

OpenMRS ID - Architecture

- [Introduction](#)
- [LDAP Objects](#)
- [Full Hierarchy](#)

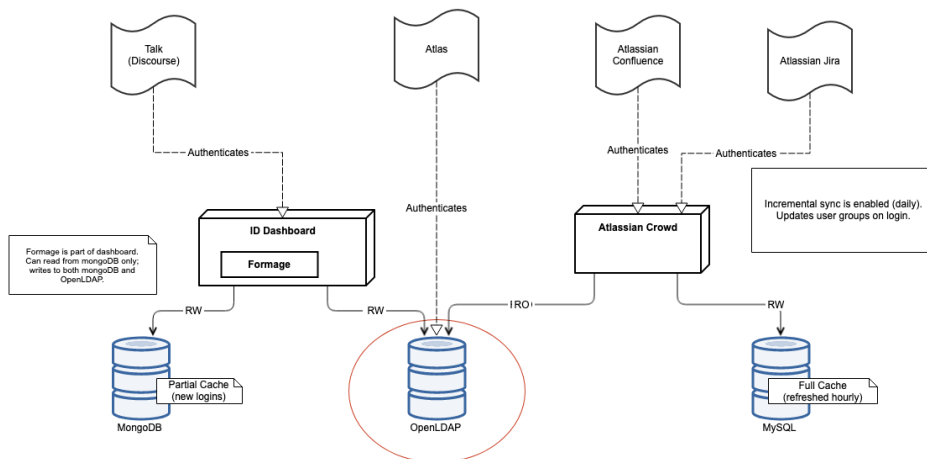
Introduction

The collective "OpenMRS ID" refers to this system of user management used by the OpenMRS community. An individual user in the system (a person with a username and password) is said to have a single "OpenMRS ID".

The ID subsystem is formed by:

- **OpenLDAP**: the data storage for all OpenMRS ID data for verified users (after checking email).
- **ID Dashboard**: web application that facilitates creation of new OpenMRS IDs, profile editing. Information is retrieved from cache in MongoDB, or loaded from OpenLDAP if not on cache.
 - **Formage**: admin screen in ID dashboard to modify users
- **Crowd**: Provides user management for Atlassian tools. It works as a bridge between LDAP and those applications.

Jira, Crowd and Wiki have a local/internal user to fix connections with Crowd/LDAP. They also an internal captcha to catch users with multiple failure attempts.



LDAP Objects

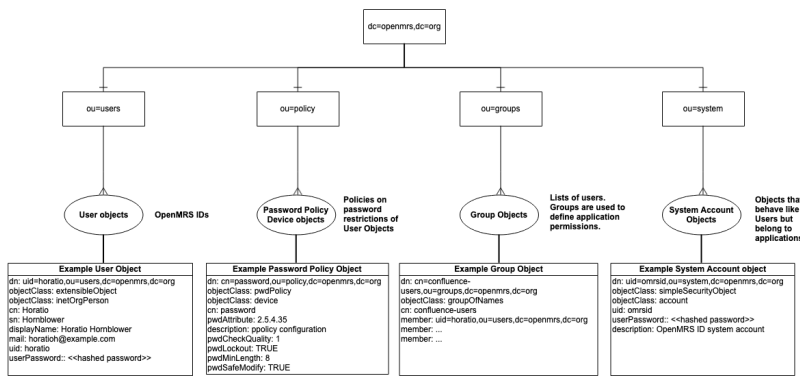
LDAP is a hierarchical data storage.

The top level node is 'dc=openmrs,dc=org'.

All users belong to 'ou=users,dc=openmrs,dc=org', what means that users is an Organization Unit (just a child node like any other) of node 'dc=openmrs,dc=org'.

A username 'jane_doe' is represented as "uid=jane_doe,ou=users,dc=openmrs,dc=org", which is 'user ID jane_doe' child node of node 'ou=users' of node 'dc=openmrs,dc=org'.

Full Hierarchy



Top-level 'organization' object in the hierarchy

'organizationalUnit' objects divide entities into logical groupings

Example User Object
 dn: uid=horatio,ou=users,dc=openmrs,dc=org
 objectClass: extensibleObject
 objectClass: inetOrgPerson
 cn: Horatio
 dn: Hornblower
 displayName: Horatio Hornblower
 mail: horatio@example.com
 uid: horatio
 userPassword: <<hashed password>>

Example Password Policy Object
 dn: cn=password,ou=policy,dc=openmrs,dc=org
 objectClass: pwdPolicy
 objectClass: device
 cn: password
 pwdAttribute: 2.5.4.35
 description: policy configuration
 pwdCheckQuality: 1
 pwdLockout: TRUE
 pwdMinLength: 8
 pwdSafeModify: TRUE

Example Group Object
 dn: cn=confluence-users,ou=groups,dc=openmrs,dc=org
 objectClass: groupOfNames
 cn: confluence-users
 member: uid=horatio,ou=users,dc=openmrs,dc=org
 member: ...

Example System Account object
 dn: uid=horatio,ou=system,dc=openmrs,dc=org
 objectClass: simpleSecurityObject
 objectClass: account
 uid: onmsid
 userPassword: <<hashed password>>
 description: OpenMRS ID system account

OpenMRS IDs

Policies on password restrictions of User Objects

Lists of users. Groups are used to define application permissions.

Objects that behave like Users but belong to applications