See also: LDAP Tracker Field

LDAP Authentication tab

Overview

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

Related Topics

- Support forum
- Bug reports and feature requests

To 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.

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
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
Port	The port number your LDAP server uses (389 is the default, 636 if you check SSL).	None

Option	Description	Default
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@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
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
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
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

Option	Description	Default
LDAP Bind Type	• **Active Directory bind** will build a RDN like username@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
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

Option	Description	Default
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
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@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

Option	Description	Default
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
Admin user		None
Admin password		None

How to know which LDAP Bind Type you need to use

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

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

If you can access with your username, it can be plain, full, or OpenLDAP
After 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

Some 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

Tiki 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 the 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 time you can use sAMAccountName in the attribute (it is a search not a bind).
Then put the attribute name you see in the DN that contains the mail

Examples

Note: What you use for baseDn and UserDn is completely dependent upon how you or your administrator has configured LDAP. Keep in mind Tiki will search for the user in the LDAP tree beginning at the level

specified in BaseDn. So the UserDN and groupDN are not strictly needed.

Unix

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

LDAP Bind Type	Default
Base DN	dc=example,dc=com
User DN	ou=users
User attribute	uid
User OC (Object Class)	inetOrgPerson
Realname attribute	cn
E-Mail attribute	mail
Group DN	ou=usergroups
Group attribute	cn
Group OC (Object Class)	groupOfNames
Member attribute	member
Member is DN	yes

Active Directory

LDAP Bind Type	Active Directory
Base DN	dc=example,dc=com
User DN	cn=Users
User attribute	sAMAccountName
User OC (Object Class)	user (usually, could be inetOrgPerson instead)
Realname attribute	displayName
E-Mail attribute	probably userPrincipalName - not sure if you use exchange
Group DN	
Group attribute	cn
Group OC (Object Class)	group
Member attribute	member
Member is DN	yes

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

UI-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 on an external LDAP server.

Also 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 has been marked as a bug).

On 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 external Groups.This proposed settings worked on 4/10/2011 on windows server 2008 with Active Directory.

Zimbra LDAP

LDAP Bind Type	Default
Base DN	dc=example,dc=com
User DN	ou=people
User attribute	uid
User OC (Object Class)	*
Realname attribute	displayName
E-mail attribute	mail
Further Instructions	http://wiki.zimbra.com

Debugging

Check 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 went wrong.

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

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

ldap connect test

```
<?php require_once ('tiki-setup.php'); if ( !function_exists( 'ldap_connect' ) ) die('Function ldap_connect does not exist. Is ldap extension enabled in php.ini?'); $con = ldap_connect('ldap://my_hostname:389'); ldap_set_option(NULL, LDAP_OPT_DEBUG_LEVEL, 7); ldap_set_option($con, LDAP_OPT_PROTOCOL_VERSION, 3); ldap_set_option($con, LDAP_OPT_REFERRALS, false); $dn = 'cn=username,dc=example,dc=com'; if(ldap_bind($con, $dn,'verrry_secret')) { echo "connect succeeded"; //and if you want to test the mail $filter = '(objectClass=*)'; $just = array('mail'); // adapt the attribute name $sr = ldap_search($con, $dn, $filter, $just); $info = ldap_get_entries($con, $sr); print_r($info); } else { $err = ldap_error($con); echo "Oops! ". $err. "<br/>"; /* Uncomment this section to (attempt to) get the extended error if (ldap_get_option($con, 0x0032, $extended_error)) { echo "Error Binding to LDAP: $extended_error"; } else { echo "Error Binding to LDAP: No additional information is available."; } */ } ?>
```

Replace Hostname, Port, binddn and password and run it with
php connect.php

Present the output your LDAP Administrator.

Useful tool: Apache Directory studio

Common Problems and Workarounds

Empty pages

When changing auth-type from "tiki" to "tiki + ldap", you might need to clear the tiki-system cache.

Certificate Problems

If you use certificates on LDAP server side where the root certificate is not trusted, you should put the root or CA certificate somewhere at your Tiki webserver and let /etc/openldap/ldap.conf know where it is. Use parameters TLS_CACERTDIR and TLS_CACERT to point it to the root or CA certificate.

If you use self signed certificates you can also simply disable certificate checking by setting TLS_REQCERT to "never" in /etc/openldap/ldap.conf.

See the manpage of "ldap.conf" to get more information.

Note that using LDAPS on Windows has a similar requirement. PHP seems to look for the file C:\OpenLDAP\sysconf\ldap.conf. If it doesn't exist, manually create it.
In the first line of the file write
TLS_REQCERT never
Restart IIS afterwards.

How it works

If a user enters his username and password in Tiki, a binddn is created and together with the password used to authenticate the user at the LDAP server. Once authenticated, the user is allowed to read data from the LDAP server. Especially he usually can read his own data and the LDAP group information. These data are used to create the user and group in Tiki. The user has the Tiki password disabled. He only can login via LDAP. On subsequent logins, the data are synchronized from LDAP to Tiki (**not the other direction!**).
The replicated data can be at the moment:

- Users full name
- Users email address
- Users country information
- Users group membership
- Group name and description

So if you change any of the above information in LDAP, the data are synchronized the next time the user logs into Tiki. You can even change group membership in LDAP and it gets synchronized to Tiki. What is not replicated to Tiki are object (user/group) deletions.

Group membership and permissions

One interesting use of LDAP with groups is to give users from specific groups more permissions. Since every user created in Tiki is assigned to the build in group "Registered", you should give "Registered" the same permissions like "Anonymous". You may want to give some LDAP usergroups special permissions. Let one user of that group login to Tiki to automatically create the group. Then assign permissions to that group.

How anonymous binding works

- connect anonymously to the LDAP server
- get the user DN
- authenticate the user by binding with the server as DN + password

LDAP Pear::Auth Troubleshooting

You can verify your connection by editing the file \tiki\lib\pear\Auth\Container\LDAP.php in line 453 for tw6.4 (441 for tw < 4)
from

```
$this->options['debug'] = false;
```

to

```
$this->options['debug'] = true;
```

After the login you see a screen with a successful binding to the AD/LDAP-Server

```
281: Connecting with host:port 288: Successfully connected to server 292: Switching to LDAP version 3 306: Switching LDAP referrals to true 312: Binding with credentials 325: Binding was successful 548: UTF8 encoding username for LDAPv3 574: Searching with ldap_search and filter (&(sAMAccountName=exampleuser)(objectClass=*)) in ou=europe,dc=xnet,dc=oe,dc=examplehost 581: User was found 636: Bind as CN=exampleuser,OU=users,OU=ode,OU=europe,DC=xnet,DC=oe,DC=examplehost 640: Bind successful 650: Authenticated
```

Be aware that after your troubleshooting you must switch off the debug option to login.

Related links

- Comparison of major LDAP web interfaces in PHP
- How to set up LDAP and Active Directory forum post here, thanks jwbrandon

Aliases

- LDAP
- AD
- Active Directory
- OpenLDAP