LOGZILLA DOCUMENTATION

LDAP Authentication

Integrate LogZilla with LDAP and Active Directory for single sign-on, including multiple server configurations, group-based access, and TLS binding

Administration · Generated May 3, 2026 · logzilla.ai/docs/administration/ldap-authentication

LogZilla supports LDAP/Active Directory authentication with multiple server configurations. The LDAP system integrates with the modern settings framework and supports advanced features like group-based access control and TLS encryption.

Important: Before enabling LDAP authentication, ensure any existing local accounts with the same usernames or email addresses as LDAP accounts are renamed or removed to prevent conflicts.

LDAP Configuration

Web Interface Configuration (Recommended)

The **recommended approach** for configuring LDAP is through the LogZilla web interface, which provides a user-friendly experience with built-in validation and testing capabilities:

Access LDAP Settings:

- Log into the LogZilla web interface as an administrator
- Navigate to **Settings** → **Authentication** → **LDAP**

Configure Connection Settings:

- **Server URL**: Enter the LDAP server URL (e.g., `ldap://ldap.company.com:389`)
- **Bind DN**: Service account for LDAP searches
- **Bind Password**: Password for the service account
- **Configuration Name**: Friendly name for this LDAP server

Set User and Group Search:

- **User Search DN**: Base DN for user searches (e.g., `ou=users,dc=company,dc=com`)
- **Group Search DN**: Base DN for group searches (e.g., `ou=groups,dc=company,dc=com`)
- **Group Object Class**: Select appropriate class (`posixGroup`, `groupOfNames`, etc.)

Configure Field Mappings:

- **Username Field**: LDAP attribute for username (`uid`, `sAMAccountName`)
- **First Name Field**: LDAP attribute for first name (`givenName`)
- **Last Name Field**: LDAP attribute for last name (`sn`)
- **Email Field**: LDAP attribute for email (`mail`)

Set Access Control (Optional):

- **Required Groups**: Specify groups users must belong to

- **Group Whitelist**: Limit which groups are imported
- **Group Blacklist**: Exclude specific groups

Configure Security (Recommended):

- **Enable TLS/SSL**: Use encrypted connections
- **Certificate Validation**: Set appropriate validation level
- **Upload Certificates**: Add CA certificates if needed

Test and Enable:

- Use the **Test Connection** button to verify settings
- Test with actual user credentials
- **Enable** the LDAP configuration once testing succeeds

Advantages of Web Interface:

- **User-friendly forms** with validation and help text
- **Built-in testing tools** for immediate feedback
- **Certificate upload functionality** for TLS/SSL
- **Multiple server management** through the interface
- **No command-line knowledge required**

Advanced: Command Line Configuration

Note: Command-line configuration is provided for advanced users who specifically require shell access. Most users should use the web interface above, which provides the same functionality with a better user experience.

For users who prefer or require command-line administration:

```
# Initialize LDAP configuration interactively
logzilla ldap init
```

This interactive wizard will prompt for the same settings available in the web interface. After initial setup, individual settings can be modified:

```
# View current settings
logzilla settings list ldap

# Modify specific settings
logzilla settings update LDAP_TLS_START_TLS=true
logzilla settings update LDAP_OPT_DISABLE_REFERRALS=true
```

LDAP Configuration Overview

Regardless of configuration method, LDAP settings are stored in the modern LogZilla settings system:

- **Primary Configuration**: `/etc/logzilla/settings/ldap.yaml`
- **Additional Servers**: `/etc/logzilla/settings/ldap__1.yaml`, `ldap__2.yaml`, etc.
- **Certificate Storage**: `/etc/logzilla/settings/` (alongside configuration files)

The system supports multiple LDAP servers for redundancy and different organizational units.

LDAP Configuration Settings

All LDAP settings can be configured using the `logzilla settings update` command. Settings are stored in `/etc/logzilla/settings/ldap.yaml`.

Core Settings

Setting	Description	Example
`LDAP_ENABLED`	Enable/disable this LDAP configuration	`true`
`LDAP_SERVER_URL`	LDAP server URL	`ldap://ldap.company.com:389`
`LDAP_BIND_DN`	Service account DN for searches	`cn=service,ou=users,dc=company,dc=com`
`LDAP_BIND_PASSWORD`	Service account password	`password`
`LDAP_CONFIG_NAME`	Friendly name for this configuration	`Primary Active Directory`

User and Group Search

Setting	Description	Example
`LDAP_USER_SEARCH_DN`	Base DNs for user searches (list)	`["ou=users,dc=company,dc=com"]`

Setting	Description	Example
`LDAP_GROUP_SEARCH_DN`	Base DNs for group searches (list)	`["ou=groups,dc=company,dc=com"]`
`LDAP_GROUP_OBJECT_CLASS`	LDAP object class for groups	`posixGroup` or `groupOfNames`
`LDAP_GROUP_SEARCH_DN_FILTER`	LDAP filter for group searches	`(objectClass=posixGroup)`

Access Control

Setting	Description	Example
`LDAP_REQUIRE_GROUP_DN`	Required group membership (list)	`["cn=logzilla-users,ou=groups,dc=company,dc=com"]`
`LDAP_GROUP_NAMES`	Whitelist of group names to import (list)	`["logzilla-admins", "logzilla-users"]`
`LDAP_GROUP_NAMES_EXCLUDE`	Blacklist of group names to exclude (list)	`["disabled-users"]`

Field Mapping

Setting	Description	Common Values
`LDAP_FIELDS_USERNAME`	LDAP attribute for username	`uid`, `sAMAccountName`
`LDAP_FIELDS_FIRST_NAME`	LDAP attribute for first name	`givenName`
`LDAP_FIELDS_LAST_NAME`	LDAP attribute for last name	`sn`
`LDAP_FIELDS_EMAIL`	LDAP attribute for email	`mail`

TLS/SSL Settings

Setting	Description	Values
`LDAP_TLS_START_TLS`	Enable StartTLS	`true`, `false`
`LDAP_TLS_REQUIRE_CERT`	Certificate validation policy	`NEVER`, `ALLOW`, `DEMAND`
`LDAP_TLS_CA_CERTFILE`	CA certificate file path	`/etc/logzilla/settings/ca.pem`
`LDAP_TLS_CERTFILE`	Client certificate file path	`/etc/logzilla/settings/client.pem`
`LDAP_TLS_KEYFILE`	Client key file path	`/etc/logzilla/settings/client.key`

Advanced Options

Setting	Description	Default
`LDAP_OPT_DISABLE_REFERRALS`	Disable LDAP referrals (helps with AD)	`false`
`LDAP_OPT_NETWORK_TIMEOUT`	Network timeout in seconds	`30`

Multiple LDAP Servers

LogZilla supports multiple LDAP servers for redundancy or different organizational units.

Adding Additional Servers (Web Interface)

Navigate to LDAP Settings: Go to **Settings** → **Authentication** → **LDAP**
Add New Server: Click **Add LDAP Server** or similar option
Configure Second Server: Follow the same configuration steps as the primary server
Test and Enable: Test the additional server before enabling

Adding Additional Servers (Command Line)

For command-line users:

```
# Create additional LDAP configuration
logzilla ldap create
```

```
# Initialize the second LDAP server
logzilla ldap init --id 1

# Configure settings for second server
logzilla settings update --id 1 LDAP_SERVER_URL=ldap://ldap2.company.com:389
logzilla settings update --id 1 LDAP_CONFIG_NAME="Secondary LDAP"

# List all LDAP configurations
logzilla ldap list
```

Note: LDAP configuration IDs start at 0. Use `--id 1` when creating an additional LDAP configuration (the primary configuration is `--id 0`).

Testing and Activation

Testing LDAP Configuration

Web Interface Testing (Recommended):

Use the **Test Connection** button in the LDAP settings page
Enter test user credentials when prompted
Verify successful authentication and group retrieval
Review any error messages and adjust settings as needed
Command Line Testing: For users managing LDAP via command line:

```
# Test primary LDAP server
logzilla ldap test -u testuser -p testpassword

# Test specific LDAP server
logzilla ldap test --id 1 -u testuser -p testpassword
```

Enabling LDAP Authentication

Web Interface Activation:

After successful testing, use the **Enable** toggle in the web interface
The change takes effect immediately
Users can now log in using their LDAP credentials
Command Line Activation:

```
# Enable primary LDAP server
logzilla ldap enable
```

```
# Enable specific LDAP server
logzilla ldap enable --id 1

# Disable LDAP server if needed
logzilla ldap disable --id 1
```

Configuration Examples

These examples show common LDAP configurations. **Use the web interface** to enter these values through the user-friendly forms, or use the command-line examples if you prefer shell access.

Active Directory Configuration

Web Interface Settings:

- **Server URL**: `ldap://ad.company.com:389`
- **Bind DN**: `cn=ldapservice,ou=Service Accounts,dc=company,dc=com`
- **User Search DN**: `ou=Users,dc=company,dc=com`
- **Group Search DN**: `ou=Groups,dc=company,dc=com`
- **Username Field**: `sAMAccountName`
- **Group Object Class**: `group`
- **Advanced Options**: Enable "Disable Referrals"

Command Line Equivalent:

```
logzilla settings update LDAP_SERVER_URL=ldap://ad.company.com:389
logzilla settings update LDAP_BIND_DN="cn=ldapservice,ou=Service Accounts,dc=company,dc=com"
logzilla settings update LDAP_USER_SEARCH_DN='["ou=Users,dc=company,dc=com"]'
logzilla settings update LDAP_GROUP_SEARCH_DN='["ou=Groups,dc=company,dc=com"]'
logzilla settings update LDAP_FIELDS_USERNAME=sAMAccountName
logzilla settings update LDAP_GROUP_OBJECT_CLASS=group
logzilla settings update LDAP_OPT_DISABLE_REFERRALS=true
```

OpenLDAP Configuration

Web Interface Settings:

- **Server URL**: `ldap://openldap.company.com:389`
- **Bind DN**: `cn=admin,dc=company,dc=com`

- **User Search DN**: `ou=people,dc=company,dc=com`
- **Group Search DN**: `ou=groups,dc=company,dc=com`
- **Username Field**: `uid`
- **Group Object Class**: `posixGroup`

Command Line Equivalent:

```
logzilla settings update LDAP_SERVER_URL=ldap://openldap.company.com:389
logzilla settings update LDAP_BIND_DN="cn=admin,dc=company,dc=com"
logzilla settings update LDAP_USER_SEARCH_DN='["ou=people,dc=company,dc=com"]'
logzilla settings update LDAP_GROUP_SEARCH_DN='["ou=groups,dc=company,dc=com"]'
logzilla settings update LDAP_FIELDS_USERNAME=uid
logzilla settings update LDAP_GROUP_OBJECT_CLASS=posixGroup
```

TLS/SSL Configuration Example

Web Interface Settings:

- **Enable TLS**: Check the TLS/SSL option
- **Certificate Validation**: Set to "Required" for production
- **Upload CA Certificate**: Use the certificate upload feature
- **For LDAPS**: Use `ldaps://ldap.company.com:636` as Server URL

Command Line Equivalent:

```
logzilla settings update LDAP_TLS_START_TLS=true
logzilla settings update LDAP_TLS_REQUIRE_CERT=DEMAND
logzilla settings update LDAP_TLS_CA_CERTFILE=/etc/logzilla/settings/ca.pem

# For LDAPS (SSL)
logzilla settings update LDAP_SERVER_URL=ldaps://ldap.company.com:636
```

Group-Based Access Control

Web Interface Settings:

- **Required Groups**: Add groups that users must belong to
- **Group Whitelist**: Specify which groups to import
- **Group Blacklist**: Specify which groups to exclude

Command Line Equivalent:

```
logzilla settings update LDAP_REQUIRE_GROUP_DN='["cn=logzilla-users,ou=groups,dc=company,dc=com"]'
logzilla settings update LDAP_GROUP_NAMES='["logzilla-admins", "logzilla-users", "logzilla-viewers"]'
logzilla settings update LDAP_GROUP_NAMES_EXCLUDE='["disabled-accounts", "temp-users"]'
```

User Authentication

Login Requirements

Users should authenticate using their LDAP username only:

Correct Login Format:

- `jdoe`
- `john.doe`

Incorrect Login Formats:

- `jdoe@company.com` ❌
- `COMPANY\jdoe` ❌
- `cn=jdoe,ou=users,dc=company,dc=com` ❌

User Account Creation

When users successfully authenticate via LDAP:

LogZilla automatically creates local user accounts
User information is populated from LDAP attributes
Group memberships are synchronized
Users inherit permissions based on their LDAP groups

Troubleshooting

Common Issues

Authentication Failures:

```
# Check LDAP connectivity
logzilla ldap test -u testuser -p testpassword
```

```
# Verify settings
logzilla settings list ldap
```

Group Synchronization Issues:

```
# Check group search configuration
logzilla settings list ldap | grep GROUP

# Test with specific group filters
logzilla settings update LDAP_GROUP_SEARCH_DN_FILTER="(objectClass=posixGroup)"
```

TLS/SSL Problems:

```
# Disable certificate validation for testing
logzilla settings update LDAP_TLS_REQUIRE_CERT=NEVER

# Check certificate paths
ls -la /etc/logzilla/settings/*.pem
```

Log Analysis

LDAP authentication events are logged to the main LogZilla log:

```
# Monitor LDAP authentication attempts
grep -i "ldap\|auth" /var/log/logzilla/logzilla.log

# Check for specific errors
grep -i "ldap.*error" /var/log/logzilla/logzilla.log
```

Best Practices

Security

- **Use TLS/SSL**: Always encrypt LDAP communications in production
- **Service Accounts**: Use dedicated service accounts with minimal privileges
- **Group-Based Access**: Implement group-based access control
- **Regular Testing**: Periodically test LDAP connectivity

Performance

- **Multiple Servers**: Configure multiple LDAP servers for redundancy

- **Network Timeouts**: Adjust timeouts based on network conditions
- **Group Filtering**: Use specific group filters to reduce search scope

Maintenance

- **Monitor Logs**: Regularly check authentication logs
- **Update Certificates**: Keep TLS certificates current
- **Test Changes**: Always test configuration changes in non-production first
- **Document Settings**: Maintain documentation of LDAP configuration