

Select Search Type

Search Types

Event Manager Search

Select this type of search to query the Event Manager. Events meeting your criteria will be displayed in Investigator.

Log Manager Search

Select this type of search to query one or more Log Managers. Logs meeting your criteria will be displayed in Investigator. Only logs currently in the Log Manager will be returned.

LogMart Search

Select this type of search to query the LogMart. Aggregate Logs meeting your criteria will be displayed in Log Miner.

Include Raw Log

Check this box to include the raw log text in the search results. If left unchecked, only meta data is returned. Including the raw log text is more resource intensive increasing the overall search time. The most common scenarios for including the raw log text are when performing a low-level forensic analysis, producing detail level reports, or exporting logs.

Select Date Range to Query

- In the Last Days
- Date is Before
- Date is After
- Date is Between and

LogRhythm's easy-to-use wizard empowers users to quickly and efficiently search through events, normalized logs and even raw log data from millions of logs over any period of time, all from a single screen. Searches can range from simple key word and Boolean searches to using multiple criteria including user and host names, IP addresses, dates and times, log and/or event types, asset value etc.