Managing Gadgets in Administrator's Guide.
- **Edit Dashboard** – For editing the general settings of a dashboard. See Adding a Dashboard in the Administrator's Guide.
- **Save Layout** – If the Dashboard's layout was modified, click this option to save it as the default layout of this dashboard.
- **Reset Layout** - For resetting the Dashboard's layout back to its default in the current display.
- **Export to PDF** – For exporting the dashboard to a PDF file (see Exporting the Dashboard to PDF/CSV).
- **Export to CSV** – For exporting the dashboard to a CSV file (see Exporting the Dashboard to PDF/CSV).
- **Set as Home Page** – For details, see Setting a Dashboard as Homepage in Administrator's Guide.
- **Copy Permalink** – This option copies to the clipboard a direct link to the dashboard. The link can be then used externally to XpoLog to present the dashboard's result (for example in an iFrame in an external portal). 2 parameters which can be added to the link:
  - Login credentials - mandatory in case Security is active in XpoLog, a user and password with the credentials to view the dashboard should be added: &autoLogin=true&username=[USER_NAME]&password=[PASSWORD]
  - Enable Zoom - optional, dashboard/gadgets contain links to zoom in back to XpoLog to see the result, by default the zoom in links are presented. It is possible to add a parameter which determines this behavior: &allowZoom=false or &allowZoom=true
  - Display in Black Theme - optional, by default the permalinks of dashboards will display the dashboards in white theme. It is possible to add a parameter which set it to black theme: &blackTheme=true

**Change Dashboard Time Frame**

By default, when displaying a dashboard all gadgets will be loaded on the default time frame that was defined for each gadget. In order to modify the time frame, click the icon and select the time frame to be applied on the dashboard. Several options are available:

- Default = the default time frame that was configured for the dashboard
- Last = last <selected_unit> from the actual execution time. For example last 1 day = from the current time until 1 day ago
- Previous = previous <selected_unit> referring to the actual execution time. For example previous 1 day = yesterday midnight to midnight
- Today = Displays shortcuts to different fixed units
- Date Range = Customized specific time frame
- Live = Near real time execution of the dashboard - all gadgets will be cleared and will display current results, the gadgets will be continuously updated while the dashboard is open
- Custom Time = Custom Last/Previous values

All gadgets will be reloaded according the selection. Click the icon again to modify or 'Default' to restore to default time.
Changing the Dashboard Layout

You can customize the look of your dashboard, by clicking the layout icon and choosing the arrangement of the gadgets on the dashboard page. If changes were made to the layout, select Save/Reset layout from the dashboard’s options menu:

- **Save Layout** – If the Dashboard’s layout was modified, click this option to save it as the default layout of this dashboard.
- **Reset Layout** - For resetting the Dashboard’s layout back to its default in the current display.

Dashboard Inputs

Users Inputs provide an interface for users to supply values that effect gadgets search terms in a visual form. Typically, the inputs are displayed in a checkbox, text area, dropdown menus or radio buttons.

The forms allow users to visually make selections which impact the underlying searches and focus only on points of interest while viewing dashboard’s results. In order to configure inputs please refer to the Dashboards Settings in the Administrator Guide.

Inputs form (if available) is displayed at the top of a dashboard, select/configure values of interest in the inputs form and click Apply, the dashboard will be reloaded displaying the correspondent results:

*Example I:* Checking the ‘INTERNAL ERROR’ checkbox and clicking Apply reloads the dashboard where gadgets display the results filtered with INTERNAL ERROR only
Example II: Specifying specific sources (servers in this example) and 'Day' granularity and clicking Apply reloads the dashboard where gadgets display the results from the selected servers only and on daily basis granularity.

Dashboard Theme

By default XpoLog presents the dashboards with a white background; it is also possible to present the dashboards with a black background. Click the icon to switch between themes.
Display Multiple Dashboards

When opening multiple dashboards to be displayed, it is possible to turn all open dashboards into a “slideshow”.

Click the 
[Play](icon) icon and XpoLog will play all open dashboards in the selected speed (from every 5 seconds and up to 1 minute). Click the [Pause](icon) icon to pause and review or the [Stop](icon) icon to stop the slideshow and return to the dashboard's main screen.

Exporting the Dashboard to PDF/CSV
You can export any dashboard to a PDF/CSV file, and then print it out or share it.

To export a dashboard to a PDF/CSV file: In the toolbar of the dashboard that you want to export, click the icon, and from the menu items that appear, click Export to PDF/CSV. A Prepare Export to PDF/CSV notification box appears, informing that it is preparing data for export. It is followed by an Export to PDF/CSV notification box. The PDF/CSV file is created and can be saved.

**Note:** If pop-ups are blocked, you are asked to click Continue to complete the export.

**Filter Dashboard Result**

When displaying a dashboard, all gadgets are loaded with the up to date result. In order filter the displayed result, click the icon to open the search query definition and enter the criteria that will be added to all gadget's queries. Click the 'Search' to activate the filter:

The filtered result is loaded:

Click the icon to remove the filter and return to the default display.

**Gadgets**

A dashboard arranges its defined gadgets in the layout selected by the user. Each gadget has a header bar, which displays the name of the gadget or the gadget type (the default; displayed if a name was not given to the gadget), the time frame the gadget is defined on and the date and time that the gadget was last refreshed, and a menu icon that can be clicked to perform actions on the gadget (see **Gadget Options**).
The gadget result is displayed below the header bar, and if relevant, one of the following links appears below in the footer of the gadget:

- **View in Search** – For performing a drilldown from the gadget results to the Search console
- **View in XpoLog** – For performing a drilldown from the gadget results to the Search console
- **View in Analytics** – For performing a drilldown from the gadget results to the Analytics console

Note: For over time display of events, if the resolution of a gadget cannot be displayed as is on screen, it is possible to zoom in by selecting a part of the graph to reduce resolution.

**Gadget Options**

You can manipulate and perform actions on any gadget by accessing the available options using the menu icon in the right hand side of the Gadget header bar.

Gadget options are:

- **Edit** – For editing a gadget definition (see Managing Gadgets in the administrator's guide).
- **Duplicate** – For duplicating a gadget definition and creating a new one (see Managing Gadgets in the administrator's guide).
- **Delete** – For removing the gadget from the dashboard; Please see Administrator's Guide for details.
- **Generate Now** – For forcing a data generation and update the gadget result.
- **Pin to Top / Unpin from Top** – For placing a gadget at the top of the dashboard or releasing a gadget which was pinned to top of the dashboard.
- **Export to PDF** – For exporting a gadget to a PDF file (see Exporting a Gadget to a PDF/CSV File).
- **Export to CSV** – For exporting a gadget to a CSV file (see Exporting a Gadget to a PDF/CSV File).
- **Copy Permalink** – This option copies to the clipboard a direct link to the gadget. The link can be then used externally to XpoLog to present the gadget's result (for example in an iFrame in an external portal). 2 parameters which should be considered to be added to the link:
  - Login credentials - mandatory in case Security is active in XpoLog, a user and password with the credentials to view the dashboard should be added: &autoLogin=true&username=[USER_NAME]&password=[PASSWORD]
  - Enable Zoom - optional, dashboard/gadgets contain links to zoom in back to XpoLog to see the result, by default the zoom in links are presented. It is possible to add a parameter which determines this behavior: &allowZoom=false or &allowZoom=true
- **Relocating a gadget** - it is possible to drag and drop gadgets to a different location within a dashboard (see Relocating a Gadget).

**Exporting a Gadget to a PDF/CSV File**

You can export any gadget to a PDF/CSV file, and then print it out.

To export a gadget to a PDF/CSV file:

1. In the header bar of the gadget that you want to export, click the **Tools** icon, and from the menu items that appear, click **Export to PDF/CSV**.
   A Prepare Export to PDF/CSV notification box appears, informing that it is preparing data for export. It is followed by an Export to PDF/CSV notification box.
   The PDF/CSV file is created and can be saved.

   **Note**: If pop-ups are blocked, you are asked to click **Continue** to complete the export.

**Relocating a Gadget**

You can move a gadget to a different location in the dashboard.

To relocate a gadget:

1. Mouse over the gadget, the relocate icon is presented.
2. Using the relocate icon, drag and drop the gadget to its new location in the dashboard.

**Out of the box Apps**

XpoLog out of the box Apps are predefined packages of searches, rules, monitors, visualizations and other knowledge about a specific system. The packages are packed as Apps and are available either in the XpoLog setup or by updating the XpoLog instance with the latest Apps updates.

In order to start using out of the box apps you need to follow few simple steps:

1. Add and prepare data from a system that have an out of the box apps. View the list of out of the box Apps here.
2. Deploy the out of the box app on the data set.

Further information about how to add and prepare data for Apps can be found here: Prepare Data for XpoLog Apps
You can view here the Out of the box Apps list.

**App - Apache Httpd (2.2)**

<table>
<thead>
<tr>
<th>Name</th>
<th>Apache Httpd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Versions</td>
<td>2.2</td>
</tr>
<tr>
<td>Web</td>
<td><a href="http://www.apache.org">www.apache.org</a></td>
</tr>
<tr>
<td>Type</td>
<td>Web Servers</td>
</tr>
<tr>
<td>logtypes</td>
<td>httpd</td>
</tr>
<tr>
<td>logtypes</td>
<td>access, w3c, error</td>
</tr>
</tbody>
</table>

In order to deploy Apache Httpd App use the following page to prepare the log data - [Preparing Apache Httpd Data](#).

**Deploying the App**

1. Deploy the Apache Httpd App available in the XpoLog setup or by getting the App package from XpoLog website.
2. Once the App is successfully deployed (by default) all logs tagged in logtype: httpd will be included in the App. To change that simply edit the App and specify which httpd logs to include or exclude.

**Open and Use the App**

1. Click on the deployed App
2. When the App will open you will see a list of available predefined dashboards. In each dashboard you can find a set of visualization gadgets, rules and searches that analyze the httpd logs.

**Httpd Dashboards and Gadgets**

Dashboard Name: Http Errors

Description: Collection of gadgets analyzing different dimension of the log data using the http response status code as a pivot for the analysis. Collection of gadgets that summarize the error code distribution, resources and referrers causing or leading to the errors and etc.

Gadgets and Inputs: Inputs are available in order to focus the gadgets on specific errors, servers, user ip or URL in order to drive better understanding of root cause in the web applications.

Required field types: referer, respstatus, remoteip, requrl, useragent

---

**App - Linux**

<table>
<thead>
<tr>
<th>Name</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Type</td>
<td>Operating System</td>
</tr>
<tr>
<td>logtypes</td>
<td>linux, linux-cron, linux-mail, linux-messages</td>
</tr>
</tbody>
</table>

In order to deploy the Linux App use the following page to prepare the log data - [Preparing Linux Event Logs Data](#).

**Deploying the App**

1. Deploy the Linux App available in the XpoLog Linux setup or by getting the App package from XpoLog website.
2. Once the App is successfully deployed (by default) all logs tagged in logtype: linux, linux-cron, linux-mail, linux-messages will be included in the App. To change that simply edit the App and specify which logs to include or exclude.

**Open and Use the App**
1. Click on the deployed App
2. When the App will open you will see a list of available predefined dashboards. In each dashboard you can find a set of visualization gadgets, rules and searches that analyze the Linux event logs.

**Linux Dashboards and Gadgets**

The Linux application contains a set of dashboards:

- **Overview** - a general overview of the Linux environment including event sources, login status, and security status.
- **Events Sources** - a console that enables events view from selected servers/domains/logs
- **Activity** - logging activity of servers and processes over time last 1 day vs. last 7 days
- **Login Status** - users activity review such as logons over time, success vs. failure authentication, failed logins, etc.
- **Problems & Errors** - a report of applications problems by event/host
- **Cron** - a console for the cron activities.
- **Mail** - a console for the mail activities.

Use the user inputs while viewing a dashboard to filter the view to the desired values such as servers, logs, processes, etc.

### App - Log4J (1.2)

<table>
<thead>
<tr>
<th>Name</th>
<th>Apache Log4J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Versions</td>
<td>1.2</td>
</tr>
<tr>
<td>Web</td>
<td><a href="http://www.apache.org">www.apache.org</a></td>
</tr>
<tr>
<td>Type</td>
<td>Logging Technology</td>
</tr>
<tr>
<td>logtypes</td>
<td>log4j</td>
</tr>
</tbody>
</table>

In order to deploy Apache Log4J App use the following page to prepare the log data - [Preparing Apache Log4J Data](#).

**Deploying the App**

1. Deploy the Apache Log4J App available in the XpoLog setup or by getting the App package from XpoLog website.
2. Once the App is successfully deployed (by default) all logs tagged in logtype: log4j will be included App. To change that simply edit the App and specify which log4j logs to include or exclude.

**Open and Use the App**

1. Click on the deployed App
2. When the App will open you will see a list of available predefined dashboards. In each dashboard you can find a set of visualization gadgets, rules and searches that analyze the log4j logs.

### App - Log4Net (2.0)

<table>
<thead>
<tr>
<th>Name</th>
<th>Apache Log4net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Versions</td>
<td>2.0.*</td>
</tr>
<tr>
<td>Web</td>
<td><a href="http://www.apache.org">www.apache.org</a></td>
</tr>
<tr>
<td>Type</td>
<td>Logging Technology</td>
</tr>
<tr>
<td>logtypes</td>
<td>log4net</td>
</tr>
</tbody>
</table>

In order to deploy Apache Log4Net App use the following page to prepare the log data - [add log4net data](#).

**Deploying the App**

1. Deploy the Apache Log4Net App available in the XpoLog setup or by getting the App package from XpoLog website.
2. Once the App is successfully deployed (by default) all logs tagged in logtype: log4net will be included App. To change that simply edit the App and specify which httpd logs to include or exclude.
Open and Use the App

1. Click on the deployed App
2. When the App will open you will see a list of available predefined dashboards. In each dashboard you can find a set of visualization gadgets, rules and searches that analyze the log4net logs.

App - Windows

<table>
<thead>
<tr>
<th>Name</th>
<th>Microsoft Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Type</td>
<td>Operating System</td>
</tr>
<tr>
<td>logtypes</td>
<td>windows, windows-application, windows-security, windows-system</td>
</tr>
</tbody>
</table>

In order to deploy the Windows App use the following page to prepare the log data - [Preparing Windows Event Logs Data](#).

Deploying the App

1. Deploy the Microsoft Windows App available in the XpoLog Windows setup or by getting the App package from XpoLog website.
2. Once the App is successfully deployed (by default) all logs tagged in logtype: windows, windows-application, windows-security, windows-system will be included in the App. To change that simply edit the App and specify which logs to include or exclude.

Open and Use the App

1. Click on the deployed App
2. When the App will open you will see a list of available predefined dashboards. In each dashboard you can find a set of visualization gadgets, rules and searches that analyze the Microsoft Windows event logs.

Windows Dashboards and Gadgets

The Windows application contains a set of dashboards:
- Overview - a general overview of the Windows environment including required restarts, updates errors, policy changes, etc.
- Events Viewer - a console that enables events view from selected servers/domains/logs
- Events Statistics - general statistics of top used sources, categories, types and event codes
- Audit - a high level analysis of top applications, sources, users operations, events, etc.
- Trends - logging activity of servers and logs over time last 1 day vs. last 7 days
- Users Overview - users activity review such as logons over time, top users operations report, logons vs. logoffs, etc.
- Application Installs - a report of total installed applications failed and successful
- Application Crashes - a report of applications crashes by event/host

Use the user inputs while viewing a dashboard to filter the view to the desired values such as servers, domains, accounts, etc.

XpoLog Search

Overview

Data is constantly entering your system’s IT infrastructure from various sources. This data is of all types – performance data and statistics, traps and alerts, log files, configurations, scripts and messages, and arrives from various sources – your logs, folders, applications, network devices, database tables, and servers.

XpoLog indexes in real time all data entering your system’s IT infrastructure from various sources, and structures and normalizes this data – both raw and rich, into a single database of a structured format.

XpoLog provides a search engine – XpoSearch, which enables you to conduct a search through this immense amount of data for anything that you like. Using the XpoSearch interface, you can search all the logs in XpoLog Center (applications, servers, network devices, database tables, and more).

Search Types

XpoSearch provides two main types of searches:
- Simple search – initial search, using simple search syntax, which results in a list of matching events
- Complex search – an advanced search, using complex search syntax, which results in a summary table of matching events, or transactions
Search Stages

A search can be run in three stages:

- Initial search
- Refined search
- Complex search

Initial Search

In the initial search, the user enters a search query of simple criteria, and the search runs on all the event data. In this simple search, the user can search the event data for a simple term or more than one term, run a Boolean search, a search with wildcards, or a column-based search.

Running the search query returns a list of all matching events from all relevant logs (latest on top). In addition, XpoSearch returns a graphical view of the distribution of the matching events over time and per data source.

Refined Search

The resulting events of a simple search can be minimized by refining the search results using either or both of the following methods:

- Filtered Search – filtering the resulting events according to the source of the event – logs, files, applications, or servers
- Analytics-based Search – adding one of the event data fields discovered during the simple search to the search criteria of the simple search

Complex Search

Complex search queries are used to perform advanced complex operations and reporting on the log events resulting from a simple search. Running a complex search query results in a summary table, and can also be visualized as gadgets in XpoLog Dashboards.

Accessing the XpoLog Search Console

You can access XpoLog Search from any page in the application.

To access the search console:

- In the Tab Bar, click the **Search** tab.
  The Search console opens, displaying the latest search query. See Search User Interface Elements.

Search User Interface Elements

XpoLog Search is equipped with a user friendly graphic user interface (GUI), which provides a complete set of tools to search for event data that meets specific criteria.
The Search user interface includes the following main elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tab Bar</strong></td>
<td>Tabs for accessing the XpoLog, Search, and Analytics applications.</td>
</tr>
<tr>
<td><strong>Main Menu</strong></td>
<td>Includes menu items and submenus for performing actions in the XpoLog applications. Available menus are:</td>
</tr>
<tr>
<td></td>
<td>- Dashboards</td>
</tr>
<tr>
<td></td>
<td>- Administration</td>
</tr>
<tr>
<td><strong>Search Query Panel</strong></td>
<td>Area for entering the search query and the time interval for running the query.</td>
</tr>
<tr>
<td></td>
<td>In addition, this panel includes the following feature:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Open the search options window</strong> button – Clicking this menu opens a window with links to four windows: Search History, Saved Searches, Simple Search Syntax, and Complex Search Syntax.</td>
</tr>
<tr>
<td><strong>Graph Area</strong></td>
<td>Displays two graphs:</td>
</tr>
<tr>
<td></td>
<td>- Main graph – a graphic distribution of the events resulting from the search query over time.</td>
</tr>
<tr>
<td></td>
<td>- The x-axis presents indications on the errors detected by XpoLog Analytics engine based on severity and number of occurrences (red=high, orange=medium, yellow=low / the size of the icon represents the relative number of occurrences in that time period compared to other periods)</td>
</tr>
<tr>
<td></td>
<td>- Zoom-in graph – shows zoom-in area with respect to original search context.</td>
</tr>
<tr>
<td></td>
<td>In addition, this panel includes the following feature:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Actions Items</strong> – you can perform the following actions: <strong>Save Search</strong>, <strong>Save Monitor</strong>, <strong>Save Gadget</strong>, <strong>Export Result to PDF/CSV</strong>, and <strong>Share Search</strong> (generates a link that can be shared of the exact query and time which was executed)</td>
</tr>
<tr>
<td></td>
<td>- <strong>Visualization Buttons</strong> – Clicking these buttons presents the search results in different way - line (aggregated/split per source), bar (aggregated/split) and pie charts.</td>
</tr>
</tbody>
</table>
Augmented Search Pane

Enables refining your simple search results. Includes the following sections:

- **Active Filters** - active filters are stored and may be removed to return to a previous view.
- **Isolate Results** - select source(s) in order to isolate results based on log/folder/application/server.
- **Analytics Insight** - a list that centralizes all the Analytics results related to the current search results. Click a suggestion to see where it appears over time and to add it to the search query.
- **Interesting Fields** - a list of logs columns which different complex functions are available on. Click a column name to see which functions may be activated on it.

Search Results Area

In the case of a simple search, displays all the events that match the search query.

In the case of a complex search, displays a summary table of the events that match the search query.

Mouse Over Events in the search results area presents 2 options on the highlighted phrase:

- **Search Actions** - add/exclude/replace the phrase from the current search.
- **Data Markers** - pick a color to paint the highlighted phrase across all results.

Search Query Panel

The Search Query Panel user interface includes the following elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>

-前不久
Open the Search Options window icon

Clicking this icon displays a window with four links:

- **Search History** – Clicking this link opens a window that displays your recent and popular searches.
- **Saved Searches** – Clicking this link opens a window with a list of the names of the searches that you saved.
- **Simple Search Syntax** – Clicking this link opens a window, which lists the syntax that you can use to formulate a simple search.
- **Complex Search Syntax** – Clicking this link opens a window, which lists the syntax that you can use to formulate a complex search.

It also includes a **Close** icon for closing the Search Options window.

Auto-complete section

When typing a query, the auto-complete section opens. The left side provides suggestions on relevant syntax and sources to run the search. The right side presents Search History and Saved Searches available for selection.
Search Status icon

Search Query

Area for typing a simple or complex search query, or for activating a saved search query. This section will dynamically be expanded when long queries are typed.
<table>
<thead>
<tr>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save Search</strong> – Selecting this item saves the search query in the system.</td>
</tr>
<tr>
<td><strong>Save Gadget</strong> – Selecting this item saves the search query as a gadget.</td>
</tr>
<tr>
<td><strong>Save Monitor</strong> – Selecting this item saves the search query as a monitor.</td>
</tr>
<tr>
<td><strong>Export to PDF/CSV</strong> – Selecting this item saves the search query and results in a PDF/CSV file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Close Augmented Search / Open Augmented Search buttons.</th>
</tr>
</thead>
<tbody>
<tr>
<td>By default, the Augmented Search Pane is open. Clicking the button closes the pane; clicking the button opens the pane.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines the time period during which the search is to be run.</td>
</tr>
<tr>
<td>Selectable time periods include:</td>
</tr>
<tr>
<td>- The entire time that the log exists: <strong>All Time</strong></td>
</tr>
<tr>
<td>- Predefined time periods: <strong>Today</strong>, <strong>Yesterday</strong>, <strong>This Week</strong>, <strong>Last 15/30/60 Minutes</strong>, <strong>Last 3/12/24 hours</strong>, <strong>Last 7/14 days</strong>, <strong>Last 1/3 months</strong></td>
</tr>
<tr>
<td>- <strong>Live</strong>: Real-time search mode will be activated and new records that match the search criteria will be loaded to the screen (see below)</td>
</tr>
<tr>
<td>- Customized time periods: <strong>Custom</strong></td>
</tr>
</tbody>
</table>
XpoLog Search provides Live mode search (near real time). The Live mode may be activated by selecting it from the list of time period options. Selected the graph area will be cleared and a red button will be presented to indicate Live is active. New records which match query criteria will be loaded to the screen every few seconds. Clicking this button after typing a search into the Search Query commences the search. While a search is being executed the pause button will be presented click it to pause the search and then resume to continue the search.

---

**Simple Search Syntax**

The following table summarizes the simple search syntax:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td><strong>AND</strong> – A and B matches events that contain A and B.</td>
</tr>
<tr>
<td></td>
<td><strong>OR</strong> – A or B matches events that contain A or B.</td>
</tr>
<tr>
<td></td>
<td><strong>NOT</strong> – A and NOT (B or C) matches events that contain A but not B or C.</td>
</tr>
<tr>
<td>Quotation Marks</td>
<td>Used to get an exact match of a term. Recommended when there is a key word (such as ( ), =, and, or, not, in, *, ?) within a searched term.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> &quot;connection(1234) failure&quot; -&gt; returns events with an exact match to connection(1234) failure.</td>
</tr>
</tbody>
</table>
| Parentheses | Used to unify a term result or to create precedence within search queries.  
| Example: | \(a \text{ or } (b \text{ in folder.my_folder})\) -> searches for events that contain \(a\), or events that contain \(b\) in sub folders and logs under the folder my_folder.  
| | \(a \text{ or } b \text{ in folder.my_folder}\) -> searches for events that contain \(a\) or \(b\) in sub folders and logs under the folder my_folder.  
| | \(a \text{ and } b \text{ or } c\) -> precedence to the key word and, this term is equivalent to \((a \text{ and } b) \text{ or } c\).  
| | \(a \text{ and } (b \text{ or } c)\) -> precedence to the key word its result and \(a\).  
| Wildcards | May be placed anywhere in a search term:  
| Example: | * – "foo, foo", f’oo, *’foo”, *"f*o*o" (\(*\) represents any characters, 0 or more times)  
| | ? – ?oo, fo?, f? o (? represents any character, exactly one time)  
| Search in a specific log/folder/application/server | Searches for a term in a specified log, folder, application, or server.  
| Example: | error in log.my_log -> searches for error only in logs whose name is my_log.  
| | error in log.my* -> searches for error only in logs whose name starts with my.  
| | error in folder.my_folder -> searches for error only in logs under folders whose name is my_folder.  
| | error in folder.my* -> searches for error only in logs under folders whose name starts with my.  
| | error in host.my_host -> searches for error only in logs whose source name is my_host.  
| | error in host.my* -> searches for error only in logs whose source name starts with my.  
| | host.my_host is equivalent to server.my_host.  
| | error in app.my_app -> searches for error only in logs associated to applications whose name is my_app.  
| | error in app.my* -> searches for error only in logs associated to applications whose name starts with my.  
| | app.my_app is equivalent to application.my_app.  
| Column-based Search | Searches for events that have a specific value in a specific column of the log.  
| Example: | column_name=search_value -> searches for events that have a column named column_name whose value is equal to search_value (relevant only for logs that have a column with that name).  
| | column_name=search_value in log.my_log -> searches for events in the log my_log that have a column column_name whose value is equal to search_value (relevant only if the log has a column with that name).  
| | column_name contains search_value -> searches for events that have a column named column_name whose value contains search_value (relevant only to logs that have a column with that name).  
| | column_name contains search_value in log.my_log -> searches for events in the log my_log, which have a column column_name whose value contains search_value (relevant only if the log has a column with that name).  
| Regular expression search | Searches in events for values represented by regular expressions.  
| Example: | regexp:\d+ in log.access -> searches for numbers in events.  
| Activate saved search | Activates a search that you previously saved.  
| Example: | search.search_name -> runs the saved search called search_name.  

**Graph Area**

The Graph Area user interface includes the following elements:
Graph toolbar includes icons for defining the graph visualization and content.

Main Graph: A graph that displays the distribution of events over time. The search query timeline is the x-axis, and the number of matching events is the y-axis.

The main graph shows the distribution of events matching the search query over the selected timeline. Any time period in the graph can be zoomed into, by selecting a time on the time axis, and dragging left/right the vertical line that appears on the graph, to the beginning/end of the time period to be zoomed into. A Zoom Out button appears on top of the zoomed-in graph, enabling return to the original search results.

Zoom-In Graph: Below the main graph. Displays zoomed-in area with respect to the original search context. For example, zooming in on one day of the last 7 days, shows in this graph all seven days, with the zoomed-in day shaded in blue. Can zoom into a time period from this graph (see explanation in Main Graph).

Graph Toolbar

The right side of the Graph toolbar includes the following buttons for defining the type of graph to generate:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graph toolbar</td>
<td>Includes icons for defining the graph visualization and content.</td>
</tr>
<tr>
<td>Main Graph</td>
<td>A graph that displays the distribution of events over time. The search query timeline is the x-axis, and the number of matching events is the y-axis. The main graph shows the distribution of events matching the search query over the selected timeline. Any time period in the graph can be zoomed into, by selecting a time on the time axis, and dragging left/right the vertical line that appears on the graph, to the beginning/end of the time period to be zoomed into. A Zoom Out button appears on top of the zoomed-in graph, enabling return to the original search results.</td>
</tr>
<tr>
<td>Zoom-In Graph</td>
<td>Below the main graph. Displays zoomed-in area with respect to the original search context. For example, zooming in on one day of the last 7 days, shows in this graph all seven days, with the zoomed-in day shaded in blue. Can zoom into a time period from this graph (see explanation in Main Graph).</td>
</tr>
</tbody>
</table>
Display Line Chart button. Clicking this icon displays a line graph of the event distribution. Mouse over this icon presents below different line charts based visualization options.

Display Summary View button. Clicking this button displays a summary view of the event distribution from all the logs/applications/servers.

Display Summary View button. Clicking this button displays the event distribution originating from each log (default application, or server (according to what you selected Distribute by selection box described in this table).

Display Column Chart button.
Clicking this button displays a column (bar) graph of the event distribution.

Mouse over this icon presents below different line charts based on visualization options:

Display Summary View button. Clicking this button displays a column chart in summary view.

Display Split View button. Clicking this button displays a column chart in split view, i.e., a vertical line for each log (default), application, or server (according to what you selected in the Distribute by selection box described in this table).
Display Stack View button. Clicking this button displays a column stack view, i.e. a horizontal bar for each log (default), application, or server (according to what you selected in the Distribute by selection box in this table).

Display Pie Chart button.
Clicking this button displays a pie chart of the event distribution.
The left side of the Graph toolbar includes the following buttons for defining additional views on the graph. The available options depend on the selected type of graph:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Augmented layers selection box</td>
<td>Enables selecting the types of problems to be represented by the dots on the time axis of the main graph:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Predefined</strong> – problems predefined by the user (using the saved search mechanism)</td>
</tr>
<tr>
<td></td>
<td>- <strong>Autodetected</strong> – problems automatically detected by XpoLog Analytics engine</td>
</tr>
<tr>
<td></td>
<td>- Both predefined and auto-detected problems</td>
</tr>
</tbody>
</table>

**Pie, Line, and Column Charts**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribute by selection box</td>
<td>Enables selecting according to what entity to distribute the information resulting from the search: <strong>Total, Logs, Applications</strong>, or <strong>Servers</strong>.</td>
</tr>
<tr>
<td></td>
<td>Selecting Logs/Applications/Servers changes the graph accordingly, and displays above the graph a color-coded legend of the different log/application/server names in the system.</td>
</tr>
</tbody>
</table>

**Search Results Area**

The contents of the Search Results Area depends on the type of search that you run:

- For a simple search, each result event meeting the search criteria is displayed.
- For a complex search, a summary table of the result events or transactions are displayed.

**Simple Search Results Area**

The following table describes the user interface of the Simple Search Results Area:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Search Results Summary Panel</strong></td>
<td>A panel that summarizes the results of the search, and provides navigation to the result event pages.</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Events Toolbar</strong></td>
<td>Includes icons for expanding/collapsing events and for disabling/enabling Analytics.</td>
</tr>
<tr>
<td><strong>Events Area</strong></td>
<td>A list of the events that match the search query.</td>
</tr>
</tbody>
</table>

**Search Results Summary Panel**

The Search Results Summary Panel includes the following details:

<table>
<thead>
<tr>
<th><strong>Element</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Summary</td>
<td>In the case of a simple search, displays the number of matching log files and the period of time searched.</td>
</tr>
<tr>
<td></td>
<td>In the case of a complex search, displays the number of results in the table, the number of events that the results are based on, the number of source logs of these events, and the period of time searched.</td>
</tr>
<tr>
<td>Previous matching events icon</td>
<td>Clicking this icon displays in the Result Page Navigation Area, the numbers of the previous ten pages, and displays the first of these pages in the Search Results Area.</td>
</tr>
</tbody>
</table>
Next matching events icon.
Clicking this icon displays in the Result Page Navigation Area the n of the next ten pages, and displays the first of these pages in the S Results Area.
Results Page Navigation Area

Displays the page numbers of up to ten pages of results. You can click the previous/next ten page numbers, by clicking the icons.

Clicking a page number displays that page of results in the Search Results Area. The current page number is highlighted in white.

**Events Toolbar**

The Events Toolbar includes the following elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>

Clicking the **Expand all Events / Collapse all Events** icons.

- The **icon** expands all events to display all their column names and respective values.
- The **icon** collapses all events to show only some of the column names and respective values.
Events Area

The Events Area includes a list of events resulting from the search, where each event contains the following elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event timestamp</td>
<td>The date and time that the event occurred, in the format MM/DD/YY HH:MM:SS</td>
</tr>
</tbody>
</table>
| **Analytics layer** | If Analytics is active, colors the fonts of the column values that Analytics detects as problematic, according to the following color-coding:
- **Red** – high severity problem
- **Orange** – medium severity problem
- **Yellow** – low severity problem
Under the timestamp, displays the severity of the most severe column value detected by Analytics in the event: high, medium, low, or non |

| **Event structure** | The structure of the event, including its column names and respective column text, in the format \([COLUMN_NAME] COLUMN_TEXT\). |

| **Event source fields** | Shows the source of the event – the log, server, and/or applications generated the event. Mouse over on the log source indicator \([Log]\) to see the full path of the source log that this message originates from. |
Expand Event icon.
Appears at the end of an event that can be expanded to show all its names and respective values.

Clicking the icon expands the event to display all its column names and respective values, and changes the icon to the Collapse Event icon, so that it can be shortened at a later time.
Mouse Over Options

Mouse over on search results (and columns names) presents two actions:

- **Search Actions**: Clicking this icon presents a list of possible search actions on the highlighted phrase: append to current search using **AND**, append current search using **OR**, excluding from current search, replacing current search.

- **Data Markers**: Clicking this icon presents colors to be selected in order to mark the highlighted phrase.

**Complex Search Results Area**

The following table describes the user interface of the Complex Search Results Area:
### Element | Description
--- | ---
**Search Results Summary Panel** | A panel that summarizes the results of the search, and provides navigation to the results pages; same as panel in Simple Search (see detailed description in Search Results Summary Panel section in Simple Search Results Area).
**Summary Table** | Displays a table that summarizes the results of the complex search. The results are clickable - clicking a result will present the log records related to that result.
**Transactions List** | Displays a list of transactions matching the transaction search criteria.

### Augmented Search Pane

The following table describes the user interface of the Augmented Search Pane:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Filters</strong></td>
<td>Lists all the suggestions that have been added to the original query, from the suggestions in the resulting events and on the graph. Any suggestion can be removed from the query by removing it from the Active Filter list.</td>
</tr>
<tr>
<td><strong>Isolated Results</strong></td>
<td>Lists the sources of the events: Logs, Folders, Servers, and Applications, and displays in parentheses near each source type, the number of events in that source type. Selecting any of these source types opens a table with a listing of its sources, enabling you to select the checkboxes of the sources by which to filter the events.</td>
</tr>
</tbody>
</table>
| **Analytics Insight** | Lists in order of importance, the field values that have been detected by Analytics as being problematic. Clicking Load more... on the bottom of the list, displays the ten next most important field values. Selecting one of these field values, enables you to refine your simple search results, by selecting one of the following:  
   - Append to query with And – searches for events that meet the criteria of your original search query, and also contain the field value selected from the Analytics Insight list.  
   - Append to query with Or – searches for events that either meet the criteria of your original search query, or contain the field value selected from the Analytics Insight list.  
   - Replace query – replaces your original search query, with a search for events with the field value selected from the Analytics Insight list.  |
| **Interesting Fields** | Lists in order of importance, the fields that appear most frequently in the events. Clicking Load more... on the bottom of the list, displays the next most interesting fields. Selecting one of these fields opens a list of functions that can be performed on the field. Selecting a function from this list initiates a complex search composed of the selected field and function, on the results of the simple search. |

### Performing a Simple Search

XpoSearch enables you to retrieve specific events from indexed event logs, by creating a search query using the XpoSearch search syntax, and then running the search. This is an extremely useful tool for investigating the cause of problems in your system. Also, you can limit any search to events that occurred during a specific time period.

### Selecting the Search Time Period

Time plays a very important role in the examination of the cause of a system problem.

Although you can run a search on events that occurred at any time, this wastes system resources, and usually results in an overwhelming number of events that are difficult for you to manage and analyze.

Therefore, XpoSearch enables you to run a search on a specific time period, so that you can narrow your results, and facilitate determining the root cause of the problem. You can select a predefined time period, or customize the time period by selecting the start and end dates and times of the time period.

To select the time period of the search:
1. In the Search Query Panel, in the Search Time Range textbox, click the down arrow.

A list of selectable time periods opens.

2. From the list of time periods, select a predefined time period (All Time (all times in the log), Last 15 Minutes, Last 30 Minutes, Last 60 Minutes, Last 3 Hours, Last 12 Hours, Last 24 Hours, Last 7 Days, Last 14 Days, Last 1 Month, Last 3 Months, Last Week, This Week, Yesterday, or Today), or select Custom to specify your own time period (see Customizing the Search Time Period for a detailed explanation on customizing the time period).

The selected time period is displayed in the textbox, and the search runs on this time period.

Creating a Search Query

You can create a search query using the search syntax supplied by XpoLog for simple searches:

- Simple terms search
- Boolean search
- Search with wildcards
- Comparison search
- Search in a specific log, folder, application, or server
- Activate a saved search by its name

Searching for Simple Terms

The simplest type of search is one that searches for terms in your log events. This includes the following:

- Searching for a single word that appears anywhere in the event.
  
  **Example:** Typing `error` searches for all events containing the word `error`.
- Searching for two or more words that appear in an event, exactly in the order that you typed them.
  
  **Example:** Typing `error log` only searches for events having the words `error` and `log` adjacent to each other in the event.
- Searching for keywords in an event – by enclosing the words in quotes. These keywords can be Boolean operators or saved words.
  
  **Example:** If you want to search for the word `NOT` in an event, and do not want it to be misinterpreted as the Boolean operator NOT, you should enclose it in quotes: `"NOT"`.

XpoSearch also provides the autocomplete feature. As you type the search query, a dropdown list of other search queries that you have created in the past and that begin with these characters is displayed, as relevant. If one of these search queries is the one that you want to run, you can simply select it instead of retyping the entire search query.

Boolean Search

XpoLog provides three Boolean operators for your use: OR, AND, NOT, evaluated in a search query in that order. These operators must be capitalized. It is also possible to change the default order of precedence, by enclosing in parenthesis the part of the search term that you want to perform first.

**Example:** Searching for `end process OR start process` returns all events containing either the phrase `end process` or the phrase `start process`.

**Note:** If you want to search in an event for any words that are the same as Boolean operators, you should enclose them in quotes, so that they are not misunderstood for the Boolean operator.

Searching with Wildcards

XpoSearch provides two wildcards:

- `?` – used in a search term to represent a single alphanumeric character.
  
  **Example:** Typing `http ?00` returns `http 100`, `http 200`, `...`, and `http 900`. It does not return `http 2000`, as the `?` only replaces a single character.
- `*` – used in a search term to represent zero to any number of any alphanumeric characters. A search term which only includes an `*` returns all events, up to the maximum allowed by the system.
  
  **Example:** Typing `http *00` returns all events beginning with `http` and ending with `00`, such as `http 300`, `http 3000`, and `http 500`.

Searching in a Specific Log/Folder/AppTag/Server

XpoSearch enables searching events in all event logs of the system, regardless of their source, or only in event logs that come from a specific source, as follows:
- Log – a specific log
- Folder – logs in a specific folder
- AppTag – logs of a specific application
- Server – logs from a specific server

Examples:
1. Running a search for `error in log.my_log` returns events only from the log named `my_log` that include the word `error`, regardless of where this log resides.
2. Running a search for `error in log.X in folder.Y` returns events only from event log `X` that resides in folder `Y`.

Column-based Search

You can run a column-based search on event data, to extract only those events which have a specific column that meets the comparison criteria. This is done by creating a search that compares a specific column to a specific value, using the comparison operators defined in the following table.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Equals</td>
</tr>
<tr>
<td></td>
<td>column_name = x returns all events with column_name value exactly equal to x.</td>
</tr>
<tr>
<td>!⇒</td>
<td>Not equals</td>
</tr>
<tr>
<td></td>
<td>column_name !⇒ x returns all events with column_name value not equal to x.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than; for numerical fields only</td>
</tr>
<tr>
<td></td>
<td>column_name &gt; x returns all events with column_name value greater than x.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than; for numerical fields only</td>
</tr>
<tr>
<td></td>
<td>column_name &lt; x returns all events with column_name value less than x.</td>
</tr>
<tr>
<td>contains</td>
<td>Used for checking if a column contains a specific value</td>
</tr>
<tr>
<td></td>
<td>column_name contains x returns all events that contain in column_name the value x.</td>
</tr>
<tr>
<td>NULL</td>
<td>Used to find empty or populated columns</td>
</tr>
<tr>
<td></td>
<td>column_name = NULL returns all events that have no value in column_name.</td>
</tr>
<tr>
<td></td>
<td>column_name returns all events that have a value in column_name.</td>
</tr>
<tr>
<td>NOT</td>
<td>Used to exclude events that have a specific value in a specific column</td>
</tr>
<tr>
<td></td>
<td>NOT (column_name contains error) returns all events that do not have error in column_name.</td>
</tr>
</tbody>
</table>

Example: Typing `Priority !⇒ Error` returns all events that do not have the value `Error` in the `Priority` column.

Regular Expression Search

XpoLog enables you to search in events for values represented by a regular expression that you specify.

Example: Typing `regexp:\d+ in log.access` searches for numbers in events.

Activating a Saved Search

XpoLog enables you to save any search query so that you can easily run it at a later time. You can either activate the saved search by selecting its name from a list of saved searches (see Running a Saved Search) or you can type `search.search_name` in the search query to run the saved search called `search_name`.

Example: Typing `search.error_search` activates the saved search named `error_search`.

Customizing the Search Time Period
You can customize the time period of a search, by selecting from calendars the beginning and end dates and times of the time period.

To customize the time period:

1. In the Search Query Panel, in the Time Period selection box, select Custom.
   Two calendars – one of the start date and one of the end date of the previous search query time period are displayed.
2. In the left calendar, repeatedly click the arrows at the left and right of the month name, to scroll to previous/following months, until you reach the desired month of the start date. Then, in the calendar, click the desired start date.
   The day is highlighted in the calendar, and is displayed below the calendar in Start Date.
3. In Start Time, type the time of day that the time period begins.
4. In the right calendar, repeatedly click the arrows at the left and right of the month name, to scroll to previous/following months, until you reach the desired month of the end date. Then, in the calendar, click the desired end date.
   The day is highlighted in the calendar, and is displayed below the calendar in End Date.
5. In End Time, type the time of day that the time period ends.
6. Click Go.
   The search runs on the selected time period, returning in the Search Results Area, the results of the search for the customized time period.
   Note: The Time Period box displays Custom.

Alternatively - select the part in the graph which you want to zoom into and the console will updated to the selected time frame.

Simple Search Examples

The following table contains examples of simple search queries:

<table>
<thead>
<tr>
<th>Query</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Searches in all logs for all log events.</td>
</tr>
<tr>
<td>Information</td>
<td>Searches in all logs for log events that contain the term Information.</td>
</tr>
<tr>
<td>Service Control Manager</td>
<td>Searches in all logs for log events that contain the phrase Service Control Manager.</td>
</tr>
<tr>
<td>“error is not caused by database”</td>
<td>Searches in all logs for log events that contain the exact phrase error is not caused by database.</td>
</tr>
<tr>
<td>Error or exception</td>
<td>Searches in all logs for log events that contain the term error or exception.</td>
</tr>
<tr>
<td>Error or exception or fail*</td>
<td>Searches in all logs for log events that contain the term error or exception or any word beginning with fail (such as fail, fails, failed, failure)</td>
</tr>
<tr>
<td>Service Control Manager OR Microsoft-Windows-Security-Auditing</td>
<td>Searches in all logs for log events that contain either of the following phrases: Service Control Manager or Microsoft-Windows-Security-Auditing.</td>
</tr>
<tr>
<td>Service Control Manager AND WinHTTP</td>
<td>Searches in all logs for log events that contain the phrase Service Control Manager and the term WinHTTP.</td>
</tr>
<tr>
<td>Service Control Manager AND NOT WinHTTP</td>
<td>Searches in all logs for log events that contain the phrase Service Control Manager but do not contain the term WinHTTP.</td>
</tr>
<tr>
<td>Service Control Manager and NOT (WinHTTP OR Multimedia)</td>
<td>Searches in all logs for log events that contain the phrase Service Control Manager but do not contain the term WinHTTP nor the term Multimedia.</td>
</tr>
<tr>
<td>703?</td>
<td>Searches in all logs for log events that contain the term 703, followed by a single character</td>
</tr>
<tr>
<td>703?</td>
<td>Note: The ? symbol stands for any single character that appears in its location in the term; for example: 7030, 7031, and 703A. The ? symbol can be placed anywhere in the search term (i.e. 7?03, 70?3, 703?).</td>
</tr>
<tr>
<td>Ser*</td>
<td>Wild card usage; Searches in all logs for log events that contain the term Ser, followed by zero or more characters.</td>
</tr>
<tr>
<td>Ser*</td>
<td>Note: The * symbol stands for zero or more characters that appear in its location; for example: Ser, Server, and Service. The * symbol can be placed anywhere in the search term (i.e. <em>Ser, Se</em>r, and Ser*)</td>
</tr>
<tr>
<td>Type = Information</td>
<td>Searches in all logs for log events in which the value in column Type is the term Information.</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type != Information</td>
<td>Searches in all logs for log events in which the value in column Type is not the term Information.</td>
</tr>
<tr>
<td>Type contains Information</td>
<td>Searches in all logs for log events in which the value in column Type contains the term Information.</td>
</tr>
<tr>
<td>Type contains Information?</td>
<td>Searches in all logs for log events in which the value in column Type contains the term Information, followed by a single character.</td>
</tr>
<tr>
<td>Type contains Inform*</td>
<td>Searches in all logs for log events in which the value in column Type contains the term Information, followed by zero or more characters.</td>
</tr>
<tr>
<td>URL contains (/website/moe/html and <em><em>304</em></em>)</td>
<td>Searches in all logs for log events in which the value in column URL contains the term /website/moe/html and a word which contains the text <em>304</em>.</td>
</tr>
<tr>
<td>error and method contains <em>java.lang</em></td>
<td>Searches for events containing error and in the log field method a word which contains the text java.lang.</td>
</tr>
<tr>
<td>Note: A log field named method is required.</td>
<td></td>
</tr>
<tr>
<td>priority = FATAL</td>
<td>Searches the log field priority for the value FATAL.</td>
</tr>
<tr>
<td>Note: A log field named priority is required.</td>
<td></td>
</tr>
<tr>
<td>message = NULL</td>
<td>Searches the log field message for an empty value.</td>
</tr>
<tr>
<td>Note: A log field named message is required.</td>
<td></td>
</tr>
<tr>
<td>message != NULL</td>
<td>Searches the log field message for a nonempty value.</td>
</tr>
<tr>
<td>Note: A log field named message is required.</td>
<td></td>
</tr>
<tr>
<td>error and message contains connection</td>
<td>Searches for log events that contain error and the word connection in the log field message.</td>
</tr>
<tr>
<td>Note: A log field named message is required.</td>
<td></td>
</tr>
<tr>
<td>error and not (message contains NullPointerException)</td>
<td>Searches for log events that contain error and do not contain NullPointerException in the log field message.</td>
</tr>
<tr>
<td>Note: A log field named message is required.</td>
<td></td>
</tr>
<tr>
<td>lineNumber &lt; 1000</td>
<td>Searches in all logs for log events in which the numeric value in column lineNumber is less than 1000.</td>
</tr>
<tr>
<td>Note: A numeric log field named lineNumber is required. Additional numeric operators: &gt; = !=</td>
<td></td>
</tr>
<tr>
<td>lineNumber &gt; 1000 AND lineNumber &lt; 2000</td>
<td>Searches in all logs for log events in which the numeric value in column lineNumber is greater than 1000 and less than 2000.</td>
</tr>
<tr>
<td>* in log.Application</td>
<td>Searches in all logs that are named Application, for all log events.</td>
</tr>
<tr>
<td>Note: The * can be replaced with any valid search query.</td>
<td></td>
</tr>
<tr>
<td>* in log.NAME</td>
<td>Searches in all logs that are named NAME, for all log events.</td>
</tr>
<tr>
<td>Note: The * can be replaced with any valid search query.</td>
<td></td>
</tr>
<tr>
<td>error or exception or fail* in log.LOG_NAME_1, log.LOG_NAME_2, ..., log.LOG_NAME_N</td>
<td>Searches for log events containing error or exception or a term beginning with fail, in all logs named LOG_NAME_1, LOG_NAME_2, ..., LOG_NAME_N.</td>
</tr>
<tr>
<td>* in folder.NAME</td>
<td>Searches in all folders that are named NAME, for all log events.</td>
</tr>
<tr>
<td>Note: The * can be replaced with any valid search query.</td>
<td></td>
</tr>
<tr>
<td>error or exception or fail* in folder.FOLDER_NAME_1, folder.FOLDER_NAME_2, ..., folder.FOLDER_NAME_N</td>
<td>Searches for log events containing error or exception or a term beginning with fail, in all logs that are under folders named FOLDER_NAME_1, FOLDER_NAME_2, ..., FOLDER_NAME_N.</td>
</tr>
</tbody>
</table>
Augmenting Simple Search Results

XpoSearch enables you to refine your simple search results, so that you can dig deeper into the cause of events.

You can augment your simple search results in any or all of the following ways:

- Filtering the resulting events, so that only events from specific logs, folders, applications, or servers are displayed
- Refining the search, using a field value discovered by Analytics
- Running a complex search on the results of the simple search, using the interesting fields that were detected by Analytics

Disabling Augmentation

By default, augmentation is enabled. However, you can choose to disable this option.
To disable augmentation:

- In the Search Query Panel, click the Close Augmented Search icon.
  The Augmented Search Pane closes.
- The icon changes to the Open Augmented Search icon, enabling you to open the Augmented Search Pane at a later time.

Filtering Simple Search Results by Event Source

Events are organized in logs. Some of these logs are arranged in the system under folders, applications, and servers. XpoSearch enables you to display search events from specific logs, or search events in logs that are under specific folders, applications, or servers. The Augmented Search Pane displays under Isolate Results, the sources of the logs that have result events, and also displays in parentheses near each of these sources, the number of logs originating from them. You can select to minimize the search results by filtering results to display only events coming from specific logs, folders, applications, or servers.

Filtering by Log(s)

System events are arranged in the system in logs of various formats; each log is assigned an XpoSearch log name. XpoSearch enables filtering
To filter simple search results by log(s):

1. In the Augmented Search Pane, under **Isolate Results**, select **logs**.
   A table opens listing the names of the logs, the number of events coming from each log, and the percentage of events coming from each log with respect to the number of events from all the logs.
2. Select the checkboxes of the logs whose events you want to display.
   The original search query is updated: the original search text is enclosed in parentheses, and to that is appended \texttt{in log.[log name 1], log.[log name 2], ...}
   The graph, search summary panel, and events list are updated.
   The number of logs selected out of the number available appears in parentheses near **Logs** in the Augmented Search Pane. Also, the numbers of folders, applications, and servers are updated, to display the numbers of logs, applications, and servers that are sources of the logs containing the filtered events.

You can also manually filter search events to display only those from specific logs, by typing the XpoSearch log names directly into the search query following the search text using Simple Search syntax, and appending to it \texttt{in log.[log name 1], log.[log name 2], ...} for each log from which you want to display events.

Filtering by Folder(s)

Events coming into the system can appear in logs under folders, which are arranged according to user or function, depending on how you built your environment. XpoSearch enables filtering events to display only those that come from logs that reside under specific folders.

To filter simple search results by folder(s):

1. In the Augmented Search Pane, under **Isolate Results**, select **folders**.
   A table opens listing the names of the folders, the number of events coming from each folder, and the percentage of events coming from each folder with respect to the number of events from all the folders.
2. Select the checkboxes of the folders whose events you want to display.
   The original search query is updated: the original search text is enclosed in parentheses, and to that is appended \texttt{in folder.[folder name 1], folder.[folder name 2], ...}
   The graph, search summary panel, and events list are updated.
   The number of folders selected out of the number available appears in parentheses near **Folders** in the Augmented Search Pane. Also, the numbers of logs, applications, and servers are updated, to display the numbers of logs, applications, and servers that are sources of the logs containing the filtered events.

You can also manually filter search events to display only those in logs from specific folders, by typing the XpoSearch folder names directly into the search query following the search text, using Simple Search syntax, and appending to it \texttt{in folder.[folder name 1], folder.[folder name 2], ...} for each folder from which you want to display events.

Filtering by Application(s)

Events coming into the system can appear in logs of applications. XpoSearch enables filtering events to display only those that come from logs that belong to specific applications.

To filter simple search results by application(s):

1. In the Augmented Search Pane, under **Isolate Results**, select **applications**.
   A table opens listing the names of the applications, the number of events coming from each application, and the percentage of events coming from each application with respect to the number of events from all the applications.
2. Select the checkboxes of the applications whose events you want to display.
   The original search query is updated: the original search text is enclosed in parentheses, and to that is appended \texttt{in app.[app name 1], app.[app name 2], ...}
   The graph, search summary panel, and events list are updated.
   The number of applications selected out of the number available appears in parentheses near **Applications** in the Augmented Search Pane. Also, the numbers of logs, folders, and servers are updated, to display the numbers of logs, folders, and servers that are sources of the logs containing the filtered events.

You can also manually filter search events to display only those in logs from specific applications, by typing the XpoSearch application names directly into the search query following the search text, using Simple Search syntax, and appending to it \texttt{in app.[app name 1], app.[app name 2], ...} for each application from which you want to display events.

Filtering by Server(s)

Events coming into the system can appear in logs of servers. XpoSearch enables filtering events to display only those that come from logs of specific servers.

To filter simple search results by server(s):

1. In the Augmented Search Pane, under **Isolate Results**, select **servers**.
   A table opens listing the names of the servers, the number of events coming from each server, and the percentage of events coming from each server with respect to the number of events from all the servers.
2. Select the checkboxes of the servers whose events you want to display.
The original search query is updated: the original search text is enclosed in parentheses, and to that is appended in server.[server name 1], server.[server name 2], ... The graph, search summary panel, and events list are updated. The number of servers selected out of the number available appears in parentheses near Servers in the Augmented Search Pane. Also, the numbers of logs, applications, and folders are updated, to display the numbers of logs, applications, and folders that are sources of the logs containing the filtered events.

You can also manually filter search events to display only those in logs from specific servers, by typing the XpoSearch server names directly into the search query following the search text, using Simple Search syntax, and appending to it in server.[server name 1], server.[server name 2], ...

Refining Simple Search Based On Analytics

While a Simple Search runs, Analytics discovers problematic field values in the events, color-codes them in each event, and also displays a list of these problematic field values in the Augmented Search Pane under Analytics Insight. The color-coded severity of each field value in the list appears to the left of each field value in the list.

You can run a refined search on the resulting events, by selecting a discovered problematic value, and then doing any of the following:

- Searching for events that include both the original search text and the discovered problematic field value (Append to query with AND)
- Searching for events that include either the original search text or the discovered problematic field value (Append to query with OR)
- Replacing the original search text with the discovered problematic field value (Replace query)

To refine simple search results based on Analytics:

1. In the Augmented Search Pane, under Analytics Insight, choose a field value to include in your refined search. On the bottom of the list, you can click Load more to see more discovered field values.
   A graph showing the distribution of events having the discovered field value is displayed, and below it, a menu with the following options: Append to query with AND, Append to query with OR, or Replace query.
2. From the menu, select one of the options for refining the search.
   The search query is automatically updated, and the search runs, displaying the resulting events.

Analyzing Search Results

Search queries run by XpoSearch return the following:

- A graphical presentation of matching events over time, with the ability to see the distribution of events over the multiple log sources
- A summary panel of the search results, with the ability to set the number of results per page and navigate to any page
- For a simple search – a table that summarizes the results of the complex search
- For a complex search – a table that summarizes the results of the complex search

Generating the Graphical Distribution of the Search Results

Running a search query returns a graph that shows the distribution of events over time. You can determine the display mode and contents of the graph. The graph has drill-down functionality, enabling you to zoom into any time period, and run the same search on that time period (see Zooming In/Out of a Time Period). It also enables you to hover over a bar or line graph to see the source of events and drill down to see the exact events in any log.

XpoLog Search enables you to generate a graph of the distribution of events in a bar chart (the default), line chart, or pie chart. These charts can be displayed in different visualizations, using the toolbar icons and features.

Detected problems are displayed on the time axis of the graph, enabling you to augment the search with a problem (see Augmenting a Search with Detected Problems).

Generating a Bar Chart

In a bar chart (also called a column chart), a bar appears at each point in time where events were found to match your search query. The height of each bar is according to the number of events that occurred at the specific time. A bar does not appear at times when no events matching your search query occurred.

A bar chart can be displayed in different visualizations:

- Split View – At any point in time where events were found, a vertical bar appears for each log (default) in the system that is the source of events. You can instead show the distribution of events for each application or server in the system, by selecting in the adjacent Distribute By selection box, Applications or Servers. The number of bars at a certain time is equivalent to the number of logs (or applications or servers) that were the source of events at that time.
- Stack View – At any point in time where events were found, a horizontal bar appears for each log (default) in the system that is the source of events. You can instead show the distribution of events for each application or server in the system, by selecting in the adjacent Distribute By selection box, Applications or Servers. The number of stacked bars at a certain time is equivalent to the number of logs (or applications or servers) that were the source of events at that time.
- Summary View – The default; At any point in time where events were found, a single vertical bar appears for events from all log, application, or server sources in the system.

To generate a Summary View bar chart:

- In the Graph Toolbar, on the right, click the Bar Chart button.
To generate a Split View bar chart:

- In the Graph Toolbar, on the right, click the Bar Chart button, and on the left, click the Split View button.
  Vertical color-coded bars appear parallel to each other for each log (default) in the system. You can instead show the distribution of events for each application or server in the system, by selecting in the adjacent Distribute By selection box, Applications or Servers. A legend appears on top of the graph, showing the color that represents each entity (log, application, or server).

To generate a Stack View bar chart:

- In the Graph Toolbar, on the right, click the Bar Chart button, and on the left, click the Stack View button.
  Horizontal color-coded bars appear parallel to each other for each log (default) in the system. You can instead show the distribution of events for each application or server in the system, by selecting in the adjacent Distribute By selection box, Applications or Servers. The legend appears on top of the graph, showing the color that represents each entity (log, application, or server).

Generating a Line Chart

A line chart shows how the number of events matching the search query changed from one point in time to the next.

A line chart can be displayed in different visualizations:

- **Split View** – the default: A line appears for each log (the default) defined in the system. You can instead show a single line for each application or server in the system, by selecting in the adjacent Distribute By selection box, Applications or Servers.
- **Summary View** – A single line represents all entities in the system (logs, applications, and servers) that have events.

To generate a split view line chart:

- In the Graph Toolbar, on the right, click the Line Chart button.
  An individual line is drawn to show the distribution of events in each log (default) in the system. You can instead show the distribution of events for each application or server in the system, by selecting in the adjacent Distribute By selection box, Applications or Servers. A legend appears on top of the graph, showing the color that represents each entity (log, application, or server).

To generate a summary view line chart:

- In the Graph Toolbar, on the right, click the Line Chart button, and on the left, click the Summary View button.
  A single line is drawn to show the distribution of events in the entire system.

Generating a Pie Chart

A pie chart shows the distribution of events over the applications, logs, or servers of the system.

To generate a pie chart:

- In the Graph Toolbar, on the right, click the Pie Chart button.
  The distribution of events in each log (default) in the system is illustrated in a pie, with each portion of pie shaded in the color representing the log, and in the size relative to the percentage of events. You can instead show the distribution of events for each application or server in the system, by selecting in the adjacent Distribute By selection box, Applications or Servers.

Viewing the Distribution of Results in Logs

You can hover over any bar or line in your graph to see the number of matching events that were produced by each log. You can then click any log in the chart, to view the log's events in the log viewer under the XpoLog tab. There, you can see the same information that is displayed as free text in the search result events, in column format.

Zooming In/Out of a Time Period

From the main graph or zoom-in graph (below the main graph), you can zoom into any time period, so that you can see a more detailed breakdown of events over a smaller period of time. For example, a search that runs for a time period of seven days shows the distribution of events that match the search criteria, per day. You can then zoom into any time period (day) to see the distribution of events during that day, and you can zoom in further to see the distribution of events in a specific hour on that day. The zoom-in graph highlights the zoomed-in time-period relative to the search context in the original time period of the search query.

At any point, you can zoom out to re-display the graphs resulting from the original search query.

To zoom into a time period:

1. On the time axis of the graph (either the main graph or zoom-in graph), hover on a time until a vertical line appears through the time.
2. Drag the vertical line left/right to the beginning/end of the time period.
3. Release the mouse button.
   - The selected time period is highlighted in blue.
   - The search on the zoomed-in time period runs and the results appear in the main graph.
4. You can repeatedly zoom in (steps 1 to 3) to see a more detailed distribution of events.

To zoom out:

Custom
In the graph, click the **Zoom Out** button. The original graph is displayed for the time period that you selected for the search query. At this point, the **Zoom Out** button is no longer displayed.

**Using the Search Results Summary Panel**

The Search Results Summary Panel is displayed above and below the search results area, enabling you to conveniently view a summary of the results of the search, set the number of results per page, and directly navigate to any page in the search results.

**Setting the Number of Results Per Page**

By default, a search displays 25 results per page - in the case of a simple search, 25 events per page; in the case of a complex search, 25 results per summary table. You can set the system to display a different number of results per page - either 10, 50, or 100.

To set the number of results per page:

- In the Search Results Summary Panel, in the Results Number per Page textbox, select from the dropdown list the number of results to display per page.

**Navigating to a Page of Results**

You can navigate to any page of search results directly from the Search Results Summary Panel.

To navigate to a page of search results:

1. In the Search Results Summary Panel, in the Page Selection Area, click the **Previous matching events** and **Next matching events** icons to display the previous/next page numbers, until the page number that you want comes into view.
2. Click the desired page number.
   
   The results on that page are displayed in the Search Results Area.

**Analyzing Simple Search Result Events**

Running a Simple Search displays all events that match the search query.

The following is displayed for each event:

- The timestamp of the event, i.e. the date and time that the event occurred
- The overall severity of the event, which is the severity of the highest problem found in the event (color-coded; high, medium, low, or none) (provided that Analytics is enabled)
- The fields and field values of the event
- The log, server, and applications of the event.

In each event, the text that you searched for is highlighted in yellow. In addition, provided that Analytics is enabled (the system default), the font of the searched text is colored according to its severity. Also, all field values that Analytics analyzes as being problematic, are color-coded in the event, according to their severity.

Severities are color-coded as follows:

- **Red** – high severity problem
- **Orange** – medium severity problem
- **Yellow** – low severity problem

Hovering over any event displays a menu which enables you to open the Analytics of the event, or view the event in the log viewer.

You also have the option to expand/collapse all events, or alternately, to hide/show the Analytics of all events.

**Expanding/Collapsing Events**

Events that span over more than a single line or are very long, are followed by an **Expand Events** icon.

XpoSearch enables you to view the detailed information of a single event, or to open at the click of a button, all events that have more than a single line or very long definitions. This feature makes it possible for you to expand an event to trace its cause.

To expand all events:

- In the Events toolbar, click the **Expand Events** icon.
  
  The entire event information opens. The toolbar icon changes to the **Collapse Events** icon, enabling you to later close the event information.

To expand a single event:

- At the end of an event that has an **Expand Event** icon, click the icon.
  
  The detailed information of the event opens. The icon changes to the **Collapse Event** icon, enabling you to later close the event information.

To collapse all events:

- In the Events toolbar, click the **Collapse Events** icon.
The detailed information of all events close. The toolbar icon changes to the **Expand Events** icon, enabling you to later reopen the detailed information of all the events.

To collapse a single event:

- At the end of the event that has a **Collapse Event** icon, click the icon.
  The detailed information of the event closes. The icon changes to the **Expand Event** icon, enabling you to later reopen the detailed information of the event.

**Showing/Hide Analytics of All Events**

By default, while XpoSearch searches for all events that match your search query, it also performs Analytics on all events, color-coding the searched field values according to their severity, displaying the severity of the events, and suggesting additional potentially problematic field values in the events, and color-coding them in the events. At the click of a button, you can hide Analytics results.

To hide Analytics of all events:

- In the Events toolbar, click the **Hide Analytics** icon.
  The severities of the events are not displayed, and problematic field values are not color-coded. The toolbar icon changes to the **Show Analytics** icon, allowing you to show Analytics at a later time.

To show Analytics of all events:

- In the Events toolbar, click the **Show Analytics** icon.
  The severities of the events are displayed, and problematic field values are color-coded. The toolbar icon changes to the **Hide Analytics** icon, allowing you to hide Analytics at a later time.

**Viewing the Analytics of an Event**

XpoSearch performs Analytics on all events resulting from a search, and enables you to navigate to the detailed Analytics of any event. To view the Analytics of an event:

1. Navigate to the page which contains the event whose Analytics you would like to view, and hover over the event.
   A menu appears to the right of the event.
2. In the menu, select **Analytics**.
   The Analytics page for this event opens under the Analytics tab. See XpoLog Analytics for a detailed explanation of this screen.

**Viewing an Event in the Log Viewer**

You can view the details of any event in the log viewer. The log viewer displays the same fields as those displayed in the result event, but in an organized tabular format. Also, in the log viewer you can see the events that preceded and followed the selected event, helping you understand what led to the event.

To view an event in the log viewer:

1. Navigate to the page which contains the event that you want to view in the log viewer, and hover over the event.
   A menu appears to the right of the event.
2. In the menu, select **Log Viewer**.
   A notification box opens, informing that the system is loading the log. The Popup Blocked notification box appears if popups are blocked. If so, click **Continue**.
   The Log Viewer opens under the XpoLog tab. See Log Viewer for a detailed explanation of this screen.

**Analyzing Complex Search Results**

A Complex Search generates a summary table which shows the number of events per field in the query.

Corresponding to the complex search parameters, the results summary table presents data such aggregation values, time, max, min or other values per the function executed in the complex search.

The values are clickable - click on each aggregated event in order to drill down to the relevant log records.

In order to understand the results data table it is imperative to understand the complex search, how data was filtered, what time interval the system computed and what functions and group by field were used.

**Performing a Complex Search**

Complex search queries can be run on search results for advanced computation and reporting on matching log events.

During a simple search, XpoLog extracts all the fields from the events, and displays in the Augmented Search Pane, under **Interesting Fields**, what it finds to be the most interesting fields. You can run a complex search on the results of the simple search, by clicking any of these interesting fields and selecting one of the available functions that can be performed on the field.

The results of a complex search are presented in tabular format, as opposed to the simple search, which displays each and every event that meets the search criteria.

The default complex search that is triggered by selecting a filed is based on the search query that was executed, grouping by the search results...
by the selected interesting field.
To perform a complex search:

1. In the Augmented Search Pane, under **Interesting Fields**, choose a field to include in your complex search. On the bottom of the list, you can click **Load more** to choose from other interesting fields.
   
   A menu of functions that can be performed on the field is displayed.

2. From the menu, select the function to perform on the interesting field.
   
   The search query is automatically updated, transforming the simple search to a complex search, and the search runs, displaying a result summary table.

Alternatively, you can type a complex search query into the Search Query Panel (see Complex Search Syntax Reference).

### Complex Search Examples

The following table contains examples of complex search queries:

<table>
<thead>
<tr>
<th>Query</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>`error</td>
<td>first 10`</td>
</tr>
<tr>
<td>`error</td>
<td>count</td>
</tr>
<tr>
<td>`error</td>
<td>count</td>
</tr>
<tr>
<td>`error</td>
<td>count</td>
</tr>
</tbody>
</table>
| `* in log.log4j | count | group by priority` | Runs on all events in the log **log4j** and aggregates unique values in the log field **priority**.  
   
   **Note:** A (log field named **priority**) is required. |
| `* in log.log4j log | count | group by priority | display count as Unique Count` | Same as the previous query example, with the exception that it “renames” the **count** column to **Unique Count**. |
| `* in log.access log | count | group by status` | Runs on all events in the log **access log** and aggregates unique values in the log field **status**.  
   
   **Note:** A (log field named **status**) is required. |
| `* in log.access log | count | group by url` | Runs on all events in the log **access log** and aggregates unique values in the log field **url**.  
   
   **Note:** A (log field named **url**) is required. |
| `* in log.access log | avg bytes sent | group by remote host` | Calculates the average of the log field **bytes sent** for each unique **remote host** in the log **access log**.  
   
   **Note:** Log fields with the names **bytes sent** and **remote host** are required. Also, **bytes sent** should be numeric so that the average of its values can be calculated. |
| `* in log.access log | avg bytes sent | group by remote host | display avg in volume format` | Calculates the average of the log field **bytes sent** for each unique **remote host** in the log **access log**, and formats the value of the **bytes sent** average to volume format instead of a regular numeric value.  
   
   **Note:** Log fields with the names **bytes sent** and **remote host** are required. Also, **bytes sent** should be numeric so that the average of its values can be calculated. |
| `* in log.access log | avg bytes sent | group by remote host | display avg in volume format (bytes, MB)` | Same as the previous query example, with the exception that in this example, **volume format** receives the parameters (INPUT_VOLUME_UNIT, DISPLAY_VOLUME_UNIT).  

   XpoLog treats the value in the log field **bytes sent** as bytes, and presents the result in Megabytes.  

   Available volume units: B, KB, MB, GB |
| `* in log. IIS Log Test | avg time-taken | group by c-ip | display avg in time format` | Calculates the average of the log field **time-taken** for each unique **c-ip** in the log **IIS Log Test**, and formats the value of the **time-taken** average to time format instead of displaying a regular numeric value.  
   
   **Note:** Log fields with the names **bytes sent** and **remote host** are required. Also, **bytes sent** should be numeric so that the average of its values can be calculated. |
<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>* in log. IIS Log Test</td>
<td>avg time-taken</td>
</tr>
<tr>
<td></td>
<td>Same as the previous query example, with the exception that in this example, time format receives the parameters (INPUT_TIME_UNIT, DISPLAY_TIME_UNIT). XpoLog treats the value in the log field time-taken as milliseconds, and presents the result in minutes. Available volume units: microsec, ms, sec, min, hour, day</td>
</tr>
<tr>
<td>* in log.access log</td>
<td>count, max bytes sent, min bytes sent, avg bytes sent</td>
</tr>
<tr>
<td></td>
<td>Calculates the number of occurrences, as well as the maximum, minimum, and average values of the log field bytes sent, for each unique remote host in the log access log. Note: Log fields with the names bytes sent and remote host are required. Also, bytes sent should be numeric so that the average of its values can be calculated.</td>
</tr>
<tr>
<td>error or exception</td>
<td>count</td>
</tr>
<tr>
<td></td>
<td>Counts the number of errors and exception in a log on a daily basis (i.e. the number of errors/exceptions per day).</td>
</tr>
</tbody>
</table>

**Running a Recent or Popular Search**

XpoLog saves the n most recent searches, as well as the n most popular searches. This enables you to run a recent search, without having to retype the search query.

To run a recent/popular search:

1. In the Search Query Panel, click the **Search Options** icon. A window with tabs for various search options opens.
2. Click the **Search History** tab. The searches that you have conducted recently, as well as popular searches, are listed.
3. Click the search that you want to run. The search runs and results are displayed.

**Saving a Search**

XpoSearch enables users with sufficient permission to save a search so that it can be quickly run in the future. This is a very handy feature for useful or interesting searches that you expect to run again, as it saves you the time of reformulating and retyping the search string. For a detailed explanation on how to run a saved search, see **Running a Saved Search**.

Saving a search is very quick and simple – the minimum that is required is for you to define a name for the search; the search string, which is also required, is automatically input by the system. You also have the option of defining the following:

- The time range for which the search is to be run (relative to the time that the search is initiated), such as **Last 3 days**. If the time range is not defined, the saved search runs on the time range selected in the Search Query Panel at the time that you ran the saved search.
- A description of the search.
- An indication of whether or not this search is to be included in the analysis that the Analytics engine performs on logs. A severity of **None** excludes this search from the analysis that the Analytics engine performs on logs. A severity of **Low**, **Medium**, or **High** indicates that the Analytics engine is to include this search in the analysis it performs on logs.

To save a search:

1. In the Search Query Panel, click **Save Search**.
2. The Save Search dialog box opens. The search query is automatically input into **Search Term**.
3. In **Name**, type a meaningful name for the search (mandatory).
4. In **Description**, type a description of the search (optional).
5. In **Time Range**, select from the dropdown list the period of time relative to the current date that the search is to be conducted (optional). Leave blank to XpoSearch to run the saved search on the time range that is displayed in the Search Query Panel at the time that the saved search runs.
6. In **Severity**, select from the dropdown list a severity of **Low**, **Medium**, or **High** if you want the Analytics engine to include this search in the analysis it performs on logs. Otherwise, leave the severity at **None**, to exclude this search from the analysis that the Analytics engine performs on logs.
7. Click **Save**. The search is saved.

**Deleting a Saved Search**

You can delete at any time a search that you previously saved.

To delete a saved search:
In the Main Menu, select **Administration**, and in the sub-menu that appears, select **Saved Searches**.

A list of saved searches is displayed.

2. Select the search to delete, and click the **Delete** button.
   A Delete Confirmation box is displayed.
3. Click **Yes** to confirm deletion.
   The search is deleted, and no longer appears in the list of saved searches.

**Editing a Saved Search**

You can edit at any time the name, search query, time period, or description of a previously saved search.

To edit a saved search:

1. In the Main Menu, select **Administration**, and in the sub-menu that appears, select **Saved Searches**.
   A list of saved searches is displayed.
2. Select the search to edit, and click the **Edit** button.
   The Save Search dialog box is displayed.
3. Modify the definition of the search, as required (see **Saving a Search**), and then click **Save**.
   The modifications to the saved search are saved.

**Running a Saved Search**

You can run searches that have previously been saved by simply opening up a list of saved searches and clicking the one that you want to run. Alternately, if you know the name of the saved search, in the search query, you can type `search` followed by the search name.

**Method 1**

To run a saved search:

1. In the Search Query Panel, click the **Search Options** icon.
   A window with tabs for various search options opens.
2. Click the **Saved Searches** tab.
   The searches that you have saved in the past are listed.
3. In the **Saved Searches** list, click the search to run.
   The search is run and results are displayed.

**Method 2**

To run a saved search:

- In the Search Query Panel, type `search.search_name`.
  The search is run and results are displayed.

**Note:** As you begin typing "search", a dropdown list with the names of all saved searches opens. Typing more characters of the saved search name narrows down the list. You can either complete typing the name, or at any point, select the desired saved search name.

**Saving a Search as a Gadget**

XpoLog Search enables users with sufficient permission to save any search as a gadget.

Saving a search as a gadget requires you to define:

- A name for the gadget
- The view of the gadget – chart or table
- The dashboard under which the gadget is to be placed – an existing or new dashboard
- The app under which the dashboard is to be placed - an existing or new app

The search string and time period of the search are automatically input by the system from the search query of the Search being saved. You can change the time period to have the gadget run the search on events from a different range of time.

**To save a search as a gadget:**

1. In the Search Query Panel, click **Save Gadgets**.
2. The Save Gadget dialog box opens. The search query is automatically input into **Search Query**.
3. In **Gadget Title**, type a meaningful name for the gadget (mandatory).
4. In **Time Range**, leave the time range of the search that ran (default), or select a different time range.
5. In **Gadget View**, select **Chart** or **Table**.
6. In **App**, select one of the following:
   - **Existing** – to place the gadget in an existing app. In the adjacent drop-down list, select the name of the app.
   - **New** – to place the gadget in a new app. In the adjacent box, type the name of the new app.
7. In **Dashboard**, select one of the following:
   - **Existing** – to place the gadget in an existing dashboard. In the adjacent drop-down list, select the name of the dashboard.
   - **New** – to place the gadget in a new dashboard. In the adjacent box, type the name of the new dashboard.
8. Do one of the following:
   - Click **Save**.
The Gadget is saved. The Search is displayed.
- Click **Save and View Dashboard.**
  The Gadget is saved, and the dashboard under which it has been saved, is opened.

### Saving a Search as a Monitor

XpoLog Search enables users with sufficient permission to save any search as a monitor so that it is run automatically by the system at scheduled intervals. Also, the results of the monitor are automatically sent to the emails of recipients that you specify. This saves users the time that it takes to set up the search and send the results to recipients.

Saving a search as a monitor is very quick and simple – the minimum that is required is for you to define a name for the monitor; the search string, which is also required, is automatically input by the system. You also have the option of defining the following:

- The frequency at which the monitor is to be run. This should not be specified, if you want to manually run the monitor.
- The emails of recipients to whom the system should automatically send alerts resulting from the monitor.

To save a search as a monitor:

1. In the Search Query Panel, click **Save Monitor.**
2. The Save Monitor dialog box opens. The search query is automatically input into **Search Query.**
3. In **Name**, type a meaningful name for the search (mandatory).
4. In **Schedule**, do one of the following:
   - Leave blank if you intend to run the monitor manually.
   - Select the frequency at which the system should automatically run the monitor: Select from the dropdown list the unit of time (**Seconds, Minutes, or Hours**) and type the number of units.
5. In **Email**, type the email addresses to which to send alerts. Separate email addresses with a comma.
6. Click **Save.**
  The monitor is saved.

### Exporting a Search to a PDF

You can save search results in a PDF file for later reference.

To export a search to a PDF: In the Search Query Panel, click **Export to PDF.** Notification appears informing you that the PDF is being generated. Then, the PDF of the search results is opened.

**Note:** If pop-ups are blocked, the system sends you a notification. In this case, click **Continue** in the notification message to open the PDF.

### Exporting a Search to a CSV

You can save search results in a CSV file for later reference.

To export a search to a CSV: In the Search Query Panel, click **Export to CSV.** Notification appears informing you that the CSV is being generated. Then, the CSV of the search results is opened.

**Note:** If pop-ups are blocked, the system sends you a notification. In this case, click **Continue** in the notification message to open the CSV.

### Complex Search Syntax Reference

A complex search is used to perform one or more complex operations on simple search results, so that search results can be summarized in a table for convenient analysis, according to criteria that you choose. The basis of the complex search structure is the pipe character (**|**), which indicates to XpoSearch to input the results of the search preceding the pipe to the complex search following the pipe.

The general syntax of a complex search is as follows:

```
search query | [function | [group] | [view]] ([function | [group] | [view]])...
```

where,

- **search query** – a simple search
- **function** – an operation that is applied on the results of the search preceding the pipe. Available functions: **count, min, max, avg, sum, time, start time, end time, country, country code, city, region, execute**
- **group** – grouping of results by a specific group type, such as columns, logs, servers, files, or applications. Available Group operations: **group by, interval**
- **view** – specifies how to display the results. Available View operations: **first, last, order by, display, where, display only, geoip, asc, desc, display first 10**
  - Grouping can only be according to a single group type. However, the group type can have a single or multiple variables.
  - A function must precede grouping, although it does not necessarily have to immediately precede it – **view** can come between the **function** and **group command**.
  - There can be multiple View types.
  - The Complex Search Syntax is iterative.

In the following example, there is one function (count), one grouping (group by) by two variables (event, user), and three views (order by ...
This chapter provides you with a reference to all the search commands available for your use in a complex search, including their syntax, description, and examples of use. You can also build complex search queries using a combination of these search commands. Complex search queries that run in the XpoSearch console, can be visualized as gadgets in XpoLog Dashboards.

Use case examples of such commands are provided in Complex Search Examples.

**avg**

**Synopsis**
Calculates the average of the values in a specified column of the search query results.

**Syntax**
avg [column_name]

**Required Arguments**
column_name

**Description:**
The name of a column header that has numeric values

**Optional Arguments**
None

**Description**
For each event in the search query results that has the specified column_name with a numeric value, adds the value to the cumulative sum, and when it has reached the last event, divides the cumulative sum by the number of events to get the average.

**Examples**

Example 1:
* in log.access | avg Bytes Sent

From the events in access log, returns the average of the values in column Bytes Sent.

Example 2:
http in log.iis log | avg time-taken | group by sc-status

From the events in log.iis log that contain http in their column values, returns the average of the values in column time-taken, grouped according to the value of the sc-status column.

**avgif**

**Synopsis**
Calculates the average of the values in a specified column of the search query results based on a query to be executed on the record.

**Syntax**
avgif [column_name] ”[search_query]”

**Required Arguments**
column_name

**Syntax:**
<character string>

**Description:**
The name of a column header that has numeric values
search_query

Syntax: <character string>

Description: The search query to be executed on the record

Optional Arguments

None

Description

For each event in the search query results that has the specified column_name with a numeric value, adds the value to the cumulative sum, and when it has reached the last event, divides the cumulative sum by the number of events to get the average.

Examples

Example 1:

* in log.access | avgif Bytes Sent *status=200*

From the events in access log, returns the average of the values in column Bytes Sent only if the value of column status is 200.

Example 2:

* in log.iis log | avgif time-taken "cs-host contains http" | group by sc-status

From the events in log.iis log that contain http in their cs-host column, returns the average of the values in column time-taken, grouped according to the value of the sc-status column.

city

Synopsis

Displays the city names extracted from the IP address column in the search result events.

Syntax

city [IP_address_column_name]

Required Arguments

IP_address_column_name

Syntax: <character string>

Description: The name of the column header that has IP address values.

Optional Arguments

None

Description

For each event that has the specified IP_address_column_name with an IP address value, extracts the city name from the IP address, using an internal database.

Examples

Example 1:

* log.access | city IPAddress1

For each event in log access, extracts the city name from the IP address in column IPAddress1.

count

Synopsis

A function that counts the number of search result events.

Syntax
count

Required Arguments
None

Optional Arguments
None

Description
When used following the initial simple search query, returns the number of events resulting from the search. When used iteratively, counts the number of results returned from the complex search preceding the pipe.

Examples
Example 1:
```plaintext
* in log.access | count
```
Returns the number of events in log access.

Example 2:
```plaintext
* in log.application | count | group by event | order by count desc
```
Returns the number of each event in the log application in a descending order

Example 3:
```plaintext
* in log.access | count | group by remote host | interval 15 minutes | count | interval 15 minutes |
display count as number of users
```
Returns the distinct number of users in 15 minutes intervals in the log access

countif

Synopsis
A function that counts the number of search result events based on a query to be executed on the record.

Syntax
```plaintext
countif "[search_query]"
```

Required Arguments
search_query

Syntax: <character string>

Description: The search query to be executed on the record

Optional Arguments
None

Description
When used following the initial simple search query, returns the number of events resulting from the search. When used iteratively, counts the number of results returned from the complex search preceding the pipe.

Examples
Example 1:
```plaintext
* in log.access | countif status=200
```
Returns the number of events containing status 200 in log access.

Example 2:
* in log.application | countif message contains error | group by event | order by countif desc

Returns the number of each event containing error in the log application in a descending order.

country

**Synopsis**

Displays the country names extracted from the IP address column in the search result events.

**Syntax**

`country` [IP_address_column_name]

**Required Arguments**

IP_address_column_name

**Syntax:** <character string>

**Description:** The name of the column header that has IP address values.

**Optional Arguments**

None

**Description**

For each event that has the specified IP_address_column_name with an IP address value, extracts the country name from the IP address, using an internal database.

**Examples**

**Example 1:**

* log.access | country IPAddress1

For each event in log access, extracts the country name from the IP address in column IPAddress1.

country code

**Synopsis**

Displays the country codes extracted from the IP address column in the search result events.

**Syntax**

`country code` [IP_address_column_name]

**Required Arguments**

IP_address_column_name

**Syntax:** <character string>

**Description:** The name of the column header that has IP address values.

**Optional Arguments**

None

**Description**

For each event that has the specified IP_address_column_name with an IP address value, extracts the country code from the IP address, using an internal database.

**Examples**

**Example 1:**

* log.access | country code IPAddress1
For each event in log access, extracts the country code from the IP address in column IPAddress1.

display

Synopsis

Changes the display names, formats, and/or time units of column(s) in the summary table resulting from the complex search(es) preceding the pipe character.

Syntax

display [Result_Column_Name] (as [New _Column_Name]) (in [Format_Type] format)("Input_Unit"),("Output_Unit") , [RESULT_COLUMN_NAME] (as [NEW_COLUMN_NAME] )...

Required Arguments

Result_Column_Name

Syntax: <character string>

Description: The name of the column header in the summary table resulting from the complex search, whose name, format, or output unit you want to change.

Optional Arguments

New_Column_Name

Syntax: <character string>

Description: The new display name of the column header in the summary table.

Format_Type

Syntax: number, simple, time, date, volume, regexp, or expression

Description: The display format of the column header values in the summary table. See format.

Description

This function is used to change the display mode of any of the column names and/or values in the summary table resulting from the Complex Search, by:

- Changing the column name to a new column name.
- Displaying the column values in a specified format.
- Displaying the column values in a specified output unit.
- Assuming that the input unit of the column values is the specified unit, and converting it to the specified output unit.

The display of several columns in the summary table of a complex search can be changed by placing them in a comma-separated list.

Note: in case the same function is applied on different fields it is possible to set the display in the function activation area itself in the query by specifying FUNCTION COLUMN_NAME AS DISPLAY_NAME. See example 3.

Examples

Example 1:

* in log.access | count , avg Bytes Sent | group by url | display avg as Average Bytes in volume format

For each URL in the access log events, show the number of log events and the average of the Bytes Sent column. In the table, replaces the avg header with Average Bytes, and shows the values in volume format in Bytes (default).

Example 2:

* in log.access | avg time taken | display avg in time format(“SEC”,“MIN”)  

In the access log events, calculates the average of the time taken column values, assumes that the input value is in seconds, and converts and displays it in minutes.

Example 3:

* in log.access | avg time taken as Average Time Taken, avg Bytes Sent as Average Bytes Sent

In the access log events, calculates the average of the time taken and bytes sent columns values, settings a result column name to each one in the function definition level.
**Synopsis**

Specifies the names of the column names resulting from the complex search that are to be displayed in the summary table, and optionally defines new display names, formats, and/or time units for these column name(s) in the summary table.

**Syntax**

```
display only [Result_Column_Name] (as [New_Column_Name]) (in [Format_Type]) ("Input_Unit"),("Output_Unit") (, [RESULT_COLUMN_NAME] (as [NEW_COLUMN_NAME] )...)
```

**Required Arguments**

**Result_Column_Name**

*Syntax:* &lt;character string&gt;

*Description:* The column names resulting from the complex search that you want to include in the displayed summary table.

**Optional Arguments**

**New_Column_Name**

*Syntax:* &lt;character string&gt;

*Description:* The new display name of the column header in the summary table.

**Format_Type**

*Syntax:* number, simple, time, date, volume, regexp, or expression

*Description:* The display format of the column header values in the summary table. See format.

**Description**

You may not be interested to display all the columns in a summary table that results from a complex search. Using `display only`, you can specify the column names that are to appear in the summary table, placing them in a comma-separated list.

This function can also be used to change the display mode of any of these column names and/or values, by:

- Changing the column name to a new column name.
- Displaying the column values in a specified format.
- Displaying the column values in a specified output unit.
- Assuming that the input unit of the column values is the specified unit, and converting it to the specified output unit.

**Examples**

**Example 1:**

```
* in log.access | count , avg Bytes Sent | group by url | display only avg as Average Bytes in volume format
```

For each URL in the `access` log events, calculates the number of log events and the average of the `Bytes Sent` column. In the resulting table, only shows the `avg` column, replacing the `avg` header with `Average Bytes`, and shows the values in volume format in Bytes (default).

**Example 2:**

```
* in log.access | avg time taken | display only avg in time format("SEC","MIN")
```

In the `access` log events, calculates the average of the `time taken` column values. In the resulting table, only shows the `avg` column, and assumes that the input value is in seconds, and converts and displays it in minutes.
Displays the distribution over time of all values under the specified column(s) as appear in the log(s).

**Syntax**

dist [column_name]

**Required Arguments**

column_name

Syntax: <character string>

Description: The name of a column header that its values should be listed

**Optional Arguments**

None

**Description**

Displays the distribution over time of all values under the specified column(s) as appear in the log(s)

**Examples**

**Example 1:**

* in log.application | dist event

Returns a distribution over time of all values under the Event in the log Application

**Example 2:**

* in log.application | dist event, type

Returns a distribution over time of all values under the columns Event and Type in the log Application

**Synopsis**

Displays the time of the last event in the group.

**Syntax**

der time

**Required Arguments**

None

**Optional Arguments**

None

**Description**

Shows the unformatted time of the last event in the group resulting from the search query. Should be formatted and displayed in date format.

**Examples**

**Example 1:**

* in log.access | end time | display end time in date format

Finds the time of the last event in log access, and in the summary table, displays this time in date format under the end time column.
Synopsis

Executes a custom complex computation on search query results.

Syntax

execute [expression] (as result1, result2)

Required Arguments

expression

Syntax: mathematical expression

Description: Performs on the search results, a mathematical expression that the user formulates using the execute search syntax.

Optional Arguments

result1, result2

Syntax: <search string>.

Description: If the results that the executed expression returns are expected to go into more than one column, the names of the columns preceded by as must be placed in parentheses following the expression.

Description

Executes on each event in the search query, an expression. If the returned results go into more than one column, they are entered under the columns whose names appear in parentheses after the expression.

Examples

Example 1:

* in log.access | execute if (total == NULL) THEN (total = 0); if (column.bytes\sent != NULL && column.bytes\sent != ";") THEN (total = total + column.bytes\sent);total | group by status | order by value desc

Computes the total of the bytes sent column of the events in log access per status, and displays the total of each status in descending order of the total value.

Example 2:

* in log.application_log | count, sum col_name | interval 1 hour | execute result = column.count * 100 / column.sum ; result | interval 1 hour

Computes the sum of a value in the field col_name in an hourly basis, and computes the percentage of that value out of the total number of events during that time.

Example 3:

* in log.iis log | avg time-taken | group by cs-uristem | execute if (count1 == NULL) THEN (count1 = 0);if (count2 == NULL) THEN (count2 = 0);if (count3 == NULL) THEN (count3 = 0);timetaken = column.avg; if (timetaken > 100 && timetaken < 300) THEN (count1 = count1 + 1);if (timetaken >= 300 && timetaken < 400) THEN (count2 = count2 + 1);if (timetaken >= 400 && timetaken < 500) THEN (count3 = count3 + 1);map = mapput(map,"100",count1);map = mapput(map,"300",count2);map = mapput(map,"400",count3);map as type,value | order by type

Computes the different type of URLs that their average time took between 100-300, 300-400 and 400-500 milliseconds based on the time-taken log field.

Example 4:

* in log.process | avg memory | interval 10 minutes | execute MB = column.Avg; if (result == NULL) then (result=""); diff=0; if (previous != NULL && (MB - previous) > 100) then (diff = MB - previous); map = mapput(map,"\n",previous);key=""; if (diff < 0) then (key = previousTime + ";" + column.time + ";" + format(previous) + ";" + format(MB)); if (diff > 0) then (result = mapput(result, key, format(diff))); previous = MB; previousTime= column.time; result as Start of Time Slot, End of Time Slot , Min Memory, Max Memory, Memory Difference
Computes the difference of an average value in more than 100 units in a 10 minutes time slot - for example increase of more than 100 MB in memory in less than 10 minutes based on performance log.

Example 5:

* in log.LOG_NAME | execute if (total == NULL) then (total = 0); if (count == NULL) then (count = 0); if (column.COLUMN_NAME == COLUMN_VALUE) then (count = count + 1); total = total + 1; (count/total)*100

Computes the percentages of the value COLUMN_VALUE in the log column COLUMN_NAME out of all events in the log LOG_NAME

- Same query with 10% (for example) threshold for monitoring. I.E. if the value COLUMN_VALUE in the log column COLUMN_NAME out of all events in the log LOG_NAME is greater than 10% it will return a result:

* in log.LOG_NAME | execute if (total == NULL) then (total = 0); if (count == NULL) then (count = 0); if (column.COLUMN_NAME == COLUMN_VALUE) then (count = count + 1); total = total + 1; (count/total)*100 | where value > 10

**execute search syntax**

**Custom Operators**

<table>
<thead>
<tr>
<th>Type</th>
<th>Operator</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numerical Operators</td>
<td>+, -, *, /: basic operators</td>
<td>(-1 + 50*2) / (2^4)</td>
</tr>
<tr>
<td></td>
<td>%: Modulo operator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>^: Power operator</td>
<td></td>
</tr>
<tr>
<td>Boolean operators</td>
<td>~, xor: operators</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&amp;&amp;, or: And operators</td>
<td></td>
</tr>
<tr>
<td></td>
<td>!, !: Or operators</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;, &lt;=: less or equal operator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&gt;, &gt;=: greater operator</td>
<td></td>
</tr>
<tr>
<td>String operators</td>
<td>==: 2 strings equals</td>
<td>&quot;string1&quot; == &quot;string2&quot;: false</td>
</tr>
<tr>
<td></td>
<td>!=: 2 strings not equals</td>
<td>&quot;string1&quot; + &quot;a&quot;: &quot;string1a&quot;</td>
</tr>
<tr>
<td></td>
<td>&lt;: The first string less lexically than the second one</td>
<td>&quot;abc&quot; &gt; &quot;aaa&quot;: true</td>
</tr>
<tr>
<td></td>
<td>&gt;: The first string great lexically than the second one</td>
<td>&quot;2yx&quot; &lt; &quot;bcd&quot;: false</td>
</tr>
<tr>
<td></td>
<td>&lt;=: The first string less or equals lexically than the second one</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&gt;=: The first string great or equals lexically than the second one</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+: Concat string</td>
<td></td>
</tr>
<tr>
<td>List operators</td>
<td>+: Concat two lists</td>
<td>(1,2)+(3,4) = (1,2,3,4)</td>
</tr>
<tr>
<td></td>
<td>-: Subtract a list to another one</td>
<td>(1,2) + 3 = (1,2,3)</td>
</tr>
<tr>
<td></td>
<td>in: Test if an element is inside a list</td>
<td>3+(1,2)=(1,2,3)</td>
</tr>
<tr>
<td>Other operators</td>
<td>=: set a variable operator</td>
<td>(1,2,3,4)-(3,4)=(1,2,4)</td>
</tr>
<tr>
<td></td>
<td>[]: absolute value</td>
<td>(1,2,3,4)-3=(1,2,4)</td>
</tr>
<tr>
<td></td>
<td>²: power 2 operator</td>
<td>2 in (1,2,3)=true</td>
</tr>
<tr>
<td></td>
<td>%: Percent operators</td>
<td>4 in (1,2,3)=false</td>
</tr>
</tbody>
</table>

2^10% = 0.1
### Conditional operators

<table>
<thead>
<tr>
<th>Condition</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>if then</td>
<td>if ( A &gt; 2 ) then (&quot;Ok&quot;)</td>
</tr>
<tr>
<td>if then else</td>
<td>if ( A &lt;=2 ) THEN (B=3) else (B=4)</td>
</tr>
</tbody>
</table>

### Custom functions

**Custom Functions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Function signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>format</td>
<td>Formats decimal number. Default format is &quot;#.##.&quot;</td>
<td>format (n) returns the decimal number n in the format &quot;#.##.&quot;</td>
</tr>
<tr>
<td>number</td>
<td>Parses string to number (double).</td>
<td>number (s) parses the string v as a double.</td>
</tr>
<tr>
<td>timeformat</td>
<td>Formats a number as date/time string. Default time format is &quot;MM/dd/yyyy HH:mm:ss.SSS&quot;.</td>
<td>timeformat (n,f) formats the double value n to the date/string f</td>
</tr>
<tr>
<td>mapput</td>
<td>Puts a key/value pair in a map. If the given map was not declared prior to this function, then this function creates it. Note: the function returns the result map.</td>
<td>mapput (m,k,v) returns the new map m after putting the value v using the key k.  mapput(m,m2) - Returns the new map m after putting the map m2 in it.</td>
</tr>
<tr>
<td>mapget</td>
<td>Returns a value from a map using a key.</td>
<td>mapget (m,k) returns the value in m to which the key k is mapped.</td>
</tr>
<tr>
<td>mapkeys</td>
<td>Returns all the map's keys.</td>
<td>mapkeys (m) returns all the keys of map m.</td>
</tr>
<tr>
<td>mapvalues</td>
<td>Returns all the map's values.</td>
<td>mapvalues (m) returns all the values of map m.</td>
</tr>
<tr>
<td>mapremove</td>
<td>Removes a mapping from a map using a key</td>
<td>mapremove (m,k) removes from the map m the mapping for key k, if present.</td>
</tr>
<tr>
<td>listget</td>
<td>Returns the element in a list at a specified position</td>
<td>listget (l,i) returns the element at position i in list l.</td>
</tr>
</tbody>
</table>

### Custom Aggregation Functions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Function Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggAvg</td>
<td>returns the aggregated average value of a parameter.</td>
<td>aggAvg (p) returns the aggregated average value of given parameter p.</td>
</tr>
<tr>
<td>aggSum</td>
<td>returns the aggregated sum value of a parameter.</td>
<td>aggSum (p) returns the aggregated sum value of given parameter p.</td>
</tr>
<tr>
<td>aggMax</td>
<td>returns the aggregated max value of a parameter.</td>
<td>aggMax (p) returns the aggregated max value of given parameter p.</td>
</tr>
<tr>
<td>aggMin</td>
<td>returns the aggregated min value of a parameter.</td>
<td>aggMin (p) returns the aggregated min value of given parameter p.</td>
</tr>
<tr>
<td>mapAggAvg</td>
<td>returns aggregated avg map for given key k.</td>
<td>mapAggAvg (k,v) returns map that each value v is aggregated avg result</td>
</tr>
<tr>
<td>mapAggSum</td>
<td>returns aggregated sum map for given key k.</td>
<td>mapAggSum (k,v) returns map that each value v is aggregated sum result</td>
</tr>
</tbody>
</table>

### Custom Basic Functions

- **random** - A random value from 0 to 1.
- **strlen** - Compute the length of a string.
- **sqrt** - Square root.

first

**Synopsis**

Used to display the first specified number of events resulting from a Simple Search, or the first specified number of summary table entries resulting from a Complex Search.

**Syntax**

`first [number_of_results] for each [group]`

**Required Arguments**

`number_of_results`

Syntax: `<numeric>`

Description: The number of first search results to display

**Optional Arguments**

`for each <column name>`

Syntax: `for each <column name>`

Description: The column name on which the first specific number should display.

**Description**

When used immediately following a Simple Search query, returns the specified number of first events resulting from the search. When used immediately following a Complex Search query, returns the specified number of first entries from the summary table resulting from the search.

**Examples**

**Example 1:**

`* in log.access | first 32`

Returns the first 32 events from access log.

**Example 2:**

`http in log.iis log| max time-taken | group by c-ip | first 21`

Returns the max time-taken value from events in log.iis log having http in their column values, for the first 21 c-ip values only.

**Example 3:**
error in log.xpologlog | count | group by class, method | first 2 for each class

Returns the 2 methods that appeared most in each class in log.xpologlog log having error in their column values.

Example 4:

error in log.xpologlog | count | group by message | interval 1 hour | first 2 for each interval

Returns the 2 messages that appeared most in each 1-hour interval in log.xpologlog log having error in their column values.

Synopsis

Displays a specified column in the complex search summary table in a specified format. Can be used only with Display, Display only, and Group by commands.

Syntax

in [format_type] format)(["Input_Unit"],)(["Output_Unit"])

Required Arguments

format_type

Syntax: number, simple, time, date, volume, regexp, expression or query

Description: The format in which to display the values of a specific column in the complex search summary table. For a time format_type, if no unit appears after time format, XpoLog assumes that the column value is in milliseconds and displays it in the maximal possible unit (for example, if the value is 2000, the output is 2 seconds; if the value is 120000, the output is 2 minutes, etc.).

Optional Arguments

"Input_Unit"

Syntax: Volume Units - B, KB, MB, GB; Time Units: microsec, ms, sec, min, hour, day

Description: The input unit of the format type.

"Output_Unit"

Syntax: Volume Units - B, KB, MB, GB; Time Units: microsec, ms, sec, min, hour, day

Description: The unit in which to convert the format type.

Note: If only one unit appears in the syntax, XpoLog assumes that it is the output unit, and that the input value is in milliseconds (for time) or bytes (for volume). If no unit appears in the syntax, XpoLog outputs the log value in milliseconds (for time) or bytes (for volume).

Description

Displays the column values in the specified format, assuming the default input and output units, if they are not specified, and converting to a specific output unit from a specific input unit, if specified.

Text can be formatted into the following format types:

- **number** – formats the text in the column to number format; ("#.##") – the decimal format of the number
- **simple** – displays columns in difference format: ("column.name1 – column.name2") – replace the columns with the values from the result
- **time** – displays the value in a time format of the default unit or of the indicated ("[OUTPUT_UNIT]", "[INPUT_UNIT]") – displays the column in output format and uses the input unit In case it is different from milliseconds.
  Time units: [microsec,ms,sec,min,hour,day]
- **date** – displays the value in day format: ("[SIMPLE DATE FORMAT]") – change the date format
- **volume** – displays the value in volume format way: ("[OUTPUT_UNIT]", "[INPUT_UNIT]", "[OUTPUT_UNIT]") – display the column in output format and use input unit in case it is different from bytes.
  Volume units: [B,KB,MB,GB]
- **regexp** – use regexp to extract values from the data: ("[REGEXP]") – display the first group that is found from the regular expression
- **expression** – displays the column result after performing an expression on the original contents.
  Display Column_Name in regexp format("REGEXP"), where REGEXP is the regular expression to be executed on the value in Column_Name ("[EXPRESSION]") – use an expression to calculate different result value
- **query** - displays an aggregated result broke into groups based on search queries constraints.
  ...group by FIELD_NAME in query format
  ("SEARCH_QUERY_1","RESULT_NAME_2","SEARCH_QUERY_2","RESULT_NAME_3",...,"SEARCH_QUERY_N","RESULT_NAME_N")
  It is possible to use "*" at the end as a query to group the undefined results of the other queries:
  status != NULL in log.access | count | group by status in query format ("status=200","VALID","*","ALL_THE_REST")
• **exception** - displays an aggregated result broke into groups based on number of lines in the stack trace.
  ...group by FIELD_NAME in exception format ("NUMBER_OF_LINES","SHOW_MESSAGE")

  error in log.log4j log | count | group by message in exception format ("1","true")

• **replace** – use replace to replace a value from the data with a custom value.

  ...group by FIELD_NAME in replace format
  ("REGEXP_1","REPLACE_TEXT_1","REGEXP_2","REPLACE_TEXT_2",...,"REGEXP_N","REPLACE_TEXT_N")

  status != NULL in log.access | count | group by status in replace format ("200","OK","302","Resource temporarily moved to a new location","304","Not Modified")

• **UserAgentDetect** – displays an aggregated result broke into groups based on types to view (browser,version,platform,os).

  ...group by FIELD_NAME in UserAgentDetect format ("TYPE_1+....+TYPE_N")

  status != NULL in log.Access Log | count | group by user agent in userAgentDetect format ("browser+version")

**Examples – Volume Format: bytes sent** column contains numeric values representing volume.

**Example 1:**

* in log.access | avg bytes sent | display avg in volume format

XpoLog formats **avg of bytes sent** in volume format, automatically assuming that the log value is in bytes.

**Example 2:**

* in log.access | avg bytes sent | display avg in volume format("MB")

XpoLog formats **avg of bytes sent** in volume format, automatically assuming that the log value is in bytes, and converts and outputs the value in MB.

**Example 3:**

* in log.access | avg bytes sent | display avg in volume format("KB","MB")

XpoLog formats **avg of bytes sent** in volume format, assuming that the log value is in KB, and converts and outputs the value in MB.

**Examples – Time Format: time taken** column contains numeric value representing time.

**Example 1:**

* in log.access | avg time taken | display avg in time format

XpoLog formats **avg of time taken** in time format, automatically assuming that the log value is in milliseconds.

**Example 2:**

* in log.access | avg time taken | display avg in time format("SEC") à format to seconds

XpoLog formats **avg of time taken** in time format, automatically assuming that the log value is in milliseconds, and converts and outputs the value in seconds.

**Example 3:**

* in log.access | avg time taken | display avg in time format("SEC","MIN") à format from seconds to minutes

XpoLog formats **avg of time taken** in time format, assuming that the log value is in seconds, and converts and outputs the value to minutes.

**Regular Expressions:**

1. XpoLog groups by URL field which has multiple parts divided by slashes / and then uses a regular expression to format the result to present only part of the URL based on the regular expression criteria, I.E. present only the last part after the last slash / in the URL:

   **URL Example:**
   [URL] /home/web-main/css/texts.css

   **XpoLog Query:**
   * in log.access log | count | group by url as formatted-url | order by count desc | display formatted-url in regexp format (".*([^/]+)")

   **Result:**
2. XpoLog uses a regular expression to format the Description field which contains multiple lines with different values based on the regular expression criteria, I.E. extract from the entire Description field only the value which comes after 'Account Name:' and group by it only (as if it was a pre-configured field in the log):

**Description Example:**

...[Description] An account was logged off.

Subject:

Security ID: S-1-5-21-3480273402-748593870-3636473903-1144
Account Name: xplg
Account Domain: XPOLOG
Logon ID: 0xa078ea24
Logon Type: 3

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

**XpoLog Query:**

(*) in log.application | count | group by Description as UserName in regexp format ("Account Name:\s+\w+")

**Result:**

<table>
<thead>
<tr>
<th>UserName</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBSMonAcct</td>
<td>116</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>438</td>
</tr>
<tr>
<td>xplg</td>
<td>165</td>
</tr>
<tr>
<td>XPOLOGDOMAIN</td>
<td>322</td>
</tr>
</tbody>
</table>

**Query Format:**

1. XpoLog groups by STATUS which has multiple values, and then based on query criteria it breaks the result to different pieces: Status values may vary from 200, 302, 404, 500, etc. but in order to break it into two groups 200 - defined as valid and not 200 as not valid the query format handles it:

**XpoLog Query:**

* in log.access | count | group by status in query format ("status=200","VALID","status != 200","NOT VALID")

**Result:**
**Synopsis**

A display function that groups result events according to the extracted elements of the IP address in one or more of its geoip columns.

**Syntax**

```
geoip ([IP_Column_Name]) group by [country,country code,city,region]
```

**Required Arguments**

- **IP_column_name**
  
  **Syntax:** `<character string>`
  
  **Description:** The name of the column header that has IP address values.
  
  country, country code, city, and/or region

**Optional Arguments**

None

**Description**

For each event that has the specified `IP_address_column_name` with an IP address value, extracts the country name, country code, city, and/or region from the IP address, using an internal database, and then shows the result of performing a specific function on the search result events, according to the country name, country code, city, and/or region, as required.

**Examples**

**Example 1:**

```
* in log.access | count | geoip client ip group by country,city | order by count desc
```

Creates a summary table of the count of all events in `log access`, grouped according to the country and the city within the country, both extracted from the IP address in the `client ip` column. This table is ordered in descending order of the number of events in each city group.

**Synopsis**

Groups events according to column values.
Syntax

`group by [column_name] in [Format_Type] format{{"Input_Unit"}},{{"Output_Unit"}}, {, [column_name] ...}`

**Required Arguments**

*column_name*

**Syntax:** `<character string>`

**Description:** The name of the column header according to which events are to be grouped.

**Optional Arguments**

*column_name*

**Syntax:** `<character string>`

**Description:** The name of additional column headers according to which events are to be sub-grouped. Column names should be comma separated.

*Format_Type*

**Syntax:** `number, simple, time, date, volume, regexp, expression, query, exception, replace, or userAgentDetect`

**Description:** The display format of the column header values in the summary table. See `format`.

**Description**

Creates a summary table that categorizes events according to their grouping. Must be preceded by a function.

**Examples**

**Example 1:**

```
* in log.access | count | group by url
```

Returns the number of events from each URL.

**Synopsis**

Classifies the search query result events into time buckets of the specified time period.

**Syntax**

`interval N [milliseconds, seconds, minutes, days, weeks, months] starting TIME`

**Required Arguments**

*N*

**Syntax:** `<numeric value>`

**Description:** The number of units of time into which to classify the search query result events

**Unit of time**

**Syntax:** `milliseconds, seconds, minutes, days, weeks, months`

**Description:** The unit of time into which to classify the search query result events

**Optional Arguments**

*starting TIME*

**Syntax:** `<start time>`

**Description:** The start time of the interval

**Description**

Classifies the search query results according to time period. Must be preceded by a function.

**Examples**
Example 1:

* in log.access | count | interval 1 day

From the events in access log, shows the number of events per day starting at 00:00:00.

Example 2:

* in log.access | count | interval 1 day starting 08:00:00

From the events in access log, shows the number of events per day starting at 08:00:00.

Example 3:

* in log.memoryUsage | avg usage | interval 50 milliseconds

From the events in memoryUsage log, shows the average of used memory (usage) in 50 milliseconds interval.

Synopsis

Filters (i.e. narrows) the search results based on a time range.

Syntax

TIME_UNIT is START_TIME-END_TIME

Required Arguments

TIME_UNIT

Syntax: time, hour, minute, second, day of week, or day of month

Description: The time unit of the time range

START_TIME

Syntax: <start time>

Description: The start time of the time range

END_TIME

Syntax: <end time>

Description: The end time of the time range

Optional Arguments

None

Description

Filters the search results based on a specific time range. The "time is" search query can be built only by using the simple search syntax (see Performing a Simple Search)

Examples

Example 1:

time is 8-16 in log.access

From the events in access log, shows the events starting at 8 and ending at 16.

Example 2:

hour is 10-14 in log.access

From the events in access log, shows the events starting at 10 and ending at 14.

Example 3:
day of week is 1-3 in log.access

From the events in **access** log, shows the events starting at Sunday and ending at Tuesday.

**Example 4:**

day of month is 10-15 in log.access

From the events in **access** log, shows the events starting at 10th and ending at 15th.

**Synopsis**

Used to display the last specified number of events resulting from a Simple Search, or the last specified number of summary table entries resulting from a Complex Search.

**Syntax**

last [number_of_results] for each [group]

*Required Arguments*

number_of_results

**Syntax:** <numeric>

**Description:** The number of last search results to display

*Optional Arguments*

for each group

**Syntax:** for each <column name>

**Description:** The column name on which the last specific number should display.

**Description**

When used immediately following a Simple Search query, returns the specified number of last events resulting from the search. When used immediately following a Complex Search query, returns the specified number of last entries from the summary table resulting from the search.

**Examples**

**Example 1:**

* in log.access | last 91

Returns the last 91 events from **access** log.

**Example 2:**

http in log.iis log| max time-taken | group by c-ip | last 3

Returns the max time-taken value from events in **log.iis** log having http in their column values, for the last three c-ip values only.

**Example 3:**

error in log.xpologlog | count | group by class, method | last 2 for each class

Returns the 2 methods that appeared least in each class in **log.xpologlog** log having error in their column values.

**Example 4:**

error in log.xpologlog | count | group by message | interval 1 hour | last 2 for each interval

Returns the 2 messages that appeared least in each 1-hour interval in **log.xpologlog** log having error in their column values.

**Synopsis**

Displays a list all values under the specified column(s) as appear in the log(s).

**Syntax**
list [column_name]

**Required Arguments**

- column_name

**Syntax:** `<character string>`

**Description:** The name of a column header that its values should be listed

**Optional Arguments**

None

**Description**

Displays a list all values under the specified column(s) as appear in the log(s).

**Examples**

**Example 1:**

```
* in log.application | list event
```

Returns a list of all values under the **Event** in the log **Application**

**Example 2:**

```
* in log.application | list event, type
```

Returns a list of all values under the columns **Event** and **Type** in the log **Application**

**Synopsis**

Calculates the maximum of the values in a specified column in the search query results.

**Syntax**

```
max [column_name]
```

**Required Arguments**

- column_name

**Syntax:** `<character string>`

**Description:** The name of a column header that has numeric values

**Optional Arguments**

None

**Description**

From all the search query results, returns the maximum value in the specified column_name.

**Examples**

**Example 1:**

```
* in log.access | max Bytes Sent
```

Returns the maximum value of the column **Bytes Sent** in the events from **access** log.

**Example 2:**

```
http in log.iis log | max time-taken | group by c-ip
```

From the events from **log.iss** log that have the text **http** in their column values, finds and returns the maximum value in the **time-taken** column per each **c-ip** column value.
maxif

Synopsis
Calculates the maximum of the values in a specified column in the search query results based on a query to be executed on the record.

Syntax
maxif [column_name] \\
"[search_query]"

Required Arguments

column_name

Syntax: <character string>

Description: The name of a column header that has numeric values

search_query

Syntax: <character string>

Description: The search query to be executed on the record

Optional Arguments
None

Description
From all the search query results, returns the maximum value in the specified column_name.

Examples

Example 1:

* in log.access | maxif Bytes Sent "status=200"

Returns the maximum value of the column Bytes Sent in the events from access log only if the value of column status is 200.

Example 2:

* in log.iis log | maxif time-taken "cs-host contains http" | group by c-ip

From the events from log.iis log that have the text http in their cs-host column, finds and returns the maximum value in the time-taken column per each c-ip column value.

min

Synopsis
Calculates the minimum of the values in a specified column in the search query results.

Syntax
min [column_name]

Required Arguments

column_name

Syntax: <character string>

Description: The name of a column header that has numeric values

Optional Arguments
None
Description

From all the search query results, returns the minimum value in the specified column_name.

Examples

Example 1:

* in log.access | min Bytes Sent

Returns the minimum value of the column Bytes Sent in the events from access log.

Example 2:

http in log.iis log | min time-taken | group by c-ip

From the events from log.iss log that have the text http in their column values, finds and returns the minimum value in the time-taken column per each c-ip column value.

Synopsis

Calculates the maximum of the values in a specified column in the search query results based on a query to be executed on the record.

Syntax

minif [column_name] "[search_query]"

Required Arguments

column_name

Syntax: <character string>

Description: The name of a column header that has numeric values

search_query

Syntax: <character string>

Description: The search query to be executed on the record

Optional Arguments

None

Description

From all the search query results, returns the minimum value in the specified column_name.

Examples

Example 1:

* in log.access | minif Bytes Sent "status=200"

Returns the minimum value of the column Bytes Sent in the events from access log only if the value of column status is 200.

Example 2:

* in log.iis log | minif time-taken "cs-host contains http" | group by c-ip

From the events from log.iss log that have the text http in their cs-host column, finds and returns the minimum value in the time-taken column per each c-ip column value.

Synopsis
Orders the complex search results according to the specified column and in the specified direction.

**Syntax**

```
order by [Result_Column_Name] [asc,desc]
```

**Required Arguments**

Result_Column_Name

**Syntax:** character string

**Description:** The column name according to which the complex search results are to be ordered.

**Optional Arguments**

asc, desc

**Description:** Indicates the direction of the ordering of the complex search results - in ascending or descending order of the column name value.

**Description**

Orders the complex search results according to the specified column in the specified direction - ascending or descending order. If no direction is specified, orders in ascending order.

**Examples**

**Example 1:**

```
* in log.access | count,start time, end time, time | group by client ip | order by time desc
```

Calculates the count, start time, end time, and time of the events in log access, groups the events by client ip, and displays them in descending order of the time.

**Synopsis**

A function that returns the percentage of search result events.

**Syntax**

```
percent
```

**Required Arguments**

None

**Optional Arguments**

None

**Description**

When used following the initial simple search query, returns the percentage of events resulting from the search. When used iteratively, Calculate the percentage of results returned from the complex search preceding the pipe.

**Examples**

**Example 1:**

```
* in log.access | percent
```

Always returns 100%

**Example 2:**

```
* in log.application | percent | group by event | order by percent
```

Returns the percentage of each event in the log application
Synopsis
Calculates the percentile of the values in a specified column of the search query results.

Syntax
percentile [percentage_value]

Required Arguments
percentage_value
Syntax: <character string>
Description: The value of a percentage

Optional Arguments
None

Description
A percentile is a measure used in statistics indicating the value below which a given percentage of observations in a group of observations fall

Examples
Example 1:
* in log.system audit | order by process time (ms) | percentile 95
From the events in system audit log, returns the percentile 95% of the events observed by column process time (ms).

Synopsis
Displays the region names extracted from the IP address column in the search result events.

Syntax
region [IP_address_column_name]

Required Arguments
IP_address_column_name
Syntax: <character string>
Description: The name of the column header that has IP address values.

Optional Arguments
None

Description
For each event that has the specified IP_address_column_name with an IP address value, extracts the region name from the IP address, using an internal database.

Examples
Example 1:
* log.access | region IPAddress1
For each event in log access, extracts the region name from the IP address in column IPAddress1.
Calculates the standard deviation of values in a specified column of the search query results.

**Syntax**

`stdev [COLUMN_NAME]`

**Required Arguments**

`COLUMN_NAME`

**Syntax:** <character string>

**Description:** The name of a column header that has numeric values

**Optional Arguments**

None

**Description**

Shows how much variation or dispersion from the average exists calculated on values from a specific log column. A low standard deviation indicates that the data points tend to be very close to the mean (also called expected value); a high standard deviation indicates that the data points are spread out over a large range of values.

**Examples**

**Example 1:**

```
* in log.access | stdev Bytes-Sent
```

Calculates the standard deviation of the values under the column Bytes-Sent in the access log

**Synopsis**

Displays the time of the first event in the group.

**Syntax**

`start time`

**Required Arguments**

None

**Optional Arguments**

None

**Description**

Shows the unformatted time of the first event in the group resulting from the search query. Should be formatted and displayed in date format.

**Examples**

**Example 1:**

```
* in log.access | start time | display start time in date format
```

Display the time of the first event in date format.

**Sum**

**Synopsis**

Displays the sum of the values in a specified column in the search query results.

**Syntax**
sum [column_name]

Required Arguments

column_name

Syntax: <character string>

Description: The name of a column header that has numeric values

Optional Arguments

None

Description

For each event in the search query results that has the specified column_name with a numeric value, adds the value to the cumulative sum, and when it reaches the last event, displays the sum.

Examples

Example 1:
* in log.access | sum Bytes Sent

Returns the sum of the values in column Bytes Sent in the events from access log.

Example 2:

http in log.iis log| sum time-taken | group by c-ip

From the events from log.iis log that have the text http in their column values, calculates the sum of the values in the time-taken column per each c-ip column value.

Synopsis

Displays the sum of the values in a specified column in the search query results based on a query to be executed on the record.

Syntax

sumif [column_name] "[search_query]"

Required Arguments

column_name

Syntax: <character string>

Description: The name of a column header that has numeric values

search_query

Syntax: <character string>

Description: The search query to be executed on the record

Optional Arguments

None

Description

For each event in the search query results that has the specified column_name with a numeric value, adds the value to the cumulative sum, and when it reaches the last event, displays the sum.

Examples

Example 1:

* in log.access | sumif Bytes Sent *status=200*
Returns the sum of the values in column Bytes Sent in the events from access log only if the value of column status is 200.

Example 2:

* in log.iis log | sumif time-taken "cs-host contains http" | group by c-ip

From the events from log.iis log that have the text http in their cs-host column, calculates the sum of the values in the time-taken column per each c-ip column value.

time

Synopsis

Displays the time between the first and last event in a group.

Syntax

time

Required Arguments

None

Optional Arguments

Date_Column_Name

Syntax: <character string>

Description: The name of a specific log column which contains a date/timestamp.

Date_Column_Format

Syntax: <character string>

Description: The date format of the column Date_Column_Name.

Description

Shows the unformatted amount of time between the first and last event in a group - calculated by default based on the log event's main date field. Should be formatted and displayed in time format.

Note: The default time is counted in milliseconds.

Examples

Example 1:

* in log.access | time | display time in time format

Displays the time between the first and last event in log access in time format.

Example 2:

10.10.10.10 in log.access | time | display time in time format

Displays the time between the first and last event with client IP 10.10.10.10 in log access in time format.

Example 3:

* in log.access | time originalTimeStamp ("MM/dd/yyyy HH:mm:ss.SSS") | display time in time format

Displays the time between the first and last event in log access based on the values of the specified log column originalTimeStamp (not the event's main date field) which has the specified date format "MM/dd/yyyy HH:mm:ss.SSS" in time format.

transaction

Synopsis

Displays a flow of correlated events from a single or multiple log sources.

Syntax
transaction ("STEP_I_QUERY", "CORRELATION_I_ID", "STEP_I_NAME"->"STEP_II_QUERY", "CORRELATION_II_ID", "STEP_II_NAME"->...->"STEP_N_QUERY", "CORRELATION_N_ID", "STEP_N_NAME")

Required Arguments
Each step is represented by the following 3 arguments:
STEP_I_QUERY = a search query that isolate all relevant events of a transaction step
CORRELATION_I_ID = the log field which is used to correlate an event of a step and the next step’s event(s)
STEP_I_NAME = the name of the transaction step that will be presented in the results

Optional Arguments
Transaction Time / STEP_NAME->STEP_NAME Time (calculates the time of a transaction or between 2 steps of the transaction)
transaction eventscount / STEP_NAME eventscount (calculates the events count of a transaction / step of the transaction)
limit time to X hours (limits the maximal time allowed from first event to last event in a given transaction - only events within the time limitation will be correlated)
use unique key (events used to open a transaction with the same key will be joined to the same transaction)
transaction fullstate = OPEN/CLOSE/PARTIAL CLOSE (OPEN = transactions the don't contain the closing events, CLOSE = transactions that contain closing events, PARTIAL CLOSE = transaction which were closed because of a time limitation specified by "limit time to X hours" or closing events but missing some events internally)

Description
Shows the unformatted amount of time between the first and last event in a group. Should be formatted and displayed in time format.

Note: By default, the Search colors matching events, step(s) which could not be correlated will be grayed. The time of each specific transaction (marked in green = faster or equals to the average time, marked in red = slower than the average time) and the time taken between each two transaction steps is presented on the mapped transactions.

To see a transaction’s events, click the ‘Show All Events’ link.

Examples

Example 1:
* in log.ORDER_FLOW | transaction
("requesting","TXID","Request"->"authorized","TXID","Authorization"->"dispensing","TXID","Dispense"->"ready transaction","TXID","Ready"->"end of","TXID","Completed")

Displays the correlated transaction from the log ORDER_FLOW based on the correlation ID (log field) - TXID.

Example 2:
* in log.LOG_1, LOG_2, LOG_3 | transaction ("start transaction in log.LOG_1","TXID","Start"->"processing transaction in log.LOG_2","TXID","Processing"->"transaction completed in log.LOG_3","TXID","End")

Displays the correlated transaction from the logs LOG_1, LOG_2, LOG_3 based on the correlation IDs (log fields) - TXID.

Example 3:
* in log.ORDER_FLOW | transaction
("requesting","TXID","Request"->"authorized","TXID","Authorization"->"dispensing","TXID","Dispense"->"ready transaction","TXID","Ready"->"end of","TXID","Completed") | avg transaction Time, max transaction Time, min transaction Time | display avg as Average Tx Time in time format, min as Fastest Tx Time in time format, max as Slowest Tx Time in time format

Displays the average, minimum and maximum transaction time.

Example 4:
* in log.ORDER_FLOW | transaction
("requesting","TXID","Request"->"authorized","TXID","Authorization"->"dispensing","TXID","Dispense"->"ready transaction","TXID","Ready"->"end of","TXID","Completed") | count | interval 5 minute | show count as Transactions Over Time
Displays the number of transactions that were correlated in 5 minutes time bucketing.

Example 5:

* in log.ORDER_FLOW | transaction
("requesting","TXID","Request"->"authorized","TXID","Authorization"->"dispensing","TXID","Dispense"->"ready transaction","TXID","Ready"->"end of","TXID","Completed") | where transaction time > 500 | order by transaction time desc

Displays all transactions that their total time to be completed took more than 500 milliseconds (result will be sorted in a descending order).

Example 6:

* in log.ORDER_FLOW | transaction
("requesting","TXID","Request"->"authorized","TXID","Authorization"->"dispensing","TXID","Dispense"->"ready transaction","TXID","Ready"->"end of","TXID","Completed") | avg request->authorization time, max request->authorization time, min request->authorization time | display avg as Average Request>Authorization in time format, max as Slowest Request>Authorization in time format, min as Fastest Request>Authorization in time format

Displays the average, minimum and maximum time of the time taken between the transaction's steps Request to Authorization.

Example 7:

* in log.ORDER_FLOW | transaction

Displays only transactions that contain exception in one or more of it's log events.

Example 8:

* in log.ORDER_FLOW | transaction

Displays the average number of events in the 'Authorization' transaction step.

Example 9:

* in log.ops | transaction
("start", "TXID_1+TXID_2", "Start"->"end", "TXID_1+TXID_2", "End")

Displays transactions which were correlated by using a combination of 2 log fields TXID_1 and TXID_2.

Example 10:

* in log.ORDER_FLOW | transaction
("requesting", "TXID", "Request"->"end of", "TXID", "Completed") use unique key

Displays the correlated transaction from the log ORDER_FLOW based on the correlation ID (log field) - TXID (events used to open a transaction with the same key will be joined to the same transaction).

where

Synopsis

Filters (i.e. narrows) the complex search results to display only those column values that meet specific criteria.

Syntax

where [SEARCH QUERY on column results]

Required Arguments

SEARCH QUERY on column results

Syntax: A search query (simple or complex)

Description: Runs a search query on the complex search summary table, to extract and display values that meet specific criteria.

Optional Arguments

None

Description
Filters the summary table resulting from a complex search, to extract and display only those values that meet specific criteria defined in the "where" search query. The "where" search query can be built using the simple search syntax (see Performing a Simple Search) or complex search syntax (see Complex Search Syntax Reference).

Examples

Example 1:

in log.access log | count | group by status | order by count desc | where count < 500

Shows only those statuses in the summary table which have less than 500 events.

Refining a Search

You can refine (augment) a search using the following two methods:

- Adding a column value of an event resulting from the original search to the search query (see Refining a Search Based on Events).
- Adding a problem detected in the original search, to the search query (see Augmenting a Search with Detected Problems).

Refining a Search Based on Events

In the Search Results Area resulting from a Simple Search, you can refine the search with column values from the resulting events.

To refine your search based on an event:

1. In the Search Results Area, hover over a column value of an event, and after it is highlighted, click it.
   
   A list of operations opens.

2. Select one of the following operations:
   
   Add to Search (AND) – To search for events matching the current search query AND the highlighted value in the event.
   
   Add to Search (OR)– To search for events matching the current search query OR the highlighted value in the event.
   
   Exclude from Search – To search for events matching the current search query, with the exception of those events that have the highlighted value in the event (AND NOT).
   
   Replace Search – To replace the search query with the highlighted value in the event.

   The new search runs.

   The added search condition appears under Active Filters in the Augmented Search Pane.

3. Repeat steps 1 and 2 for all event values that you want to include in your search query.

   At any point, you can restore the original query, or remove a filter based on an event, by removing it from the Active Filters list (see Managing Active Filters).

Augmenting a Search with Detected Problems

As there are many logs with myriads of information, it may be difficult for a user to decide what to search for.

XpoLog Search assists the user in deciding what to search for by displaying for each time period, problems that occurred at that time, along with the severity of these problems. Although these problems are not errors, they can in fact be the root cause of an error, so that adding them to a search can be very beneficial.

The user can decide whether to show only predefined problems, autodetected problems, or all problems (see Selecting Augmented Layers for full details).

Note: The detected problems are not related to the search query.

Dots of varying colors and sizes are displayed on the time axis of the search, representing the problems detected at this time.

The size of a dot is relative to the number of problems found on the time axis. A larger dot represents more detected problems; a smaller dot, less detected problems.

The color of the dot indicates the severity of the most serious problem found at that time, as follows:

- Yellow – low severity
- Orange – medium severity
- Red – high severity

Hovering on a dot opens a list of suggestions, from which you can drill down to see the events associated with it. It is recommended to hover on a dot with the most highest-severity problems.

The user can augment a search with a problem from the list by clicking it. The selected problem is then added to the search query with the logical OR operator.

To augment your search with a detected problem:

1. In the Augmented Layers selection box, select the problems that the system should show on the time axis: Predefined, Autodetected, or all problems.
2. Hover on a dot on the time-axis, and select a problem from the list of problems. The problem is appended to the search query with the logical OR operator. 
   **Note:** If there is no search query, it is added to the search query as is. 
   The added detected problem appears under **Active Filters** in the Augmented Search Pane.

3. Repeat step 2 to add an additional problem to your search.

   At any point, you can restore the original query, or remove from the query a filter based on a problem, by removing it from the Active Filters list (see **Managing Active Filters**).

**Selecting Augmented Layers**

The time axis of the main graph of a search query displays problems detected by XpoLog at any specific time.

You can define the types of problems that should be presented on the time axis of the XpoLog Search graph:

- **Predefined** – user-defined problems
- **Autodetected** – problems automatically detected by XpoLog
- **Both Predefined and Autodetected** problems (the default)

To select the augmented layers of the search:

- In the Graph toolbar, in the Augmented Layers selection box, click **Predefined**, **Autodetected**, or both. 
  The dots on the time axis of the graph refresh according to your selection.

**Managing Active Filters**

In the Augmented Search Pane, under Active Filters, are listed all the filters that were added to your original search query, based on an event or a detected problem.

You can remove a filter from the search query, by removing it from the Active Filters list, and you can also restore the original search query.

**Removing a Filter From the Search Query**

Removing the filter from the Active Filters list removes it from the search query, and automatically runs the search with the resulting query.

To remove a filter from the search query:

- In the Augmented Search pane, under **Active Filters**, click the Remove Filter icon adjacent to the filter that you want to remove. 
  The filter is removed from the Active Filters list, and the resulting search query runs.

**Resetting the Search Query**

You can restore a search query to its original state, regardless of the number of filters that have been added to it.

To reset a search query:

- In the Augmented Search pane, under Active Filters, click **Reset**. 
  The Active Filters list closes, the original search query is restored, and automatically runs.

**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 knowledgebase, 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 activated, **Servers Metrics Analysis** displays the CPU, memory, and disk problems on the source servers from which the logs originated. The problems definition for metrics can be easily customized to meet the environmental constraints.

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.
Accessing the Analytics Console

You can access Analytics from the XpoLog Center homepage or from any page in the application. To access the Analytics console:

- In the homepage, in the navigation pane under Quick Actions, click the Analytics icon OR
- From any XpoLog page, in the Tab Bar, click the Analytics tab.

The Analytics console opens, displaying the analysis of the logs in the system. See Analytics User Interface.

Analytics User Interface

Analytics is equipped with a user friendly graphic user interface (GUI), which provides a complete set of tools to analyze detected problems. The Analytics user interface includes the following main elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab Bar</td>
<td>On the left side, XpoLog, XpoSearch, and Analytics tabs. On the right side, an XPLG icon. For details, see Tab Bar.</td>
</tr>
<tr>
<td>Main Menu</td>
<td>On the left side, includes the following menu items and submenus for performing actions in Analytics.</td>
</tr>
<tr>
<td></td>
<td>• Dashboards</td>
</tr>
<tr>
<td></td>
<td>• Administration</td>
</tr>
<tr>
<td></td>
<td>• Indexing</td>
</tr>
<tr>
<td></td>
<td>On the right side, has a Home button for navigating to the XpoLog homepage, and in organizations where security is activated, also displays the Username and a Logout button.</td>
</tr>
<tr>
<td>View Type Panel</td>
<td>Provides three buttons for selecting the graph view type: Folders and Logs, Applications view, or Servers view. See</td>
</tr>
</tbody>
</table>
### Graph Display and Time Control Panel

The graph display area enables filtering the graph to show analysis for logs under specific Folders, Applications, or Servers. It also provides buttons for zooming into or out of the graph, viewing the default view, and has a toolbar with buttons for hiding metrics, summary view, split view, risk view, and total view.

The time control area enables users to select the time frame for which the Analytics analysis is presented; this time frame can be changed easily at any point.

<table>
<thead>
<tr>
<th>Problems Graph</th>
<th>Displays a graphic distribution of the analysis.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems Summary Table</td>
<td>Presents detailed information of the data displayed in the problems graph. For each member in the Folders and Logs, Application, or Server (according to what you selected), a summary of the analysis is displayed, each relevant to the specified time frame.</td>
</tr>
<tr>
<td>Most Severe Problems Table</td>
<td>For each selected view type and time frame, the Analytics presents the top 10 problems (with the highest severity) that were found in the analysis.</td>
</tr>
</tbody>
</table>

### View Type Panel

The View Type panel user interface includes the following buttons for selecting the graph view:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folders and Logs view</td>
<td>Clicking this button displays Analytics on the logs in the Folders and Logs structure, as defined in XpoLog Manager.</td>
</tr>
</tbody>
</table>
Applications view – Clicking this button displays Analytics on logs under the context of their associated applications.

Servers view – Clicking this button displays Analytics on logs under the context of the servers on which they are located. Under this view, server metrics analysis is also available.

Graph Display and Time Control Panel

- Time control area – enables users to select the time frame for which Analytics is presented; this time frame can be easily changed at any point.
- Graph toolbar – Buttons for selecting the type of analysis displayed by the Problems Graph.
The Graph Display and Time Control Panel includes the following elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default view</strong> button</td>
<td>Clicking this button displays the graph in default view, i.e. in Folders and Logs Total Summary view for the last seven days.</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>Displays the contents of the graph, according to the selected view type, filter entities, and display view.</td>
</tr>
<tr>
<td><strong>Zoom-Out</strong> button</td>
<td></td>
</tr>
</tbody>
</table>
**Time Period**

Defines the time period during which Analytics is to be run.

Selectable time periods include:

- Predefined time periods: **Last hour**, **Last 3 hours**, **Last 12 hours**, **Last 24 hours**, **Last 3 days**, **Last 7 days**, **Last 2 weeks**, **Last 3 weeks**, **Last 4 weeks**, **Last 3 months**, **Last 6 months**, **Last 12 months**
- Customized time periods: **Custom**.

**Start and End Dates and Times**

Displays the start and end dates and times of Analytics, according to the default or selected time period. Clicking this box opens up calendars for selecting a customized time period (see **Customizing the Analytics Time Period**).
**Open Calendar** button. Clicking this button opens up calendars for selecting a customized time period (see Customizing the Analytics Time Period).

<table>
<thead>
<tr>
<th><strong>Filter Entities / Clear Filter</strong></th>
<th>Clicking the <strong>Filter Entities</strong> link opens a filter for filtering Analytics according to specific folders and logs, applications, or servers. Clicking the <strong>Clear Filter</strong> link clears the checkboxes in the filter so that you can select new selection criteria.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Graph Toolbar</strong></td>
<td>This toolbar of buttons above the Problems Graph includes buttons for adjusting the display of the Problems Graph (see below).</td>
</tr>
</tbody>
</table>

**Graph Toolbar**

The Graph Toolbar includes the following buttons:

<table>
<thead>
<tr>
<th><strong>Button</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>

Total View button.

Clicking this button displays a total view of the problem events. The information displayed in the graph can be either of the following, depending on whether the Summary View or Split View button is selected:

- **Total Summary**: When the Summary View button is also selected; in this case, the graph presents the total number of events on all the selected logs.
- **Total Split**: When the Split View button is also selected; in this case, the graph presents each of the members (based on the view: logs/applications/servers) individually with its own problems mapped over time. In the background, the total summary graph is presented.

On top of either graph, you can see measurement points in different colors that indicate problems of varying severities:

- **Green**: no problems were found at that time.
- **Yellow**: problems of low severity (at most) were found at that time.
- **Orange**: problems of medium severity (at most) were found at that time.
- **Red**: problems of high severity were found at that time.

**Note**: A severity level is assigned to all problems automatically by Analytics. On the other hand, users determine the severity level of predefined problems and server metrics.

Hovering the mouse over a measurement point, presents a summary of all the problems that were detected at that time.

Risk View button.

Clicking this button changes the graph to bars format. In the background, the total summary graph is presented. The information displayed in the bar graph can be either of the following, depending on whether the Summary View or Split View button is selected:

- **Risk Summary**: When the Summary View button is also selected. For each time slot, the bar level represents the maximal severity that was found at that time.
- **Risk Split**: When the Split View button is also selected. For each time slot, each bar level represents the maximal severity that was found at that time for a specific member (based on the view –logs/applications/servers).

Hovering the mouse over a bar presents a summary of all the problems that were detected at that time.

Bar Graph icon.

Clicking this icon displays a bar graph of the event distribution.
Toggle button for Show Metrics / Hide Metrics. Clicking this button shows the server metrics below the Problems Graph. Clicking this button once again hides the server metrics.

Split View button.
Clicking this button displays the event distribution originating from each log, separately.

Summary View button.
Clicking this button displays a summary view of the event distribution from all the logs.

The Problems Graph Area user interface includes the following elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems Graph</td>
<td></td>
</tr>
</tbody>
</table>
| **Graph** | A graph with the Analytics timeline in the x-axis, and the number of events in the y-axis. The graph shows the distribution of events over the selected timeline. On the graph there are measurement points that indicate problems. The severity of these problems is according to the following color-coding:  
- Green – no problems were found at that time.  
- Yellow – problems of low severity (at most) were found at that time.  
- Orange – problems of medium severity (at most) were found at that time.  
- Red – problems of high severity were found at that time.  
**Note:** The severity level is assigned to all problems automatically by Analytics, except for predefined problems and server metrics, which are determined by users. Hovering the mouse over a measurement point displays a summary of all the problems that were detected at that time. |
| **Metrics** | Displays Metrics information (CPU/Memory), provided that Show Metrics is activated - **this feature is deprecated as of version 6.4808** |
| **Previous/Next timeslot buttons.** | Clicking these buttons located in the left and right edges below the graph, displays the distribution of events in the previous/next timeslot. |
The Problems Summary Area includes the following elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems Summary Table</td>
<td>Enables viewing the table in flat or hierachic view, as well as the parent of an item in the table, if it exists</td>
</tr>
<tr>
<td>Problems Summary Table</td>
<td>Presents detailed information of the data displayed in the Problems graph. For each member (Folders and Logs/Application/Server), a summary of the analysis is displayed (each relevant to the specified time frame)</td>
</tr>
<tr>
<td>Search and Navigation Bar</td>
<td>Enables searching for a specific term, and in cases where there is more than one page of problems, navigating to a different page of problems</td>
</tr>
</tbody>
</table>

**Problems Summary Table Toolbar**

The Problems Summary Table Toolbar includes the following button:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Parent button; this button appears in the toolbar after performing a drilldown on a folder/log/application/server. Enables viewing the analytics before the drilldown.</td>
<td></td>
</tr>
</tbody>
</table>
Flat View button; presents the list of logs without their hierarchical context.

Hierarchic View button (default); presents the folders/logs/applications/servers under their hierarchical context, i.e. parent folder/application/server on the top view with drilldown options.

**Problems Summary Table**

The Problems Summary Table presents detailed information of the data displayed in the Problems Graph.

For each member (Folders and Logs/Application/Server), a summary of the analysis is displayed (each relevant to the specified time frame), as described in the following table:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the folder/log/application/server that contains the problem. Clicking the name performs the same function as the Drill-down button. See below.</td>
</tr>
<tr>
<td><strong>Logs Status</strong></td>
<td>The maximal severity problem found in the logs under the folder/log/application/server</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Server Metrics</strong></td>
<td>Shows a C, M, and/or D icon to indicate that there are CPU, Memory, and/or Disk Space metrics available for the server. Hovering over any of these icons, shows a table of the count for each of these metrics.</td>
</tr>
<tr>
<td><strong>Logs Events</strong></td>
<td>The total number of events found in the logs under the folder/log/application/server</td>
</tr>
<tr>
<td><strong>Logs Problems</strong></td>
<td>The total number of problems under found in the logs under the folder/log/application/server</td>
</tr>
<tr>
<td><strong>Predefined</strong></td>
<td>The number of predefined problems in the logs under the folder/log/application/server</td>
</tr>
<tr>
<td><strong>Autodetected</strong></td>
<td>The number of automatically detected problems in the logs under the folder/log/application/server</td>
</tr>
<tr>
<td><strong>% of Problems</strong></td>
<td>The percentage of the total number of problems currently presented in the console.</td>
</tr>
<tr>
<td>Select/Unselect toggle button; Clicking this button displays this member’s analysis individually on top of the Problems Graph; clicking this button again displays it.</td>
<td></td>
</tr>
<tr>
<td>Drill-down / Search in XpoSearch button; clicking this button drills down and displays the analysis only for a specific member and its submembers until the problem level, at which point, clicking this button searches for the problem in XpoSearch.</td>
<td></td>
</tr>
</tbody>
</table>

**Search and Navigation Bar**

The Search and Navigation Bar includes the following elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search button; Clicking this button opens a textbox for typing a specific term to find in Analytics under your current time frame (error code, exception, user, etc.). Analytics refreshes itself with the search results. After the search has completed, can press the <strong>Clear</strong> link to return to the previous Analytics results.</td>
<td></td>
</tr>
<tr>
<td>Paging</td>
<td>The table presents the analysis of 10 folders/logs/applications/servers per page. If there are more than 10 folders/logs/applications/servers, you can use the paging to navigate through the entire list.</td>
</tr>
</tbody>
</table>

**Most Severe Problems Table**

For each selected view type and time frame, Analytics presents the top 10 problems (with the highest severity) that were found in the analysis:
For each detected problem there is an option to modify its severity or exclude it from the analysis directly in the console.

The Most Severe Problems Table includes the following columns:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The source folder/log/application/server that contains the problem</td>
</tr>
<tr>
<td>Problem</td>
<td>A short description of the problem; clicking the problem has the same function as clicking the Search in XpoSearch button (see below).</td>
</tr>
<tr>
<td>Type</td>
<td>The problem type; can be Predefined, Autodetected, Statistical, or Metrics</td>
</tr>
<tr>
<td># of Occurrences</td>
<td>The number of occurrences of this problem</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity assigned to this problem</td>
</tr>
</tbody>
</table>

Search in XpoSearch button; clicking this button enables searching for the event in the log.
Selecting the Graph View Type

You can view the Analytics graph distribution according to any of the following three views:

- **Folders and Logs** – Logs are presented under their Folders and Logs structure, as defined in XpoLog Manager.
- **Applications** – Logs are presented under the context of their associated applications.
- **Servers** – Logs are presented under the context of the servers on which they reside. Under this view, server metrics analysis is also available.

Hovering on any point in the graph displays the distribution of the problems in the logs that reside under the selected view type.

To select the view type:

- In the View Type panel (see its user interface in View Type Panel), select one of the following three buttons: **Folders and Logs, Applications, or Servers**.
  The graph is refreshed according to the View Type selection.

Selecting the Analytics Time Period

Time plays a very important role in the examination of the cause of a system problem.

Although Analytics is automatically performed on the log events from the last seven days, you can set Analytics to run on events that occurred at any time.

You can select a predefined time period, or customize the time period by selecting the start and end dates and times of the time period.

To select the time period of Analytics:

1. In the Graph Display and Time Control Panel (see its user interface in Graph Display and Time Control Panel), in the Analytics Time Range textbox, click the down arrow.

   ▼
A list of selectable time periods opens.

2. From the list of time periods, select a predefined time period (Last hour, Last 3 hours, Last 12 hours, Last 24 hours, Last 3 days, Last 7 days, Last 2 weeks, Last 3 weeks, Last 4 weeks, Last 3 months, Last 6 months, or Last 12 months), or select Custom to specify your own time period (see Customizing the Analytics Time Period for a detailed explanation on customizing the time period).

The selected time period is displayed in the textbox, and Analytics runs on this time period.

Customizing the Analytics Time Period

You can customize the time period of Analytics, by selecting from calendars the beginning and end dates and times of the time period.

To customize the time period:

1. In the Graph Display and Time Control Panel, in the Time Period selection box, select Custom

   OR

   Click the Open Calendar icon.

   Two calendars – one of the start date and one of the end date of the previous Analytics time period are displayed.

2. In the left calendar, repeatedly click the arrows at the left and right of the month name, to scroll to previous/following months, until you reach the desired month of the start date. Then, in the calendar, click the desired start date.

   The day is highlighted in the calendar, and is displayed below the calendar in Start Date.

3. In Start Time, type the time of day that the time period begins.

4. In the right calendar, repeatedly click the arrows at the left and right of the month name, to scroll to previous/following months, until you reach the desired month of the end date. Then, in the calendar, click the desired end date.

   The day is highlighted in the calendar, and is displayed below the calendar in End Date.

5. In End Time, type the time of day that the time period ends.

6. Click Go.

   Analytics runs on the selected time period, returning the Analytics results for the customized time period.

Note: The Time Period box displays Custom.

Displaying the Default View

By default, any log added to XpoLog is analyzed automatically. Analytics refreshes its analysis every five minutes (the predefined default), and displays its results in default view – analysis of all logs under Folders and Logs in Total Summary view, during the last 7 days, with Metrics displayed. You can run Analytics for a different view type, view, and/or time interval, can zoom in or out of time intervals, and can hide metrics. At any point, you can redisplay the default view.

To display the default view:

- In the Graph Display and Time Control Panel, click the Default view button.

The Analytics results are displayed in default view – Folders and Logs Total Summary view for the last 7 days, and with Metrics.

Understanding the Analytics Problems Graph

Analytics returns a Problems Graph that shows the distribution of problems over time. You can determine the display mode and contents of the graph. The graph has drilldown functionality, enabling you to zoom into the entire graph or into any timeslot, and run Analytics on the new time period or timeslot. It also enables you to hover over a measurement point to see the source of problems and drill down to see the exact problems in any log. You can also view the Analytics of the previous or next timeslot.

Defining the Problems Graph

XpoLog enables you to determine the contents and display of the Problems Graph using the buttons located on the Problems Graph toolbar – on the left, the display control buttons: Total View and Risk View, and on the right, the content control buttons: Summary View and Split View.

A graph in Split View displays one line per source of problems in that timeslot, where each line represents the number of problems in a single source of problems. Also, the Summary View is displayed in the background.

A graph in Summary View displays a single line to represent all problems from all problem sources.

A graph in Total View shows the distribution of problems in a line graph (the default). A line graph shows how the number of problems change from one point in time to the next.

A graph in Risk View shows the distribution of problems in a bar graph. The height of each bar is according to the number of problems that occurred at the specific time. A bar does not appear at times when no problems were detected.

The Problems Graph can display four types of analyses, from the four possible combinations of display and control buttons, as follows:

- Total Summary
- Total Split
- Risk Summary
- Risk Split

Total Summary

The Total Summary graph presents the total number of events in all the selected logs, with the top of the graph showing different measurements points of different colors that indicate the severity of the problems:

- Green – No problems were found at that time.
- Yellow – Most of the problems found at that time are of low severity.
- Orange – Most of the problems found at that time are of medium severity.
- Red – Problems of high severity were found at that time.

Note: Analytics automatically assigns a severity level to all problems, except predefined problems and server metrics, for which users determine the severity level. Hovering over a measurement point displays a table for a single source of problems, unless the measurement point is the same for more than one problem source, in which case the table shows the problem distribution for all the problem sources passing through that point.

To display your graph in Total Summary View:

- In the Problems Graph Toolbar, on the left side, click the Total View button, and on the right side, click the Summary View button.

Total Split

The Total Split graph presents each of the members (based on the view – logs/applications/servers) individually, with its own problems mapped over time. In the background, the Total Summary graph is presented.

To display your graph in Total Split View:

- In the Problems Graph Toolbar, on the left side, click the Total View button, and on the right side, click the Split View button.

Risk Summary

The Risk Summary graph is the same as the Total Summary Graph, but in bars format. For each time slot, the bar level represents the maximal severity that was found at that time. In the background, the Total Summary graph is presented.

To display your graph in Risk Summary View:

- In the Problems Graph Toolbar, on the left side, click the Risk View button, and on the right side, click the Summary View button.

Risk Split

The Risk Split graph is the same as the Total Split graph, but in bars format. For each time slot, each bar level represents the maximal severity that was found at that time for a specific member (based on the view – logs/applications/servers). In the background, the Total Summary graph is presented.

To display your graph in Risk Split View:

- In the Problems Graph Toolbar, on the left side, click the Risk View button, and on the right side, click the Split View button.

Filtering the Problems Graph

By default, the Problems Graph shows the results of Analytics on all folders and logs, applications, or servers, depending on the view type that you selected. You can show the Problems Graph on specific logs, applications, or servers, by using the Filter feature. You can also change the View Type directly from the Filter feature.

To filter the entities in the Problems Graph:

1. In the Graph Display and Time Control panel, click the Filter Entities link.
   A filter opens for selecting specific items under the selected view type - folders and logs, applications, or servers.
2. Select the checkboxes of the specific items for which you want to view the Problems Graph. You can also click the Open list icon to select a different View Type.
3. Click the Go button.
   The Problems Graph is generated for the selected entities.

Clearing the Filter

You can refresh the Problems Graph to display all the entities under the selected view type.

To remove the filter:

1. In the Graph Display and Time Control panel, click the Clear Filter link.
   The Problems Graph is generated for all entities of the selected View Type.

Hiding/Showing Server Metrics

XpoLog measures CPU level, memory level, and disk usage on any server that contains logs that XpoLog analyzes. You can choose to show or hide a graph of these server metrics below the Problems Graph, and in parallel, show or hide the Server Metrics links in the Problems Summary table.

To show server metrics in Analytics:

- In the Graph Display and Time Control panel, click the Show Metrics button.
  The server metrics graph is displayed below the problems graph, and the Server Metrics column appears in the Problems Summary table. The Show Metrics button toggles to a Hide Metrics button.

To hide server metrics in Analytics:
In the Graph Display and Time Control panel, click the Hide Metrics button. The server metrics graph below the problems graph is hidden, and the Server Metrics column is concealed in the Problems Summary table. The Hide Metrics button toggles to a Show Metrics button.

**Zooming Into / Out of the Graph**

You can zoom into the Analytics graph, so that you can see a more detailed breakdown of problems over a smaller period of time. Zooming into the graph displays the Analytics graph for half the length of the previous time interval, showing more specific results for each unit of time.

You can also zoom out of the graph, so that you can see a breakdown of problems over a longer period of time. Zooming out displays the Analytics graph for twice the length of the previous time interval, showing less specific results for each unit of time.

**Zooming Into the Analytics Graph**

To zoom into the Analytics graph:

- In the Graph Display and Time Control Panel, click the Zoom-In button.
  
  The graph is displayed for half of the previous time interval.

**Zooming Out Of the Analytics Graph**

To zoom out of the Analytics graph:

- In the Graph Display and Time Control Panel, click the Zoom-Out button.
  
  The graph is displayed for twice the previous time interval.

**Zooming Into /Out of a Timeslot**

You can zoom into a specific timeslot in your graph, so that you can see a more detailed breakdown of problems over a smaller period of time. For example, in an Analytics graph that shows the distribution of problems for a period of seven days, you can zoom into any timeslot (day) to focus on the distribution of problems during that day, and you can zoom in further to see the distribution of problems in a specific hour on that day. At any point, you can zoom out repeatedly until you reach the graph resulting from the original time period.

**Zooming Into a Timeslot**

To zoom into a timeslot:

- In the graph, in the timeslot which you want to zoom into, click the Zoom-In button.
  
  The zoomed-in timeslot is subdivided into smaller timeslots. The Zoom-Out button appears, enabling you to zoom out to the previous display. The time period of Analytics is automatically changed to Custom.
  
  You can repeatedly click the Zoom-In button to see an increasingly more detailed distribution of the problems.

**Zooming Out of a Timeslot**

To zoom out of a timeslot:

- In the graph, click the Zoom-Out button.
  
  You can repeatedly click the Zoom-Out button until the graph is displayed for the original Analytics time period. At this point, the Zoom-Out button is no longer displayed.

**Viewing the Previous/Next Timeslot**

You can display directly from the graph, a graphical representation of the problems in the previous or next timeslot.

To display the previous timeslot:

- Below the graph, on the left, click the Previous Timeslot button.
  
  The entire problems graph shifts to the left to display the previous timeslot.

To display the next timeslot:

- Below the graph, on the right, click the Next Timeslot button.
  
  The entire problems graph shifts to the right to display the next timeslot.

**Viewing the Distribution of Problems**

You can hover over any measurement point in the graph to view a table with the number of problems that were found under Folders and Logs, Applications, or Servers (depending on the chosen View Type). From this table, you can drill down on a specific Folder or Log, Application log, or Server log in that timeslot. You can keep drilling down until the actual problems are displayed in the table. At this point, the drilldown feature changes into an XpoSearch feature; you can run XpoSearch to search for the problem in all events in the log for the drilled down timeslot, by clicking the problem directly in the table.

For example, initiating Analytics for Applications results in a problems graph for all entities under Applications. Hovering over a measurement
point in the resulting problems graph displays a table with the distribution of problems for Windows Event Logs, App1, App2, and App3. Drilling down on Windows Event Logs displays a graph of the distribution of the Security, System, and Application Logs over the timezone of the previous measurement point. Hovering over a measurement point displays a table of the distribution of problems in the Security, System, and Application Logs. Drilling down on any of these logs shows the various problems in the logs and their distribution. For example, drilling down on the Applications log shows problems message was not found and shutting down. At this point, you can click a problem to run XpoSearch to find all events in the log in the timeslot of the measurement point, which contain this problem. For example, clicking message was not found automatically runs XpoSearch for “message was not found” in log.Application.

To view the distribution of problems at a specific point in time:

- Hover over a measurement point in the graph.
- A table displays the distribution of problems in the entities under the selected View Type (Folders and Logs, Applications, or Servers).

**Drilling Down**

You can drill down repeatedly on any entity under Folders and Logs, Applications, or Servers in a Problem Distribution Table, until you get to the most detailed level - a table of the problems detected by Analytics.

To drill down on an entity in the Problem Distribution Table:

- Click the name of the entity to drill down
- Or
- Click the Drill-Down button on the row of the entity

**Analyzing Analytics Problems**

The Problems Summary table presents detailed information of the data displayed in the Problems graph (see Problems Graph). For each member (from Folders and Logs, Applications, or Servers), a summary of the analysis is displayed for the specified time frame.

You can view the table in either Hierarchic view (the default) or Flat view.

From this table, you can:

- Drill down on any member in the table to view the Analytics analysis only for a specific member and its sub members.
- View a specific member’s analysis presented individually on top of the problems graph
- Run a search for a specific term that you would like to find in the Analytics under your current time frame (error code, exception, user, etc.)
- Use the paging to navigate through the entire list of problems, if the analysis presents more than 10 members.

**Viewing Server Metrics**

You can view details of the CPU, memory, and disk usage of servers in Analytics, provided that you selected to show metrics.

To view server metrics:

1. In the Problems Summary table, under the Server Metrics column, click the C, M, or D icon.
   - A table appears showing the CPU, memory, and disk usage.

**Viewing the Problems Summary Table in Hierarchic/Flat View**

You can view the Problems Summary table in either of the following two views:

- **Hierarchic View** (default) – presents the members under their hierarchical context, i.e. parent folder/application/server on the top view with drilldown options
- **Flat View** – presents the list of logs without their hierarchical context

To view the Problems Summary table in Hierarchic View:

- In the Problems Summary table toolbar, click the Hierarchic View button.

To view the Problems Summary table in Flat View:

- In the Problems Summary table toolbar, click the Flat View button.

**Drilling Down**

You can drill down on any element in the table to see an analysis of its members. You can keep drilling down until you get to the lowest level - a list of problems in the table.

To drill down on a table element:
Click the name of the member or click the drilldown button at the end of the table row. Analytics refreshes to show the analysis for the selected member only. Above the lowest level, the submembers of the selected member are listed in the table; at the lowest level, the problems are listed.

Searching For a Problem

Once you identify an interesting problem, XpoLog provides a number of options. You can either choose to investigate the data source for more problems, or expand the analysis to more sources under the same Application or Server. In addition, a common option that is available is to search for the problem in the data source using the search engine, or to search for other specific problems that were discovered in the Analytics console.

Searching For a Problem in the Analytics Console

You can search for a problem in the Analytics console by clicking the Search button located on the left side of the Search and Navigation Bar below the list of data sources or problems in the Problems Summary table.

For example, searching for "Failure" at the problem level, shows all problems containing the word "failure", such as "Login failure" and "Audit failure". Searching for "Failure" at the log, application, or server level, shows the distribution of problems containing the word "Failure" in these members.

To search for a problem in the Analytics console:

1. Below the Problems Summary table, on the left side of the Search and Navigation Bar, click the Search icon.
   A Search textbox opens.
2. In the textbox, type the text to search for in the list of problems that was detected by Analytics, and then click the Search button.
   The console loads data sources that contain the problems that meet your search criteria. If the search was made on a number of Logs, Applications, or Servers, the search results are presented across those data sources.

Searching for a Problem in XpoSearch

You can search in the log for any problem that is detected by Analytics, by zooming into the XpoSearch search engine from any problem in the Problems Summary table. If XpoSearch finds the problem, it displays it in the search results area, and the Analytics engine highlights the priority accordingly.

To search for a problem in XpoSearch:

- In the Problems Summary Table, click the problem or click the Search in XpoSearch button at the end of the row of the problem.
  XpoSearch opens, running a search for the problem in the log events. The problem text is highlighted in the events of the log.

For example, drilling down on the Windows Event Logs folder lists the distribution of problems in the Security, Application, and Systems logs. Drilling down on the Application log, displays the problems in the log, including "error code". Clicking "error code" starts a search in XpoSearch: "error code" in folder.Windows Event Logs in log.Application, and the resulting events have "error code" highlighted in them.

Customizing the Severity of a Severe Problem

You can customize the severity level of a problem in the Most Severe Problems table. For example, you can change a problem assigned a severity level of High to Medium or Low. Customization changes take effect only in future analyses.

To change the severity of a problem:

1. In the Most Severe Problems table, at the end of the row of the problem whose severity you want to change, click the Customize problem severity link.
2. In the menu that opens, click the severity that you want to assign to the problem.

Excluding a Severe Problem from Analysis

You can exclude a problem in the Most Severe Problems table from future analyses.

To exclude a problem from future runs of Analytics:

1. In the Most Severe Problems table, at the end of the row of the problem which you want to exclude, click the Customize problem severity link.
2. In the menu that opens, click Exclude from analysis.

Searching for a Severe Problem in XpoSearch

You can search in the log for any problem that is detected by Analytics as one of the ten most severe problems, by zooming into the XpoSearch search engine from any problem in the Most Severe Problems table. If XpoSearch finds the problem, it displays it in the search results area, and the Analytics engine highlights the priority accordingly.

To search for a most severe problem in XpoSearch:

- In the Most Severe Problems Table, click the problem or click the Search in XpoSearch button at the end of the row of the problem.
  XpoSearch opens, running a search for the problem in the log events. The problem text is highlighted in the events of the log.

XpoLog Manager

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.

Accessing XpoLog Manager

You can access XpoLog Manager from any page in the application.

To access the XpoLog Manager console:

- In the Tab Bar, click the XpoLog tab. The XpoLog Manager console opens. See XpoLog Manager User Interface Elements.

XpoLog Manager User Interface Elements

XpoLog Manager is equipped with a user friendly graphic user interface (GUI), which provides a complete set of tools for administrators to
manage log information, and for end-users to navigate through system logs, and view, filter, customize. and export them. It also provides a Log Monitor that verifies the logs' contents and sends alerts when a rule matches the log records.

The XpoLog Manager user interface includes the following main elements:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab Bar</td>
<td>On the left side, Apps, Search, and Analytics tabs. On the right side, the Manager tab. For details, see Tab Bar at XpoLog Homepage.</td>
</tr>
<tr>
<td>Main Menu</td>
<td>On the left side, includes the following menu items and submenus for performing actions in XpoLog Manager.</td>
</tr>
<tr>
<td></td>
<td>• Log Actions</td>
</tr>
<tr>
<td></td>
<td>• Administration</td>
</tr>
<tr>
<td></td>
<td>• Configuration</td>
</tr>
<tr>
<td></td>
<td>• Tools</td>
</tr>
<tr>
<td></td>
<td>• Settings</td>
</tr>
</tbody>
</table>

The main XpoLog logo on the left hand side, is the Home button for navigating to the XpoLog homepage, and in organizations where security is activated, on the right hand side also displays the Username and a Logout button.

<table>
<thead>
<tr>
<th>Main Pane</th>
<th>Contains icons that can be clicked to navigate to Log Viewer, Log Monitor, etc. as well as icons that can be clicked to perform the following actions: Add Log, Add Logs Directory, Application Detection Wizard, Create Monitor and Settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>More Actions</td>
<td>Contains several shortcuts to different administrative tasks: Create Application, Add Account, Add Task, and View Wizards.</td>
</tr>
<tr>
<td>Get Help Section</td>
<td>The items in this section can be used to get help from the XpoLog support team. Contact us by email (<a href="mailto:support@xplg.com">support@xplg.com</a>), visit our online knowledge base or submit tickets online to get assistance from our team. Presents detailed information of the data displayed in the problems graph. For each member in the Folders and Logs, Application, or Server (according to what you selected), a summary of the analysis is displayed, each relevant to the specified time frame. Submit ticket online, Online knowledge base, Read tutorials, and Send email to XpoLog.</td>
</tr>
</tbody>
</table>

**XpoLog Manager Main Menu**

The Main Menu of the XpoLog Manager console includes the following items:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Actions</td>
<td>This menu enables navigating directly to the following consoles of the Log Manager:</td>
</tr>
<tr>
<td></td>
<td>• Start Page</td>
</tr>
<tr>
<td></td>
<td>• Log Viewer</td>
</tr>
<tr>
<td></td>
<td>• Monitors</td>
</tr>
<tr>
<td>Administration</td>
<td>This menu enables administrators to navigate directly to the following administrative consoles and wizards of the Log Manager:</td>
</tr>
<tr>
<td></td>
<td>• Folders and Logs – a console that presents all the folders and logs defined in XpoLog and enables users to create and/or modify folders and logs.</td>
</tr>
<tr>
<td></td>
<td>• Add Logs Directory – a wizard that enables adding multiple logs that are located under a directory to XpoLog.</td>
</tr>
<tr>
<td></td>
<td>• Add Log – a wizard that enables adding a local or remote log to XpoLog.</td>
</tr>
<tr>
<td></td>
<td>• AppTags – a console that presents all the AppTags defined in XpoLog and allows users to create and/or modify them.</td>
</tr>
<tr>
<td></td>
<td>• Collection Policies – a console that manages the collection policies defined in XpoLog.</td>
</tr>
<tr>
<td></td>
<td>• Cloud – Cloud accounts management.</td>
</tr>
</tbody>
</table>

See Administration Guide

<table>
<thead>
<tr>
<th>Configuration</th>
<th>This menu enables administrators to do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Templates – configure predefined settings for a specific type of log; used to accelerate and automate the configuration process. Templates include the log data pattern, filters, and metadata.</td>
</tr>
<tr>
<td></td>
<td>• Save as Template – enables saving a log as a template.</td>
</tr>
<tr>
<td></td>
<td>• Export Template – enables exporting user defined templates to another instance of XpoLog.</td>
</tr>
<tr>
<td></td>
<td>• Import Template – enables importing user defined templates from another instance of XpoLog.</td>
</tr>
<tr>
<td></td>
<td>• Global Filters – defining global filters that will be available on all logs when opened in the Log Viewer.</td>
</tr>
</tbody>
</table>

See Administration Guide
### Tools

This menu enables performing the following:

- **Export Log** – exports a log from XpoLog
- **Import Log** – imports a log to XpoLog, provided that it was exported with its configuration from XpoLog
- **Export Folder** – exports a folder from XpoLog
- **Import Folder** – imports a folder to XpoLog, provided that it was exported with its configuration from XpoLog
- **Address Book** – presents all the connectivity accounts that are available in XpoLog and enables creating, modifying, or removing the account.
- **Snapshots** – presents all the snapshots that are available in XpoLog and enables viewing, modifying, exporting, and removing snapshots.
- **Tasks** – presents all the tasks (operations that can be executed by XpoLog based on a scheduler) that are available in XpoLog and enables creating, modifying, and removing tasks.
- **System Status** – presents the system status console.

### Settings

This menu enables administrators to open a page to configure the settings for the following:

- **License** – used to update the license of XpoLog
- **Bug Tracking Systems** – contains integration to several Bug tracking systems such as Bugzilla by the Mozilla projects and JIRA by Atlassian
- **Log Viewer** – used to update settings common to all log views
- **Environment Variables** – used to specify variables that can be used all across XpoLog
- **Audit** – used to generate a filtered log view on audited data
- **About** – used to view XpoLog’s version and installed patches

See Administration Guide

### Username

Only displayed in organizations where security is activated.

### Logout button

Only displayed in organizations where security is activated. Clicking this button logs you out of XpoLog Center.

---

### Log Viewer

Any log that has been added to XpoLog (local, remote, Windows machine, remote UNIX machine, database tables, remote XpoLog instances, merged logs, and more) can be viewed, searched, and more in the Log Viewer in realtime.

Once a log is mapped to XpoLog, a simple click on the log presents it in the Log Viewer console.

In the Log Viewer, you can open, view, and investigate multiple logs from multiple remote data sources in different tabs, for an enhanced view of several logs. To view multiple log sources in a single screen you should use the **XpoLog Search**. The Log Viewer is a dedicated view per log source in your browser.

You can specify the number of log records that are displayed in the Log Viewer, and then easily and conveniently browse through the log using the toolbar buttons, to navigate to the next page, previous page, end of log, or beginning of log.

You can also use the Search and Quick Filter features to perform fast searches and quick filters on the log, using specific terms, regular expressions, time range, and more. For more complex searches, you can use a regular filter.

You can also save any filter in the system for later use.

### Opening a Log in the Log Viewer

The Log Viewer can be opened from the homepage, or from the XpoLog console's Log Manager, Folders and Logs menu, or Log Actions menu item.

The system folders and logs that can be opened in the Log Viewer are arranged in the left pane under **Folders and Logs**, according to a hierarchy decided in the organization.

**Note:** A regular log is preceded by a Log icon. A merged log, composed of log records from more than one log, is preceded by a split Log icon (i.e. with a line down the middle). A merged log has a **Source** column as its first column, which contains the name of the source log of the record.

To open the Log Viewer:

1. In the XpoLog homepage,
   - Under **Quick Actions**, click the Log Viewer icon
   - OR
   - Click the **XpoLog** tab, and in the XpoLog console that opens, click one of the following:
     - A log under **Folders and Logs** in the left pane; in this case, the log opens in the Log Viewer; proceed to the end of this procedure.
The Log Viewer icon under Log Manager, and then a log under **Folders and Logs** in the left pane
Log Viewer in the Log Actions menu, and then a log under **Folders and Logs** in the left pane

The Log Viewer opens in the main pane.

The system folders and logs, arranged according to a hierarchy decided in the organization, are displayed in the left pane.

2. In the left pane, under **Folders and Logs**, expand the relevant folder until you reach the lowest level – the Log level, and then click the log that you want to open.

The Log Viewer opens, displaying the selected log in the main pane in tabular view.

After a log is displayed in the Log Viewer, the **Quick Filter**, **Filters**, and **Actions** menus appear in the left pane, for quick filtering, filtering, and performing actions on the log displayed in the Log Viewer.

**Loading Realtime Records into the Log Viewer**

At any time, you can load the last 25 realtime log records into the Log Viewer.

**Note:** The last 25 records are loaded, regardless of the number of records that you selected to display.

To load realtime records:

1. In the status bar, click the **Tail** button.

   The Log Viewer displays the 25 tail records of the log.

   The **Tail** button becomes red.

It is possible to deactivate the tail at any time by clicking the **Stop** button, located in the status bar to the left of the Tail button. In this case, the Tail button reverts to its regular color (gray).

**Maximizing Log Viewer**

Upon opening the Log Viewer, the Log Viewer is displayed in the main pane, and the menu is displayed in the left pane. You can maximize the Log Viewer over the entire width of the screen.

To maximize the Log Viewer:

- In the top-left corner of the Log Viewer, click the **Maximize** button.

  The left pane is hidden, and the Log Viewer is displayed on the entire screen.

  The Maximize button becomes a Minimize button.

**Restoring Log Viewer to Normal View**

You can restore the maximized Log Viewer to its normal view.

To restore the Log Viewer to its normal view:

- In the top-left corner of the Log Viewer, click the **Minimize** button.

  The left pane is open, and the Log Viewer is displayed in the main panel.

  The Minimize button becomes a Maximize button.

**Refreshing the Log Viewer**

At any time, you can refresh the Log Viewer to display the most recent log records. Also, refreshing is required after you change the **Number of Records** value in the toolbar.

To refresh the Log Viewer:

1. In the status bar, click the **Refresh** button.

   The Log Viewer is refreshed with the latest log records, according to the number of records selected in the toolbar.

**Selecting the Log Viewer Display Mode**

You can view the log records in the Log Viewer in either list view or tabular view (default).

To view the log records in list view:

- In the Log Viewer toolbar, click **List View**.

  The log records are listed in the Log Viewer in their raw format.

To view the log records in tabular view:

- In the Log Viewer toolbar, click **Tabular View**.

  A table is presented; its column headers are the field names of the log, and each table row contains the field values of a log record.
Displaying Specific Log Records

A log can have millions of records, and therefore it is not possible to display them all. The Log Viewer enables you to select the number of records that you display in the Log Viewer. You can select to display 25, 50, 100, 250, or 500 log records at a time. You can then use the navigation arrows to display the previous group of records in the log, the first group of records in the log, the next group of records in the log, or the last group of records in the log.

For a simple display, the Log Viewer displays the final number of records that you selected. For a character string search, the selected number is the number of records that are searched from the beginning of the log, and for a quick filter or regular filter, the selected number is the number of records that are filtered from the beginning of the log.

To select the number of log records to display in the Log Viewer:

1. In the navigation area in the toolbar, in the Number of Records textbox, click the down arrow and from the dropdown list that opens, select the number of records to display.
2. In the status bar, click the Refresh button.

The Log Viewer displays the last group of records in the log, consisting of the number of records that you selected.

Displaying the Previous Group of Records

You can display the previous group of records, consisting of the number of records that you selected, provided that the currently displayed records are not at the beginning of the log.

For example, if you selected to display 50 records, and you now click the Previous Records button, the previous 50 records are displayed. To display the previous group of records in the log:

1. In the navigation area in the toolbar, click the Previous Records button.

The previous group of records in the log is displayed, consisting of the number of records that you selected.

Displaying the Next Group of Records

You can display the next group of records, consisting of the number of records that you selected, provided that the currently displayed records are not at the end of the log.

For example, if you selected to display 100 records, and you now click the Next Records button, the next 100 records are displayed. To display the next group of records in the log:

1. In the navigation area in the toolbar, click the Next Records button.

The next group of records in the log is displayed, consisting of the number of records that you selected.

Displaying the First Group of Records

You can display the first group of records, consisting of the number of records that you selected.

For example, if you selected to display 250 records, and you now click the First Records button, the first 250 records in the log are displayed. To display the first group of records in the log:

1. In the navigation area in the toolbar, click the First Records button.

The first group of records in the log is displayed, consisting of the number of records that you selected.

Displaying the Last Group of Records

You can display the last group of records, consisting of the number of records that you selected.

For example, if you selected to display 500 records, and you now click the Last Records button, the last 500 records are displayed. To display the last group of records in the log:

1. In the navigation area in the toolbar, click the Last Records button.

The last group of records in the log is displayed, with the group containing the number of records that you selected.

Quick Find - Searching for Text in Log Records

You can search for any character string in the log records using the Quick Find feature. The search displays in the Log Viewer, the first group of records, consisting of the number of records selected in the toolbar, which has at least one record containing the character string, and highlights the character string in yellow. You can then navigate to the first, last, previous, or next group of records in the log, to view the highlighted character string in other records in the log. For example, searching for "Head" displays the first group of records in the log that contains in at least one of its records the string "Head".

Note: The search is not case sensitive.
To search for text in your log records:

- In the textbox adjacent to the Find button, type the character string to search for, and then click the Find button.
  The text is highlighted in yellow in the first group of records in the log, consisting of the selected number of records.
  A Reset button is displayed near the Find button, enabling you to reset the Log Viewer display to its state before the Find (see Resetting the Log Viewer).

Quick Filtering Log Records

You can filter the log records to display only those records that contain the search string. The XpoLog Manager displays the first records in the log containing the found string, according to the number of records that you selected, and highlights in yellow, the string in each record. It also places a zoom-in icon at the head of each filtered record. For example, searching for "Get" displays the first records in the log containing the string "Get", according to the number of records that you selected.

Note: The search is not case sensitive.

To quick filter log records:

- In the textbox adjacent to the Filter button, type the string to use as filtering criteria, and then click the Filter button.
  Only those records containing the string are displayed, according to the number selected in the dropdown box, and the string is highlighted in yellow in each record.
  A Zoom-in icon is displayed to the left of each record.
  A Reset button is displayed near the Filter button, enabling you to reset the Log Viewer display to its state before the Quick Filter.
  The Quick Filter criteria is saved, and can later be run by selecting it from the Filter Selection dropdown list.

Filtering Log Records

Filtering the log data in order to find specific data format, ID, problem or other pieces of information is crucial in any data mining process. The filtering mechanism allow visual, form type query definition of filtering rules that either search for data in log source or alternatively filter out noise from the view in order to focus on specific data set.

The filter section will explain how to use, create and edit filters. The section will also explain how to browse the log data while filter is actively applied.

Creating a New Filter

You can create a new filter for the log displayed in the Log Viewer, by filling in the parameters in the customized form that XpoLog provides for this log.

A newly created filter is automatically saved in the system, and can be used at a later time, by simply selecting it from a list of saved filters.

To create a new filter:

1. In the Log Viewer toolbar, click the Filter Menu button, and in the menu that appears, click New.
   The Filter definition dialog box opens. A name is automatically generated for the filter.
2. In Name, type a meaningful name for the filter to replace the name automatically generated by the system.
3. Leave the use search engine checkbox selected; this indicates to the filter to use indexing, which expedites the search.
4. In Description, type a meaningful description for the filter.
5. In Query, type a search query using the simple and complex search syntax rules.
6. Under Date and Time, select the Dates limit option to show the log records that arrived before or after a specific date and time, or select the second option (dynamic) to show log records from a period of time relative to the time that the filter is run.
7. Under Text, in the textbox, type a numeric or character string, and from the dropdown list, indicate whether to search for records that equals / not equals (for numeric strings), or contain / not contain (for character strings) the text.
8. Select one of the following checkboxes:
   - match whole word - only highlight words in records that are an exact match to the searched text, and do not highlight words that contain the searched text.
   - case sensitive - only highlight words in records that are the same case as the searched text.
   - regular expression - only highlight regular expressions in the records that match the searched text.
9. Repeat steps 7 and 8 for each search text (up to four).
10. Select one of the following options:
    - search in all columns - to search for the text in all columns of the record
    - search in these columns - to search in specific columns of the record; in this case, select a column to add, and click Add to place it under the Only list.
11. If you want Analytics to regard this filter as a predefined rule, set the severity of the filter rule to Low, Medium, or High. Otherwise, leave none.
12. Click Save.
   The filter is saved and run on the log.

Editing an Existing Filter

You can edit the parameters of an existing filter, as required.

To edit a filter:
1. In the Log Viewer toolbar, click the **Saved Filters** button.

   A list opens, displaying all the saved filters for this log.
2. Select the filter that you want to edit.
3. Click the **Filter Menu** button, and in the menu that appears, click **Edit**.

   The Filter definition dialog box for the selected filter opens.
4. Modify the parameters as required, and then click **Save**.

   The modifications are saved and the filter runs on the log.

**Creating a New Filter from a Combination of Existing Filters**

You can create a new filter with a new name from the combination of existing filters. You must also specify whether records are to be filtered according to the criteria of all the combined filters (AND operation) or any of the filters (OR operation).

To combine filters into a single filter:

1. In the Log Viewer toolbar, click the **Filter Menu** button, and in the menu that appears, click **Multi**.

   The Multi Filter definition dialog box opens. A name is automatically generated for the filter. A list of all the filters existing for this log appears in the **Filters** section under the **Filters** list.
2. In **Name**, type a meaningful name for the filter to replace the name automatically generated by the system.
3. In the **Filters** section, under the **Filters** list, select the filter to include in the new filter, and click **Add**.
   
   The selected filter is placed under the **Filters to use** list.
   
   **Note:** You can remove a filter from the **Filters to use** list, by selecting it and clicking **Remove**.
4. Repeat Step 3 for all filters that you want to include in the combined filter.
5. In **Logical operation between filters**, select **AND** or **OR**.
6. If you want Analytics to regard this filter as a predefined rule, set **Filter Rule Severity** to **Low**, **Medium**, or **High**. Otherwise, leave **None**.
7. Click **Save**.

The filter is saved and run on the log.

**Creating a Filter Based on an Existing Filter**

You can create a filter that is similar to an existing filter, by using the existing filter as a basis for the new one, and then modifying the parameters unique to this filter, as required. This saves you the time of defining the filter from scratch.

To create a filter based on an existing filter:

1. In the Log Viewer toolbar, click the **Saved Filters** button, and in the menu that appears, click **Duplicate**.

   The Filter definition dialog box for the selected filter opens. A name is automatically generated for the duplicate of the filter: **copy of <filter name>**.
2. In **Name**, type a meaningful name for the new filter to replace the automatically generated name.
3. Modify the parameters as required, and then click **Save**.

   The new filter is saved and the filter runs on the log.

**Creating a Filter from the Negation of Existing Filter(s)**

You can create a new filter that displays records resulting from the negation of an existing filter or the combination of existing filters. In the case that the filter is created from the negation of a combination of records, you must specify whether records in the combination are to be filtered according to the criteria of all the combined filters (AND operation) or any of the filters (OR operation). Remember that the negation of \( A \) AND \( B \) is \( \text{NOT} A \text{ OR NOT} B \), and that the negation of \( A \text{ OR} B \) is \( \text{NOT} A \text{ AND NOT} B \).

To create a filter that is the negation of existing filter(s):

1. In the Log Viewer toolbar, click the **Filter Menu** button, and in the menu that appears, click **Negate**.

   The Multi Filter definition dialog box opens. A name is automatically generated for the filter. A list of all the filters existing for this log appears in the **Filters** section under the **Filters** list.
2. In **Name**, type a meaningful name for the filter to replace the name automatically generated by the system.
3. In the **Filters** section, under the **Filters** list, select the filter to include in the new filter, and click **Add**.
   
   Note: You can remove a filter from the **Filters to use** list, by selecting it and clicking **Remove**.
4. Repeat Step 3 for all filters that you want to include in the combined filter.
5. In **Logical operation between filters**, select **AND** or **OR**.
6. If you want Analytics to regard this filter as a predefined rule, set **Filter Rule Severity** to **Low**, **Medium**, or **High**. Otherwise, leave **None**.
7. Click **Save**.
The filter is saved and run on the log.

**Removing a Filter**

You can remove a filter from the list of saved filters of a log.

To remove a filter:

1. In the Log Viewer toolbar, click the **Saved Filters** button.
   
   A list opens, displaying all the saved filters for this log.
2. Select the filter that you want to remove.
3. Click the **Filter Menu** button, and in the list that appears, click **Remove**.

The Saved Filters list is refreshed, and no longer includes the removed filter.

**Running a Saved Filter**

All filters that have been created for a log are saved in the system and can be quickly accessed and run from the Log Viewer toolbar.

**Note:** (G) preceding a filter name indicates that it is a global filter, as defined in Configuration > Global Filters (see Administrator's Guide).

To run a saved filter:

1. In the Log Viewer toolbar, click the **Saved Filters** button.
   
   A list opens, displaying all the saved filters for this log.
2. Select the filter that you want to run, and then click the **Go** button.
   
   The selected filter is run on the log, and the results are displayed in the Log Viewer.
   
   The status bar indicates the number of records that were filtered, and the filtering time.

**Zooming Into a Filtered Record**

Log Viewer facilitates troubleshooting to find the cause of an event, by enabling you to zoom into any filtered log record to see the log records preceding and following it. Zooming into a filtered record displays an equal number of records preceding and following the zoomed in record, with the total number of displayed records equivalent to the number selected in the toolbar. For example, if you select to display 25 records in the Log Viewer, zooming into a filtered record displays 12 records before and 12 records after, and emphasizes the zoomed-in record in boldface.

To zoom into a filtered log record:

- Click the **Zoom-In** icon at the head of the filtered record which you want to zoom into.

The Log Viewer displays the log records preceding and following the zoomed-in record, and emphasizes the selected record in boldface.

**Zooming Out of a Record**

After zooming into a filtered record, you can zoom out of the record to return to the previous log viewer state.

To zoom out of a filtered log record:

- In the Log Viewer toolbar, click the **Zoom-Out** or **Back** button.

The Log Viewer is restored to its previous state.

**Resetting the Log Viewer**

After performing a search, quick filter, or filter on the Log Viewer, a Reset button appears in the toolbar, enabling you to reset the Log Viewer to its state prior to the performed action.

To reset the Log Viewer:

- In the Log Viewer toolbar, click the **Reset** button.

The Log Viewer presents the records that were displayed prior to the action that was performed on it.

**Interrupting a Process**

You can interrupt any process running on the log in your Log Viewer, such as a search, quick filter, or regular filter.

To stop a process:

1. In the status bar, click the **Stop** button.

The process is interrupted.

**Performing Actions on a Log**

Actions can be performed on a log displayed in the Log Viewer from the **Actions** menu in the left pane and from the right-click menu of log record(s).
Actions can also be performed on any log in the system displayed in the left pane under **Folders and Logs** from the right-click menu of a log.

The following table lists the log actions, how they can be accessed, and a link to the topic that explains the procedures in full detail.

<table>
<thead>
<tr>
<th>Log Action</th>
<th>Perform Action From ...</th>
<th>Explained in ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate</td>
<td>Right-click menu of a log under <strong>Folders and Logs</strong> in the left pane</td>
<td>See Administrator’s Guide.</td>
</tr>
<tr>
<td>Edit</td>
<td>Right-click menu of a log under <strong>Folders and Logs</strong> in the left pane</td>
<td>See Administrator’s Guide.</td>
</tr>
<tr>
<td>Remove</td>
<td>Right-click menu of a log under <strong>Folders and Logs</strong> in the left pane</td>
<td>See Administrator’s Guide.</td>
</tr>
<tr>
<td>Export</td>
<td><strong>Actions</strong> menu in the left pane of the Log Viewer</td>
<td>Exporting a Log</td>
</tr>
<tr>
<td>Add Monitor</td>
<td>Right-click menu of a log under <strong>Folders and Logs</strong> in the left pane</td>
<td>Log Monitor</td>
</tr>
<tr>
<td>Save as Template</td>
<td><strong>Actions</strong> menu in the left pane of the Log Viewer</td>
<td>Saving a Log as a Template</td>
</tr>
<tr>
<td>Copy</td>
<td>Right-click menu of selected log record(s) displayed in the Log Viewer</td>
<td>Copying Log Record(s)</td>
</tr>
<tr>
<td>Open a bug in Bugzilla</td>
<td>Note: This action is available only if Bugzilla has been configured in Settings &gt; Bug Tracking Systems.</td>
<td>Sending Log Bugs to a Bug Tracking System</td>
</tr>
<tr>
<td>Publish an issue in JIRA</td>
<td>Note: This action is available only if JIRA has been configured in Settings &gt; Bug Tracking Systems.</td>
<td>Sending Log Bugs to a Bug Tracking System</td>
</tr>
<tr>
<td>Find</td>
<td>Right-click menu of a selected log record field displayed in the Log Viewer</td>
<td>Finding Occurrences of a Log Record Field Value</td>
</tr>
<tr>
<td>Filter</td>
<td>Right-click menu of a selected log record field displayed in the Log Viewer</td>
<td>Filtering Records According to Record Field Value</td>
</tr>
<tr>
<td>Filter in... Filter date in...</td>
<td>Right-click menu of a selected log record field displayed in the Log Viewer</td>
<td>Filtering a Merged Log for a Log Viewer Record Value</td>
</tr>
<tr>
<td>Search</td>
<td>Right-click menu of a selected log record field displayed in the Log Viewer</td>
<td>Searching for a Log Record Field Value in a Search Engine</td>
</tr>
<tr>
<td>Add Snapshot OR Add to &lt;snapshot name&gt; and Select Snapshot</td>
<td>Right-click menu of selected log record(s) displayed in the Log Viewer</td>
<td>Adding Log Records to a Snapshot</td>
</tr>
<tr>
<td>Customize</td>
<td><strong>Actions</strong> menu in the left pane of the Log Viewer</td>
<td>See Administrator’s Guide.</td>
</tr>
<tr>
<td>Print</td>
<td><strong>Actions</strong> menu in the left pane of the Log Viewer</td>
<td>Printing the Log Viewer Records</td>
</tr>
<tr>
<td>Create Monitor</td>
<td><strong>Actions</strong> menu in the left pane of the Log Viewer</td>
<td>Log Monitor</td>
</tr>
</tbody>
</table>

**Selecting Multiple Log Viewer Records**

You can select multiple Log Viewer records (log or snapshot records), and then right-click the records to perform an action on all the selected records at once. You can either select a group of consecutive log records, or records displayed anywhere on the Log Viewer screen.
To select multiple consecutive Log Viewer records:

- In the Log Viewer, click the first record, press and hold down **SHIFT**, and then click the last record.
  All the records between the first and last clicked record inclusive, are selected.

**Note:** You can also press and hold down **SHIFT** and then click a record, to select all records preceding and including the selected record in the Log Viewer screen.

To select multiple Log Viewer records:

- In the Log Viewer, for each record that you want to select, click **Ctrl** and then click the record to select.

**Note:** You can deselect any selected record, by clicking **Ctrl** and clicking the record.

**Copying Log Record(s)**

You can copy a single or multiple log records.

You can then paste the copied record(s) in any document, email, and more, using standard Paste methods (i.e. by right-clicking the mouse and then selecting **Paste**, or by pressing **Ctrl V** on your keyboard).

To copy a log record:

- In the Log Viewer, right-click a log record, and from the menu that appears, click **Copy**.
  The record is copied to the clipboard.

To copy multiple log records:

- In the Log Viewer, select multiple log records (see Selecting Multiple Log Viewer Records), right-click the selected records, and from the menu that appears, click **Copy**.
  The records are copied to the clipboard.

**Note:** The Copy feature is currently operational in Internet Explorer only.

**Exporting a Log**

XpoLog enables you to export the log displayed in the Log Viewer either from the **Actions** menu in the left pane or from **Tools > Export Log** in the main menu. You can also export any log (not necessarily the one displayed in the Log Viewer) from the right-click menu of a log under the **Folders and Logs** menu in the left pane. You can either export the log 'with its configuration, i.e. in the format in which it is displayed in the Log Viewer so that it can be easily imported into the Log Viewer at a later time, or you can export the log data after transforming it into another format (XML, CSV, Tab Delimited, Raw data, or SQL Database Table).

To export a log:

1. Open a log in the Log Viewer (see Opening a Log in the Log Viewer), and in the Log Viewer left pane, open the **Actions** menu, and click **Export** or in the main menu, in the **Tools** menu item, click **Export Log**.
   Alternately, in the Log Viewer left pane, under the **Folders and Logs** menu, right-click a log, and click **Export**.
   The Export Log page opens.

2. Select one of the following options:
   - **Export the log together with its configuration, to enable future import**
   - **Only transform the current data to the following type,** and select from the dropdown list, one of the following types: **XML, CSV, Tab Delimited, Raw data, or SQL Database Table**

3. Click **export**.
   If a database account is not available for the file type selected, the System Notification page opens, with the notification: **No databases accounts available. Please define accounts first.** In this case, click **OK**, define an account, and then perform the export.
   Otherwise, the zip log status page opens with the notification: **The zip was created successfully**, and the File Download dialog box also opens. In the File Download dialog box, click **Save**.

4. In the **Save as** dialog box that opens, select the **Save in** location and type the **file name** of the zipped file, and then click **Save**.
   The file is downloaded to the selected location.

5. In the Zip log status page, click the **back to log viewer** link.
   The Log Viewer opens, displaying the last log or snapshot that was downloaded there (and not necessarily the one that you exported).

**Printing the Log Viewer Records**

You can print in tabular format all or selected records currently displayed in the Log Viewer.

**Printing All Records Displayed in the Log Viewer**

To print all records currently displayed in the Log Viewer:

1. In the Log Viewer left pane, open the **Actions** menu, and select **Print**.
   A Web page opens with the Log Viewer records arranged in tabular format. The Print options dialog box is also displayed.

2. Select the relevant print options and then click **Print**.
   The Web page is printed to the selected destination.
Printing Selected Record(s) Displayed in the Log Viewer

To print selected record(s) currently displayed in the Log Viewer:

1. Open a log or snapshot in the Log Viewer (see Opening a Log in the Log Viewer), click a single record or multiple records (see Selecting Multiple Log Viewer Records), and right-click.
2. In the right-click menu that opens, click Print. A Web page opens with the selected Log Viewer record(s) arranged in tabular format. The Print options dialog box is also displayed.
3. Select the relevant print options and then click Print. The Web page is printed to the selected destination.

Finding Occurrences of a Log Record Field Value

From a selected Log Viewer record, you can quickly and easily find all the occurrences of one of its field values, in all the records of the log displayed in the Log Viewer. This is similar to the Quick Find (see Quick Find - Searching for Text in Log Records).

To find occurrences of a field value:

- In the Log Viewer, right-click the field value that you want to find in all records of the log, and in the menu that appears, click Find. The field value is displayed in the box adjacent to the Find textbox. The search text is highlighted in yellow in all records in the Log Viewer.

Adding Log Records to a Snapshot

You can add log records to an existing snapshot, or to a new snapshot that you create. These snapshots can assist you in your workflow and in troubleshooting.

Adding Log Records to a New Snapshot

To add log records to a new snapshot:

1. In the Log Viewer, select a single record or multiple records (see Selecting Multiple Log Viewer Records) to place in the snapshot, and then right-click.
   - If there are no snapshots defined in the system, the menu displays the Add Snapshot option. Proceed as described in Creating the First Snapshot in the System.
   - If there is at least one snapshot already defined in the system, the menu displays the Select Snapshot option. Proceed as described in Adding Snapshots to the Snapshot Library.

Adding Log Records to a Recent Snapshot

To add log records to the most recently added to snapshot:

1. In the Log Viewer, select a single record or multiple records (see Selecting Multiple Log Viewer Records) to place in the snapshot, and then right-click.
2. From the right-click menu, click Add to <name of most recently added to snapshot>. The selected log records are added to the snapshot.

Adding Log Records to the Snapshot of Your Choice

To add log records to the snapshot of your choice:

1. In the Log Viewer, select a single record or multiple records (see Selecting Multiple Log Viewer Records), and then right-click.
2. From the right-click menu, click Select Snapshot. The Select Snapshot dialog box is displayed.
3. From the list of snapshots, select the snapshot to which to add the log records, and then click Apply. Note: If you have many snapshots defined in the system, you can filter the snapshot list according to the name of the snapshot. Typing more characters in the Name Filter field of the filter, minimizes the number of selectable snapshots appearing in the list.

   The selected log records are added to the snapshot. If the snapshot already contains records from another log, a Security record is added to the snapshot.

Searching for a Log Record Field Value in a Search Engine

XpoLog enables searching for a log record field value in XpoSearch (see Searching for a Field Value in XpoSearch), or in external search engines, such as the defaults – Google and Java Docs (see Searching for a Field Value in Google and Searching for an Error in Java Docs). The search can also be conducted in additional external search engines, as set in Settings > Log Viewer (see Administrator's Guide).

Searching for a Field Value in Google

You can look up an XpoLog record filed value in an external search engine, such as Google, to find out more about it. To search for a field value in Google:
1. In the Log Viewer, select a log record, and right-click the field value which you want to search for.
   The right-click menu opens.
2. In the right-click menu, click **Search > Google**.
   Google opens in a separate webpage with the results of running the search for the selected field value (displayed in the Google search box).

**Searching for a Field Value in XpoSearch**

You can run XpoSearch to search for occurrences of a log record field value in other records in the log, directly from the Log Viewer. You can do this by right-clicking the field value in the record in the Log Viewer, and selecting **Search > XpoSearch**.

To search for a field value in other log records:

1. In the Log Viewer, select a log record, and right-click the field value which you want to search for.
   The right-click menu opens.
2. In the right-click menu, select **Search > XpoSearch**.
   XpoSearch opens in a separate webpage, with a search running for the selected field value (displayed in the search query). After the search is completed, all log records with the searched for field value are displayed in the results.

**Searching for an Error in Java Docs**

You may notice a Java error in a record of your log. XpoLog enables you to look up this error in the Java Docs online documentation directly from the Log Viewer. All you have to do is right-click the Java error in the log field that you want to look up, select **Search > JDocs**, and a Java Docs webpage opens with the results of the Java Docs search engine look-up of the selected term.

To search for an error in Java Docs:

1. In the Log Viewer, select a log record, and right-click the field value (Java error), which you want to look up in Java Docs.
   The right-click menu opens.
2. In the right-click menu, click **Search > JDocs**.
   The Java Docs webpage opens, running a search for the log term in Java Docs.

**Sending Log Bugs to a Bug Tracking System**

XpoLog provides integration to several bug tracking systems, such as Bugzilla by Mozilla, and JIRA by Atlassian.

XpoLog enables you to submit a bug or issue from single or multiple log records displayed in the Log Viewer, directly into a bug tracking system, provided that you have defined the bug tracking system in **Settings > Bug Tracking Systems**.

**Opening a Bug in Bugzilla**

You can investigate a bug that you see in a log, by sending single or multiple records to the Bugzilla bug tracking system.

**To open a bug in Bugzilla based on log record(s):**

1. In the Log Viewer, select a single log record or multiple log records (see **Selecting Multiple Log Viewer Records**), and then right-click.
2. In the right-click menu that appears, click **Open a bug in Bugzilla**.
   The Add a Bug notification box appears to inform you that it is loading information into Bugzilla, and then the Bugzilla Login page appears.
3. In the Bugzilla Login page, type your **Username** and **Password**, and click **Login**.
   Bugzilla opens, and investigates the bug loaded from the log record(s).

**Publishing an Issue in JIRA**

You can investigate an issue that you see in a log, by sending single or multiple log records to the JIRA issue tracking system.

**To publish an issue in JIRA based on log record(s):**

1. In the Log Viewer, select a single log record or multiple log records (see **Selecting Multiple Log Viewer Records**), and then right-click.
2. In the right-click menu, click **Publish an issue in JIRA**.
   The Add a Bug notification box appears to inform you that it is loading information into JIRA, and then the JIRA Login page appears.
3. In the JIRA Login page, type your **Username** and **Password**, and click **Login**.
   JIRA opens, and investigates the bug loaded from the log record(s).

**Filtering Records According to Record Field Value**

You can filter all the records displayed in the Log Viewer, according to the selected field value of a record. For example, right-clicking the **Process Id** field value of 1506 in Syslog, and clicking **Filter**, displays all records containing 1506 in the **Process Id** field, and highlights the value in the filtered records.

To filter records according to a record field value:

- In the Log Viewer, right-click the field value according to which you want to filter all records of the log, and in the menu that appears, click **Filter**.
  The filter value is displayed in the box adjacent to the GO button.
The records having the selected value appear in the Log Viewer, with the filtering criteria highlighted in yellow in each record in the Log Viewer.

**Running a Composite Filter**

Once you have run a filter on records in the Log Viewer, the Composite Filter feature becomes available for running a filter on two or more fields of a record. The composite filter enables specifying whether the filtered records should contain all field values (AND) or at least one field value (OR). For example, right-clicking the **Process Name** field value of `popa3d` in a record resulting from the filtering example above, and clicking **Composite Filter > AND** displays all records from the log file that contain both 1506 in the **Process Id** and `popa3d` in the **Process Name** field, whereas clicking **Composite Filter > OR** displays all records from the log file that either contain 1506 in the **Process Id** field or `popa3d` in the **Process Name** field.

To run a composite filter according to a record's field values:

1. In the Log Viewer, right-click the field value according to which you want to run the composite filter, and in the menu that appears, click **Composite Filter > AND** or **Composite Filter > OR**.
   - The composite filter is displayed in the box adjacent to the GO button.
   - The records having the selected value appear in the Log Viewer, with the filtering criteria highlighted in yellow in each record in the Log Viewer.

**Filtering a Merged Log for a Log Viewer Record Value**

You can filter a merged log according to the value of a date or non-date field of a record in the Log Viewer. Right-clicking a field value in a record, displays in the right-click menu either **Filter in** for a non-date value, or **Filter in date** for a non-date value.

To filter a merged log:

1. In the Log Viewer, right-click a field value in a record, and click **Filter in** or **Filter in date** (depending on whether the right-clicked value is a date or non-date value).
   - The Select Log(s) to Filter dialog box displays a logs selection tree.
2. In the logs selection tree, select the checkboxes of the logs on which to run the filter, and then click the **View** button.
   - An ‘on the fly’ merged file containing the records filtered from the selected logs according to the clicked field value, is displayed in the Log Viewer, with the filtering criteria highlighted in yellow.

**Log Monitor**

In Log Monitor, XpoLog enables you to create rule(s) to monitor any log in the system. In Log Monitor, you define parameters and rules, the scheduling of the monitor, and the alerts that are to be sent if matching events (that meet the defined rules) are detected.

These defined monitors are automatically run on the specified logs at the predefined scheduled times, with XpoLog's advanced monitoring engine searching in the log for events that match the defined rules. The Monitor sends alerts to notify users of events in the log that match the defined rules. You can define that the monitor send the alerts from any of a wide range of available alerts - Email, SNMP trap, JMS message, Script, and more. The Monitors can add to an alert that it sends, the matching log events with the detected errors.

You can also create a complex monitoring mechanism by creating multiple Monitors that are executed together and report on failures in the logs.

Please see the Administration Guide for details.

**Snapshot Management**

XpoLog enables you to capture a set of log records into a snapshot. These snapshots can be used during your workflow and assist you in troubleshooting and in future analysis.

Snapshots defined in the system are global, and can include records from various logs in the system. This means that you can add log records displayed in the Log Viewer to a new snapshot or to an already existing snapshot (see Adding Log Records to a Snapshot).

Once a snapshot is defined in the system, you can access the management options from the **Tools > Snapshots** menu, from the right-click menu of a snapshot under the **Snapshots** menu in the left pane, or from the right-click menu of selected snapshot record(s) in the Log Viewer.

The following table lists the snapshot actions, how they can be accessed, and a link to the topic that explains the procedures in full detail.

<table>
<thead>
<tr>
<th>Snapshot Action</th>
<th>Perform Action From ...</th>
<th>Explained in ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Right-click menu of a snapshot under the <strong>Snapshots</strong> menu in the left pane</td>
<td>Viewing a Snapshot</td>
</tr>
<tr>
<td></td>
<td>From the <strong>View</strong> button in the main menu <strong>Tools &gt; Snapshots</strong> item</td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>Right-click menu of a snapshot under the <strong>Snapshots</strong> menu in the left pane</td>
<td>Editing a Snapshot Definition</td>
</tr>
<tr>
<td></td>
<td>From the <strong>Edit</strong> button in the main menu <strong>Tools &gt; Snapshots</strong> item</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Right-click menu of selected snapshot record(s) displayed in the Log Viewer</td>
<td></td>
</tr>
</tbody>
</table>
### Creating a Snapshot

You can create a snapshot by selecting at least one record in the Log Viewer pane, and then selecting either of the two options:

- **Add Snapshot** – only appears in the menu if no snapshots exist in the system. Follow the procedure in Creating the First Snapshot in the System.

---

<table>
<thead>
<tr>
<th>Right-click menu of a snapshot under the Snapshots menu in the left pane</th>
<th>Removing a Snapshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Delete button in the main menu Tools &gt; Snapshots item</td>
<td>Removing a Snapshot</td>
</tr>
<tr>
<td>Right-click menu of a snapshot under the Snapshots menu in the left pane</td>
<td>Exporting a Snapshot</td>
</tr>
<tr>
<td>From the Export button in the main menu Tools &gt; Snapshots item</td>
<td>Exporting a Snapshot</td>
</tr>
<tr>
<td>Right-click menu of log record(s) displayed in the Log Viewer</td>
<td>Copying a Snapshot's Contents</td>
</tr>
<tr>
<td>Right-click menu of a snapshot under the Snapshots menu in the left pane</td>
<td>Copying a Snapshot's Contents</td>
</tr>
<tr>
<td>Right-click menu of selected snapshot record(s) displayed in the Log Viewer</td>
<td>Copying a Snapshot's Contents</td>
</tr>
<tr>
<td>Right-click menu of a snapshot under the Snapshots menu in the left pane</td>
<td>Copying a Snapshot Link</td>
</tr>
<tr>
<td>Right-click menu of selected snapshot record(s) displayed in the Log Viewer</td>
<td>Copying a Snapshot Link</td>
</tr>
<tr>
<td>Right-click menu of a snapshot under the Snapshots menu in the left pane</td>
<td>Sending Snapshot Bugs to a Bug Tracking System</td>
</tr>
<tr>
<td>Right-click menu of selected snapshot record(s) displayed in the Log Viewer</td>
<td>Sending Snapshot Bugs to a Bug Tracking System</td>
</tr>
<tr>
<td>Right-click menu of a selected snapshot record field displayed in the Log Viewer</td>
<td>Finding Occurrences of a Log Record Field Value</td>
</tr>
<tr>
<td>Right-click menu of a selected snapshot record field displayed in the Log Viewer</td>
<td>Filtering Records According to Record Field Value</td>
</tr>
<tr>
<td>Right-click menu of a selected snapshot record field displayed in the Log Viewer</td>
<td>Filtering a Merged Log for a Log Viewer Record Value</td>
</tr>
<tr>
<td>Right-click menu of a selected snapshot record field displayed in the Log Viewer</td>
<td>Searching for a Snapshot Record Field Value in a Search Engine</td>
</tr>
<tr>
<td>Right-click menu of selected snapshot record(s) displayed in the Log Viewer</td>
<td>Removing Record(s) From a Snapshot</td>
</tr>
<tr>
<td>Right-click menu of selected snapshot record(s) displayed in the Log Viewer</td>
<td>See Administrator's Guide.</td>
</tr>
<tr>
<td>Right-click menu of selected snapshot record(s) displayed in the Log Viewer</td>
<td>Printing Snapshot Record(s)</td>
</tr>
</tbody>
</table>
Adding Snapshots to the Snapshot Library

Perform the following procedure to add a snapshot to the library of already existing snapshots in the system.

To add a snapshot to the library of snapshots:

1. In the Log Viewer, while pressing Ctrl on the keyboard, select the log records that you want to add to a snapshot, and then right-click.
2. From the right-click menu, select Select Snapshot.
   The Select Snapshot dialog box opens.
3. In the Select Snapshot dialog box, click the Create New button.
   The Create Snapshot dialog box opens.
4. In the Create Snapshot dialog box, type a Name and Description for the snapshot, and then click Save.
   The newly created snapshot appears on the top of the Snapshots list in the left pane.

Creating the First Snapshot in the System

Perform the following procedure to create the first snapshot in the system.

To create the first snapshot:

1. In the Log Viewer, while pressing Ctrl on the keyboard, select the log records that you want to add to a snapshot, and then right-click.
2. From the right-click menu, select Add Snapshot.
   The Create Snapshot dialog box opens.
3. In the Create Snapshot dialog box, type a Name and Description for the snapshot, and then click Save.
   The newly created snapshot appears under Snapshots in the left pane.

Accessing the Snapshot Management Options

You can manage a snapshot either from the Tools > Snapshots menu, or from the right-click menu of a snapshot under the Snapshots menu in the left pane. You can also modify the contents of a snapshot and perform other management options from the right-click menu of a snapshot record displayed in the Log Viewer.

Note: From the Tools > Snapshots menu, you can view, edit, delete, or export a snapshot. From the Snapshots menu, you can also copy a snapshot link or copy a snapshot's contents.

Accessing the Snapshot Management Options from the Snapshots Menu

To access the snapshot management options:

1. In the left pane, open the Snapshots menu.
   The snapshots defined in the system are displayed.
2. Right-click a snapshot.
   The right-click menu displays the actions that can be performed on the snapshot: View, Edit, Remove, Export, Copy to Clipboard, and Copy snapshot link. The actions Open a bug in Bugzilla and Publish an issue in JIRA are also available, provided that they have been configured in Settings > Bug Tracking Systems.

Accessing the Snapshot Management Options from the Tools Menu

To access the snapshot management options:

1. In the menu bar, select Tools > Snapshots.
   The Snapshots page opens, with a list of snapshots defined in the system.
2. Select a snapshot from the list.
   The following buttons are enabled for performing actions on the snapshot: Edit, Delete, View, and Export.

   Note: If you have many snapshots defined in the system, you can filter the snapshot list according to the name and/or description of the snapshot. Typing more characters in the Name and Description fields of the filter, minimizes the number of selectable snapshots appearing in the list.

Accessing the Snapshot Management Options from the Log Viewer

To access the snapshot management options from the Log Viewer:

1. In the left pane, open the Snapshots menu, and in the right-click menu of a snapshot, click View.
   The snapshot is displayed in the Log Viewer.
2. Right-click a snapshot record.
   The right-click menu displays the actions that can be performed on the snapshot and on the snapshot record: Copy, Find, Filter, Filter date in, Search, Copy Snapshot Link, Remove from Snapshot, Customize, Export, and Print. The actions Open a bug in Bugzilla and Publish an issue in JIRA are also available, provided that they have been configured in Settings > Bug Tracking Systems.

Viewing a Snapshot

You can view the contents of any snapshot in the system, either from the Tools > Snapshots menu, or from the right-click menu of a snapshot under the Snapshots menu in the left pane. A snapshot that contains log records from more than one log, contains a Security record.
**Viewing Snapshot Contents**

To view the contents of a snapshot:

- In the left pane, under the **Snapshots** menu, right-click a snapshot, and in the menu that appears, click **View**.
- OR
- Under the **Snapshots** menu, click a snapshot.
- OR
- In the **Tools > Snapshots** menu, select a Snapshot and then click the **View** button.

The snapshot is displayed in the Log Viewer.

**Editing a Snapshot Definition**

You can rename a snapshot or modify its definition, either from the **Tools > Snapshots** menu bar item, or from the right-click menu of a snapshot under the **Snapshots** menu in the left pane.

**Editing a Snapshot Definition**

To edit a snapshot:

1. In the left pane, under the **Snapshots** menu, right-click a snapshot, and in the menu that appears, click **Edit**.
   - OR
   - In the **Tools > Snapshots** menu, select a Snapshot and then click the **Edit** button.

   The Edit Snapshot dialog box opens.

2. In the Edit Snapshot dialog box, modify the **Name** and/or **Description**, and then click the **Apply** button.

   The snapshot definition is updated.

**Removing a Snapshot**

You can remove from the system any snapshot, which you no longer require, either from the **Tools > Snapshots** menu, or from the right-click menu of a snapshot under the **Snapshots** menu in the left pane.

To remove a snapshot:

1. In the left pane, under the **Snapshots** menu, right-click a snapshot, and in the menu that appears, click **Remove**.
   - OR
   - In the **Tools > Snapshots** menu, select a Snapshot and then click the **Delete** button.

   A delete confirmation dialog box opens.

2. Click **Yes**.

   The snapshot is removed from the system and no longer appears under the Snapshots menu.

**Exporting a Snapshot**

XpoLog enables you to export any snapshot defined in XpoLog after transforming it into another format (XML, CSV, Tab Delimited, Raw data, or SQL Database Table).

Export can be performed either from **Tools > Snapshots** in the main menu, from the right-click menu of a snapshot under the **Snapshots** menu in the left pane, or from the right-click menu of the snapshot displayed in the Log Viewer.

To export a snapshot:

1. In the Log Viewer left pane, under **Snapshots**, right-click the snapshot that you want to export, and click **Export**.
   - OR
   - In the main menu, select **Tools > Snapshots**, and in the dialog box that opens, select the snapshot, and then click the **Export** button.

   Open the Snapshot in the Log Viewer, and in the right-click menu, click **Export**.

   **Note:** It is also possible to open the snapshot in the Log Viewer, and then proceed to export it as a regular log file (see **Exporting a Log**). The Export Log dialog box is displayed.

2. Select the **Only transform the current data to the following type** option, and then select from the dropdown list, one of the following types: XML, CSV, Tab Delimited, Raw data, or SQL Database Table.

3. Click **export**.

   If a database account is not available for the file type selected, the System Notification page opens, with the notification: **No databases accounts available. Please define accounts first.** In this case, click **OK**, define an account, and then perform the export.

   Otherwise, the zip log status page opens with the notification: **The zip was created successfully**, and the File Download dialog box also opens.

4. In the File Download dialog box, click **Save**.

5. In the **Save as** dialog box that opens, select the **Save in** location and type the **file name** of the zipped file, and then click **Save**.

   The file is downloaded to the selected location.

6. In the Zip log status page, click the **back to log viewer** link.

   The Log Viewer opens, displaying the last log or snapshot that was downloaded there (and not necessarily the one that you exported).

**Copying Snapshot Record(s)**

You can copy all the records in a snapshot to your clipboard. You can also copy a single or multiple snapshot record(s) from the right-click menu of the selected snapshot record(s) in the Log Viewer.

After copying, you can paste the copied snapshot contents in any document, email, and more, using standard Paste methods (i.e. by right-clicking...
the mouse and then selecting Paste, or by pressing Ctrl V on your keyboard).

**Copying Entire Snapshot Content**

To copy a snapshot's contents:

- In the left pane, under the Snapshots menu, right-click a snapshot, and in the menu that appears, click Copy to Clipboard. The snapshot's records are copied to the clipboard.

**Copying Selected Snapshot Record(s)**

To copy a snapshot's record(s):

1. Open a snapshot in the Log Viewer (see Viewing a Snapshot), and select a single record or multiple records (see Selecting Multiple Log Viewer Records).
2. Right-click the record(s), and in the menu that appears, click Copy. The selected snapshot record(s) are copied to the clipboard.

**Copying a Snapshot Link**

You can copy the link to any snapshot from the Snapshots menu in the left panel or from the snapshot records displayed in the Log Viewer.

You can then paste the copied snapshot link into your browser, using standard Paste methods (i.e. by right-clicking the mouse and then selecting Paste, or by pressing Ctrl V on your keyboard), and navigate to the Log Viewer to view the snapshot.

To copy the link to a snapshot:

1. In the left pane, under Snapshots, do one of the following:
   - Right-click a snapshot, and in the menu that appears, click Copy snapshot link
   - OR
   - Select a snapshot, right-click in the snapshot records that appear in the Log Viewer, and in the menu that appears, click Copy snapshot link.
   - In the right-click menu of the snapshot, click Copy snapshot link.
   - The snapshot link is copied to your clipboard.

**Removing Record(s) From a Snapshot**

You can remove a single or multiple records from a snapshot.

To remove record(s) from a snapshot:

1. Open a snapshot in the Log Viewer (see Viewing a Snapshot), and select a single record or multiple records (see Selecting Multiple Log Viewer Records) that you want to remove from the snapshot.
2. Right-click the record(s), and in the menu that appears, click Remove from Snapshot.
   - The selected record(s) are removed from the snapshot.

**Sending Snapshot Bugs to a Bug Tracking System**

XpoLog provides integration to several bug tracking systems, such as Bugzilla by Mozilla, and JIRA by Atlassian.

XpoLog enables you to submit a bug or issue from a selected snapshot, or single or multiple records in a snapshot, directly into a bug tracking system, provided that you have defined the bug tracking system in Settings > Bug Tracking Systems.

**Opening a Bug in Bugzilla**

You can investigate a bug that you see in a snapshot, by sending the entire snapshot, or a single or multiple records, to the Bugzilla bug tracking system.

To open a bug in Bugzilla based on a snapshot:

1. In the left pane, under the Snapshots menu, right-click a snapshot, and click Open a bug in Bugzilla.
   - The Add a Bug notification box appears to inform you that it is loading information into Bugzilla, and then the Bugzilla Login page appears.
2. In the Bugzilla Login page, type your Username and Password, and click Login.
   - Bugzilla opens, and investigates the bug loaded from the snapshot.

To open a bug in Bugzilla based on snapshot record(s):

1. In the Log Viewer, select a single snapshot record, or multiple records (see Selecting Multiple Log Viewer Records), and then right-click.
2. In the right-click menu that appears, click Open a bug in Bugzilla.
   - The Add a Bug notification box appears to inform you that it is loading information into Bugzilla, and then the Bugzilla Login page appears.
3. In the Bugzilla Login page, type your Username and Password, and click Login.
   - Bugzilla opens, and investigates the bug loaded from the snapshot record(s).
Publishing an Issue in JIRA

You can investigate an issue that you see in a snapshot, by sending the entire snapshot, or a single or multiple records to the JIRA issue tracking system.

To publish an issue in JIRA based on a snapshot:

1. In the left pane, under the Snapshots menu, right-click a snapshot, and click Publish an issue in JIRA.
   The Add a Bug notification box appears to inform you that it is loading information into JIRA, and then the JIRA Login page appears.
2. In the JIRA Login page, type your Username and Password, and click Login.
   JIRA opens, and investigates the issue loaded from the snapshot.

To publish an issue in JIRA based on snapshot record(s):

1. In the Log Viewer, select a snapshot record, or multiple snapshot records (see Selecting Multiple Log Viewer Records), and then right-click.
2. In the right-click menu, click Publish an issue in JIRA.
   The Add a Bug notification box appears to inform you that it is loading information into JIRA, and then the JIRA Login page appears.
3. In the JIRA Login page, type your Username and Password, and click Login.
   JIRA opens, and investigates the bug loaded from the snapshot record(s).

Troubleshooting XpoLog

The following helpful ways can be used to troubleshoot XpoLog in order to identify problems with the installation, configuration, and operations status.

- **XpoLog System Status console** – XpoLog contains an internal monitoring mechanism, which sends different alerts to the system administrator(s) on the system's health. There are several sections which present the current statuses of managed data, utilized storage, memory, and more.
- **XpoLog Support portal** – XpoLog contains a comprehensive portal that helps administrators view system logs, manage information, and fine-tune XpoLog.
- **XpoLog System logs** - Information regarding XpoLog logs including all system back end information as well as users activity (audit).
- **Common Scenarios** - Information regarding some scenarios in which XpoLog is not reachable that should be checked.
- **Rollback XpoLog** - Information regarding how to rollback XpoLog to an earlier configuration phase.

XpoLog System Status console

The XpoLog Center System Status console contains several sections, which monitor and report on the system health. The system report does not necessarily indicates on problems that should be addressed rather than a general indication on the system behavior at a given time - the purpose of the console is to help XpoLog Administrators review summaries with regards to XpoLog activity, memory, disk utilization, data, network connectivity, configurations, etc.

An individual status containing these sections is available for each node in the cluster. In each section's settings, it is possible to enable, disable, or modify the monitoring thresholds.

To open the XpoLog Center System Status console:

1. Select the XpoLog tab. The XpoLog Manager opens.
2. In the Tools menu item, select System Status.
   The XpoLog Center System Status console opens, showing the Overview information.
3. Browse through the different sections presented on the left to see the latest information. For customizing the settings, thresholds and alerts of each section click the 'edit' link next to each section's title.

Overview

The Overview section presents a summary of all section statuses – data, system tasks, memory usage, disk space usage, storage response time, network, configuration, and general system information.

In addition, it presents a summary of the latest alerts which were sent by the system to report issues that have to be addressed.
To open the Overview section of the XpoLog Center System Status console:

- In the System Status console left navigation pane, click **Overview**.

  The Overview section of the System Status console is displayed.

Data

The Data section presents data statistics that may be viewed by several dimensions: Folders, Logs, Applications, Servers and Collection Policies. For each dimension, the Data section presents Total data, Today's data, Last Hour's data, Daily Average data, Daily Maximum data, last collection execution and summary of data monitoring rules.

The monitoring rules cover several aspects related to the data management and collection of XpoLog:
- Alerts on volume of data which exceeds defined limitations in a period of time
- Alerts on sources which data was not collected from in a period of time

The monitoring rules may be applied on Folders, Individual Logs, Applications, Servers and Collection Policies. It is also possible to define separate rules for **Business Hours and Non-Business Hours**.

In addition, XpoLog monitors the configuration accuracy which is applied on the collected data - parsing, time zones, etc.

Administration Section Options (presented on 'edit'):

**General**
Configure if this section is enabled/disabled, whether alerts should be added and execution interval to calculated results

**Properties**
Configure on which status alerts will be processed

**Thresholds**
Configure the Thresholds that will determine the status of data processing based on the current license volume utilization

**Rules**
Configure alerting rules based on server/applications/logs/folders and the constraints that will be monitored for business hours and non business hours

**Data Configuration**
The data section also verifies the logs configuration applied in XpoLog to ensure it is valid. For example if there are parsing problems of the log, time zone differences, etc. it will be indicated in this section - it is recommended, but not mandatory, to review the indicated log's configuration to ensure it is configured properly.

Customize the default configuration monitoring parameters if needed

**Alerting Policy**
Configure whether Email alerts and/or SNMP Traps should be sent and after an alert is sent, when status changes if a positive alert should be sent as well. By default alerts are sent to the system administrator which can be customized in this section to specific recipient(s)

**Exceptions**
Presents exceptions that are marked on specific alerts, if such exists

**Section Alerts:**

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Data): Abnormal data behavior for [XPLG_RULE_NAME] ([XPLG_SOURCE])**
  XpoLog sends this alert when a data issue is detected. [XPLG_RULE_NAME] = the rule name of the data issue; [XPLG_SOURCE] = the source of the data issue.

To open the Data section of the XpoLog Center System Status console:

- In the System Status console left navigation pane, click **Data**.

  The Data section of the System Status console is displayed

System Tasks

The System Tasks section presents statistics on all the tasks that XpoLog performs and their average execution time.

Administration Section Options (presented on 'edit'):

**General**
Configure if this section is enabled/disabled, whether alerts should be added and execution interval to calculated results

**Properties**
Configure on which status alerts will be processed

**Thresholds**
Configure the Thresholds that will determine the status of different activities execution time

**Alerting Policy**
Configure whether Email alerts and/or SNMP Traps should be sent and after an alert is sent, when status changes if a positive alert should be sent as well. By default alerts are sent to the system administrator which can be customized in this section to specific recipient(s).

Exceptions
Presents exceptions that are marked on specific alerts, if such exists.

Section Alerts:

  XpoLog sends this alert when a performance issue is detected. [XPLG_PERFORMANCE_INFO] = details about the detected problem.
  Common reasons / actions: Contact XpoLog support for further investigation.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Performance): Scan directory performance issue on directory [XPLG_OBJECT_ID]**
  XpoLog sends this alert when there are issues while scanning a directory for log detection. [XPLG_OBJECT_ID] = the directory in which XpoLog encountered problems while scanning.
  Common reasons / actions: Slow connectivity to the remote machine, numerous number of files/subdirectories which cause slowness. It is recommended to use include/exclude and subdirectories limitation in the scan directory wizard advanced settings. You are welcome to contact XpoLog support for further investigation.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (System Tasks): The system task named [XPLG_JOB_NAME] is running slowly**
  XpoLog sends this alert when a slowness of a system task is detected. [XPLG_JOB_NAME] = the name of the system task.
  Common reasons / actions: Contact XpoLog support for further investigation.

To open the System Tasks section of the XpoLog Center System Status console:

- In the System Status console left navigation pane, click System Tasks. The System Tasks section of the System Status console is displayed

Listeners

The Listeners section presents general information on all the configured listeners and their statuses.

Administration Section Options (presented on 'edit'):

General
Configure if this section is enabled/disabled, whether alerts should be added and execution interval to calculated results

Properties
Configure on which status alerts will be processed

Thresholds
Configure the Thresholds that will determine the status based on memory consumption level

Alerting Policy
Configure whether Email alerts and/or SNMP Traps should be sent and after an alert is sent, when status changes if a positive alert should be sent as well. By default alerts are sent to the system administrator which can be customized in this section to specific recipient(s)

Exceptions
Presents exceptions that are marked on specific alerts, if such exists.

Section Alerts:

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Listeners): Listener [XPLG_LISTENER_NAME] is down**
  XpoLog sends this alert when a listener is not running as expected. [XPLG_LISTENER_NAME] = the name of the listener.
  Common reasons / actions: Contact XpoLog support for further investigation.

To open the Listeners section of the XpoLog Center System Status console:

- In the System Status console left navigation pane, click Listeners. The Listeners section of the System Status console is displayed

Memory Usage

The Memory Usage section presents the system's memory utilization over time.

Administration Section Options (presented on 'edit'):

General
Configure if this section is enabled/disabled, whether alerts should be added and execution interval to calculated results

Properties
Configure on which status alerts will be processed

Thresholds
Configure the Thresholds that will determine the status based on memory consumption level

Alerting Policy
Configure whether Email alerts and/or SNMP Traps should be sent and after an alert is sent, when status changes if a positive alert should be sent as well. By default alerts are sent to the system administrator which can be customized in this section to specific recipient(s)

Exceptions
Presents exceptions that are marked on specific alerts, if such exists
sent as well. By default alerts are sent to the system administrator which can be customized in this section to specific recipient(s)

Exceptions
Presents exceptions that are marked on specific alerts, if such exists

Section Alerts:

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Memory): High Memory [XPLG_ALERT_SUBJECT]**
  XpoLog sends this alert when high memory is detected and may cause XpoLog not to function well. [XPLG_ALERT_SUBJECT] = details about the memory consumption.
  **Common reasons / actions:** Insufficient memory allocation to XpoLog. 32-bit installations can be allocated with maximum memory of 1.5 GB; 64-bit installation should be allocated 75% of the available machine’s memory. The memory allocation is done in the file XpoLog.lax (Windows) or XpoLog.sh.lax (Linux), which is placed inside the installation directory of XpoLog. The default allocation is 1024 m (-Xmx1024 m) and should be changed accordingly. Restart is required after the change is applied. For additional information, contact XpoLog support.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] Positive System Alert (Memory): High Memory [XPLG_ALERT_SUBJECT]**
  Resolved
  XpoLog sends this alert in case a memory issue is resolved. It is sent after a system alert notifying about a memory problem. [XPLG_ALERT_SUBJECT] = details about the memory consumption.

To open the Memory Usage section of the XpoLog Center System Status console:
- In the System Status console left navigation pane, click Memory Usage. The Memory Usage section of the System Status console is displayed.

**Disk Space Usage**

The Disk Space Usage section presents the current usage of all storage devices, which XpoLog uses (installation, data, configuration, etc.)

Administration Section Options (presented on 'edit'):
- **General**
  Configure if this section is enabled/disabled, whether alerts should be added and execution interval to calculated results
- **Properties**
  Configure on which status alerts will be processed
- **Thresholds**
  Configure the Thresholds that will determine the status of different disk space utilization
- **Alerting Policy**
  Configure whether Email alerts and/or SNMP Traps should be sent and after an alert is sent, when status changes if a positive alert should be sent as well. By default alerts are sent to the system administrator which can be customized in this section to specific recipient(s)

Exceptions
Presents exceptions that are marked on specific alerts, if such exists

Section Alerts:

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Disk Space Usage): High disk space usage on [XPLG_DISK_SPACE_PATH]**
  XpoLog sends this alert when a high disk space issue is detected. [XPLG_DISK_SPACE_PATH] = the storage device which ran out of space.
  **Common reasons / actions:** Not enough storage is allocated to XpoLog. It is very important to free space for XpoLog; otherwise, the software will stop working.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Disk Space Usage): Critical disk space usage on [XPLG_DISK_SPACE_PATH]**
  XpoLog sends this alert when a very high disk space issue is detected and jeopardizes the system activity. [XPLG_DISK_SPACE_PATH] = the storage device which ran out of space.
  **Common reasons / actions:** Not enough storage is allocated to XpoLog. It is very important to free space for XpoLog; otherwise, the software will stop working.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] Positive System Alert (Disk Space Usage): High disk space usage on [XPLG_DISK_SPACE_PATH] resolved.**
  XpoLog sends this alert in case a storage issue is resolved. It is sent following a system alert notifying that the allocated storage is filled up. [XPLG_DISK_SPACE_PATH] = the storage device that was alerted and is now resolved.

  XpoLog sends this alert in case a storage issue is resolved. It is sent following a system alert notifying that the allocated storage is filled up. [XPLG_DATA_VOLUME_NAME] = the XpoLog storage that was alerted and is now resolved.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Disk Space Usage): Critical data storage usage on [XPLG_DATA_VOLUME_NAME]**
  XpoLog sends this alert when XpoLog is about to fill its allocated storage limitation. [XPLG_DATA_VOLUME_NAME] = the XpoLog storage that ran out of space.
  **Common reasons / actions:** Not enough storage is allocated to XpoLog. It is very important to free space / allocate more storage to XpoLog; otherwise, the software will stop working when it reaches this limitation. Allocation is done in Collection Policies under XpoLog>Settings>Log Collection Policies.

XpoLog sends this alert in case a storage issue is resolved. It is sent following a system alert notifying that the allocated storage is filled up. \([XPLG\_DISK\_SPACE\_PATH]\) = the storage device that was alerted and is now resolved.

To open the Disk Space Usage section of the XpoLog Center System Status console:

- In the System Status console left navigation pane, click **Disk Space Usage**.
  The Disk Space Usage section of the System Status console is displayed.

**Storage Response Time**

The Storage Response Time section presents the time that it takes XpoLog to reach out to its allocated storage devices.

Administration Section Options (presented on 'edit'):

- **General**
  Configure if this section is enabled/disabled, whether alerts should be added and execution interval to calculated results

- **Properties**
  Configure on which status alerts will be processed

- **Thresholds**
  Configure the Thresholds that will determine the status of different response times of the used storage(s)

- **Alerting Policy**
  Configure whether Email alerts and/or SNMP Traps should be sent and after an alert is sent, when status changes if a positive alert should be sent as well. By default alerts are sent to the system administrator which can be customized in this section to specific recipient(s)

- **Exceptions**
  Presents exceptions that are marked on specific alerts, if such exists

Section Alerts:

- **XpoLog [XPLG\_MACHINE\_NAME\_FULL\_UID] System Alert (Storage Response Time): slow load time of index status of log [XPLG\_OBJECT\_NAME] ([XPLG\_OBJECT\_ID])**
  XpoLog sends this alert when the loading time of an index status is taking longer than expected. You can see in the alert more details about the expected and actual time. \([XPLG\_OBJECT\_NAME]\) = log name; \([XPLG\_OBJECT\_ID]\) = log ID
  **Common reasons / actions:** slowness of the XpoLog storage.

- **XpoLog [XPLG\_MACHINE\_NAME\_FULL\_UID] System Alert (Storage Response Time): slow load time of log [XPLG\_OBJECT\_NAME] ([XPLG\_OBJECT\_ID])**
  XpoLog sends this alert when the loading time of a log is taking longer than expected. You can see in the alert more details about the expected and actual time. \([XPLG\_OBJECT\_NAME]\) = log name; \([XPLG\_OBJECT\_ID]\) = log ID
  **Common reasons / actions:** slowness of the XpoLog storage.

- **XpoLog [XPLG\_MACHINE\_NAME\_FULL\_UID] System Alert (Storage Response Time): slow load time of Analytics result of log [XPLG\_OBJECT\_NAME] ([XPLG\_OBJECT\_ID])**
  XpoLog sends this alert when the loading time of the Analytics results is taking longer than expected. You can see in the alert more details about the expected and actual time. \([XPLG\_OBJECT\_NAME]\) = log name; \([XPLG\_OBJECT\_ID]\) = log ID
  **Common reasons / actions:** slowness of the XpoLog storage.

- **XpoLog [XPLG\_MACHINE\_NAME\_FULL\_UID] System Alert (Storage Response Time): Slow response time on [XPLG\_DISK\_SPACE\_PATH]**
  XpoLog sends this alert when it encounters a slow response time from a storage device. \([XPLG\_DISK\_SPACE\_PATH]\) = the storage device to/from which XpoLog encounters slowness.
  **Common reasons / actions:** slow load on the storage / XpoLog machine, slow connectivity to the storage.

- **XpoLog [XPLG\_MACHINE\_NAME\_FULL\_UID] Positive System Alert (Storage Response Time): Slow response time on [XPLG\_DISK\_SPACE\_PATH] resolved**
  XpoLog sends this alert when slowness to a storage device is resolved. It is sent following a system alert notifying of slowness. \([XPLG\_DISK\_SPACE\_PATH]\) = the storage device to/from which XpoLog encounters slowness.

To open the Storage Response Time section of the XpoLog Center System Status console:

- In the System Status console left navigation pane, click **Storage Response Time**.
  The Storage Response Time section of the System Status console is displayed.

**Network**

The Network section presents general information on the remote data source with which XpoLog interacts, and in addition data sources which cannot be reached or have slow connectivity, which may impact the system.

Administration Section Options (presented on 'edit'):

- **General**
  Configure if this section is enabled/disabled, whether alerts should be added and execution interval to calculated results

- **Properties**
  Configure on which status alerts will be processed

- **Thresholds**
  Configure the Thresholds that will determine the status of different connectivity time to remote sources

- **Alerting Policy**
  Configure whether Email alerts and/or SNMP Traps should be sent and after an alert is sent, when status changes if a positive alert should be
sent as well. By default alerts are sent to the system administrator which can be customized in this section to specific recipient(s)

Exceptions

Presents exceptions that are marked on specific alerts, if such exists

Section Alerts:

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Network): Connection problem between [XPLG_MACHINE_NAME_UID] and [XPLG_HOST]**
  XpoLog sends this alert when it is unable to connect to a remote machine. [XPLG_MACHINE_NAME_UID] = the XpoLog instance which tried to establish a connection. [XPLG_HOST] = the remote machine which XpoLog fails to connect to.
  Common reasons / actions: Remote machine is not active, network problem, security constraints which block the connection.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] Positive System Alert (Network): Connection Problem between [XPLG_MACHINE_NAME_UID] and [XPLG_HOST] resolved**
  XpoLog sends this alert when a connection problem between XpoLog and a remote machine is resolved. It is sent following a system alert notifying of a connectivity failure.
  [XPLG_MACHINE_NAME_UID] = the XpoLog instance which tried to establish a connection. [XPLG_HOST] = the remote machine which XpoLog fails to connect to.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Network): Remote XpoLog connection problem to [XPLG_HOST]**
  XpoLog sends this alert when there is a connectivity problem to a remote XpoLog instance. [XPLG_HOST] = the remote XpoLog to which the centralized XpoLog is unable to connect.
  Common reasons / actions: Remote XpoLog is down, FW constraints which block the connection, incompatible ports usage when trying to connect to a remote XpoLog, and usage of username/password in case the remote XpoLog is with security activated.

  XpoLog sends this alert when a connection problem between XpoLog and a remote XpoLog is resolved. It is sent following a system alert notifying of the connectivity failure. [XPLG_HOST] = the remote XpoLog to which the centralized XpoLog fails to connect to.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Network): SSH connection problem to [XPLG_HOST]**
  XpoLog sends this alert when there is a connectivity problem over SSH to a remote machine. [XPLG_HOST] = the remote machine which the XpoLog fails to connect to over SSH.
  Common reasons / actions: Connectivity credentials are not valid, remote machine is down, FW constraints that block the connection, incompatible ports usage when trying to connect to a remote machine over SSH. It is recommended to open an SSH terminal directly from the XpoLog machine to the remote machine using the exact same details, and then verify connectivity. It is also recommended to try configuring the SSH account to use SCP instead of the default SFTP protocol (under Tools > Address Book, edit the SSH account, and set SCP in the advanced section).

  XpoLog sends this alert when a connection problem between XpoLog and a remote machine over SSH is resolved. It is sent following a system alert notifying of the connectivity failure. [XPLG_HOST] = the remote machine which XpoLog was unable to connect to over SSH.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Network): Windows Network connection problem to [XPLG_HOST]**
  XpoLog sends this alert when there is a connectivity problem to a remote Windows machine. [XPLG_HOST] = the remote Windows machine which the XpoLog fails to connect to.
  Common reasons / actions: Connectivity credentials are not valid, remote machine is down, FW constraints that block the connection. It is recommended to save a service account on the XpoLog service in the Windows Service console, with the required permissions to connect to and read the logs from a remote machine and in addition, to log in to the XpoLog machine using the same user which is used to run the XpoLog service and open a Windows files explorer to the remote location to verify connectivity.

  XpoLog sends this alert when a connection problem between XpoLog and a remote Windows machine is resolved. It is sent following a system alert notifying of the connectivity failure. [XPLG_HOST] = the remote Windows machine which XpoLog was unable to connect to.

To open the Network section of the XpoLog Center System Status console:

- In the System Status console left navigation pane, click Network.
  The Network section of the System Status console is displayed.

Configuration

The Configuration section presents detailed information on all the configuration that XpoLog manages and whether there are issues to be addressed.

Administration Section Options (presented on ‘edit’):

General
Configure if this section is enabled/disabled, whether alerts should be added and execution interval to calculated results

Properties
Configure the system configuration backup parameters
Alerting Policy
Configure whether Email alerts and/or SNMP Traps should be sent and after an alert is sent, when status changes if a positive alert should be sent as well. By default alerts are sent to the system administrator which can be customized in this section to specific recipient(s)

Exceptions
Presents exceptions that are marked on specific alerts, if such exists

Section Alerts:
- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Configuration): Failed to collect data from [XPLG_COLLECTION_INFO]**
  XpoLog sends this alert when it fails to collect data from a log. [XPLG_COLLECTION_INFO] = information about the collector that failed.
  **Common reasons / actions:** Connectivity problem to the remote server, source file(s) does not exist.

To open the Configuration section of the XpoLog Center System Status console:
- In the System Status console left navigation pane, click Configuration.
  The Configuration section of the System Status console is displayed.

System Information
The System Information section presents general information on the XpoLog installation, versions, license, hardware, and allocated resources.

Administration Section Options (presented on 'edit'):
- **General**
  Configure if this section is enabled/disabled, whether alerts should be added and execution interval to calculated results
- **Properties**
  N/A
- **Alerting Policy**
  Configure whether Email alerts and/or SNMP Traps should be sent and after an alert is sent, when status changes if a positive alert should be sent as well. By default alerts are sent to the system administrator which can be customized in this section to specific recipient(s)

Exceptions
Presents exceptions that are marked on specific alerts, if such exists

Section Alerts:
- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (Configuration): Conflict between installation and configuration versions**
  XpoLog sends this alert when the installation version of XpoLog is different than the configuration version, as this may cause issues with the software.
  **Common reasons / actions:** Not all nodes in XpoLog cluster were updated; a configuration migration to a different XpoLog deployment.
- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] Positive System Alert (System Information): Conflict between installation and configuration versions resolved**
  XpoLog sends this alert in case a version conflict is resolved. It is sent following a system alert notifying of a version conflict.
- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (System Information): Current Java version is not optimal**
  This alert is sent in case the JAVA version is earlier than JAVA 1.7, which is the recommended version. Features that do not work on versions earlier than JAVA 1.7 are: Hadoop HDFS Support, Disk space monitoring, and some performance optimizations which are available only with JAVA 1.7.
  **Common reasons / actions:** Current XpoLog version uses JAVA 1.5 or JAVA 1.6. In this case, contact XpoLog support team to update to JAVA 1.7.
- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (System Information): XpoLog Center processor node has changed to [XPLG_MACHINE_NAME]**
  XpoLog sends this alert when the processor node has been changed from the defined one to [XPLG_MACHINE_NAME]. [XPLG_MACHINE_NAME] = the new host which now manages as the processor node.
  **Common reasons / actions:** Processor node is down or has lost connectivity to the allocated storage. Check the processor node to ensure it is up and running and connected to the storage.
- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] Positive System Alert (System Information): XpoLog Center processor node has changed back to [XPLG_MACHINE_NAME]**
  XpoLog sends this alert when the processor node has been recovered and is now managing back as the processor node. This alert is sent following an alert that notified that the processor node is not functioning as the processor.
- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (System Information): Current limit of open files is too low**
  XpoLog sends this alert on Linux installations only where the number of allowed open files is too low. This limitation is critical to XpoLog functionality and should be changed immediately.
Common reasons / actions: Post Installation Recommendations

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (License): Allowed data volume exceeded**
  XpoLog sends this alert when it reaches the licensed volume limitation.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (License): XpoLog Center license will expire in [XPLG_DAYS] days**
  XpoLog sends this alert to notify that the license is about to expire. \([XPLG_DAYS] = \text{days left until the software will be deactivated}\).

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (License): XpoLog Center license is not valid**
  XpoLog license is not valid and it is not possible to use the software. Contact XpoLog support to renew/activate your updated license.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (License): Allowed number of logs was reached**
  XpoLog sends this alert when it reaches the maximum number of allowed logs in your license. Contact XpoLog support to expand your license.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (License): Server key is invalid**
  XpoLog sends this alert when the server key which is used in the license is not valid. XpoLog stops working until this issue is resolved.

- **XpoLog [XPLG_MACHINE_NAME_FULL_UID] System Alert (License): Server key is valid**
  XpoLog sends this alert in case a server key license issue is resolved. It is sent following a system alert notifying that the server key is not valid as a verification that XpoLog continues to run as usual.

**To open the System Information section of the XpoLog Center System Status console:**

- In the System Status console left navigation pane, click **System Information**.

  The System Information section of the System Status console is displayed.

**System Alerts**

The System Alerts section centralizes all the alerts that were sent by the System Status monitoring mechanism for the administrator's reference.

To open the System Alerts section of the XpoLog Center System Status console:

- In the System Status console left navigation pane, click **System Alerts**.

  The System Alerts section of the System Status console is displayed.

**System Alerts Settings**

- **General**
  Configure how long to keep alerts in the system and the default time frame when loading this section.

- **Alerting Policy**
  Set system administrators email address and whether to send general system alerts by email and / or SNMP traps.

- **Exceptions**
  Presents exceptions that are marked on specific alerts, if such exists.

**Note:** In order to send **Email alerts** - email settings must be configured and validated. In order to send **SNMP traps** - SNMP system account must be configured and validated.

**XpoLog Support Portal**

The XpoLog support portal is accessible via the XpoLog > Settings > About menu item, by clicking the Open XpoLog Center Support Portal link.

Only users associated with the Administrators group can open the portal. The portal enables system administrators to view systems logs, change logging level, review the general configuration that XpoLog uses, track real time activity, and manage all the data that XpoLog stores. This information may be viewed in several sections, by selecting from the drop down list the following options: Basic Information, Activity Information, Data Information, Site Statistics, Actions, and Advanced Settings.

**Use of this portal should be permitted only to trained system administrators.**

In case XpoLog runs with several cluster nodes, it is possible to view/manage each node’s information separately by selecting the required node in the combo-box on top of the screen, or using the default option that includes all information from all nodes.

To open the XpoLog Support portal:

1. Click the XpoLog tab.
   The XpoLog Manager opens.
2. Click the **Settings > About** menu item.
   The About XpoLog Center console opens.
3. Click the **Open XpoLog Center Support Portal** link.
   The XpoLog Support portal opens.

**Basic Information**

The Basic Information section of the XpoLog Support portal includes two tabs:

- **System Logs** – Displays a table of all system logs, and their general information including **Name, Size, Last Modified, Number of Files**
and **Logging Level**. In this tab, Administrators can view a log, change its logging level, and export a log by selecting the log in the table, and clicking the relevant button (View, Export, Export Light, or Change Logging Level). It is also possible to add a system log (by clicking the Add XpoLog System Logs button), export all system logs (by clicking the Export All Information button), or export light all information (by clicking the Export All Light button).

- **System Information** – General information on XpoLog such as version and build, time zone, used JAVA, and more.

To open the Basic Information section:

- In the XpoLog Support portal, in the header bar dropdown list, select **Basic Information**. The Basic Information section opens.

**Activity Information**

The Activity Information section of the XpoLog Support portal includes five tabs:

- **Processes** – Displays a table of all active processes in XpoLog (indexing, reports, dashboard analysis, monitors, etc.). Administrators can stop a process during its operation by selecting the process, and then clicking the **Stop** button.

  **Note:** Stopping a process during its operation might affect users that expect different results.

- **Threads** – Displays a table of all active threads and their stack traces (JAVA 1.5+) in XpoLog. Administrators can interrupt a thread during its operation by selecting it and clicking the **Interrupt** button.

  **Note:** Interrupting a thread during its operation might affect users that expect different results.

- **SSH Connections** – Displays a table of all active SSH connections in XpoLog. Administrators can terminate a connection during its operation by selecting it and clicking the **Terminate** button.

  **Note:** Terminating a connection during its operation might affect users that expect different results.

- **Jobs** – Displays a table of all active jobs and their statuses. Administrators can stop a job during its operation by selecting the job, and then clicking the **Stop** button.

  **Note:** Stopping a job during its operation might affect users that expect different results.

- **HTTP Sessions** – Displays an HTTP Sessions table, which presents all open clients (browsers) to XpoLog. Administrators can destroy a session by selecting it and clicking the **Destroy** button.

  **Note:** Destroying a session might affect users that expect different results.

To open the Activity Information section:

- In the XpoLog Support portal, in the header bar drop down list, select **Activity Information**. The Activity Information section opens.

**Data Information**

The Data Information section of the XpoLog Support portal includes six tabs:

- **Indexing** – Displays a table of all logs and their index status and details. Administrators can delete a log’s index or re-index it by selecting the log and clicking the **Delete** or **Re-index** button, respectively.

- **Monitors** – Displays a table of all monitors and their details. Administrators can delete a monitor or reset its reference by selecting the monitor and clicking the **Delete Monitor** or **Reset Monitor** button, respectively.

- **Analytics Logs** – Displays an Analytics table of all logs analysis details. Administrators can delete a log analysis by selecting it, and then clicking the **Delete Data** button.

  **Note:** Stopping a job during its operation might affect users that expect different results.

- **Analytics Hosts** – Displays an Analytics table of all hosts analysis details. Administrators can delete a host analysis by selecting it, and then clicking the **Delete Data** button.

  **Note:** Destroying a session might affect users that expect different results.

To open the Data Information section:

- In the XpoLog Support portal, in the header bar drop-down list, select **Data Information**. The Data Information section opens.

**Site Statistics**

Site Statistics presents a summary of the total logs, logs volume, and index status at the **Applications**, **Folders**, and **Logs** levels. It is possible to schedule the statistics report to be sent by email as HTML or CSV, periodically.

**Advanced Settings**

The Advanced Settings section of the XpoLog Support portal includes three tabs:

- **Properties** – It is highly recommended NOT to change any property under Advanced Settings without consulting XpoLog Support. Changes of properties may result in significant change in system behavior and results.

- **Jobs Groups** –

- **Resource Manager** – The resource manager determines the maximal allowed number of threads that can work in parallel per operation in XpoLog.

A restart of XpoLog may be required for changes made in the Advanced Settings section to take effect.
To open the Advanced Settings section:

- In the XpoLog Support portal, in the header bar drop down list, select **Advanced Settings**. The Advanced Settings section opens.

### XpoLog System logs

XpoLog manages a set of log files which contains errors, events, system activity, users activity and more. The logs are located under the 'log' directory in the XpoLog allocated storage (by default under the installation directory). XpoLog uses Log4J to log its activity and errors and it is possible to modify the Log4J properties if needed (located under `<XpoLog-Config>/conf/general/log4jXpolog.properties`). [Click here to see an example of how to change the default Log4J configuration](#).

In order to view the XpoLog system log please go to the support portal, select the log you would like to view and click the view button. It is also possible to add the system logs to be presented in XpoLog to get access to all logs directly from the console - from the support portal, basic section click the 'Add System Logs' button and then refresh the browser ([this functionality will not not work if the Log4J default settings are modified](#)).

Following is a summary of the logs that XpoLog manages:

#### audit

The audit logs contain detailed information on all users activity in XpoLog. XpoLog is auditing all user's operations starting from signing in through all other available operations in the system. XpoLog fully complies with IT regulations of auditing and storing EVERYTHING which is done in the system by Administrators and Users - the logs containing this information may be stored for as long as needed to provide details and reports of the usage.

#### system audit

The system audit logs contain detailed information on all the system's activity. All the operation which are executed by the server side are logged - data collection, indexing, monitoring executions, dashboards generation, etc.

#### XpoLog log

The XpoLog logs contain detailed information on all errors which XpoLog encounters.

#### ssh

The ssh logs contain detailed information on all SSH related errors which XpoLog encounters while trying to establish connections, collect data or monitor remote sources over SSH.

#### scanner

The scanner logs contain detailed information on the the data scanning operations that XpoLog performs such as which sources are scanned, number of logs identified and added to the system, etc.

#### XpoLog memory

The XpoLog memory logs contain details on the memory consumption of XpoLog.

#### Servlet Container

The Servlet Container logs are the logs of the internal Servlet Container which runs XpoLog.

#### Cluster Activity

The Cluster activity logs contain detailed information on all cluster related issues - in case multiple instances of XpoLog run as a cluster.

#### Data Activity

The Data activity logs contain detailed information on all the data collection and management done by XpoLog.
Ant

The Ant.out file contains information on Ant related operations that are executed such as deployment of an update patch on the system.

Events

The events logs contain details on all the events in XpoLog which are sent out from XpoLog to users such as monitors alerts, exporting of dashboards / reports, tasks executions, etc.

System Alerts

The System alerts logs contain details on all the alerts which XpoLog internal monitoring mechanism is sending (see more details at XpoLog System Status console).

XpoLog Log4J Configuration

XpoLog system logs are located under the 'log' directory in the XpoLog allocated storage (by default under the installation directory). XpoLog uses Log4J to log its activity and errors and it is possible to modify the Log4J properties if needed. The configuration is stored at the file <XpoLog-Config>/conf/general/log4jXpolog.properties but since it is the default one it should not be changed since it will be overridden on system updates.

If you wish to customize the default configuration, you may copy the file <XpoLog-Config>/conf/general/log4jXpolog.properties and create a new file named <XpoLog-Config>/conf/general/log4jXpolog.user.properties (if this file exists, it will be used before the default one).

In general, XpoLog uses the default Apache Log4J configuration syntax. There is an appender definition for each of the system logs which defines its pattern, rotation policy, number of files to keep, etc.

For this example, we'll use the configuration of XpoLog Application log (xpologlog.log*):

**Default Configuration:**
This configuration rotates a file every 5000K and keeps 10 files in total based on the pattern specified.

```properties
#Appender data for xpolog
log4j.appender.xpolog=org.apache.log4j.RollingFileAppender
log4j.appender.xpolog.File=${xpolog.root.path}log/${xpolog.machine.name}.pathxpologlog.log
log4j.appender.xpolog.MaxFileSize=5000KB
log4j.appender.xpolog.MaxBackupIndex=10
log4j.appender.xpolog.layout=org.apache.log4j.PatternLayout
```

**Modified Configuration:**
If the below replaces the default configuration, then XpoLog will keep a daily file (unlimited by size) for 30 days based on the pattern specified.

```properties
#Appender data for xpolog
log4j.appender.xpolog=xpolog.eye.util.logging.DateFormatFileAppender
log4j.appender.xpolog.File=${xpolog.root.path}log/${xpolog.machine.name}.pathxpologlog.log
log4j.appender.xpolog.DatePattern=yyyy-MM-dd
log4j.appender.xpolog.MaxFilesToKeep=30
log4j.appender.xpolog.layout=org.apache.log4j.PatternLayout
```

**Note:**
- Changing the Log4J configuration requires all XpoLog cluster nodes to be restarted.
- Upon changing the default logging settings the view of XpoLog logs via XpoLog support portal may not work, the logs may be defined in XpoLog using their modified configuration.
- Make sure you take into consideration the required disk space when changing the default settings. By default XpoLog log directory (per instance in cluster) may reach approximately 1GB on full capacity.

Rollback XpoLog

XpoLog Rollback is an operation which returns the configuration to an earlier state, it may be required if there was an undesired configuration change, unintended removal of an object, etc.
XpoLog stores a daily backup of all its configuration and keeps the last 30 days backups.

Note: it is critical to stop all XpoLog nodes while performing a roll back.

In order to perform a rollback follow the steps below:
The entire configuration is managed in the EXTERNAL_CONFIGURATION_DIRECTORY, if it exists. If not, it is found in the
INSTALLATION_DIRECTORY.

1. Stop XpoLog Service
2. IMPORTANT: prior to performing a rollback, it is highly recommended to store the current configuration state of XpoLog:
   a. Go to the EXTERNAL_CONFIGURATION_DIRECTORY/ and rename conf directory to conf.current
   b. Go to the EXTERNAL_CONFIGURATION_DIRECTORY/collection/ and rename conf directory to conf.current
3. Go to the EXTERNAL_CONFIGURATION_DIRECTORY/ temp/backups/ and unzip the desired backup file from the date you wish to roll back to.
4. A collection and conf directories will appear. Copy the unzipped collection and conf directories to EXTERNAL_CONFIGURATION_DIRECTORY/
5. Start XpoLog Service

Common Scenarios

Problem

XpoLog services in not starting or starting and terminated immediately

Solution

Due to different reasons, it may be that some key XML configuration files were damaged which may cause such a problem. Review steps below for more information.

<table>
<thead>
<tr>
<th>Root Cause Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Service Level</strong></td>
</tr>
<tr>
<td>Make sure that there is no XpoLog service running in the background, if there is terminate all XpoLog related process and then try to run the service again.</td>
</tr>
<tr>
<td><strong>2. Application Server Level</strong></td>
</tr>
<tr>
<td>Go to XPOLOG_INSTALLATION/ServletContainer/conf/ and ensure the file tomcat-users.xml is not empty. Go to XPOLOG_INSTALLATION/ServletContainer/conf/Catalina/localhost/ and ensure the file logeye.xml is not empty.</td>
</tr>
<tr>
<td>If any of these files are empty it mean the application server which is used to run XpoLog cannot start - contact <a href="mailto:support@xpolog.com">support@xpolog.com</a> with this diagnosis for further steps.</td>
</tr>
<tr>
<td><strong>3. Application Level</strong></td>
</tr>
<tr>
<td>Go to XPOLOG_INSTALLATION/conf/general/ and ensure the file xpolog.xml is not empty. If it is empty, retrieve a valid xpolog.xml file from the backup directory XPOLOG_EXTERNAL_CONF/temp/backup/LATEST_BACKUP_FILE/conf/general/ replace the empty file and restart XpoLog.</td>
</tr>
<tr>
<td><strong>4. Infrastructure Level</strong></td>
</tr>
<tr>
<td>a. Storage</td>
</tr>
<tr>
<td>Ensure that both XPOLOG_INSTALLATION and XPOLOG_EXTERNAL_CONF directories are not out of space. If so, allocate more space or advise XpoLog Support regarding other options to clear space.</td>
</tr>
<tr>
<td>b. Users Permissions (commonly seen on UNIX based deployments)</td>
</tr>
<tr>
<td>It may occur that there are permissions gaps between the user that ran or currently tries to run XpoLog and the user the that owns the directories and files in XPOLOG_INSTALLATION and/or XPOLOG_EXTERNAL_CONF directories.</td>
</tr>
<tr>
<td>If that is the case, first stop XpoLog, then run the command <code>chown -R XPOLOG_USER:XPOLOG_GROUP /XPOLOG_INSTALLATION</code> and only then start XpoLog using the XPOLOG_USER.</td>
</tr>
<tr>
<td>c. Ports</td>
</tr>
<tr>
<td>Ensure that XpoLog required ports are not occupied which blocks the execution of the XpoLog service. Most common port on a standalone installation of XpoLog is its shutdown port 8095. Additional ports can be reviewed in the System Requirements section.</td>
</tr>
<tr>
<td>It is possible to modify ports in case default ports are already occupied and cannot be available at XPOLOG_INSTALLATION/ServletContainer/conf/server.xml.</td>
</tr>
</tbody>
</table>

INDEX:

XPOLOG_INSTALLATION = The absolute path of the XpoLog installation directory

XPOLOG_EXTERNAL_CONF = The absolute path of the XpoLog configuration directory. To determine this path go to XpoLog Manager > Settings > General and check the configured path of XpoLog Configuration Directory, if it is empty then consider this parameter to be identical to XPOLOG_INSTALLATION (see value above)

XPOLOG_USER:XPOLOG_GROUP = The user and group which should be used to run XpoLog and have the required permissions on all folders and files in _INSTALLATION and XPOLOG_EXTERNAL_CONF
Getting Assistance

From the **Get Help** section in the left pane of the XpoLog homepage, you can get assistance in any or all of the following ways:

- Contacting XpoLog by email to get help from our support team ([support@xplg.com](mailto:support@xplg.com))
- Visiting our Online Knowledge Base
- Reading the XpoLog User Manual

Contacting XpoLog

You can send an email to XpoLog Support with any question that you have regarding XpoLog Center.

To contact XpoLog:

1. In the XpoLog homepage, in the left pane, under the **Get Help** section, click **Contact XpoLog**.
   An email opens in your default email server, addressed to [support@xplg.com](mailto:support@xplg.com) and with the subject: Questions regarding XpoLog Center.
2. Fill in the body of the email with your question, and send the email.

Reading the XpoLog User Manual

You can read about any topic in XpoLog Center in the XpoLog User Manual.

To open the XpoLog User Manual:

- In the XpoLog homepage, in the left pane, under the **Get Help** section, click **XpoLog Center User Manual**.
  The XpoLog Center User Manual opens.

Visiting our Online Knowledge Base

You can visit our online knowledge base to look up information on XpoLog Center.

To visit our online knowledge base:

- In the XpoLog homepage, in the left pane, under the **Get Help** section, click **Online knowledge base**.
  The XpoLog knowledge base opens.

White Papers and Brochures

Resources

Please download the following white papers, brochures and data sheets for more information about XpoLog:

- XpoLog Center Summary
- XpoLog Center ROI
- XpoLog Center Deployment
- XpoLog Center Data Sheet
- XpoLog Center Comparison Sheet
- XpoLog Center Augmented Search
- XpoLog Center Augmented Search for Webapps
- XpoLog Center Augmented Search for Apps
- XpoLog Center Augmented Search for IT and Application Logs Analytics
- XpoLog Center Augmented Search for Operations Analytics
- XpoLog Center Augmented Search for Log Management in the Cloud
- XpoLog Center Augmented Search for Software and Application Testing
- XpoLog Center Architecture