

**LOGZILLA DOCUMENTATION**

# Command Line Tools

LogZilla command line reference for system administration, data management, query automation, and scripted workflows outside the web interface

Command Line Tools · Generated June 11, 2026 · [logzilla.ai/docs/command-line-tools](https://logzilla.ai/docs/command-line-tools)

## Command Line Tools

LogZilla provides comprehensive command line tools for system administration, data management, and automation. These tools enable administrators to configure systems, manage data lifecycles, and build automated workflows without requiring web interface access.

## Documentation Overview

### **[CLI Overview and Setup](https://www.logzilla.ai/docs/command-line-tools/cli-overview)** (<https://www.logzilla.ai/docs/command-line-tools/cli-overview>)

Learn the fundamentals of LogZilla command line tools including authentication, common patterns, and basic usage. Essential reading for all CLI users.

#### **Key Topics:**

- Command structure and help system
- Authentication methods (API tokens, config files)
- Environment variables and best practices
- Common patterns and error handling

### **[System Administration Commands](https://www.logzilla.ai/docs/command-line-tools/system-commands)** (<https://www.logzilla.ai/docs/command-line-tools/system-commands>)

Master system configuration, service management, and administrative tasks. These commands handle core system operations and maintenance.

#### **Key Topics:**

- Settings and license management
- Application installation and updates
- User management and LDAP configuration
- Service control and system maintenance

### **[Data Management Commands](https://www.logzilla.ai/docs/command-line-tools/data-commands)** (<https://www.logzilla.ai/docs/command-line-tools/data-commands>)

Control the complete data lifecycle from ingestion to archival. These tools manage data flow, storage optimization, and processing rules.

**Key Topics:**

- Archive management and retention policies
- Event statistics and performance monitoring
- Data forwarding and network analysis
- Parser rules and trigger management

**[Query Command Basics](https://www.logzilla.ai/docs/command-line-tools/query-basics) (<https://www.logzilla.ai/docs/command-line-tools/query-basics>)**

Introduction to LogZilla's powerful query system for data analysis and reporting. Learn core query types and parameter structures.

**Key Topics:**

- Authentication and configuration setup
- Basic query types (Search, TopN, EventRate)
- Time ranges, filters, and operators
- Output formats and result handling

**[Advanced Query Types](https://www.logzilla.ai/docs/command-line-tools/advanced-query-types) (<https://www.logzilla.ai/docs/command-line-tools/advanced-query-types>)**

Explore specialized queries for system monitoring, performance analysis, and advanced data aggregation.

**Key Topics:**

- System performance monitoring queries
- LogZilla internal statistics
- Advanced aggregation features
- Administrative and workflow queries

**[Query Examples and Automation](https://www.logzilla.ai/docs/command-line-tools/query-examples) (<https://www.logzilla.ai/docs/command-line-tools/query-examples>)**

Practical examples, automation scripts, and integration patterns for building comprehensive LogZilla workflows.

**Key Topics:**

- Report generation examples
- System monitoring automation
- SIEM and ticketing system integration
- Scheduled automation and best practices

# Quick Start Guide

## Essential First Steps

### Authentication Setup

```
# Create API token
logzilla authtoken create --user admin
export LOGZILLA_API_KEY="your-token"
```

### System Status Check

```
# Verify LogZilla is running
logzilla version
logzilla license info
```

### Basic Query

```
# Simple data query
echo '{"time_range": {"preset": "last_1_hours"}}' > test.json
logzilla query --type Search --params test.json
```

## Common Use Cases

Task	Primary Commands	Documentation
System setup	settings, license, apps	<a href="https://www.logzilla.ai/docs/command-line-tools/system-commands">System Commands</a> (https://www.logzilla.ai/docs/command-line-tools/system-commands)
User management	password, authtoken, ldap	<a href="https://www.logzilla.ai/docs/command-line-tools/system-commands">System Commands</a> (https://www.logzilla.ai/docs/command-line-tools/system-commands)
Data lifecycle	archives, events, drop	<a href="https://www.logzilla.ai/docs/command-line-tools/data-commands">Data Commands</a> (https://www.logzilla.ai/docs/command-line-tools/data-commands)
Event processing	rules, triggers, forwarder	<a href="https://www.logzilla.ai/docs/command-line-tools/data-commands">Data Commands</a> (https://www.logzilla.ai/docs/command-line-tools/data-commands)
Data analysis	query with various types	<a href="https://www.logzilla.ai/docs/command-line-tools/query-basics">Query Basics</a> (https://www.logzilla.ai/docs/command-line-tools/query-basics)

Task	Primary Commands	Documentation
System monitoring	System performance queries	<a href="https://www.logzilla.ai/docs/command-line-tools/advanced-query-types">Advanced Queries</a> (https://www.logzilla.ai/docs/command-line-tools/advanced-query-types)
Automation	Scripts and scheduled tasks	<a href="https://www.logzilla.ai/docs/command-line-tools/query-examples">Query Examples</a> (https://www.logzilla.ai/docs/command-line-tools/query-examples)

## Command Categories

### Administrative Commands

- **System Configuration:** `settings, license, https`
- **Service Management:** `start, stop, restart, version`
- **Application Management:** `apps install/uninstall`
- **User Management:** `password, authtoken, ldap`

### Data Management Commands

- **Storage Lifecycle:** `archives, events, drop`
- **Data Flow:** `forwarder, sniffer`
- **Processing Rules:** `rules, triggers`
- **Performance:** Event statistics and optimization

### Query and Analysis Commands

- **Basic Queries:** `Search, TopN, EventRate, LastN`
- **System Monitoring:** `System_CPU, System_Memory, System_DF`
- **Internal Statistics:** `StorageStats, ProcessingStats`
- **Administrative:** `Notifications, Tasks`

## Best Practices Summary

### Security

- Use API tokens instead of passwords for automation
- Protect configuration files with appropriate permissions

- Rotate credentials regularly
- Monitor command execution and access

## Performance

- Use specific time ranges to limit query scope
- Apply filters to reduce data processing
- Schedule resource-intensive operations during off-peak hours
- Monitor system resources during large operations

## Automation

- Validate parameters and handle errors gracefully
- Implement logging and monitoring for automated tasks
- Use configuration files for complex parameters
- Test automation in development environments first

## Documentation and Maintenance

- Document automation purposes and dependencies
- Keep scripts and configurations under version control
- Monitor automation success rates and performance
- Maintain up-to-date parameter templates

## Getting Help

Each command provides detailed help information:

```
# General help
logzilla --help

# Command-specific help
logzilla <command> --help
logzilla query --help
logzilla settings --help
```

For complex scenarios and troubleshooting, refer to the specific documentation sections above or contact LogZilla support with detailed command output and system information.

The LogZilla CLI provides powerful tools for every aspect of log management. Start with the basics and progressively build more sophisticated workflows as your requirements evolve.