Active Directory (AD) Federation

Requirements

- Keycloak 26.X installation
- Active Directory Domain Controller with Port 389/636 available
- Active Directory User with Directory Search Permissions and configured Password (non-interactive Service Accounts will not work)

Setup

1. Log into Keycloak, go to User federation
2. Click Add new provider and select LDAP from the Dropdown Menu
3. Configure a UI display name and set Vendor to Active Directory
4. Apply the following Settings

- Connection Url: `(ldap|ldaps)://<ip>:(389|636)`
- Enable StartTLS *Off* / *On* based on your Setup
- Use Truststore SPI *Always*
- Connection pooling *On*
- Bind type to *simple*
- Bind DN to your Active Directory User DN (example: `CN=Ldap Bind,OU=Service Accounts,DC=example,DC=local`)
- Bind credentials to your Active Directory User Password

- Edit mode *READ_ONLY* for Federation only or *WRITEABLE* for 2-way sync
- User DN to the base DN of your AD Structure (example: `cn=users,dc=example,dc=local`)
- Username LDAP attribute to `sAMAccountName`
- User object classes to `person, organizationalPerson, user`
- User LDAP Filter to `(&(objectClass=person)(mail=*))` if you want to require a configured Mail Address. Good for allowing only real Accounts
- Search Scope to *Subtree* for recursive searches or otherweise *One Level*

Synchronization Settings based on your desire.

Revision #1
Created 6 June 2026 15:19:37 by Oliver Karger
Updated 6 June 2026 15:26:18 by Oliver Karger