

Edit Server ☆

[Home](#) » [Administration](#) » [Configuration](#) » [People](#) » [Servers](#)

SERVER

Name *

Choose a unique *name* for this server configuration.

Machine-readable name *

A unique machine-readable name. Can only contain lowercase letters, numbers, and underscores.

Enabled

Disable in order to keep configuration without having it active.

LDAP Server type

This field is informative. It's purpose is to assist with default values and give validation warnings.

Server address *

The domain name or IP address of your LDAP Server such as "ad.unm.edu".

For SSL use the form ldaps://DOMAIN such as "ldaps://ad.unm.edu"

Server port *

The TCP/IP port on the above server which accepts LDAP connections. Must be an integer.

Network timeout *

How long to wait for a response from the LDAP server in seconds.

Use Start-TLS

Secure the connection between the Drupal and the LDAP servers using TLS.

Note: To use START-TLS, you must set the LDAP Port to 389.

BINDING

Binding Method for Searches

- Service Account Bind: Use credentials in the Service Account field below to bind to LDAP
 - This option is usually a best practice.
 - This is also required for provisioning LDAP accounts and groups.
 - For security reasons, this pair should belong to an LDAP account with stripped down permissions.
- Bind with Users Credentials: Use user's entered credentials to bind to LDAP
 - This is only useful for modules that execute during user logon such as LDAP Authentication and LDAP Authorization.
 - This option is not a best practice in most cases.
 - The user's dn must be of the form "cn=[username],[base dn]" for this option to work.
- Anonymous Bind for search, then Bind with Users Credentials
 - Searches for user dn then uses user's entered credentials to bind to LDAP.
 - This is only useful for modules that work during user logon such as LDAP Authentication and LDAP Authorization.
 - The user's dn must be discovered by an anonymous search for this option to work.
- Anonymous Bind: Use no credentials to bind to LDAP server
 - This option will not work on most LDAPS connections.

DN for non-anonymous search *

USERS

Base DNs for LDAP users, groups, and other entries.

DNs that have relevant entries, e.g. `ou=campus accounts,dc=ad,dc=uiuc,dc=edu`.

Keep in mind that every additional basedn likely doubles the number of queries.

Place the more heavily used one first and consider using one higher base DN rather than 2 or more lower base DNs.

Enter one per line in case if you need more than one.

AuthName attribute

The attribute that holds the user's login name. (eg. `cn` for eDir or `sAMAccountName` for Active Directory).

AccountName attribute

The attribute that holds the unique account name. Defaults to the same as the AuthName attribute.

Email attribute

The attribute that holds the user's email address. (eg. `mail`). Leave empty if no such attribute exists

Email template

If no attribute contains the user's email address, but it can be derived from other attributes, enter an email "template" here. Templates should have the user's attribute name in form such as [cn], [uin], etc. such as [cn]@mycompany.com. See also the drupal.org documentation on LDAP tokens.

Thumbnail attribute

The attribute that holds the user's thumbnail image. (e.g. thumbnailPhoto). Leave empty if no such attribute exists

Persistent and Unique User ID Attribute

Login attributes are not always persistent (e.g. change in last name or email). Most setups should set this attribute to avoid creation of duplicate accounts or other issues. In cases where DN does not change, enter 'dn' here. If no such attribute exists, leave this blank.

Does the *Persistent and Unique User ID Attribute* hold a binary value?

You need to set this if you are using a binary attribute such as objectSid in ActiveDirectory for the PUID.

Expression for user DN. Required when "Bind with Users Credentials" method selected.

%username and %basedn are valid tokens in the expression.

Typically it will be: cn=%username, %basedn which might evaluate to cn=jdoe,ou=campus accounts,dc=ad,dc=mycampus,dc=edu

Testing Drupal Username

This is optional and used for testing this server's configuration against an actual username. The user need not exist in Drupal and testing will not affect the user's LDAP or Drupal Account.

DN of testing username

This is optional and used for testing this server's configuration against an actual username, e.g. cn=hpotter,ou=people,dc=hogwarts,dc=edu. The user need not exist in Drupal and testing will not affect the user's LDAP or Drupal Account.

GROUPS

Groups are not relevant to this Drupal site. This is generally true if LDAP Groups and LDAP Authorization are not in use.

Nested groups are used in my LDAP

If a user is a member of group A and group A is a member of group B, user should be considered to be in group A and B.
If your LDAP has nested groups, but you want to ignore nesting, leave this unchecked.

LDAP Group Entry Attribute Holding User's DN, CN, etc.

e.g. uniquemember, memberUid

DERIVE FROM GROUP

Name of Group Object Class

e.g. groupOfNames, groupOfUniqueNames, group.

User attribute held in "LDAP Group Entry Attribute Holding..."

This is almost always "dn" (which technically isn't an attribute). Sometimes its "cn".

DERIVE FROM USER ATTRIBUTE

A user LDAP attribute such as `memberOf` exists that contains a list of their groups.

Active Directory and openLdap with memberOf overlay fit this model.

Using this ignores "derive from group"

Attribute in User Entry Containing Groups

e.g. memberOf (*case sensitive*).

DERIVE FROM DN

Groups are derived from user's LDAP entry DN.

This group definition has very limited functionality and most modules will not take this into account. LDAP Authorization will.

Attribute of the user's LDAP entry DN which contains the group

e.g. ou

Testing LDAP Group DN

This is optional and can be useful for debugging and validating forms.

Testing LDAP Group DN that is writable.

WARNING: the test script for the server will create, delete, and add members to this group!
This is optional and can be useful for debugging and validating forms.

PAGINATION

Use LDAP Pagination.

Pagination size limit.

This should be equal to or smaller than the max number of entries returned at a time by your LDAP server. 1000 is a good guess when unsure. Other modules such as LDAP Query or LDAP Feeds will be allowed to set a smaller page size, but not a larger one.

[Save](#)

[Delete](#)