

# LDAP Directory Manager Plugin for LDAP or Active Directory Integration

This plugin provides a user directory implementation that retrieves user and group information from an LDAP server. To use it, go to System Setting > Directory Manager Setting, select "LDAP Directory Manager" from the drop-down list and click on the **Select** button.

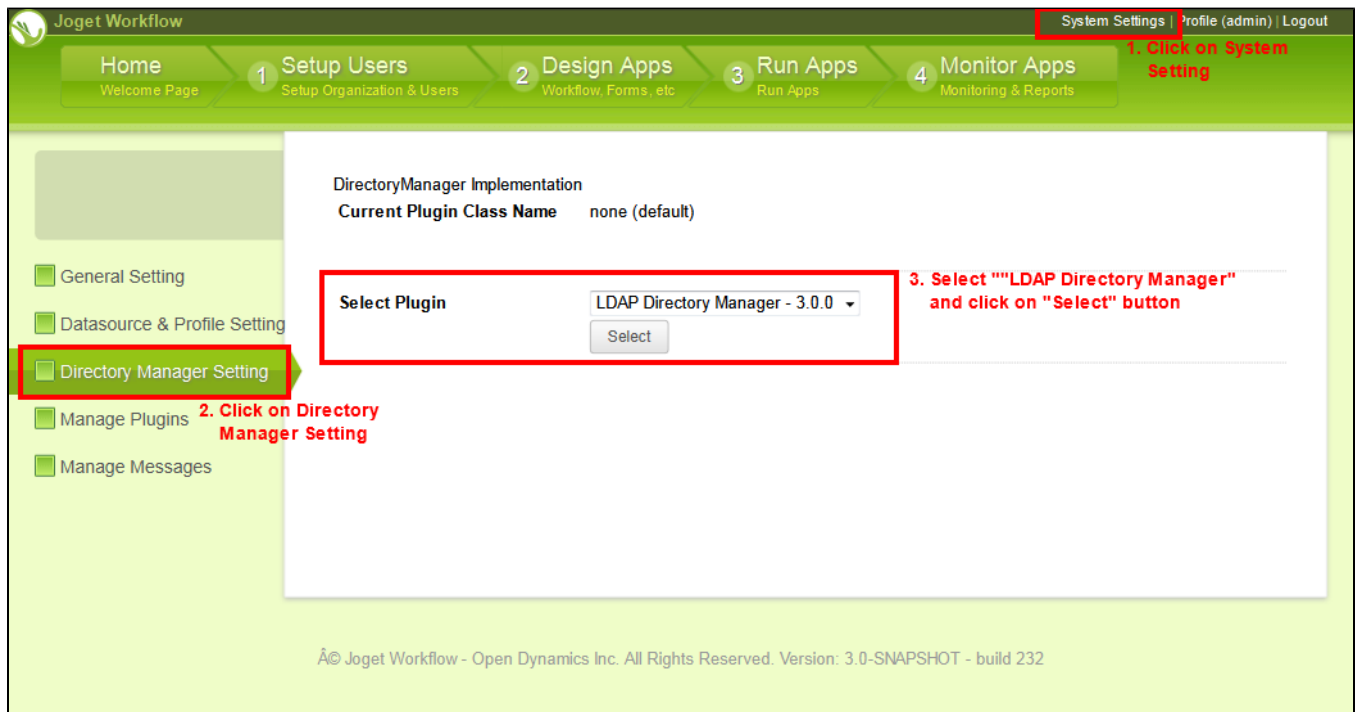


Figure 1 : Steps to Enable LDAP Directory Manager

After that, a configuration screen (as in Figure 2) will appear. Set the LDAP Directory Manager according to your LDAP organization structure, then submit.

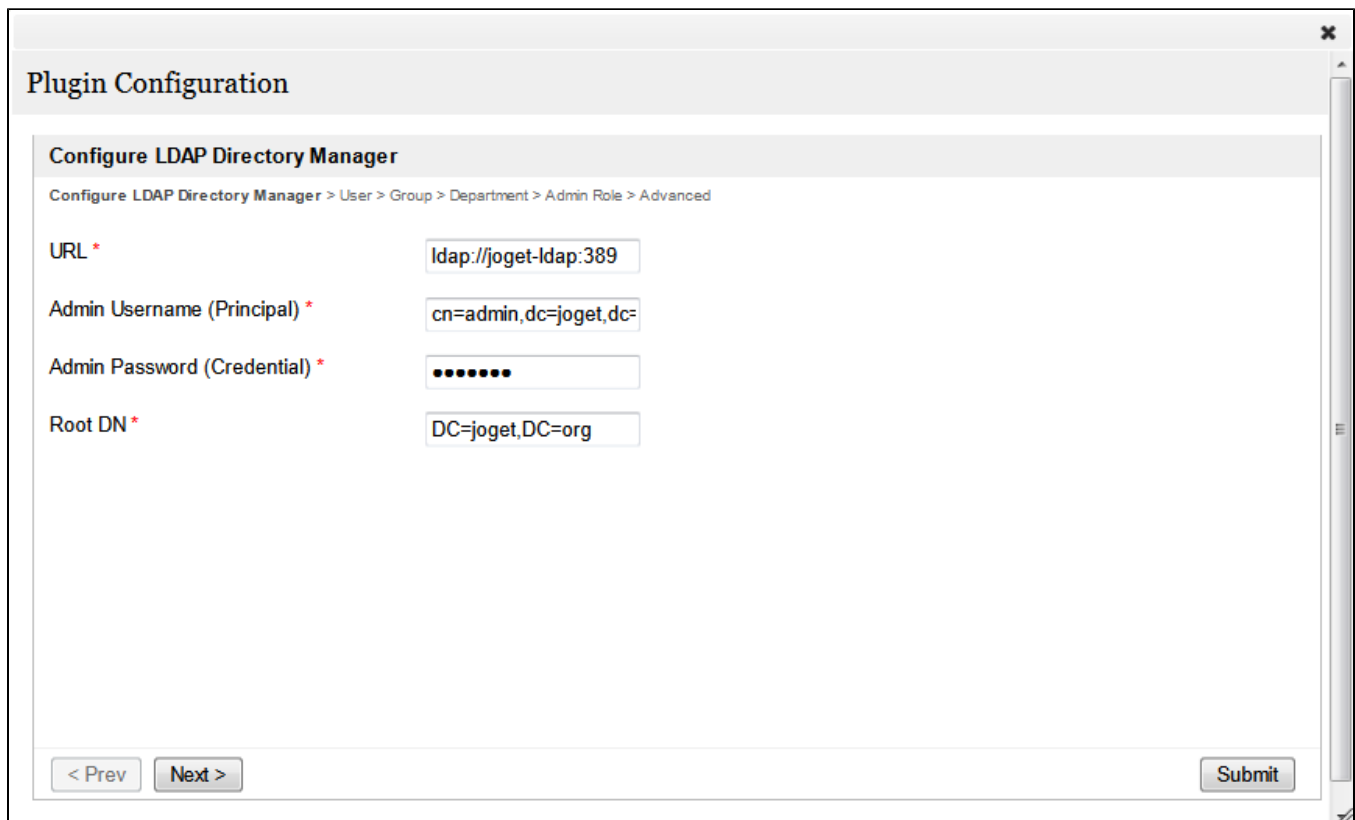


Figure 2: LDAP Directory Manager Configuration Screen

After the configurations have been set correctly, the LDAP directory manager implementation will be enabled. You will be required to log out and then to log in again. You can use the value set in the "Admin Username (Principal)" and "Admin Password (Credential)" to log in to the Workflow Management Console as admin in case your LDAP directory manager configuration doesn't work. Note that when the LDAP directory manager implementation is enabled, **Setup Users** in the main navigator of Workflow Management Console is disabled.

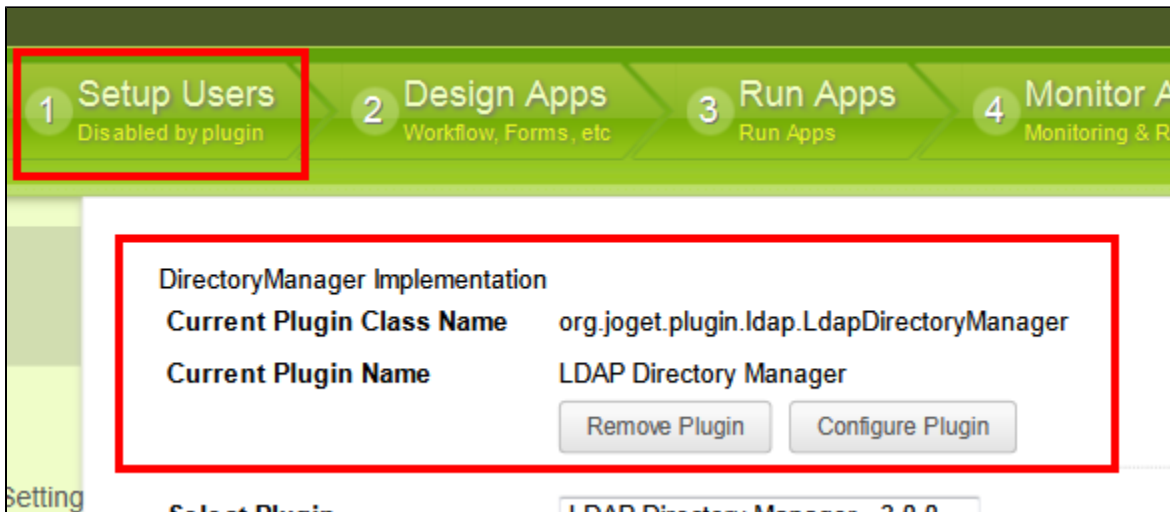


Figure 3: After LDAP Directory Manager Is Enabled

## Configuration Explanation

[Page 1 : Configure LDAP Directory Manager](#)

**URL :** URL of the LDAP server

**Admin Username (Principal) :** Login username (also known as principal) of the LDAP user who has permission to browse the targeted LDAP server. It can also be used to log in to the Workflow Management Console as admin (useful in the event that the LDAP Plugin configuration doesn't work).

**Admin Password (Credential) :** Login password (also known as credential) of the LDAP user that has permission to browse the targeted LDAP server. It can also be used to log in to the Workflow Management Console as admin (useful in the event that the LDAP Plugin configuration doesn't work).

**Root DN :** Root DN to be queried for LDAP entries

[Page 2 : User](#)

**User Base DN :** Base DN of the LDAP user entries; if not specified, the Root DN will be used.

**User Import Search Filter :** LDAP filter query to return LDAP user entries. eg. "(objectClass=person)"; refer to [LDAP Filter Syntax](#).

**Attribute Mapping - Username :** LDAP entry attribute that returns the username of the user (e.g., "sAMAccountName")

**Attribute Mapping - First Name :** LDAP entry attribute that returns the first name of the user

**Attribute Mapping - Last Name :** LDAP entry attribute that returns the last name of the user

**Attribute Mapping - Email :** LDAP entry attribute that returns the email of the user

**Attribute Mapping - Status :** LDAP entry attribute that returns the status of the user; the returned value should be either 1 or 0. If not specified, the value will be set to 1 for all users.

**Attribute Mapping - Time Zone :** LDAP entry attribute that returns the time zone of the user; the returned value should be a number from -12 to 12 ( $\geq -12$  and  $\leq 12$ ).

**Attribute Mapping - Report To :** LDAP entry attribute that returns the primary attribute value of an LDAP user entry which a user is reporting to (e.g., "manager"); the "reportTo" takes higher precedence than the HOD defined in Department

**Map To "Report To" Entry Attribute :** the primary attribute of an LDAP entry that returns by "Report To" (e.g., "distinguishedName")

**Attribute Mapping - Groups :** LDAP entry attribute that returns the primary attribute value of an LDAP group entry which a user belongs to (e.g., "memberOf"); used only when group info is also kept in the LDAP user

**Map To LDAP Group Entry Primary Attribute :** the primary attribute of an LDAP entry that returns by "Groups" (e.g., "distinguishedName")

**Attribute Mapping - Departments :** LDAP entry attribute that returns the primary attribute value of an LDAP department entry which a user belongs to (e.g., "memberOf"); used only when department info is also kept in the LDAP user.

**Map To LDAP Department Entry Primary Attribute :** the primary attribute of an LDAP entry that returns by "Departments" (e.g., "distinguishedName")

[Page 3 : Group](#)

**Group Base DN** : Base DN of LDAP group entries; if not specified, the Root DN will be used.

**Group Import Search Filter** : LDAP filter query to return LDAP group entries, e.g., "(objectClass=group)"; if not specified, no group will be queried. Refer to [LDAP Filter Syntax](#).

**Attribute Mapping - Id** : LDAP entry attribute that returns the ID of the group (e.g., "distinguishedName")

**Attribute Mapping - Name** : LDAP entry attribute that returns the name of the group

**Attribute Mapping - Description** : LDAP entry attribute that returns the description of the group

**Attribute Mapping - Users** : LDAP entry attribute that returns the primary attribute value of an LDAP user entry (e.g., "member")

**Map To LDAP User Entry Primary Attribute** : the primary attribute of an LDAP entry that returns by "Users" (e.g., "distinguishedName")

[Page 4 : Department](#)

**Department Base DN** : Base DN of the LDAP department entries; if not specified, the Root DN will be used.

**Department Import Search Filter** : LDAP filter query to return LDAP department entries, e.g., "(objectClass=group)"; if not specified, no department will be queried. Refer to [LDAP Filter Syntax](#).

**Attribute Mapping - Id** : LDAP entry attribute that returns the ID of the department

**Attribute Mapping - Name** : LDAP entry attribute that returns the name of the department

**Attribute Mapping - Description** : LDAP entry attribute that returns the description of the department

**Attribute Mapping - HOD** : LDAP entry attribute that returns the primary attribute value of an LDAP user entry which represents a head of department (e.g., "manager")

**Attribute Mapping - Users** : LDAP entry attribute that returns the primary attribute value of an LDAP user entry (e.g., "member")

**Map To LDAP User Entry Primary Attribute** : the primary attribute of an LDAP entry that returns by "HOD" and "Users" (e.g., "distinguishedName")

[Page 5 : Admin Role](#)

**Admin Role Base DN** : Base DN of the LDAP admin role entries; if not specified, the Root DN will be used.

**Admin Role Import Search Filter** :LDAP filter query to return LDAP department entries, e.g., "(objectClass=group)"; if not specified, no user with administrator role will be queried. Refer to [LDAP Filter Syntax](#).

**Attribute Mapping - Users** : LDAP entry attribute that returns the primary attribute value of an LDAP user entry (e.g., "memberZ"); returned LDAP user entries will be granted with admin role in the Workflow Management Console.

**Map To LDAP User Entry Primary Attribute** : the primary attribute of an LDAP entry that returns by "Users" (e.g., "distinguishedName")

[Page 6 : Advanced](#)

**Result Size Per Paged Search** : controls the total number of entries that can be returned by a paged search; to disable paged search, set the value to 0.

**Debug Mode** : if ticked, debugging messages will be logged to help troubleshooting.

## Sample Configuration

[sample-ldap-joget.org.ldif](#) (click to download), contains a sample LDAP structure assembling the standard organization chart and user base bundled into the Joget Workflow database in default installation.

For a brief graphical illustration, the LDAP structure looks like this:

The screenshot displays two windows from the Windows Server 2008 R2 environment. The left window, titled 'LDAP Browser', shows a hierarchical tree of LDAP entries. The right window, titled 'LDAP Explorer', shows the details of a selected entry.

**LDAP Browser (Left Window):**

- DIT
  - Root DSE (2)
    - dc=joget,dc=org (8)
      - cn=admin
      - cn=CEO-Office (1)
        - cn=terry
      - cn=Finance (1)
        - cn=tina
      - cn=Human-Resource-Admin (2)
        - cn=julia
        - cn=sasha
      - cn=Marketing (2)
        - cn=etta
        - cn=roy
      - cn=Product-Development (3)**
        - cn=cat
        - cn=clark
        - cn=tana
      - cn=Support-Services (1)
        - cn=david
      - cn=Training-Consulting (1)
        - cn=jack

**LDAP Explorer (Right Window):**

DN: cn=Product-Development,dc=joget,dc=org

| Attribute   | Description | Value                                           |
|-------------|-------------|-------------------------------------------------|
| objectClass |             | groupOfNames (structural)                       |
| objectClass |             | top (abstract)                                  |
| cn          |             | Product-Development                             |
| member      |             | cn=cat,cn=Product-Development,dc=joget,dc=org   |
| member      |             | cn=clark,cn=Product-Development,dc=joget,dc=org |
| member      |             | cn=tana,cn=Product-Development,dc=joget,dc=org  |
| description |             | Product Development                             |
| owner       |             | cn=clark,cn=Product-Development,dc=joget,dc=org |

Using this sample LDAP structure, the LDAP Plugin is configurable. Here is a sample configuration:

**URL :** ldap://hostname:389 (please change this accordingly)

**Admin Username (Principal) :** cn=admin,dc=joget,dc=org

Admin Password (Credential) : admin

**Root DN :** DC=joget,DC=org

User Base DN :

User Import Search Filter : (objectClass=person)

Attribute Mapping - Username : cn

**Attribute Mapping - First Name :** givenName

Attribute Mapping - Last Name : sn

Attribute Mapping - Email : mail

Attribute Mapping - Status :

Attribute Mapping - Time Zone : 8

**Attribute Mapping - Report To :**

Map To "Report To" Entry Attribute :

**Map To LDAP Group Entry Primary Attribute :**

**Attribute Mapping - Departments :**

Map To LDAP Department Entry Primary Attribute :

**Group Base DN :**

Group Import Search Filter : (objectClass=groupOfNames)

Attribute Mapping - Id : cn

**Attribute Mapping - Name :** description

**Attribute Mapping - Description :** description

Attribute Mapping - Users : member

**Map To LDAP User Entry Primary Attribute :** distinguishedName

Department Base DN :

**Department Import Search Filter** : (objectClass=groupOfNames)

**Attribute Mapping - Id** : cn

**Attribute Mapping - Name** : description

**Attribute Mapping - Description** : description

**Attribute Mapping - HOD** : owner

**Attribute Mapping - Users** : member

**Map To LDAP User Entry Primary Attribute** : distinguishedName

**Admin Role Base DN** :

**Admin Role Import Search Filter** : (cn=clark)

**Attribute Mapping - Users** : distinguishedName

**Map To LDAP User Entry Primary Attribute** : distinguishedName

**Result Size Per Paged Search** : 100

**Debug Mode** :

1. We can login to the Workflow Management Console as admin using one of these users:#\* username: cn=admin,dc=joget,dc=org, password: admin#\* username: clark, password: password
2. These are the departments and user groups that will be pulled:#\* CEO's Office#\* Finance#\* Human Resource & Admin#\* Marketing#\* Product Development#\* Support & Services#\* Training & Consulting