LDAP Authentication tab

verview

Tiki can authenticate users using a LDAP (Active Directory) server

o Access

From the Login Admin page, click the **LDAP** tab.

- Note that the PHP ldap module must be installed for LDAP authentication to work. See PHP LDAP Module for more information.

Related Topics
- Support forum
- Bug reports and feature requests

Option	Description	Default
Create user if not registered in Tiki	If a user was externally authenticated, but not found in the Tiki user database, Tiki will create an entry in its user database. ⚠ *If this option is disabled, this user wouldn't be able to log in.* Create the user | Deny access	Create the user
Require admin validation for LDAP users	When externally authenticated user is created in Tiki database either allow immediate login or create in disabled state that requires an administrator to approve the account before user can login to Tiki.	Disabled
Create user if not in LDAP	If a user was authenticated by Tiki's user database, but not found on the LDAP server, Tiki will create an LDAP entry for this user. ⚠ *As of this writing, this is not yet implemented, and this option will probably not be offered in future.*	Disabled
Use Tiki authentication for Admin log-in	If this option is set, the user "admin" will be authenticated by only using Tiki's user database and not via LDAP. This option has no effect on users other than "admin".	Enabled
Use Tiki authentication for users created in Tiki	If this option is set, users that are created using Tiki are not authenticated via LDAP. This can be useful to let external users (ex.: partners or consultants) access Tiki, without being in your main user list in LDAP.	Disabled

Option	Description	Default
Host	The hostnames, ip addresses or URIs of your LDAP servers. Separate multiple entries with Whitespace or ‘,’. If you use URIs, then the settings for Port number and SSL are ignored. Example: “localhost ldaps://master.ldap.example.org:63636” will try to connect to localhost unencrypted and if if fails it will try the master LDAP server at a special port with SSL.	None
Port	The port number your LDAP server uses (389 is the default, 636 if you check SSL).	None
Write LDAP debug information in Tiki Logs	Write debug information to Tiki logs (Admin -> Tiki Logs, Tiki Logs have to be enabled). ⚠ *Do not enable this option for production sites.*	Disabled
Use SSL (ldaps)		Disabled
Use TLS		Disabled
LDAP Bind Type	• **Active Directory bind** will build a RDN like username at example.com where your basedn is (dc=example, dc=com) and username is your username • **Plain bind** will build a RDN username • **Full bind** will build a RDN like userattr=username, userdn, basedn where userattr is replaced with the value you put in ‘User attribute’, userdn with the value you put in ‘User DN’, basedn with the value with the value you put in ‘base DN’ • **OpenLDAP bind** will build a RDN like cn=username, basedn • **Anonymous bind** will build an empty RDN ☰ Default: Anonymous Bind | Full: userattr=username,UserDN,BaseDN | OpenLDAP: cn=username,BaseDN | Active Directory (username@domain) | Plain Username	Default: Anonymous Bind
Search scope	Used after authentication for getting user and group information. ☰ Subtree | One level | Base object	Subtree
Base DN		None
User DN		None
User attribute		Uid
User OC		InetOrgPerson
Realname attribute	Synchronize Tiki user attributes with the LDAP values.	DisplayName

Option	Description	Default
Country attribute	Synchronize Tiki user attributes with the LDAP values.	None
Email attribute	Synchronize Tiki user attributes with the LDAP values.	None
Admin user		None
Admin password		None

Option	Description	Default
Create user if not registered in Tiki	If a user was externally authenticated, but not found in the Tiki user database, Tiki will create an entry in its user database. ⚠ *If this option is disabled, this user wouldn't be able to log in.* Create the user | Deny access	Create the user
Require admin validation for LDAP users	When externally authenticated user is created in Tiki database either allow immediate login or create in disabled state that requires an administrator to approve the account before user can login to Tiki.	Disabled
Create user if not in LDAP	If a user was authenticated by Tiki's user database, but not found on the LDAP server, Tiki will create an LDAP entry for this user. ⚠ *As of this writing, this is not yet implemented, and this option will probably not be offered in future.*	Disabled
Use Tiki authentication for Admin log-in	If this option is set, the user "admin" will be authenticated by only using Tiki's user database and not via LDAP. This option has no effect on users other than "admin".	Enabled
Use Tiki authentication for users created in Tiki	If this option is set, users that are created using Tiki are not authenticated via LDAP. This can be useful to let external users (ex.: partners or consultants) access Tiki, without being in your main user list in LDAP.	Disabled
Host	The hostnames, ip addresses or URIs of your LDAP servers. Separate multiple entries with Whitespace or ','. If you use URIs, then the settings for Port number and SSL are ignored. Example: "localhost ldaps://master.ldap.example.org:63636" will try to connect to localhost unencrypted and if if fails it will try the master LDAP server at a special port with SSL.	None

Option	Description	Default
Port	The port number your LDAP server uses (389 is the default, 636 if you check SSL).	None
Write LDAP debug information in Tiki Logs	Write debug information to Tiki logs (Admin -> Tiki Logs, Tiki Logs have to be enabled). ⚠ *Do not enable this option for production sites.*	Disabled
Use SSL (ldaps)		Disabled
Use TLS		Disabled
LDAP Bind Type	• **Active Directory bind** will build a RDN like username at example.com where your basedn is (dc=example, dc=com) and username is your username • **Plain bind** will build a RDN username • **Full bind** will build a RDN like userattr=username, userdn, basedn where userattr is replaced with the value you put in 'User attribute', userdn with the value you put in 'User DN', basedn with the value with the value you put in 'base DN' • **OpenLDAP bind** will build a RDN like cn=username, basedn • **Anonymous bind** will build an empty RDN ☰ Default: Anonymous Bind | Full: userattr=username,UserDN,BaseDN | OpenLDAP: cn=username,BaseDN | Active Directory (username@domain) | Plain Username	Default: Anonymous Bind
Search scope	Used after authentication for getting user and group information. ☰ Subtree | One level | Base object	Subtree
Base DN		None
User DN		None
User attribute		Uid
User OC		InetOrgPerson
Realname attribute	Synchronize Tiki user attributes with the LDAP values.	DisplayName
Country attribute	Synchronize Tiki user attributes with the LDAP values.	None
Email attribute	Synchronize Tiki user attributes with the LDAP values.	None

Option	Description	Default
Admin user		None
Admin password		None

How to know which LDAP Bind Type you need to use

you do not know, the best is to use a tool to access the directory like Apache Directory Studio

you can enter your directory with your email, it is probably an Active Directory

you can access with your username, it can be plain, full, or OpenLDAP
fter with your tool navigate to select a user, the DN of the user will be shown and you will be able to guess the method

ome tips:

- You can not build a RDN/DN like this "sAMAccountName=username,dc=example,dc=com". If you would like to do so because the CN is the real name and not the username, it is probably because you have chosen the wrong bind method (it can be an active directory method)
- Use want to use the search scope *subtree* at the beginning, then once it is working, switch to a specifc OU for better performance

How to get the email and other attributes back in Tiki

ki builds another DN to get the attributes. This time, Tiki uses a search and not a bind. The DN is userattr=username, userdn, basedn where userattr is he attribute you put in 'User Attribute', username is the username, userdn the value you put in 'User DN' and basedn is the value you put in basedn. This me you can use sAMAccountName in the attribute (it is a search not a bind).
hen put the attribute name you see in the DN that contains the mail

Examples

ote: What you use for baseDn and UserDn is completely dependent upon how you or your administrator has configured LDAP. Keep in mind Tiki will earch for the user in the LDAP tree beginning at the level specified in BaseDn. So the UserDN and groupDN are not strictly needed.

Unix

hese settings should work on most Unix & OpenLDAP systems that use LDAP for authentication and as information store:

DAP Bind Type	Default
ase DN	dc=example,dc=com
ser DN	ou=users
ser attribute	uid
ser OC (Object Class)	inetOrgPerson
ealname attribute	cn
-Mail attribute	mail
roup DN	ou=usergroups
roup attribute	cn
roup OC (Object Class)	groupOfNames
ember attribute	member
ember is DN	yes

Active Directory

DAP Bind Type	Active Directory
ase DN	dc=example,dc=com
ser DN	cn=Users
ser attribute	sAMAccountName
ser OC (Object Class)	user (usually, could be inetOrgPerson instead)
ealname attribute	displayName
-Mail attribute	probably userPrincipalName - not sure if you use exchange
roup DN	
roup attribute	cn
roup OC (Object Class)	group
ember attribute	member

Member is DN	yes

ote: The default install of Active Directory places user accounts (and groups) in the container "cn=Users, dc=example,dc=com". But, most large rganizations reorganize AD to suit their needs. See the note above regarding searches.

I-Note: after Tiki 6.1 the LDAP configuration UI has changed. Group setup is done under "LDAP External groups" even though the groups does not reside n an external LDAP server.

lso note that Tiki above 6.1 does not support custom characters i.e. the scandinavien letters "æ,ø,å" in CN name. (potentially in other fields too). (this ha een marked as a bug).

n Tiki 7.1-7.2 the GUI has changed and now there is the "LDAP" tab and the "LDAP external groups" tab.Click here for LDAP tab and here for LDAP xternal Groups.This proposed settings worked on 4/10/2011 on windows server 2008 with Active Directory.

Zimbra LDAP

DAP Bind Type	Default
ase DN	dc=example,dc=com
ser DN	ou=people
ser attribute	uid
ser OC (Object Class)	*
ealname attribute	displayName
-mail attribute	mail
urther Instructions	http://wiki.zimbra.com

Debugging

heck the box at "Write LDAP debug Information in Tiki Logs:" and try to authenticate in another browser. Check Tiki Logs (tiki-syslog.php) to see what ent wrong.

TTENTION: Uncheck the debug settings once you managed to set up your connection. Else, your logs will get flooded!

this even does not help, you can use this code to check whats wrong:

ldap connect test