FileMaker Authentication

FileMaker Authentication

On this page:

Note: The information on this page is accurate for FileMaker 16. Certain features and settings may either not apply to or differ from prior versions.

FileMaker Security Basics

Using FileMaker securely rests first and foremost on employing and setting up FileMaker's existing authorization features thoughtfully. For hosted and single-user files alike, it is critical that you make sure that all accounts are password protected and that you have set up privilege sets to manage user activities appropriately. This document addresses some of the things that you should consider when setting up user accounts and access control in FileMaker.

Internal Authentication

By far the most common method of defining users for FileMaker databases is to utilize FileMaker's internal account feature. When creating a new user, this is the type of account that is specified by default. See FileMaker Help: Create Accounts for an overview on internal FileMaker authentication.

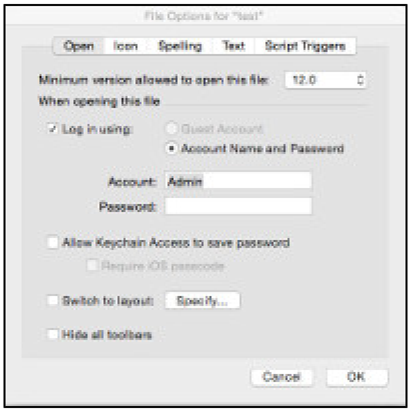
The following sections all refer to internally authenticated accounts.

Full-Access Accounts

By default, FileMaker files are created with a full-access Admin account with no password. A critical first step is to either set a password for this account, or disable this account in conjunction with creating another (user-specific) password protected full-access account. Beginning with version 15, FileMaker Server provides a setting that will disallow hosting of files that have full-access account(s) with no password set. We strongly recommend enabling this setting whenever databases are hosted with FileMaker Server, but note this feature is not available for non-hosted files. After setting authorizations correctly, making sure that your files reside on secure machines is the next critical piece to providing security for your database solutions. Wherever you have data that is sensitive, it is strongly recommended that you host the file on an IS&T-managed server.

More About FileMaker's Default Account Settings

In addition to having a default Admin account with no password set, FileMaker files are set by default to auto-login with this Admin account. In the **File > File Options > Open** tab, uncheck the **Log in using:** box. Unless there is a compelling reason to do so, do not set the file to auto-login with a particular account.



Minimum version allowed to open this file: 12.0

When opening this file

☑ Log in using: ○ Guest Account ● Account Name and Password

Account: Admin

Password:

□ Allow Keychain Access to save password

□ Require iOS passcode

□ Switch to layout:

□ Hide all toolbars

Note: While you should not set up files to auto-login with a particular account, users may configure their individual FileMaker Pro client to set a default account name to appear in the login window so that they only need to type their password. This can be done by choosing **FileMaker Pro > Preferences** (Mac) or **Edit > Preferences** (Windows), and then in the General tab specify a User Name.

Set Up Individual User Accounts

FileMaker allows for individual user accounts and group privilege sets. All users should have individual user accounts; never employ shared accounts. Setting up privilege sets with appropriate access controls and creating individual user accounts assigned to an appropriate privilege set is the first and best security mechanism available in every circumstance.

Note: Individual users can be given control over their own passwords in FileMaker, but users should be advised against reuse of Kerberos passwords in FileMaker. Forgotten passwords can be reset by a full-access user at any time.

External Authentication

When hosting files with FileMaker Server, it is possible to enable external authentication to leverage local server accounts, LDAP accounts and groups, and (new in version 16) OAuth identity provider accounts. See FileMaker Help: Set Up External Authentication for an overview on external authentication.

Configuring FileMaker for Kerberos Authentication at MIT

It is possible, and recommended, to configure hosted FileMaker databases at MIT to utilize Kerberos-based external authentication. For more information, refer to Configuring FileMaker Databases For Kerberos Authentication.

External Authentication and Full Access Accounts

It is generally not recommended to use external authentication with full access accounts in FileMaker, as this practice carries potential security risks. If an illegitimate user gains physical access to a FileMaker file with an external full access account, they may easily spoof the external group and gain entry to the file. If you choose to employ an external full access account, securing the server and any backup locations is of paramount importance. In addition, external full access accounts cannot be used to commit changes made in the Manage Security dialog; this must be done with an internal full access account.

Server-Based Security Features Related to Authentication

Requiring Password-Protected Databases

Starting with version 15, FileMaker Server has a setting for restricting the hosting of databases to those that are password protected. This should be enabled. In the Admin Console, navigate to the **Database Server pane > Security** tab, and check off **Host password-protected databases only**.

Hiding Files

There is also a setting that restricts the display of hosted files to only those files for which a user is allowed access when the user browses a server via the Launch Center or File > Open Remote. When this setting is turned on, the user will be prompted twice for authentication: once to view available files on the server, and again to open a selected file. In the Admin Console, navigate to the **Database Server pane > Security tab**, and check off **List only the databases each user is authorized to access**.