



LDAP/ActiveDirectory/eDirectory

Use this service to authenticate with a corporate directory server using LDAP (e.g. Windows Active Directory, Novell eDirectory, OpenLDAP, etc.).

MindTouch Open Source LDAP Authentication Module

Assembly: mindtouch.deki.services

Class: MindTouch.Deki.Services.LdapAuthenticationService

SID: [sid://mindtouch.com/2007/05/ldap-authentication](#)

MindTouch Standard/Enterprise LDAP Authentication Module

Assembly: mindtouch.enterpriseldap.dll

Class: MindTouch.Deki.Services.LdapEnterpriseAuthenticationService

SID: [sid://mindtouch.com/ent/2009/03/ldap-authentication](#)

Configuration

Name	Type	Description
bindingdn	string	The DN to use for binding to LDAP. Use \$1 to substitute with user name. Enter a DN of a specific user if also providing a bindingpw. ActiveDirectory example: \$1@sd.mindtouch.com OpenLdap example: CN=\$1,DC=sd,DC=mindtouch,DC=com
bindingpw	string	Optional password for binding. Combined with a valid bindingdn account, queries to this service can be done without requiring credentials.
displayname-pattern	string?	Returns a friendlier name that can be customized by ldap attributes. Example: {sn}, {givenname}
ssl	bool?	Use LDAPS mode. This requires your LDAP server to be running with SSL and for the certificate to be recognized on the machine running this LDAP service. (default: false)
ssl-ignore-cert-errors	bool?	Allows you to use self signed or expired certificates. This should only be used for testing. (default: false)
hostname	string	Hostname or ip of domain controller or ldap server. By default port 389 is used with a plaintext connection and 636 is used with SSL enabled. A port can be specified with a :port suffix.

searchbase	string	The distinguished name (DN) of the domain. For example: 'DC=sd,DC=mindtouch,DC=com'
timeout	int?	Timeout for directory operations in milliseconds
userquery	string	The search query to use for looking up users. Use \$1 to substitute with user name. ActiveDirectory example: samAccountName=\$1 OpenLdap example: cn=\$1
groupquery	string?	LDAP query for group lookup by name. \$1 is replaced by username. Default: (&(objectCategory=group)(cn=\$1))
groupmembershipquery	string?	Use a custom query to return the groups a user belongs to where \$1 is the username. Only use this if you're having issues returning groups that a user belongs to. OpenLDAP example: (&(uniqueMember=\$1)(objectClass=groupOfUniqueNames))
groupqueryall	string?	LDAP query for looking up all groups. Default: (objectCategory=group)
groupmembersattribute	string?	LDAP attribute for looking up members of a group. Default: memberof (works for AD). Use groupmembership for eDirectory
usernameattribute	string?	LDAP attribute for retrieving a users account name. Provide an attribute to always use rather than trying a series of common attributes. Default: attempts to use sAMAccountName -> uid -> name -> cn.
groupnameattribute	string?	LDAP attribute for retrieving a group name. Provide an attribute to always use rather than trying a series of common attributes. Default: attempts to use sAMAccountName -> uid -> name -> cn.
verboselogging	bool?	Will output more details to the log as TRACE level. Warning: usernames+passwords are included as well. Default: false

Setup and Support

Refer to the [LDAP Howto](#) for integrating your MindTouch installation with LDAP using this service. Additional support is available on [irc](#), [forums](#), or by contacting [MindTouch sales/support](#).

Enterprise LDAP Authentication module

The enterprise LDAP module adds new functionality over the open core module tailored for enterprise use. These features will be guided by customer requests and will be developed by working closely with customers. MindTouch is focusing on the development of this Enterprise module and will only be porting critical bug fixes to the open core version. The open core edition continues to be GPL licensed and community contributions such as patches for bug fixes and enhancements are still encouraged as well as bug reports are still encouraged. The open core module will continue to

ship as part of the release packages. The Enterprise edition is also included and can be used on the trial and commercial editions of MindTouch. More info on the initial announcement on the [blog post](#).

Current Enterprise-only features

Nested groups

In larger organizations it's very common for groups to contain other groups. Such as a Sales group containing other groups like Widget Sales and Different Widget Sales. This is generally used for simpler file permissions on shared documents, email distribution groups, access to applications, etc. Deki's open core LDAP module only understands immediate group membership and ignores the group hierarchy. With this addition, the enterprise LDAP module is able to return the groups that a user is a member of indirectly as a result of a group they're in being a member of another group. The hierarchy is thus flattened and a full list of groups is returned to MindTouch. This allows page permissions to be set at a higher level and including multiple groups of people which allows better and simpler management of access for larger organizations.

Additional configuration settings for Enterprise LDAP Module

Name	Type	Description
nestedgroups	bool?	Resolve nested groups by flattening the hierarchy. (Default: false)
nestedgroupsdepth	int?	If nestedgroups is enabled then limit queries to groups nested this many levels deep. (Default: 5)

Enhancement ideas for enterprise module

- Configurable batching of large results
- Result caching
- Failover to backup controllers
- Multiple configured domain controllers allowing auth with any domain without trust relationships
- Customizable population of user properties with data from LDAP
- Require membership of a group in order to return the user (may be a core deki feature instead)
- **Custom read-only queries of LDAP data as an extension** (similar to mysql extension)

Development and open bugs for open core service

[View open authentication bugs](#)

