# External Authentication in aACE

Last Modified on 07/20/2022 3:54 pm EDT

This guide explains how to set up external authentication in aACE. It is intended for system administrators.

For increased security and streamlined user access, aACE can help you leverage the FileMaker functionality for external authentication.

With the external authentication feature, aACE internal user accounts are deactivated and your Open Directory account (or Active Directory account for PC) is used to validate users, pass authentications, and set privileges in aACE. This puts the IT Department in direct control of user access for maximum security — you can update a user's record in the Open Directory account to prevent access to aACE. Another benefit is that when users click the aACE launcher, they can log in using the same credentials for logging into their workstation — this reduces the number of credentials that your users must manage.

## Requirements for External Authentication

To activate this feature, you must set up the following requirements:

- A properly configured Open Directory server (or Active Directory server for PC) on a separate machine
- A connection (i.e. 'binding' or 'joining') between your Open Directory server and your FileMaker server (FMS)
- A user group in Open Directory (e.g. aaceusers) and corresponding user group in aACE
- FMS configured for external authentication
- aACE configured for external authentication

Of these requirements, only the configuration tasks are within the scope of aACE support (see below). For the other requirements, we recommend that your IT staff coordinate closely with your aACE partner.

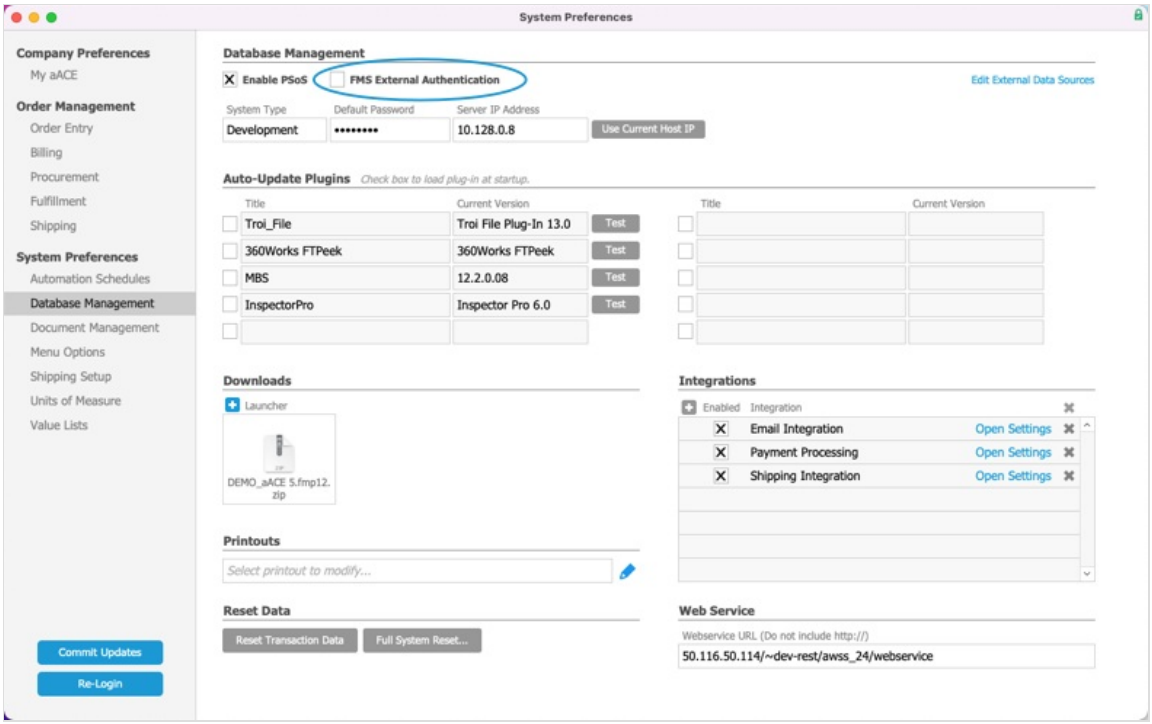
### Configuring Your FileMaker Server for External Authentication

Login to FMS, then navigate to Admin Console > Administration > External Authentication tab. In the Database Sign In section, enable the External Server Accounts setting. Please see FileMaker's help guide on external authentication (https://help.claris.com/en/server-help/content/config-auth-

db.html) for details.

### Configuring Your aACE Preferences for External Authentication

Login to aACE, then navigate from Main Menu > System Admin > Preferences > Database Management. Mark the flag for FMS External Authentication, then click Commit Updates.




## Troubleshooting External Authentications

Working with external authentication processes may include unique situations to address.

### Team Member Records not Constrained by External Authentication

Only Team Member records of the "Employee" type are affected by external authentication. Team Member records with the "Resource" record type are *not* affected.

This means that any programmer accounts and any consultant accounts can still be used to log in directly to your aACE system.

### Logging In after Deactivating External Authentication

When you activate external authentication, aACE continues to store the direct access

password for each team member. If you later deactivate external authentication, aACE will require your team members to again use these FileMaker-based account passwords.

If team members do not remember their old passwords, you will have to reset them.

## Issues from Upgrading FMS

When you upgrade to a new version of FMS, the Client Authentication setting may get reset to the default (i.e. FileMaker accounts only). This will disrupt any team members that have been logging in with external authentication credentials.

You must login to FMS and again enable the 'External Server Accounts' setting.

If you are unable to immediately update the server before your users require access to aACE, you can reset their password, enabling them to login directly to aACE for a time.

---