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

funtion – 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 ... desc**, **first**, **display as**):

```
in app.windows event logs | count | group by event, user | order by count desc | first 10 | display count as Our Example
```

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.