LDAP Directory Manager

Introduction

The **LDAP Directory Manager** allows you to integrate Joget with your existing AD/LDAP server. The enhanced LDAP Directory Manager implements all methods on the Joget Directory Manager class. In other words, it has been made possible to list and navigate through user, department and group entities in Joget itself.

Cautions And Warnings

Do not **lock yourself out** when you are configuring any Directory Manager plugin. Keep your browser session open and perform actual test in other machine/browser so that in case of any wrong configurations used, you can still continue to make amends.
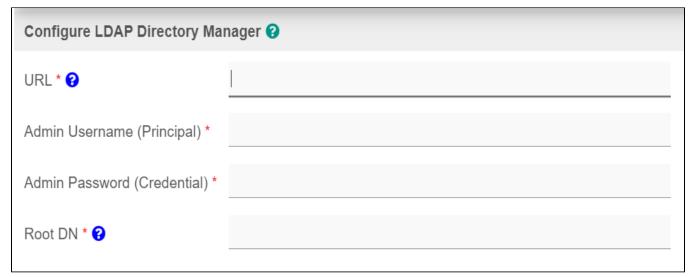
User license determines how many eventual users (sorted alphabetically by username in ascending order) from your LDAP/AD who can login to Joget. Make sure that you configure the plugin accordingly.

In case you have a misconfiguration and cannot login, you can make use of the credential set above (**Admin Username (Principal) & Admin Password (Credential)**) to login as the administrator.

The LDAP Directory Manager has a **Debug Mode** (option in the last tab) which is highly recommended to be turned on when configuring the LDAP plugin for the first time or when you are having issues. When debug mode is on, you can find all the search queries performed by the directory manager. They will all be logged into the joget.log files. From there, you can observe the search filter string and improve the accuracy and performance of the lookup. You can remove the debug checkbox once everything is running well.

LDAP Directory Manager Properties

Configure LDAP Directory Manager

Figure 1: Configure LDAP Directory Manager

Name	Value
URL	• ldap://IP_ADDRESS:389 • ldaps://IP_ADDRESS:636
Admin Username (Principal)	LDAP username with read permission to LDAP/AD. Example: cn=admin,dc=joget,dc=org
Admin Password (Credential)	admin
Root DN	DC=joget,DC=org

Users

User

User Base DN	
User Import Search Filter ❓	(objectClass=person)
Attribute Mapping - Username *	sAMAccountName
Attribute Mapping - First Name	givenName
Attribute Mapping - Last Name	sn
Attribute Mapping - Email	userPrincipalName
Attribute Mapping - Status ❓	
Attribute Mapping - Time Zone ❓	
Attribute Mapping - Locale ❓	

Figure 2: Users Properties

Name	Value	Screen (Click to view)

User Base DN	User Base DN
	
	Tips
	
	If you set the "User Base DN" to your LDAP Root DN, it means that the search will start from the Root DN until it finds all the results that matched the search filter.
	
	So, setting the "User Base DN" precisely is very important as it will decide where the search is starting from. It will save all the unnecessary search between the Root DN to your "User Base DN".
	
	Root DN
	
	`DC=joget,DC=org`
	
	Under the Root DN, you have the following DN:
	
	`DC=HR,DC=joget,DC=org`
	`DC=Product Department,DC=joget,DC=org`
	`DC=Operation,DC=joget,DC=org`
	`DC=Users,DC=joget,DC=org`
	
	If your users are all under "DC=Users,DC=joget,DC=org", you should set this to "User Base DN".
	
	By doing this, it will not go through all the other entries and it's child entries before reaching "DC=Users,DC=joget,DC=org".
		Figure 2: Users Properties

User Import Search Filter	(objectClass=person) **Tips** **Value** `(&(objectClass=person)(|(cn=admin)(cn=cat)(cn=jack)(cn=john)(cn=jackie)))` This mean all the LDAP entries which have "objectClass" attribute equals to "person" and "cn" attribute equals to either "admin", "cat", "jack", "john" or "jackie" are Joget users. So, when a login is performed by "admin", the search filter will add additional filter and become "(&(&(objectClass=person)(|(cn=admin)(cn=cat)(cn=jack)(cn=john)(cn=jackie)))(cn=admin))". You will notice an extra (cn=admin) is added to the search filter to make sure it return only the "admin" user. **User License** User license determines on how many eventual users (sorted alphabetically) from your LDAP/AD can log in into the system. You can make use of this attribute to control amount of users returned from your LDAP. Please refer to other LDAP Search Filter syntax.	
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 - Locale	en_US

Employment

Figure 3: Employment Properties

Name	Value
Attribute Mapping - Employee Code	
Attribute Mapping - Job Title	
Attribute Mapping - Report To	
Map To "Report To" Entry Attribute	
Attribute Mapping - Groups	

Map To LDAP Group Entry Primary Attribute	dn
	ⓘ **DN** A distinguished name (usually just shortened to "**DN**") uniquely identifies an entry and describes its position in the DIT. ... DNs are comprised of zero or more comma-separated components called relative distinguished names, or RDNs. | Directory Service	DN Entity Name
OpenLDAP	entryDN
Microsoft AD	distinguishedName	
Attribute Mapping - Departments	
Map To LDAP Department Entry Primary Attribute	dn
Attribute Mapping - Grade	
Map To LDAP Grade Entry Primary Attribute	dn
Attribute Mapping - Metas	Additional attributes to retrieve using #user.USERNAME.meta.KEY# or #currentUser.meta.KEY# | Name	Description
Key	Key name
Attribute	Attribute name in LDAP	

Group

Figure 4: Group Properties
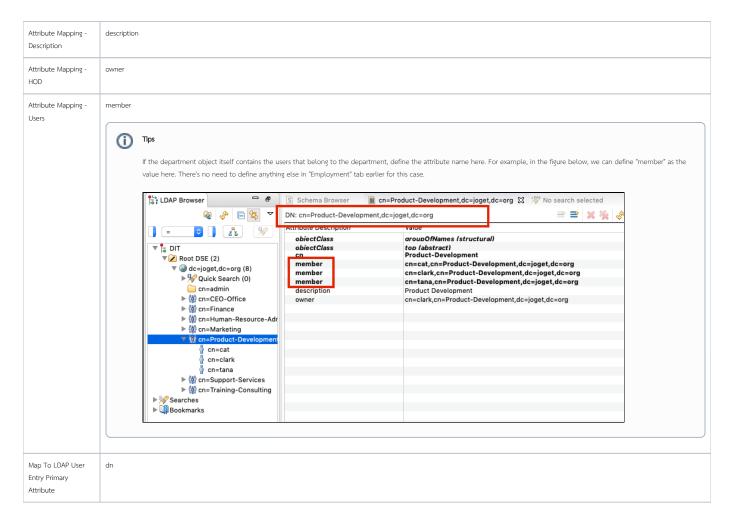
Name	Value
Group Base DN	
Group Import Search Filter	(objectClass=groupOfNames) Please refer to other LDAP Search Filter syntax.
Attribute Mapping - ID	cn
Attribute Mapping - Name	description
Attribute Mapping - Description	description
Attribute Mapping - Users	member
Map To LDAP User Entry Primary Attribute	dn

Department

Figure 5: Department Properties

Name	Value
Department Base DN	
Department Import Search Filter	(objectClass=groupOfNames) Please refer to other LDAP Search Filter syntax.
Attribute Mapping - ID	cn
Attribute Mapping - Name	description

Attribute Mapping - Description	description
Attribute Mapping - HOD	owner
Attribute Mapping - Users	member **Tips** If the department object itself contains the users that belong to the department, define the attribute name here. For example, in the figure below, we can define "member" as the value here. There's no need to define anything else in "Employment" tab earlier for this case.
Map To LDAP User Entry Primary Attribute	dn

Grade

Figure 6: Grade Properties

Name	Value
Grade Base DN	
Grade Import Search Filter	Please refer to other LDAP Search Filter syntax.
Attribute Mapping - ID	
Attribute Mapping - Name	
Attribute Mapping - Description	
Attribute Mapping - Users	
Map To LDAP User Entry Primary Attribute	

Admin Role

Figure 7: Admin Role Properties

Name	Value
Admin Role Base DN	
Admin Role Import Search Filter	(&(objectClass=person)(cn=admin)) Please refer to other LDAP Search Filter syntax.
Attribute Mapping - Users	cn
Map To LDAP User Entry Primary Attribute	dn

Advanced

Figure 8: Advance Properties

Name	Value
Result Size Per Paged Search	100
Debug Mode	Click checkbox to enable helpful debugging messages in your Joget logs.

Configuring The User Import Search Filter

The following articles might be useful to you to understand how to filter users based on the groups in LDAP:

- https://flylib.com/books/en/1.434.1/optimizing_search_performance.html
- https://stackoverflow.com/questions/9890049/ldap-query-to-list-all-users-of-a-certain-group
- https://stackoverflow.com/questions/17664101/ldap-list-all-users-in-specific-groups
- https://stackoverflow.com/questions/48361525/ldap-query-to-retrieve-members-of-a-group

- LDAP Search Filter Syntax: https://docs.microsoft.com/en-us/windows/desktop/adsi/search-filter-syntax

You can use the pipe symbol '|' to denotes 'OR' and include a second (or more) search parameters, for example:

(|(objectClass=person)(objectClass=user))

Related Documentation

Sync LDAP User Directory Manager