LDAP is a widely used protocol to centralize authentication processes within a network and to administer access rights to unique systems; for example to store, organize and manage information and access rights concerning the computer network's users and network resources (e.g. email accounts, software application usage permissions, etc.).

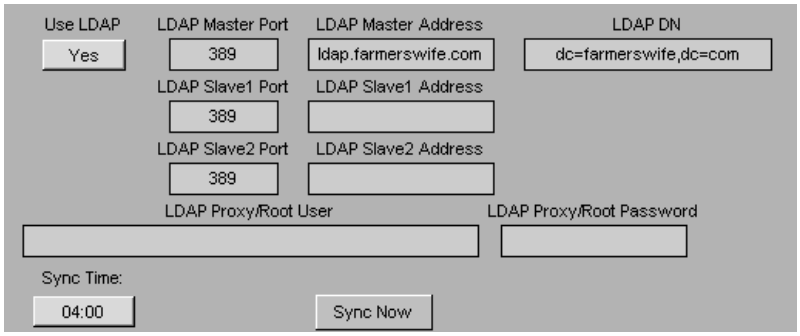
Since version 4.6 Farmers WIFE Advanced (in the following text referred to as farmerswife) can authenticate users of a computer network as part of a directory service through a local LDAP (Lightweight Directory Access Protocol) Server. Besides the actual access authentication to WIFE, the association of WIFE's in-application pre-defined user Permission Profiles to each LDAP user (i.e. the translated user's job description into WIFE's user Permission Profile) is the other integral part of the LDAP integration.

Please note that the LDAP integration is not required in order to run Farmers WIFE Advanced. It is an add-on integration option subject to additional licensing fees and conditions and the use of this integration is only recommended for large or multi site facilities on a case-by-case basis; skilled in-house IT Administrator(s) with experience with LDAP are prerequisite and LDAP are 3rd party applications not subject to Farmers WIFE support. LDAP integration to other parts of Farmers WIFE Advanced are subject to custom development.

Configuring the LDAP settings within the WIFE Server Setup

Go to the Server Setup and select the Users tab:

IMPORTANT: The LDAP functionality must be licensed in order to be able to see the LDAP configuration section in the right side next to the 3rd user category column. Here you define the LDAP connection parameters:



Use LDAP: Enables/Disables the use of LDAP if the LDAP functionality has been licensed. Once enabled, all client authentication will be validated by the LDAP server.
LDAP Master Port: Enter here the port number of the LDAP Master Server. By default this is set to 389.
LDAP Master Address: Enter here the LDAP Master address; e.g. ldap.farmerswife.com
Slave1/Slave2: The same as the settings for the LDAP Master. You don't need redundancy LDAP slaves, but if you're using LDAP you will probably have fall back slave LDAP servers already running.
LDAP DN: The Domain Name (dn) that will be used when connecting to the LDAP server; this is composed of different Domain Controllers (dc); this is the root of your LDAP server.
LDAP Proxy/Root User/Password: Depending on your system it might not be possible to connect "anonymously", therefore enter here your LDAP Proxy, Root User and Password settings. farmerswife needs to perform some queries to the LDAP system therefore it needs to identify itself to LDAP.
Sync Time: The LDAP integration is designed so that it can synchronize the whole user base with LDAP every 24h; define here the time which is most convenient and does not conflict with other scheduled WIFE or system tasks (e.g. running a Force Shutdown or a Full Backup at the same time is not the recommended configuration).
Sync Now: Clicking this button will instantly manually sync all configured LDAP users with farmerswife.

Configuring the LDAP Server so WIFE can connect to it

Together with your license, which enables you to use LDAP, please make sure you also received an “LDAP schema” file. This file “farmerswife.schema” needs to be copied into your LDAP “schema” directory; e.g. “/etc/openldap/schema” and it also must be included in “/etc/openldap/sladp.conf” file within the include section (paths are taken as examples from “openLDAP”). The following three steps need to be configured and are explained in more detail on the next pages:

Create an “ou” (= ”Your organizationalUnit’s name for the farmerswife server”, e.g. FWServer) and create as many entries as needed, using the FarmerswifeServer objectClass, see the section “farmerswife Server Definition Entry” below.

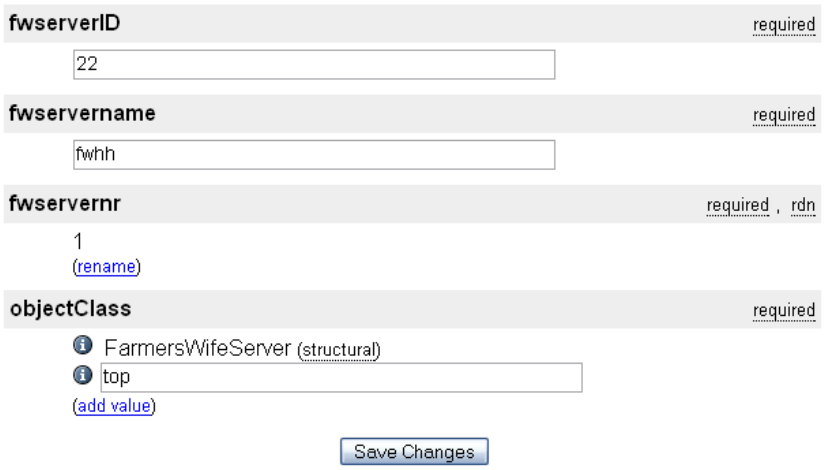
Create another “ou” (e.g. FWPermissions) and create as many entries (matching the farmerswife’s user Permission Profile names) as needed, using the FarmerswifePermissionLevel objectClass, see section “farmerswife Permission Level Entry” below.

Create as many FarmerswifeUserInfo objectClasses in every LDAP user that should have access to the farmerswife Server, see “farmerswife user definition entry on LDAP” below.

The following LDAP example configuration screenshots originate from “phpLDAPadmin v1.0.1”.

farmerswife Server Definition Entry

Here the farmerswife server is defined. In a standard configuration only one farmerswife server needs to be created, but some enterprise style companies have multiple farmerswife servers running and need to configure multiple different Permission Profiles for the same user depending on to which farmerswife server the user will log-in.



fwserverID: That’s the same ID that will be entered in WIFE Server Setup > General tab in the “Division ID” field; this is required by the WIFE-LDAP schema.
fwservername: A plain text description name of the WIFE Server in addition to the ID; this is required by the WIFE-LDAP schema.

farmerswife Permission Level Entry

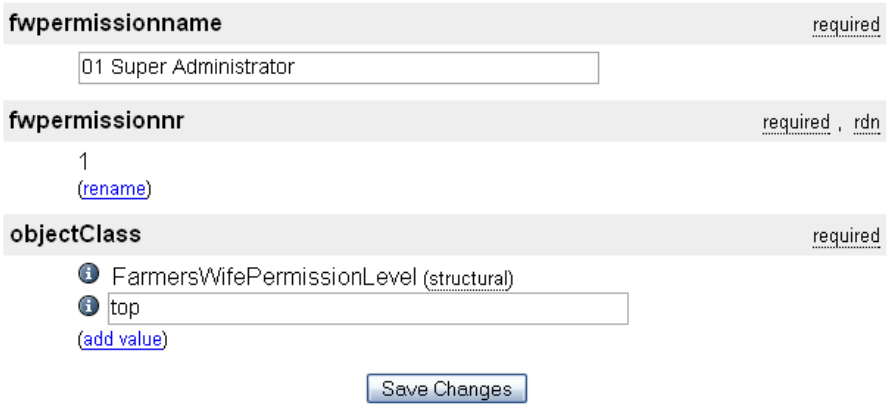
Here the farmerswife user Permission Profile must be created. The name ideally matches with the corresponding farmerswife Permission Profile which must be configured on the farmerswife Server prior to testing the connection

to LDAP. Once LDAP is configured use WIFE's "Map LDAP Profiles" functionality to map the WIFE user permission profiles with the ones configured on LDAP.

Path example:
ou= "Your organizationalUnit's name for WIFE's user permissions" /
"number of WIFE's user permission profile"=1 (FarmerswifePermissionLevel)

ou=*FWPermissions*/fwpermissionnr=1 (FarmerswifePermissionLevel)
ou=*FWPermissions*/fwpermissionnr=2 (FarmerswifePermissionLevel)
etc.

NOTE If more than one farmerswife Server is being managed by LDAP, multiple "FarmerswifeUserInfo" objects can be created per user.



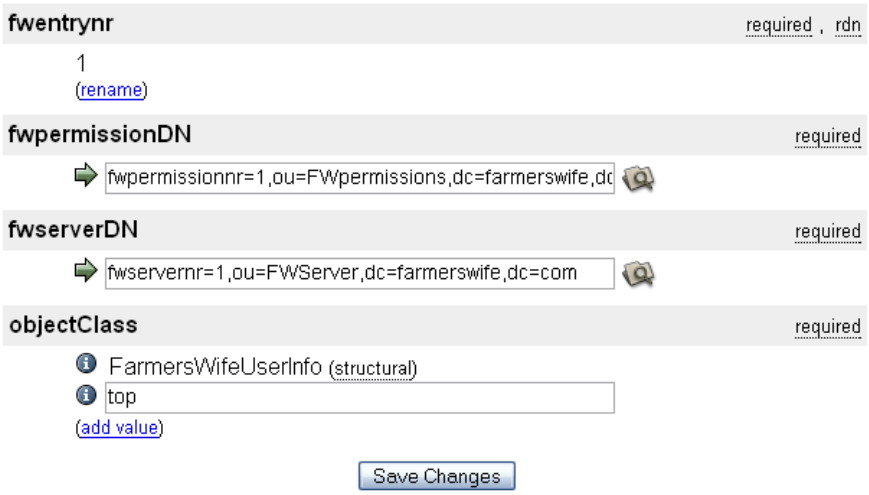
fwpermissionname: This is the name of the actual WIFE user permission. Here you should type the same profile name that you have already configured in your WIFE system to easily identify it; this is required by the WIFE-LDAP schema.

farmerswife user definition entry on LDAP

A new "child" entry has to be added to every user to access farmerswife. The following picture is an example of a child entry of an LDAP user.
Here the permission access level for each LDAP user is defined and to which farmerswife Server the connection is allowed (if multiple WIFE Servers are involved within the system). If a user doesn't have this entry correctly defined he/she will not be allowed to connect to farmerswife through the Client application.

Path help with three examples:
ou=level1/ou=level2/cn=person (inetOrgPerson)/fwentrynr=1 (FarmerswifeUserInfo)
ou=post/ou=producer/cn=Peter Moore (inetOrgPerson)/fwentrynr=1 (FarmerswifeUserInfo)
ou=post/ou=editor/cn=Lisa Haddad (inetOrgPerson)/fwentrynr=1 (FarmerswifeUserInfo)

NOTE If more than one WIFE Server is being managed by LDAP, multiple "FarmerswifeUserInfo" objects can be created per user.



fwpermissionDN: Is the DN (Domain Name) path to the Permission definition; this is required by the WIFE-LDAP schema.
fwserverDN: Is the DN (Domain Name) path to the Server definition; this is required by the WIFE-LDAP schema.

First time connecting WIFE with LDAP

Following the above mentioned steps, by now your WIFE Server and your LDAP server should be configured to be able to connect to each other. The first step is to synchronize WIFE with LDAP; use the above mentioned “Sync Now” button. Once clicked and everything is configured correctly, the new “LDAP“ users will always appear in the third column of users in the WIFE Server Users section. If users were previously already created within farmerswife and these users don’t exist in LDAP or the user’s details don’t exactly match, then these users will be deactivated. If they exist in LDAP, exactly match the one in farmerswife and have access to farmerswife then they will remain active within their existing user category location.

The LDAP system is now the MASTER to authenticate the WIFE system users (only supports the types Super Users and User). This means that only users that exist in LDAP and are properly configured will be allowed to connect to farmerswife.
To successfully connect every user will need to use their LDAP “uid” and password. It is recommended to disable the setting “Allow Client Remember Password” located within the Server Setup > General tab.

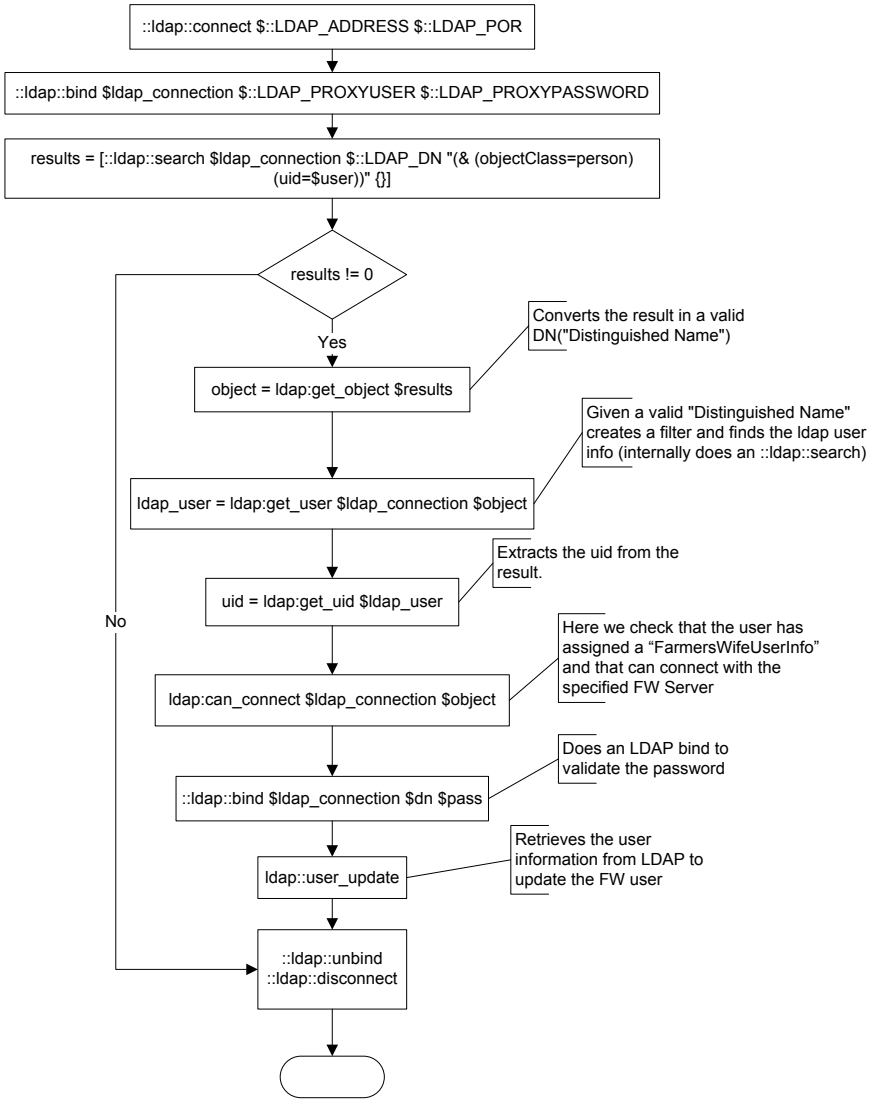
FAQ’s:

- No user can connect to WIFE and if I do a “Sync Now” no LDAP users are imported:
  That means that your LDAP or farmerswife servers are not correctly configured to work with each other. Please revise the documentation and contact Farmers WIFE Support if the problem persists.

- Does WIFE store the user passwords?
  No, farmerswife doesn’t store the user passwords. It always checks with the LDAP server.

- I can’t login anymore and my user appears to be deactivated in the WIFE Server Setup!
  That means that your user is not properly configured in the LDAP system, please contact your LDAP system administrator.

User Connection Workflow



1. Try to manually sync to the LDAP Server. If this fails this could mean that the LDAP Server is not correctly configured. farmerswife will try to connect with the Master LDAP server, if fails it will try with Slave1 and Slave2 (if they have been configured).
2. Once it's connected farmerswife will bind with LDAP to perform the necessary queries to retrieve the information needed for the connection.
3. farmerswife searches in LDAP for a user with the specified "uid" in the farmerswife Client login dialog.
4. farmerswife checks that a user exists with this "uid".
5. farmerswife retrieves the proper DN (*Distinguished Name*).
6. farmerswife assigns the uid to this DN, because farmerswife login process is case sensitive and LDAP is not. farmerswife needs to double-check that the "uid" that LDAP considers to be valid, is also valid for farmerswife
7. farmerswife checks if this user has the correct permissions to connect with the farmerswife Server. This is done by retrieving the *FarmerswifeUserInfo* assigned to the LDAP user and checking that this *FarmerswifeUserInfo* is configured to access the correct farmerswife Server using the *Division ID.*
8. Now the actual binding with LDAP can take place. In this step the password, using the encryption that was defined in LDAP is validated.
9. farmerswife retrieves the user's LDAP info to update the farmerswife user.
10. farmerswife disconnects from LDAP, nothing else is needed.

farmerswife – LDAP Synchronization