LOGZILLA DOCUMENTATION

Using LogZilla AI for Log Analysis and Management

LogZilla AI capabilities for log analysis, natural language querying, documentation lookup, and result presentation, with usage examples and tips

LogZilla AI · Generated November 6, 2026 · logzilla.ai/docs/logzilla-ai/using-logzilla-ai

© LogZilla Corporation · logzilla.ai

Overview

LogZilla AI is the integrated assistant for log analysis in LogZilla. It combines natural language processing with access to LogZilla's query engine, allowing operators to run log searches and analysis through conversational prompts.

Features

1. Natural Language Log Query Processing

- Query LogZilla data using everyday language without specialized syntax
- Extract information from events, statistics, and system status
- Run searches and filters through conversational requests
- Identify patterns across distributed log sources
- Produce vendor-aware results by applying the schema and tag taxonomy of every installed LogZilla application, covering FortiGate, SonicWall, Cisco, Palo Alto, and other supported platforms

2. System Information and Assistance

- Understand incoming log data through natural language queries
- Obtain explanations about system configurations and settings
- Receive guidance on LogZilla features and functionality
- Access troubleshooting information for common system issues

3. Contextual Documentation Integration

- Instant access to relevant LogZilla documentation sections on demand
- Context-aware assistance based on current system state and user activity
- Configuration recommendations drawn from LogZilla documentation
- Step-by-step troubleshooting guidance for analytics scenarios

4. Log Data Presentation

- Present query results in organized, readable formats
- Display log data in structured tables when requested
- Format results to highlight relevant information
- Assist with interpreting log patterns and events

© LogZilla Corporation · logzilla.ai

Intuitive User Interface

Efficient Conversation Management

- **Left Sidebar**:
  - `New Conversation` button to start fresh interactions
  - List of existing conversations
  - Edit conversation titles (click pen icon)
  - Delete conversations (click trash icon)
  - Switch between conversations by clicking

Main Interface

- **Chat Area**:
  - Displays conversation history
  - Shows user questions and AI responses
  - Supports markdown formatting for better readability
  - Includes interactive charts and tables when requested

Control Elements

- **Input Field**: Located at bottom for entering questions
- **Top Right Corner**:
  - User information display
  - Current version information
  - LLM model selection options

Long-Running Answers

An answer keeps being built on the server after the browser leaves the page, loses its connection, or closes the tab. Reopening the conversation shows the progress of the answer still under way and then the answer itself; an answer that finished while nobody was watching is already in the conversation history.

Two things end an answer early: the stop button beside the input field, shown while an answer is being built, and the Agent Max Run Time limit set in `Settings` > `System Settings` > `LogZilla AI`. In both cases the searches behind the answer stop with it, and the conversation shows a message saying why the answer stopped. An answer that is under way when LogZilla

restarts is not completed; the conversation then shows the question without an answer, or reports that the response was interrupted, and the question can be asked again.

Practical Usage Guide

1. Effective Log Query Examples

```
"Show error events from the last hour"
"How many events occurred in the last 24 hours?"
"What does this error pattern mean?"
"Help me understand these SSH failure logs"
"Where can I find information about configuring alerts?"
"Show all critical error events from the last hour regarding authentication"
"Display total event count and trend analysis from the last 24 hours"
"Create an automated rule to forward security-related events to Splunk"
"Analyze and explain these unusual SSH failure patterns across servers"
"Identify potential security incidents in the last 24 hours"
```

2. Core Capabilities

LogZilla AI assists with log management through:

- Event search and pattern analysis using natural language
- Access to LogZilla documentation and knowledge resources
- System information and configuration guidance
- Log data visualization and interpretation
- Basic troubleshooting assistance

3. Operational Best Practices

- Specific, targeted queries produce more actionable log analysis results
- Including system context and timeframes significantly improves accuracy
- Strategic follow-up questions help refine understanding of complex events
- Leveraging conversation history provides continuity for extended troubleshooting sessions
- Starting with broader queries before narrowing focus often yields better results

LogZilla Integration

- Access to LogZilla's query engine for log data retrieval

- Queries run with the asking user's permissions: host permissions filter searches, top values, and event rates, while storage statistics are instance-wide event totals that are not filtered by host (see Role Based Access Control (https://www.logzilla.ai/docs/administration/role-based-access-control))
- Shared authentication with the main LogZilla system
- Integration with LogZilla documentation resources
- Available through the LogZilla navigation menu

Implementation Considerations

- AI-generated log analysis requires verification before critical implementation
- Response times vary based on query complexity and data volume
- Review of generated suggestions remains essential before production deployment
- Professional judgment should accompany all AI-assisted operations

Usage Tips

- Including specific time ranges in queries helps produce more relevant results; a question that names no time range is answered from the last 24 hours first, and from the last 7 days when those 24 hours hold no answer or the question is about the past week
- Questions about a period older than the online data are answered from archived data when the archive holds it (see Data Archiving and Retention (https://www.logzilla.ai/docs/administration/data-archiving-and-retention)); such answers take longer, and a narrower time range shortens the wait
- Managing conversations by creating new ones for different topics improves organization
- Clear, concise questions typically yield better responses
- Following up with clarifying questions helps refine results