5.5 Light Weight Directory Access Protocol(LDAP) Users

Starting from OpenClinica 3.1.4, OpenClinica can be set up to authenticate users against an LDAP/Active Directory server to support single user accounts across the multiple applications and systems used in the organization.

The integration with an Active Directory server supports the following capabilities:

Querying available Active Directory accounts within OpenClinica
Assignment of study roles and user privileges within OpenClinica
Authentication of username and password via Active Directory

Ldap/Active directory authentication can be turned off or on from the datainfo properties. These settings are described as under.

Adding an LDAP user to OpenClinica is described here. These users should already be exisiting in the active directory.

The SOAP based webservices are not supported for LDAP users.

5.5.1 LDAP/Active Directory Configuration

In order to have OpenClinica configured to authenticate users using LDAP/Active Directory, these configuration values need to be defined in datainfo properties. As of 3.1.4, these are the new properties that are added to the datainfo properties and need to be set in order to enable LDAP.

Property name	Description
ldap.enabled	Set to true if LDAP/ActiveDirectory should be used to authenticate users in OpenClinica. Values allowed for this field are true and false.
ldap.host	LDAP/ActiveDirectory server host address. Example: ldap://ldapserver:389

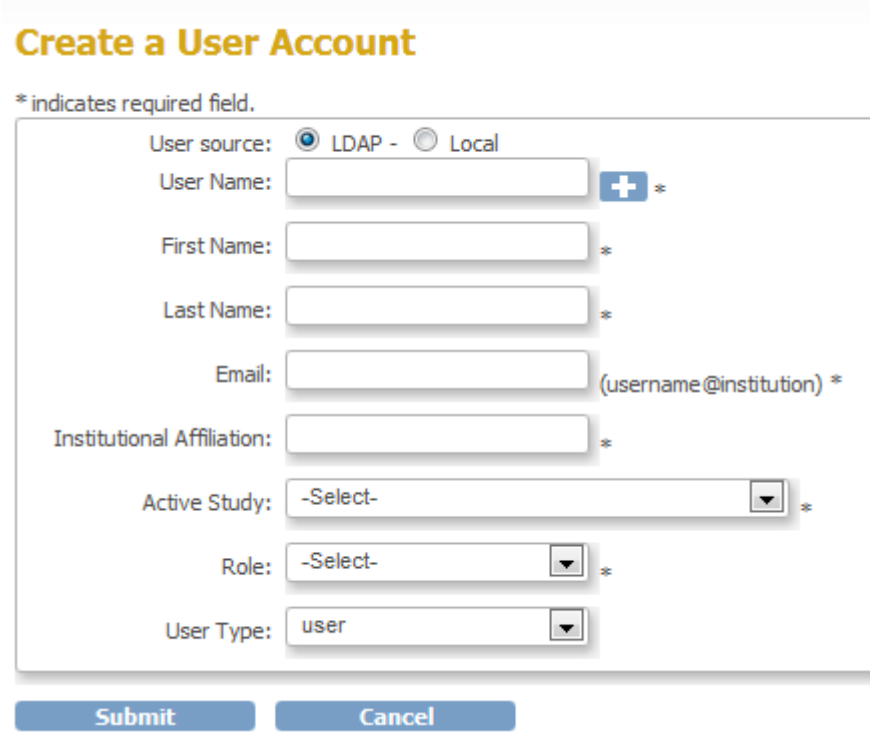
Property name	Description
ldap.userDn	Distinguished name (DN) of the user account which can authenticate to LDAP/ActiveDirectory, to perform the authentication of OpenClinica users. This user must have privileges to search the LDAP structure. We recommend creating a dedicated LDAP/ActiveDirectory account to be used in this property. Example: CN=openclinica,OU=example,OU=com
ldap.password	Password of the user configured in the property ldap.userDn.
ldap.loginQuery	Query used during login to retrieve an LDAP account by username, where the placeholder {0} is replaced by the username typed in the login screen. This query must never return more than one account. To increase overall application security, this query should never return a user account that has no access to OpenClinica (e.g., by filtering accounts that belong to a specific group). Example: (&(memberOf=CN=group,OU=example,OU=com)(sAMAccountName=*{0}*))
ldap.passwordRecoveryURL	URL to redirect LDAP/ActiveDirectory users when the forgotten password link is clicked.
ldap.userSearch.baseDn	Base DN to search for user accounts in LDAP/ActiveDirectory. Only user accounts that belong to this base DN can be configured as an OpenClinica user account. Example: OU=example,OU=com
ldap.userSearch.query	LDAP query used to search for users in the LDAP Users Search screen, where the placeholder {0} is replaced by the text entered in the Search field. To increase overall application security, this query should never return a user account that has no access to OpenClinica (e.g., by filtering accounts that belong to a specific group). Example: (&(memberOf=CN=group,OU=example,OU=com)(sAMAccountName=*{0}*))
ldap.userData.distinguishedName	Name of the LDAP property from which the distinguished name (DN) will be retrieved.
ldap.userData.username	Name of the LDAP property from which the username will be retrieved.
ldap.userData.firstName	Name of the LDAP property from which the first name will be retrieved.
ldap.userData.lastName	Name of the LDAP property from which the last name will be retrieved.
ldap.userData.email	Name of the LDAP property from which the email will be retrieved.
ldap.userData.organization	Name of the LDAP property from which the organization will be retrieved.

5.5.2 Adding a LDAP User to OpenClinica.

The first time you log in to OpenClinica, you must use a local account with Business or Technical Administrator privileges (i.e. root). Once you have created the first LDAP/Active Directory account in OpenClinica with Business or Technical Administrator privileges, you will not need the local account again (unless you are using web services.)

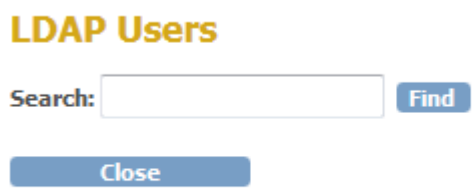
Follow these quick steps to add an LDAP/Active Directory

1. Select Tasks > Users (under the Administration section)
2. Select the Create New User link and you will be presented with the Create a User Account page.



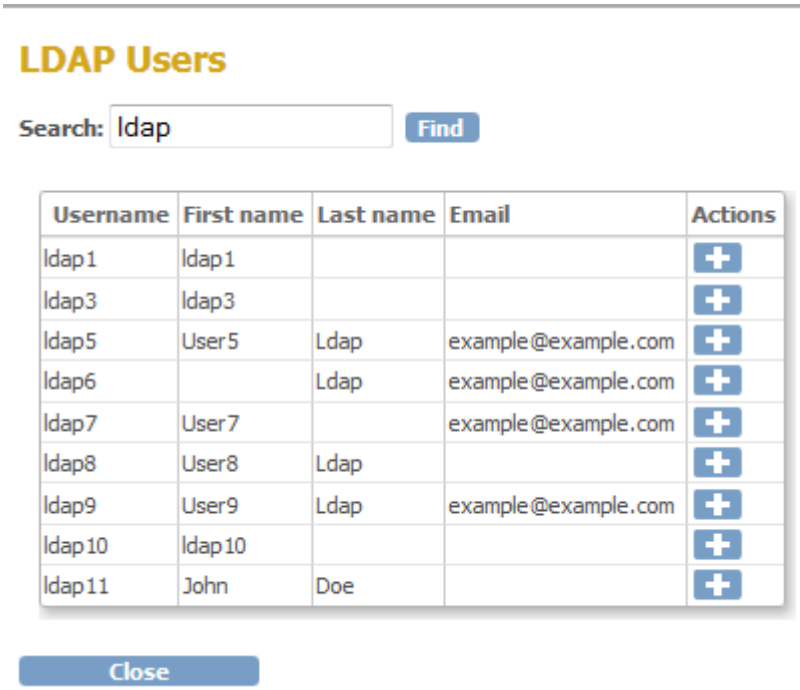
3.When LDAP/Active Directory authentication is enabled, the LDAP radio button will be pre-selected

4.Select the + next to the User Name field and a popup window will appear



5. Enter search criteria in the text box to find an account in the LDAP/Active Directory system based on either user name or email address and select Find

Only users that have been assigned to a particular Group in the LDAP/Active Directory system will be searched against. The Group is defined by your Systems Administrator in the Administration > Users > Configure Password Requirements screen.



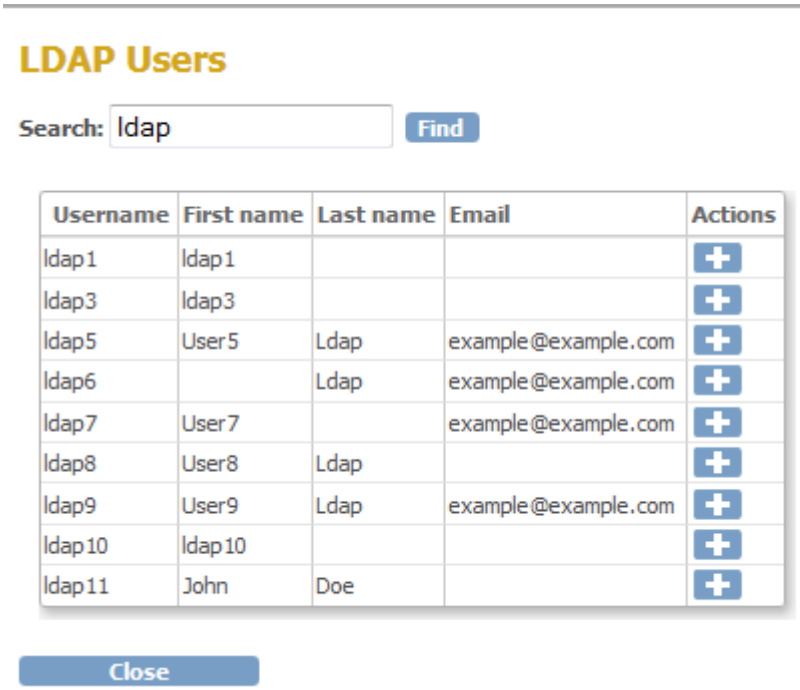
6. Select the to populate the users information to the Create a User Account page
7. The popup window will close and you will be brought back to the Create a User Account page

a. Depending on the amount of information contained in the LDAP system, the following fields will be populated:

i. User Name
ii. First Name
iii. Last Name
iv. Email
v. Institutional Affiliation

b. The following fields will still need to be configured:

i. Active Study
ii. Role
iii. User Type



The user account is now created. This user can log in to OpenClinica and the system will authenticate with the LDAP system. All Study or Site privileges will continue to be managed by OpenClinica. This new user can be assigned to any other Study or Site you determine

8. Select or Enter values for the remaining required fields as indicated by the * symbol to the right of the field. Select the 'Submit' button.