LDAP Configuration

A user with **System Administration** privileges must perform this operation.

This page refers to the current version of LAMS (2.2). For the relevant 2.0.5/2.1 page, see http://wiki.lamsfoundation.org/pages/viewpage.action?pageId=7831573.

Configuring LDAP Authentication

1. Login to LAMS as a sysadmin.
2. Go to the sysadmin screens, and click 'Edit Configuration Details'.
3. Setup the LDAP server connection parameters according to the table below.
4. Enable automatic user creation by setting LDAPProvisioningEnabled to 'true'.
5. (Optional) Setup the LDAP user attributes to use for creating a LAMS user according to the table below. At a minimum, set LDAPLoginAttr, LDAPFNameAttr, and LDAPLNameAttr.
    - A note on LDAPLocaleAttr. The value of this attribute will be used to attempt to match to one of LAMS' supported locales in the following order:
        - The locale's name e.g. 'en_AU'
        - The language ISO code e.g. 'en'
        - The country ISO code e.g. 'AU'
        - The LAMS server's default locale.
    - LDAPDisabledAttr refers to an LDAP attribute that marks a user as enabled or disabled (disabled users in LAMS cannot login and are removed from all group lists).
        - Values of '1' or 'true' are understood to mean true.
        - Prefix the attribute name with a '!' if the attribute is an 'enabled' flag in LDAP (as opposed to the 'disabled' flag as in LAMS).
6. (Optional) Setup the LDAP attributes used to place the user into a LAMS group with appropriate roles.
    - The value of the LDAPOrgAttr attribute is used to find a LAMS group to add the user to - the LAMS group itself must already exist. Configure LDAPOrgField to set which organisation field to search on (name, code, or description).
    - e.g. LDAPOrgAttr=schoolCode and LDAPOrgField=code will place LDAP users with a schoolCode=schoolA into the LAMS group with a 'code' value of 'schoolA'.
    - The values of LDAPRolesAttr when combined with LAMSLearnerMap, LAMSAuthorMap, etc. are used to map user roles in LDAP to LAMS roles.
7. Configure LDAP preferences:
    - LDAPUpdateOnLogin - set to 'true' to update the LAMS user account from LDAP whenever the user logs in.
    - LDAPOnlyOneOrg - set to 'true' to restrict the LAMS user to the group matching their LDAPOrgAttr value. Set to 'false' if LAMS users should be allowed to be members of other groups.
    - LDAPEncryptPasswordFromBrowser - set to 'true' for normal LAMS authentication (password will be encrypted before sending to LAMS server). For LDAP authentication, set to 'false' - this means user's passwords will be sent to LDAP in cleartext for authentication. In this case, you may want to consider using SSL.
    - LDAPSearchResultsPageSize - if your server has set a limit on the size of a paged results' page size, set this parameter to a compatible value. Used during synchronisation.

Configuration Items

LDAP server connection parameters

	Configuration Key	Description	Example/s
LDAP Server URL	LDAPProviderURL	URL of the LDAP server	ldap://ldap.example.com, ldap://ldap.example.com:389
Authentication Mechanism	LDAPSecurityAuthentication	Authentication mechanism, use 'none' for anonymous access, 'simple' for cleartext passwords	none, simple
Search Filter	LDAPSearchFilter	Search filter used to retrieve user's full distinguished name, where {0} will be replaced by their username.	(cn={0}), (&(cn={0})(objectClass=person))
BaseDN	LDAPBaseDN	Base DN where search will start from; includes all sub trees.	ou=Users,dc=melcoe,dc=mq,dc=edu,dc=au
Security Protocol	LDAPSecurityProtocol	Set to 'ssl' if connecting over SSL	ssl

If your LDAP server uses SSL, set the following values for the SSL certificate under the 'System Configuration' section.

SSL Certificate Path	TrustStorePath	File system path to LDAP server's ssl certificate on LAMS server, if it has one	/path/to/cert
SSL Certificate Password	TruststorePassword	Certificate's password if it has one	secrettext

Optional - intial bind user, if your ldap server doesn't allow anonymous reads. Leave blank if anonymous bind is allowed.

Bind User Distinguished Name	LDAPBindUserDistinguishedName	DN of user with read permission over other users who will authenticate with LAMS	cn=admin,ou=Users,dc=melcoe,dc=mq,dc=edu,dc=au
Bind User Password	LDAPBindUserPassword	Password of the above user	secrettext

Automatic user creation

	Configuration Key	Description	Example/s
Enable Provisioning	LDAPProvisioningEnabled	Enabled auto-creation of LAMS users based on LDAP attributes	true, false
Login	LDAPLoginAttr	LDAP attribute used to create LAMS username	uid, cn
First Name	LDAPFNameAttr	LDAP attribute used for LAMS user's first name	givenName
Last Name	LDAPLNameAttr	LDAP attribute used for LAMS user's last name	sn
Email	LDAPEmailAttr	LDAP attribute used for LAMS user's email	mail
Address Line 1	LDAPAddr1Attr	LDAP attribute used for LAMS user's address	
Address Line 2	LDAPAddr2Attr	LDAP attribute used for LAMS user's address	
Address Line 3	LDAPAddr3Attr	LDAP attribute used for LAMS user's address	
City	LDAPCityAttr	LDAP attribute used for LAMS user's city	l
State	LDAPStateAttr	LDAP attribute used for LAMS user's state	st
Postcode	LDAPPostcodeAttr	LDAP attribute used for LAMS user's postcode	postalCode
Country	LDAPCountryAttr	LDAP attribute used for LAMS user's country	c
Day Phone	LDAPDayPhoneAttr	LDAP attribute used for LAMS user's daytime phone number	telephoneNumber
Evening Phone	LDAPEveningPhoneAttr	LDAP attribute used for LAMS user's evening phone number	homePhone
Fax	LDAPFaxAttr	LDAP attribute used for LAMS user's fax number	facsimileTelephoneNumber
Mobile Phone	LDAPMobileAttr	LDAP attribute used for LAMS user's mobile number	mobile
Locale	LDAPLocaleAttr	LDAP attribute used for LAMS user's locale	preferredLanguage
Disable	LDAPDisabledAttr	LDAP attribute used for lAMS user's disabled flag	!accountStatus
Group	LDAPOrgAttr	LDAP attribute used to match the LAMS group or subgroup user should be placed in	schoolCode
Roles	LDAPRolesAttr	LDAP attribute containing list of roles	memberOf
Learner Role Map	LDAPLearnerMap	List of possible values from LDAPRolesAttr that are given the LAMS Learner role	Student;Staff;...
Monitor Role Map	LDAPMonitorMap	List of possible values from LDAPRolesAttr that are given the LAMS Monitor role	Staff;Teacher;...
Author Role Map	LDAPAuthorMap	List of possible values from LDAPRolesAttr that are given the LAMS Author role	Staff;Teacher;...
Group Admin Role Map	LDAPGroupAdminMap	List of possible values from LDAPRolesAttr that are given the LAMS Group Admin role	Staff;...
Group Manager Role Map	LDAPGroupManagerMap	List of possible values from LDAPRolesAttr that are given the LAMS Group Manager role	Staff;Principal;...
Group Field Map	LDAPOrgField	LAMS organisation field used to match value from LDAPOrgAttr	name,code,description

Preferences

	Configuration Key	Description	Example/s
Update on Login	LDAPUpdateOnLogin	Update a user's attributes and group membership/roles when they login	true, false
Only One Group	LDAPOnlyOneOrg	If LDAPUpdateOnLogin is true, removes membership of other groups user may be a member of when they login	true, false
Encrypt Password From Browser	LDAPEncryptPasswordFromBrowser	If enabled, password is encrypted when sent from the browser to LAMS; however to perform authentication against an LDAP repository, the password will most likely need to be in cleartext, so set this to false. If LDAP is not being used, this should be set to true.	true, false
Search Results Page Size	LDAPSearchResultsPageSize	When synchronising with LDAP, LAMS requests this number of paged results, if the feature is supported by the LDAP server; otherwise it is ignored. Defaults to 100.	100

Synchronise with LDAP

With a single button you can bulk update LAMS with the user details from LDAP. It searches the LDAP repository for users using the base DN from LDAPPrincipalDNSuffix, and creates or updates a user in LAMS based on each result returned. If LDAPOrgAttr, LDAPOrgField, LDAPRolesAttr, and LDAP[Learner|Author|Monitor|GroupAdmin|GroupManager]Map are also configured, and a LAMS group exists that matches LDAPOrgAttr, then the user will also be added to that group, with the roles set in the roles mappings.

⚠ Groups are not created in LAMS during the synchronise - these must be created manually.

Note that this process may take some time depending on the number of users contained in your LDAP tree. It's best to perform this operation when the LAMS server will not be under load.

The LDAP server will either need to support paged results, or have a limit on search results high enough to return all users, for this feature to work as intended.