Using LDAP to enroll macOS/iOS/Android devices

Use this document if you are trying to point your enrollment of device to directory services (Active Directory, Open Directory, eDirectory or OpenLDAP). This is used for Android Device and well as iOS devices or macOS devices enrolling OTA (over the air) as well as Apple's DEP (Device Enrollment Program) enrollment for both iOS and macOS devices.

This process consists of:
1- Backing up the current config
2- Editing a new config file to properly read the LDAP structure
3- Restarting the Apache Process so it reads the new config file

Getting the files ready

Open a Terminal Window or use SSH to get into the computer running FileWave Server

Gain root credentials

```
sudo -s
```

Enter your login password

Navigate to the FileWave Apache configurations folder

OS X / Linux:
```
cd /usr/local/filewave/apache/conf/
```

Backup your current mdm_auth.conf by making a copy

```
cp mdm_auth.conf mdm_auth.conf.bac
```

Make a copy of the LDAP example and rename it

```
cp mdm_auth.conf.example_ldap_auth mdm_auth.conf
```

Making the changes

Open it up using your preferred text editor (nano mdm_auth.conf or vi mdm_auth.conf).
it will look like this:

```
<Location /ios/enroll>
# This is an example of ldap based user auth
        AuthType Basic
        AuthBasicProvider ldap
        AuthName "Enroll IOS Device"
        AuthLDAPURL "ldap://10.1.10.25:389/cn=Users,dc=saturn,dc=filewave,dc=us?uid"
        Require valid-user
# If you need to bind to the ldap server, use these lines
#       AuthLDAPBindDN "cn=Admin,o=myorg"
#       AuthLDAPBindPassword "secret1"
         LDAPReferrals Off
</Location>

<Location /ios/dep_enrollment_profile>
# This is an example of ldap based user auth
        AuthType Basic
        AuthBasicProvider ldap
        AuthName "Enroll IOS Device"
        AuthLDAPURL "ldap://10.1.10.25:389/cn=Users,dc=saturn,dc=filewave,dc=us?uid"
        Require valid-user
        ErrorDocument 401 "Enrollment credentials are needed."
# If you need to bind to the ldap server, use these lines
#       AuthLDAPBindDN "cn=Admin,o=myorg"
```

```
#       AuthLDAPBindPassword "secret1"
           LDAPReferrals Off
</Location>

<Location /android/enroll>
# This is an example of ldap based user auth
        AuthType Basic
        AuthBasicProvider ldap
        AuthName "Enroll Android Device"
        AuthLDAPURL "ldap://10.1.10.25:389/cn=Users,dc=saturn,dc=filewave,dc=us?uid"
        Require valid-user
# If you need to bind to the ldap server, use these lines
#       AuthLDAPBindDN "cn=Admin,o=myorg"
#       AuthLDAPBindPassword "secret1"
           LDAPReferrals Off
</Location>

<Location /android/project_number>
# This is an example of ldap based user auth
        AuthType Basic
        AuthBasicProvider lda4
        AuthName "Google Cloud Messaging configuration"
        AuthLDAPURL "ldap://10.1.10.25:389/cn=Users,dc=saturn,dc=filewave,dc=us?uid"
        Require valid-user
# If you need to bind to the ldap server, use these lines
#       AuthLDAPBindDN "cn=Admin,o=myorg"
#       AuthLDAPBindPassword "secret1"
           LDAPReferrals Off
</Location>
```

The different sections correspond with the different enrollment URLs.
For example, if my servers hostname was server.filewave.com:

mdm_auth.conf

URL	Use
https://server.filewave.com:20443/ios/enroll	Over the air enrollment portal
https://server.filewave.com:20443/ios/dep_enrollment_profile	URL iOS or macOS Devices request when a DEP device is enrolling. This URL is not accessible from a normal browser.
https://server.filewave.com:20443/android/enroll	Downloading the APK FileWave Client
https://server.filewave.com:20443/android/project_number	Used by the FileWave Android client to talk to server

Open Directory & eDirectory

OD (by default) does not require a user to authenticate to read the structure.
You will not need to uncomment the bind options.

AuthName - The title of the login window
AuthLDAPURL - Where and what groups are allowed to login and there for enroll. The example above would allow anyone in the 'Users' group to enroll a device.

Make the appropriate changes and then save the .conf

Active Directory

AD (by default) requires you bind to the directory to read. Many people create a read-only directory account.

AuthName - The title of the login window
AuthLDAPURL - Where and what groups are allowed to login and there for enroll. The example above would allow anyone in the 'Users' group to enroll a device.
AuthLDAPBindDN - From specific to most general. Username, what group that is in, what group (or organizational unit) that group is in, and the server. The example above would allow the user 'TestDir Reader' who is in the group 'User' who is in the Org Unit 'IT' on the Active Directory server of ad-ldap.filewave.com to bind.
AuthLDAPBindPassword - Password for user account being used to bind to AD.

Make the appropriate changes and then save the .conf
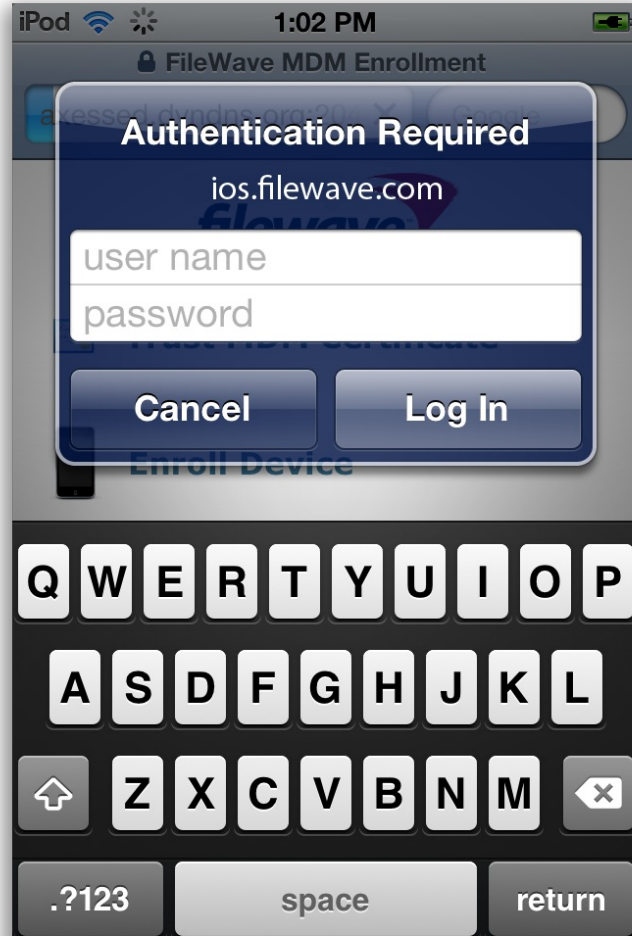
Restarting Apache

Once saved, restart the FileWave Apache process/service

OS X / Linux:

```
/usr/local/filewave/apache/bin/apachectl graceful
```

Now when a device attempts to enroll (by pressing the Enroll Device option on the site). They will be prompted to enter their username and password from the directory server.

Using several authentication sources for the same enrollment type

When we want to use several authentication sources (not nested locations) , we need to use AuthnProviderAlias sections to define those sources. The same format for binding to a single source (see above) apply for configuring each AuthnProviderAlias section , as in the following example

At the start of the file we define an alias by using:

```
<AuthnProviderAlias ldap ALIAS_NAME0>
    AuthLDAPBindDN ""
    AuthLDAPBindPassword ""
    AuthLDAPURL ""
</AuthnProviderAlias>
```

Then below that you specify the location and call for the alias

```
<Location /ios/enroll>
    AuthBasicProvider ALIAS_NAME0 ALIAS_NAME1 ALIAS_NAME2
    AuthType Basic
    AuthName "Enroll IOS Device"

    Require valid-user
</Location>
```

A final MDM_auth.conf would look something like this:

```
<AuthnProviderAlias ldap Student>
    AuthLDAPBindDN "cn=BindUserName,dc=filewave,dc=net"
    AuthLDAPBindPassword "YourBindPassword"
    AuthLDAPURL "ldap://ldap.filewave.net:389/OU=student,dc=filewave,dc=net?sAMAccountName"
</AuthnProviderAlias>

<AuthnProviderAlias ldap Faculty>
    AuthLDAPBindDN "cn=BindUserName,dc=filewave,dc=net"
    AuthLDAPBindPassword "YourBindPassword"
    AuthLDAPURL "ldap://ldap.filewave.net:389/OU=staff,dc=filewave,dc=net?sAMAccountName"
</AuthnProviderAlias>

<Location /ios/enroll>
    AuthBasicProvider Faculty Student
    AuthType Basic
    AuthName "Enroll IOS Device"

    Require valid-user
</Location>
```

Troubleshooting tips

Take a look at the log files for apache:

OS X / Linux:

```
<br>/usr/local/filewave/apache/logs/error_log<br>          <br>
```

Below are some sample errors and what they typically mean.

NOT Bound:

```
[Thu Feb 09 22:10:19 2012] [error] [client 192.168.1.109] user diradmin: authentication failure for "/ios/enroll":
Password Mismatch, referer: https://192.168.1.95:20443/ios/
```

Bound but user entered info wrong OR ldap url pointed to wrong group:

```
[Thu Feb 09 22:29:16 2012] [error] [client 192.168.1.109] user diradmin: authentication failure for "/ios/enroll":
Password Mismatch
```

Bound w/ Bad User

```
[Thu Feb 09 22:29:00 2012] [error] [client 192.168.1.109] user lkajshdg not found: /ios/enroll
```

Could be Bound or not but not filtering by the correct ?uid ?sAMAccountName at end of URL (?UID is an OD or eDir, AD is typically ?sAMAccountName)

```
[Thu Feb 09 22:17:31 2012] [error] [client 192.168.1.109] user admin not found: /ios/enroll, referer:
https://192.168.1.95:20443/ios/
```

Something wrong in the mdm_auth.conf file. Like AuthzLDAPAuthoritative isn't off or shoudn't be there.

```
apache require directives present and no authoritative handler
```

Recursive issues

Does it appear that your server only looks at the one group/unit pointed to and not sub-groups? try adding ?sub at the end of your AuthLDAPURL lines:

```
AuthLDAPURL "ldap://ldap.filewave.net:389/OU=student,dc=filewave,dc=net?sAMAccountName?sub"
```

Always feel free to contact support for further assistance.