LOGZILLA DOCUMENTATION

Server Settings

LogZilla YAML-based server configuration in /etc/logzilla/settings/ managed through the logzilla settings CLI for advanced backend parameters

Administration · Generated April 29, 2026 · logzilla.ai/docs/administration/server-settings

LogZilla uses a modern YAML-based configuration system that provides advanced settings not available through the web interface. These backend settings control core system behavior, performance parameters, and security features.

Warning: Changing these settings may cause system instability or data loss. Exercise extreme caution and test changes in a non-production environment first.

Modern Configuration System

LogZilla stores configuration in YAML files located in `/etc/logzilla/settings/`. Each file corresponds to a specific configuration group (e.g., `smtp.yaml`, `ldap.yaml`, `generic.yaml`).

Configure with the command line

Administrators use the `logzilla settings` command to manage configuration:

```
# List all available settings
logzilla settings list

# List settings for a specific group
logzilla settings list ldap

# Update a setting value
logzilla settings update SETTING_NAME=new_value

# Update multiple settings at once
logzilla settings update SMTP_SERVER=mail.company.com SMTP_PORT=587

# Manage multiple instances (e.g., secondary LDAP server)
logzilla settings update --id 1 LDAP_ENABLED=true
```

Edit the configuration file directly

Advanced users with root access can edit YAML files directly:

```
# Navigate to settings directory
cd /etc/logzilla/settings/

# Edit a configuration file
vim smtp.yaml
```

After direct edits, see Applying Changes to reload the affected configuration group.

Applying Changes

After making configuration changes, apply them using one of these methods:

Method 1: Automatic Application (Recommended)
The `logzilla settings update` command automatically applies changes to compatible modules.

Method 2: Manual Reload (After Direct Edits)
If editing YAML files directly, notify the system of changes:

```
# Reload a specific configuration group
logzilla settings reload smtp
logzilla settings reload ldap
```

Method 3: Container Restart (When Required)
Some settings require container restarts to take effect:

```
# Restart specific containers
logzilla restart -c gunicorn celeryworker celerybeat

# Or restart all LogZilla services
logzilla restart
```

Note: API and Celery containers typically require restart for changes to take effect, while core processing modules support live reloading for most settings.

These are the modules used by LogZilla, which can be restarted with `logzilla restart -c <module>`:

Module	Description
celerybeat	Schedules periodic background tasks for the platform.
gunicorn	API server for the LogZilla backend.
celeryworker	Executes background jobs and module orchestration tasks.
parsermodule	Parses, normalizes, and enriches incoming events using rules/apps.
querymodule	Runs searches/analytics, evaluates triggers, and publishes live results.
storagemodule-1	Event storage and indexing service (dedup, archiving, aggregates).
ai	AI Copilot backend; powers AI features when enabled.

Module	Description
watcher	Orchestrates, monitors, and restarts LogZilla containers.
snmptrapd	Receives SNMP traps (UDP 162) and injects them as events.
httpreceiver	HTTP/HTTPS event ingest API (token-protected) into LogZilla.
sec	Simple Event Correlator for stateful, multi-event correlation.
scriptserver	Runs user-defined scripts for trigger actions/correlation.
front	Web frontend serving UI and proxying API/ingest endpoints.
syslog	Syslog-ng receiver for BSD/RFC5424, JSON, RAW, and TLS inputs.
logcollector	Collects and consolidates internal container logs for diagnostics.
mailer	Outbound SMTP service for alerts and test emails.
telegraf	Collects internal metrics and ships them to time-series storage.
qdrant	Vector database backing AI features (embeddings/search).
influxdb	Time-series database for metrics and aggregates.
postgres	Primary relational store for users, dashboards, triggers, settings.
redis	In-memory caching and queues for ephemeral data.

Configuration Files and Settings

The following sections organize settings by their configuration files in `/etc/logzilla/settings/`:

Generic Settings (`generic.yaml`)

Setting	Description	Default	Range
`SEARCH_DEFAULT_LIMIT`	Default max results limit for search queries	`1000`	Integer
`FREE_DISK_SPACE_SOFT_LIMIT_GB`	Warning threshold for free disk space	`10`	Integer (GB)

Setting	Description	Default	Range
FREE_DISK_SPACE_HARD_LIMIT_GB	Critical threshold for free disk space	2	Integer (GB)
EXTERNAL_BASE_URL	External URL of the LogZilla instance	null	Valid URL
TIME_ZONE	Server timezone	UTC	Timezone string
RBAC_ENABLED	Enable Role Based Access Control	true	true, false
TASKS_ENABLED	Enable Tasks feature	true	true, false
AIR_GAPPED	Disable external service communication	false	true, false
PRUNE_DOCKER_IMAGES	Remove old Docker images during upgrades	true	true, false
SHOW_ADVANCED_SETTINGS	Show advanced settings in UI	false	true, false

Search Settings (`sphinx.yaml`)

Setting	Description	Default	Range
SPHINX_MIN_WORD_LENGTH	Minimum word length to index	-	Integer
SPHINX_MIN_PREFIX_LENGTH	Minimum prefix length to index	-	Integer
SPHINX_MIN_INFIX_LENGTH	Minimum infix length to index	-	Integer
SPHINX_MAX_DOCUMENTS_PER_INDEX	Max documents per index	-	Integer
SPHINX_MAX_INDEXING_TIME	Max indexing time per chunk (seconds)	-	Integer
SPHINX_MIN_INDEX_LEN	Min events per indexing batch	-	Integer

Setting	Description	Default	Range
SPHINX_REINDEX_PROC_MAX	Max concurrent indexing processes	-	Integer
SPHINX_MERGING_PROC_MAX	Max concurrent merging processes	-	Integer
SPHINX_REINDEX_DELAY	Delay between reindexing (seconds)	-	Integer
SPHINX_MAX_MATCHES	Maximum matches per query	-	Integer
SPHINX_MYSQL_PORT	Sphinx MySQL port (0 to disable)	-	Integer
SPHINX_HTTP_PORT	Sphinx HTTP port (0 to disable)	-	Integer
SPHINX_REALTIME_MODE	Enable realtime mode (experimental)	-	true, false

Trigger Settings (`triggers.yaml`)

Setting	Description	Default	Range
TRIGGERS_ENABLED	Enable or disable triggers	true	true, false
SEND_MAIL_PERIOD	Email resend interval (seconds)	60	Integer
SEND_WEBHOOK_PERIOD	Webhook resend interval (seconds, 0=always)	0	Integer
EXEC_SCRIPT_PERIOD	Script rerun interval (seconds)	60	Integer

SMTP Settings (`smtp.yaml`)

Setting	Description	Default	Range
MAIL_SENDER	Email address used as sender	logzilla@localhost	Email address
SMTP_SERVER	SMTP server address	localhost	Hostname/IP
SMTP_PORT	SMTP server port	25	Integer
SMTP_AUTH_REQUIRED	Enable SMTP authentication	false	true, false

Setting	Description	Default	Range
SMTP_USER	SMTP username for authentication	(empty)	String
SMTP_PASS	SMTP password for authentication	(empty)	String
SMTP_CRYPT	Encryption method	NONE	TLS, SSL, NONE
SMTP_TIMEOUT	Connection timeout (seconds)	30	Integer

Syslog Daemon Settings (`syslogng.yaml`)

Setting	Description	Default
SYSLOG_BSD_TCP_PORT	TCP port for BSD syslog (0 to disable)	514
SYSLOG_BSD_UDP_PORT	UDP port for BSD syslog (0 to disable)	514
SYSLOG_RFC5424_PORT	Port for RFC5424 syslog (0 to disable)	601
SYSLOG_JSON_PORT	Port for JSON syslog (0 to disable)	515
SYSLOG_RAW_PORT	Port for RAW TCP events (0 to disable)	516
SYSLOG_RAW_UDP_PORT	Port for RAW UDP events (0 to disable)	516

Setting	Description	Default
SYSLOG_TLS_PORT	Port for TLS syslog (0 to disable)	6514
SYSLOG_TLS_CERT_FILE	Path to TLS certificate file	/etc/logzilla/nginx/server.crt
SYSLOG_TLS_KEY_FILE	Path to TLS key file	/etc/logzilla/nginx/server.key
SYSLOG_MAX_CONNECTIONS	Maximum concurrent TCP connections	500
SYSLOG_FLOW_CONTROL	Enable flow control	true
SYSLOG_DISK_BUFFER	Enable disk buffer	false
SYSLOG_BUFFER_RELIABLE	Enable reliable disk buffer	false
SYSLOG_MEMORY_BUFFER_SIZE_MB	Memory buffer size (MB)	4
SYSLOG_MEMORY_BUFFER_LENGTH	Memory buffer length (messages)	50000
SYSLOG_DISK_BUFFER_SIZE_MB	Disk buffer size (MB)	1
SYSLOG_DESTINATION_WORKERS	Number of destination workers	2

Setting	Description	Default
SYSLOG_DESTINATION_BATCH_LINES	Lines per batch	10000
SYSLOG_DESTINATION_BATCH_TIMEOUT	Batch timeout (milliseconds)	500
SYSLOG_DEBUG	Enable debug logging (TSV format)	false
SYSLOG_DEBUG_JSON	Enable debug logging (JSON format)	false
PCI_COMPLIANT_LOGS	Enable PCI compliant logging	false

Application Ports (`application_ports.yaml`)

Dedicated syslog ports for vendors whose log format requires separate handling. Events received on these ports are automatically tagged for processing by the corresponding application rules. Each port listens on both TCP and UDP.

Setting	Description	Default	Range
SYSLOG_ARISTA_EOS_PORT	Arista EOS syslog port (0 to disable)	0	Integer
SYSLOG_CHECKPOINT_PORT	Check Point syslog port (0 to disable)	0	Integer
SYSLOG_DATAPOWER_PORT	IBM DataPower syslog port (0 to disable)	0	Integer
SYSLOG_DELL_N_SERIES_PORT	Dell N-Series switch syslog port (0 to disable)	0	Integer
SYSLOG_FIREEYE_PORT	FireEye syslog port (0 to disable)	0	Integer
SYSLOG_INFOBLOX_PORT	Infoblox NIOS syslog port (0 to disable)	0	Integer

Setting	Description	Default	Range
SYSLOG_MERAKI_PORT	Cisco Meraki syslog port (0 to disable)	0	Integer
SYSLOG_PALOALTO_PORT	Palo Alto syslog port (0 to disable)	0	Integer
SYSLOG_PALOALTO_SDWAN_ION_PORT	Palo Alto Prisma SD-WAN ION syslog port (0 to disable)	0	Integer
SYSLOG_SYMANTEC_PORT	Symantec Endpoint Protection syslog port (0 to disable)	0	Integer
SYSLOG_UNIFI_PORT	Ubiquiti UniFi syslog port (0 to disable)	0	Integer
SYSLOG_VMWARE_PORT	VMware syslog port (0 to disable)	0	Integer

SNMP Trap Settings (`snmptrapd.yaml`)

Setting	Description	Default	Range
SNMPTRAPD_ENABLED	Enable SNMP trap daemon module	False	True, False
SNMPTRAPD_FORMAT	Message field format (see snmptrapd(8))	See below	-
SNMPTRAPD_PROGRAM	Program field value for SNMP trap events	SNMPTrap	-
SNMPTRAPD_FACILITY	Facility field value for SNMP trap events	LOCAL0	-
SNMPTRAPD_SEVERITY	Severity field value for SNMP trap events	INFO	-
SNMPTRAPD_PORT	SNMP trap daemon port	162	-

Additional Configuration Files

Other important configuration files include:

- **`storage.yaml`**: Event storage, deduplication, and archiving settings
- **`parser.yaml`**: Message parsing engine configuration
- **`logger.yaml`**: Logging levels for different components
- **`forwarder.yaml`**: Event forwarding to external systems

- **`sec.yaml`**: Simple Event Correlator (SEC) integration
- **`front.yaml`**: Nginx frontend proxy configuration (HTTP/HTTPS ports)
- **`ldap.yaml`**: LDAP/Active Directory integration (supports multiple instances)
- **`ai.yaml`**: AI/ML feature settings
- **`httpreceiver.yaml`**: HTTP event receiver configuration
- **`influxdb.yaml`**: InfluxDB integration settings
- **`django_login.yaml`**: Django authentication settings
- **`license.yaml`**: License configuration
- **`secrets.yaml`**: Sensitive configuration data

Configuration Management Best Practices

Multi-Instance Configuration

LogZilla supports multiple instances of certain configurations. For example, to configure a secondary LDAP server:

```
# Configure primary LDAP server
logzilla settings update LDAP_ENABLED=true LDAP_SERVER=ldap1.company.com

# Configure secondary LDAP server
logzilla settings update --id 1 LDAP_ENABLED=true LDAP_SERVER=ldap2.company.com
```

This creates `ldap.yaml` and `ldap__1.yaml` files respectively.

Configuration Validation

The `logzilla settings` command validates all changes against predefined schemas before saving, preventing invalid configurations:

```
# This will fail with validation error if port is invalid
logzilla settings update SMTP_PORT=invalid_port
```

Backup and Recovery

Before making significant configuration changes, backup the settings directory:

```
# Create backup
cp -r /etc/logzilla/settings /etc/logzilla/settings.backup.$(date +%Y%m%d)
```

```
# Restore from backup if needed
cp -r /etc/logzilla/settings.backup.20241201 /etc/logzilla/settings
logzilla settings reload generic  # Reload as needed
```

Important Notes

Live Reloading vs Container Restart

Live Reloading: Core processing modules (parser, storage, query) support live reloading for most settings through the pub/sub mechanism.

Container Restart Required: API and Celery containers require restart for changes to take effect:

- SMTP settings
- LDAP configuration
- Database connections
- Security settings

SMTP Configuration

SMTP settings control outgoing email functionality for alerts and notifications. After changing SMTP settings, restart the API containers:

```
docker restart lz_gunicorn_1 lz_celeryworker_1
```

Configuration File Access

Inspect settings with the command line
The `logzilla settings list` command prints the current values for a specific configuration group:

```
logzilla settings list generic
logzilla settings list smtp
```

Inspect the configuration file directly
Administrators with root access can read the raw YAML file on disk:

```
cat /etc/logzilla/settings/generic.yaml
```

SNMP Trap Format Default

The default `SNMPTRAPD_FORMAT` setting is:

```
Enterprise OID: %N, Trap Type: %W, Trap Sub-Type: %q,
Uptime: %T, Description: %W,
PDU Attribute/Value Pair Array: %v
```

Legacy Configuration Command

Deprecated: The `logzilla config` command is deprecated and should not be used. It lacks support for multi-instance configurations and validation. Use `logzilla settings` instead.