

# LDAP Preferences

FileWave supports connecting your LDAP network directory – Active Directory, Open Directory, or eDirectory – to your FileWave Server. This capability provides access to directory information for use in Smart Groups and parameterized profiles. You can also use LDAP for enrollment authentication. Using LDAP to authenticate your devices gives you a way to know who (which LDAP user) enrolled what device.

## Creating an LDAP server entry in Preferences

Authentication server: FW USA ☒ use it for extraction

Name	Host	Type
Preview LDAP	ldap.preview...	Active Directory
FW USA	adserv.filew...	Active Directory

+ - Synchronize Now

LDAP Server Details

Name: FW USA

Host / IP: adserv.filewave.com

Port: 389

Protocol: LDAP ☒ Check Server Certificate

Server Type: Active Directory

Base DN: DC=filewave,DC=com

LDAP User DN: filewave\administrator

LDAP User Password: .....

Refresh Interval (sec): 3600

Change Limit (%): 50

Remove missing items after: 24 consecutive missing extractions. ☒ Enable Automatic Group updates for this LDAP

Test Connection

Use the [+] button to create a new LDAP server entry and enter the needed connection information as described below:

- Name - a reference name used by you to differentiate your LDAP servers
- Host / IP - enter either a FQDN or IP address for your LDAP server
- Port - enter the TCP port required to access your LDAP server (you may need to check with your network support)
- Protocol – select LDAP, LDAPS, STARTSSL.
  - For LDAPS and STARTSSL you have a checkbox that you can potentially uncheck so that the server certificate is not checked against the machine's trust store.

IF LDAPS or STARTSSL it is recommended to be using a trusted LDAP cert.

- Server Type - choose Active Directory, Open Directory, or eDirectory
- Base DN - enter the primary distinguished names (DN) for your LDAP server using the domain components separated by commas. For example, if the LDAP server is running on the same box as the FileWave server, your base DN may be as simple as "dc=home,dc=local"; but if the LDAP server is running on a different system, the value of the base DN may be involve using a more extended value, such as "dc=tanner,dc=filewave,dc=net".
- LDAP User DN - if you are doing authenticated binds to your LDAP server, you will need to enter a valid user account that has been designated for binding. If you are doing anonymous binding, this entry is left blank.
- LDAP User Password - enter a password to complete the authenticated bind; not needed for anonymous binds
- Refresh Interval (sec) - enter a value in seconds for the FileWave Server to contact the LDAP server to refresh the available data. If you are just setting up a FileWave server on a network with an established LDAP server, you should set the interval relatively short (~120 seconds) while you are testing and making changes. Once you go into production mode, you should change the interval to 24 hr. (86,400 seconds).
- Change Limit (%) - LDAP related items will not be removed if more than the given percentage of the items disappear after a sync. This is to avoid loss of data if something goes wrong with the LDAP configuration.

If for example an entire OU is suddenly missing that makes up 25% of your LDAP directory, then the amount of change will be so large that FileWave will not initially accept the changes if you set Change Limit from 1% to 25%, but if you had it set to 26% it would accept that removal. When considering the next option in conjunction with this it can still take X amount of syncs for removals to occur.

- Remove Missing items after - 0 means that records not found in the LDAP server, but are still present in FileWave will be removed immediately.

Setting it to a number that is equivalent to 24 hrs is recommended for safety.



(Refresh Interval / 60(second to min) / 60(min to hrs)) \* x = 24(hrs)

So if I wanted an interval of 1800 seconds (30min), I would set my interval to 48

Enable Automatic Group updates for this LDAP creates a visible set of entries (Smart Groups) in the Clients pane under an LDAP designator. These Smart Groups will be updated by FileWave at the designated refresh interval. The information provided in the Clients pane for LDAP is a one-way view of your directory server. While changes made at the LDAP server are automatically reflected in FileWave; changes made in FileWave Admin do not affect the LDAP directory information.



Choosing to enable the automatic Group updates creates a visible set of entries in the Clients pane of FileWave Admin, and keeps that information up to date; however, for an LDAP environment of over a few hundred records, the load on the LDAP server can get extremely heavy.

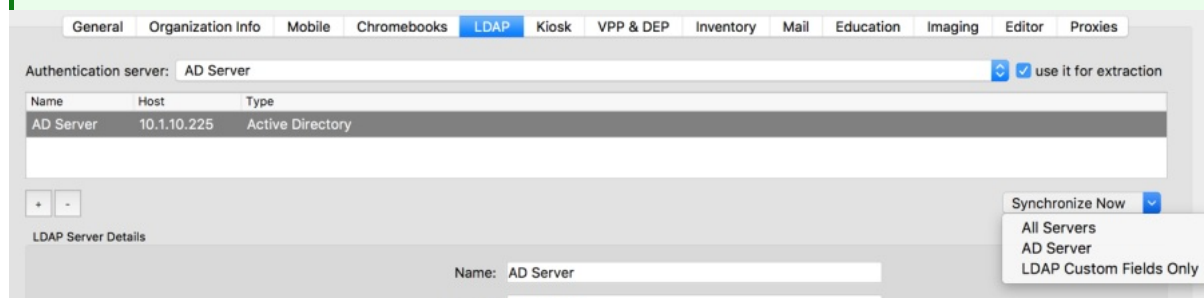
The Test Connection button pings the server to see if it is online; but does not verify all connection settings. You should always use an LDAP browser tool to verify the link to your server.

You can create entries for multiple LDAP servers, and an LDAP server can be running on the same device or VM as the FileWave Server.

An LDAP server can be chosen as the Authentication server which, in this case, means that the directory for that server will be used for profiles that support parameterized settings. Selecting the use it for extraction setting adds the directory information to the FileWave database. You can view the LDAP settings in the Assistants/LDAP Browser in FileWave Admin.



At the Bottom right of the LDAP server pane, there is a Synchronize Now option. This option will allow you to synchronize all your LDAP servers, just one, or sync LDAP Custom Fields.



🔄Revision #4

★Created 12 July 2023 01:49:21 by Josh Levitsky

✎Updated 7 August 2024 14:05:03 by Josh Levitsky