Listeners (Syslog TCP/UDP)

XpoLog may be configured to monitor incoming Syslog messages and decode the messages to be available in XpoLog. XpoLog can listen on a UDP or TCP port for syslog data arriving from one or more source devices. You can use XpoLog to receive syslog data from these source devices for easy searching, reporting and alerting - XpoLog can automatically split the received syslog data and create a dedicated log per source device.

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 destination port is usually 1468). 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.

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 a TCP Listener account

Adding a UDP Listener account