



FileMaker Security Guide

The Key to Securing Your Solutions

Table of Contents

Overview.....	3
Configuring Security Within FileMaker Pro or FileMaker Pro Advanced.....	5
Prompt for Password	5
Give the Admin Account a password	5
Create Privilege Sets	5
Define Data Access and Design privileges	7
Define Extended Privileges	8
Define Other Privileges	10
Setup Accounts or External Server Groups for authentication	10
Authentication and Multi-file Solutions.....	14
Use File Access to authorize access to files	14
Database Encryption	15
Use scripts, functions and more to enhance security	17
Enable or disable plug-ins	17
Security Configuration of FileMaker Server	19
Install FileMaker Server With All or Some of the Components Behind Your Firewall	19
Enable External Authentication	20
Limit Display of Files.....	21
Turn on SSL Encryption	21
Other SSL Options	22
Use Server Idle Timeout	22
Define Administrator Groups	23
Viewing Log File Entries in the Admin Console	23
Set up Scheduled or Progressive Backups to a Secure File Location.....	23
Testing Security Settings	24
Appendix A – Other Considerations.....	25
Appendix B – Quick Reference Guide for Day-to-Day Operations	26
Appendix C – Types of Encryption Used by FileMaker.....	27
Appendix D – Process for Installing a Custom Certificate for SSL	28



FileMaker How To Guide – The Key to Securing Your Solutions

Best practices for configuring security options in FileMaker Pro and FileMaker Server

This informative guide outlines best practices when using the FileMaker Platform to create, manage and deploy solutions to meet your organization's security needs.

There are three principles to consider:

- **Confidentiality.** Ensure that unauthorized people cannot access the data.
- **Integrity.** Allow authorized users to create and update data while preventing unintentional changes. You must also restrict access to unauthorized users who may tamper with the files.
- **Availability.** Ensure that the data is available to users when it is needed.

This guide will walk you through the steps of securing your solutions using the FileMaker Platform's built-in security. Depending on your security compliance and certification requirements, there may be additional steps you need to take. It is up to you to fully understand these requirements.

NOTE: This guide assumes you have already created a file that you want to secure.

Overview

The FileMaker Platform provides a complete suite of tools to help you control data access, operations and development within a FileMaker file, and enable you to help you meet auditing and regulatory compliance requirements, even in shared environments. Key capabilities include:

- **Strong authentication.** Credentials that are stored within FileMaker files are encrypted once and never decrypted thereafter. Users can also be authenticated via Active Directory or Open Directory.
- **Granular control.** You decide who can see and do what, down to the table, layout, record or even individual field level.
- **Data encryption.** The data stored within a FileMaker file can be encrypted, and you can require SSL encryption of data between FileMaker Server and FileMaker Pro, FileMaker Go, and FileMaker WebDirect.

The FileMaker Platform employs a unified security model where the security that you establish for a file is in effect across all clients - iPad, iPhone, Windows, Mac and the Web (Figure 1). When the file is hosted by FileMaker Server, the security that you establish using FileMaker Server and between FileMaker Server and your directory server, other databases, and your web server, applies to all the files hosted by FileMaker Server.



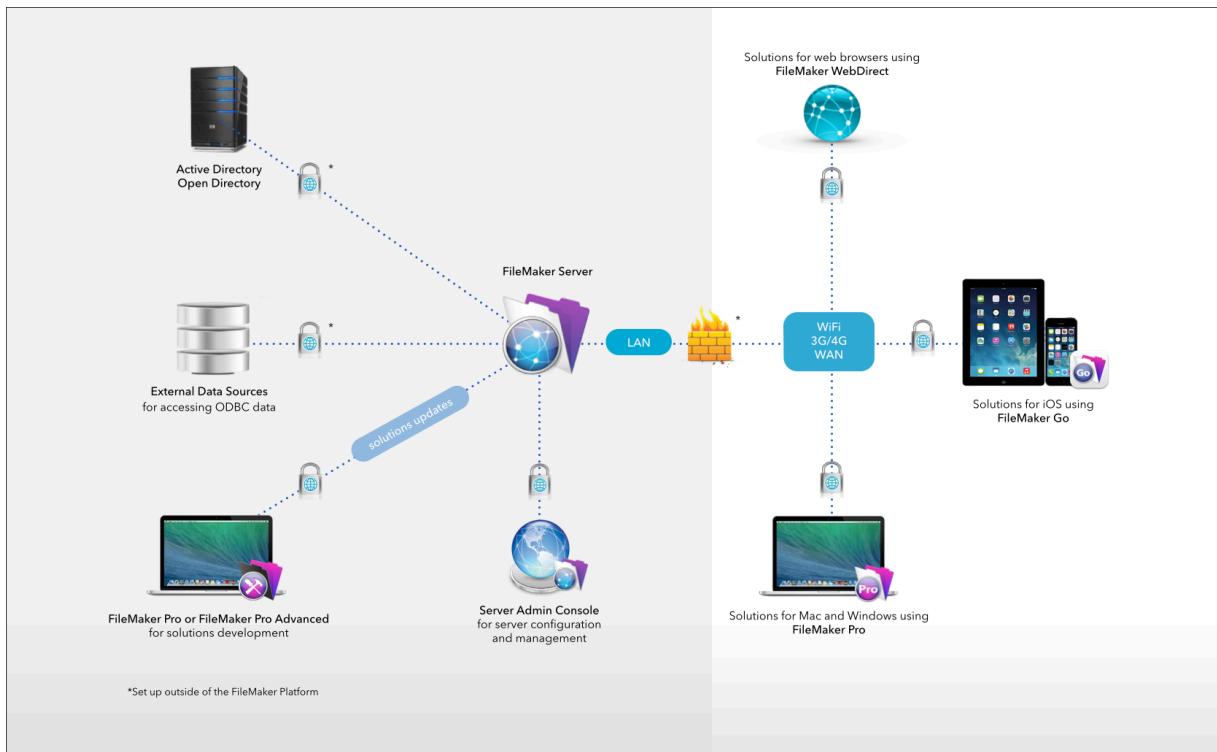


Figure 1. High-level security diagram with a single machine FileMaker Server deployment

The FileMaker security model is based on two key components:

1. **Accounts** — identify the individual user
2. **Privilege Set** — define access limits for user(s)

Accounts, known in information security compliance guidelines as Identity, control access to the file for each individual. Account Name and Password are together referred to in information security compliance guidelines as Identity. Each account contains an account name and a password.

The Privilege Set controls what the user can see and do. Privilege Sets allow you to define what is referred to in information security compliance guidelines as Access Management.

Security settings defined within the file using FileMaker Pro are largely file-specific. Accounts and privilege sets established in one file control access to the information and schema stored in that file.

Security settings configured within FileMaker Server are server-specific and apply to all files hosted by the server.



Configuring Security Within FileMaker Pro or FileMaker Pro Advanced

Most of the security for a solution is controlled within FileMaker Pro. The following sections outline the steps for setting up file security within FileMaker Pro or FileMaker Pro Advanced.

Prompt for Password

When a new file is created in FileMaker Pro, the file does not prompt for the user's account name and password when opened. Before you do anything else, change this by following the steps below:

1. Choose **File** menu > **File Options**
2. Uncheck **Log in using**
3. Click **OK**

Learn more about setting file options:

http://fmhelp.filemaker.com/fmhelp_13/en/html/create_db.8.6.html - 10657433

Give the Admin Account a password

When a new file is created in FileMaker Pro, a full access **Admin** account is automatically created.

This full access **Admin** account does not have a password. Therefore, before you do anything else, it's important to assign a password to this account. Doing this will prevent unauthorized access to your data and database structure.

To rename the **Admin** account, follow the steps below:

1. Choose **File** menu > **Manage** > **Security**.
2. From the **Accounts** tab, select the **Admin** account, and click **Edit**.
3. Rename the **Admin** account name and add a password. Be sure to use complex password conventions, including upper and lowercase letters and numbers.

Learn more about editing an existing account:

http://fmhelp.filemaker.com/fmhelp_13/en/html/passwords.14.11.html#1028147

Create Privilege Sets

Privilege sets grant access to what a user can see and do. Privilege sets allow you to control access to data and schema (layouts, fields, tables and scripting).

Every new FileMaker file contains three pre-defined privilege sets:

1. **Full Access** - Allows complete access to the file, including all development functions.
2. **Data Entry Only** - Allows creating, editing and deleting records, and importing and exporting data. It does not allow access to any development functions.
3. **Read-Only Access** - Allows viewing and exporting record data. It does not allow any modifications to the file.

You cannot change or delete the pre-defined privilege sets except to enable or disable extended privileges.



Please familiarize yourself with the pre-defined privilege sets to see if they will meet your needs. If you think that these three options will suit your needs initially, you can skip to [Setup Accounts](#) or [External Server Groups](#) for authentication.

You can also create new privilege sets to meet your specific requirements. Typically, you will create a privilege set for each unique role in your organization. A privilege set is comprised of the access options below:

- **Data Access and Design Privileges** - provide access to a wide range of security control, including records, layouts, value lists and scripts.
- **Extended Privileges** - determine the data sharing options that are permitted for a privilege set in the file.
- **Other Privileges** - allow printing, exporting, and some other functions.

To create a new privilege set, follow the steps below:

1. Choose **File** menu > **Manage** > **Security**.
2. From the **Privilege Sets** tab, click on the **New** button.

By default, almost all privileges are turned off. This enforces the Rule of Least Privileges which states that a user should have no more privileges than those necessary to fulfill his or her role.

You can save time by duplicating an existing privilege set and then modifying it to meet your needs. Simply select a privilege set, click on the **Duplicate** button then click the **Edit...** button (Figure 2). In either case, the Edit Privilege Set dialog will appear, allowing you to define or modify the privilege set (Figure 3).

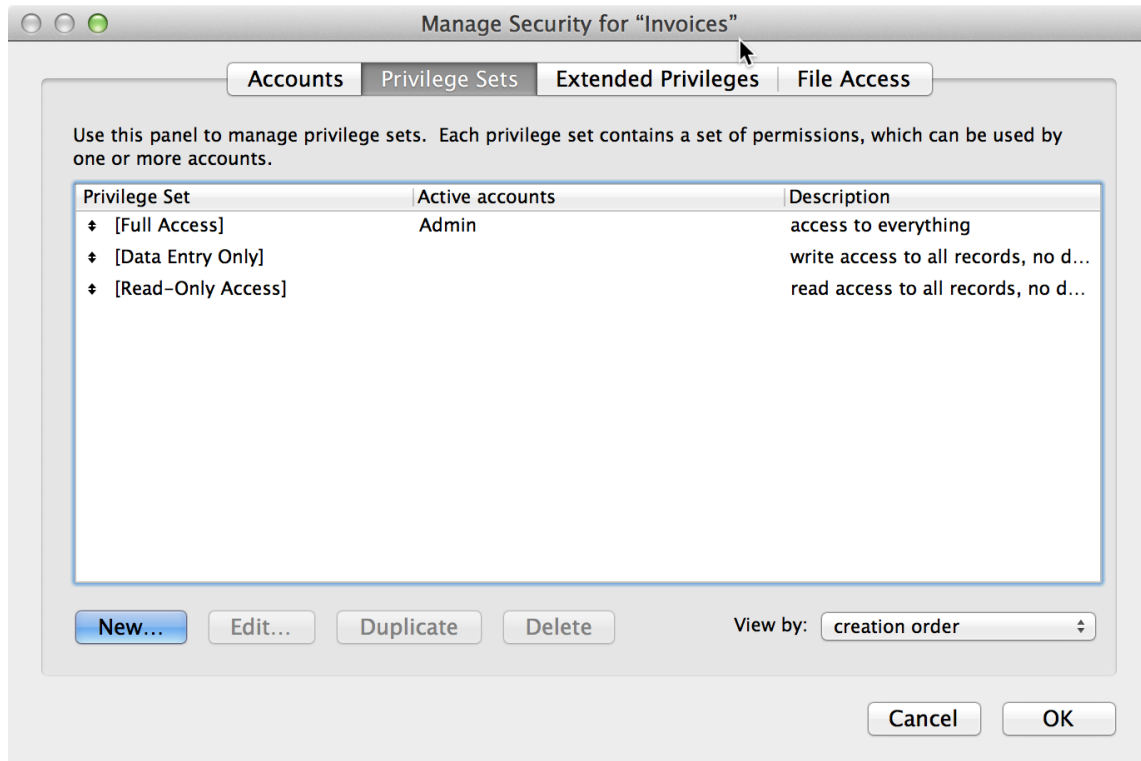


Figure 2. The Privilege Sets tab lets you create, edit or duplicate privilege sets.



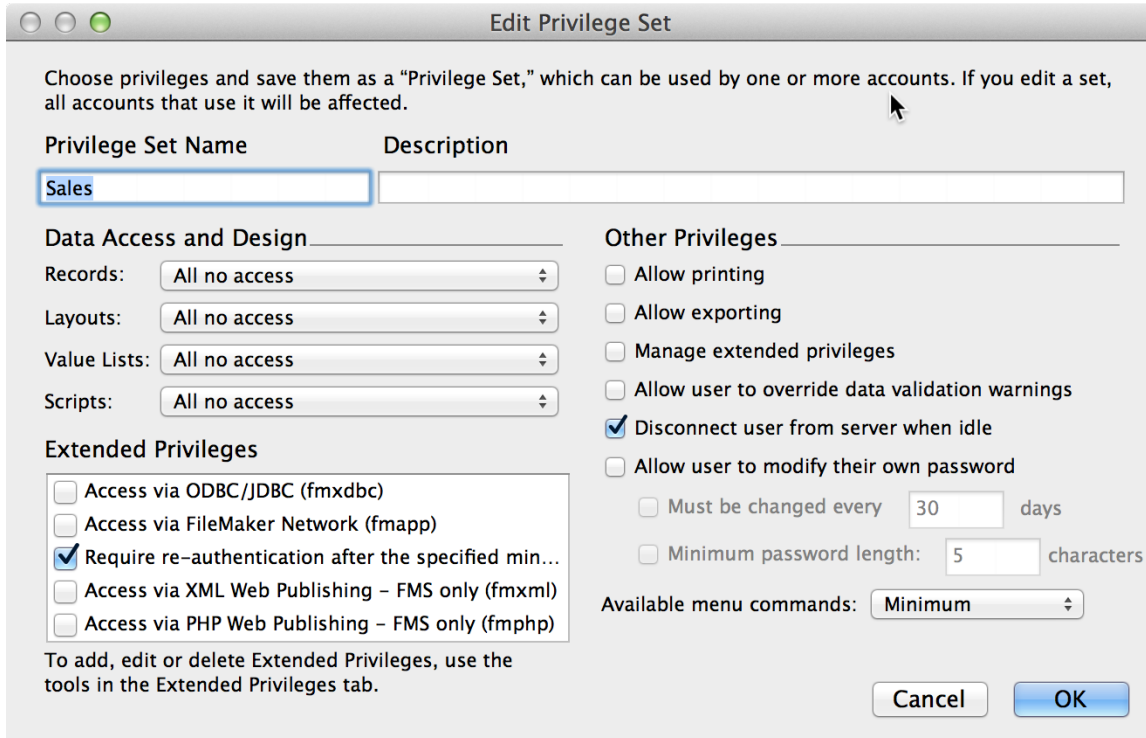


Figure 3. In the Edit Privilege Set dialog, select the privileges you wish to grant. Then click OK.

Creating or editing a privilege set may impact the currently connected users. It is recommended that you do not make changes to the privilege sets in a shared file while others are using it.

Learn more about creating and managing privilege sets:

http://fmhelp.filemaker.com/fmhelp_13/en/html/passwords.14.15.html#1028570

Define Data Access and Design Privileges

The Data Access and Design section contains drop downs that grant access to different parts of the file. The options in these drop downs apply to all tables, layouts, value lists and scripts on a functional basis.

Each drop down also contains an option for Custom Privileges. Custom Privileges gives you more granular control over access privileges.

Custom Privileges for Records is often useful when you need to control user access on a table-by-table or record-by-record basis. For example, you may have a CRM system where the Sales management can see all the records but individual Sales reps only see the records of his or her own customers and prospects.

Custom Privileges for Layouts allows you to control both the ability of the user to view or modify a layout, and also whether users can view or modify records when on that layout. The FileMaker Platform always uses the most secure combination of access rules; a user who can generally edit records will be prevented from doing so when on a layout that doesn't allow those privileges.



You can also use Custom Privileges to determine for each value list or script whether the user can view or run it, modify or delete it, or create new ones.

Define Extended Privileges

Extended privileges determine whether and how a shared file is accessible. For a file, you can set which privilege sets are permitted to:

Keyword in dialog box	Description
fmwebdirect	Access a file from a web browser via FileMaker WebDirect – FileMaker Server only
fmjdbc	Access a file as an ODBC or JDBC data source
fmapp	Access a file with FileMaker Pro or FileMaker Go
fmreauthenticate[X]	Sets how long a user can be away before re-authentication is required – FileMaker Go clients only.
fmxml	Access via XML Web Publishing – FileMaker Server only
fmphp	Access via PHP Web Publishing – FileMaker Server only

While editing a privilege set, you can enable and disable extended privileges for that privilege set (see bottom left corner of Figure 3).

Extended Privileges can also be assigned to multiple Privilege Sets at once by clicking on the **Extended Privileges** tab. Select the extended privilege and click **Edit...** (Figure 4). Then check the boxes for the Privilege Sets that you wish to assign that extended privilege (Figure 5).

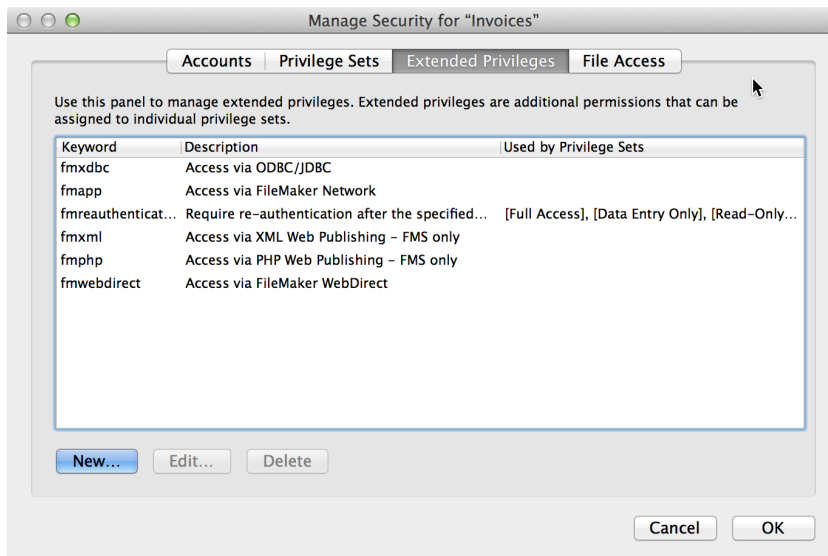


Figure 4. Click on the Extended Privileges tab to manage extended privileges.



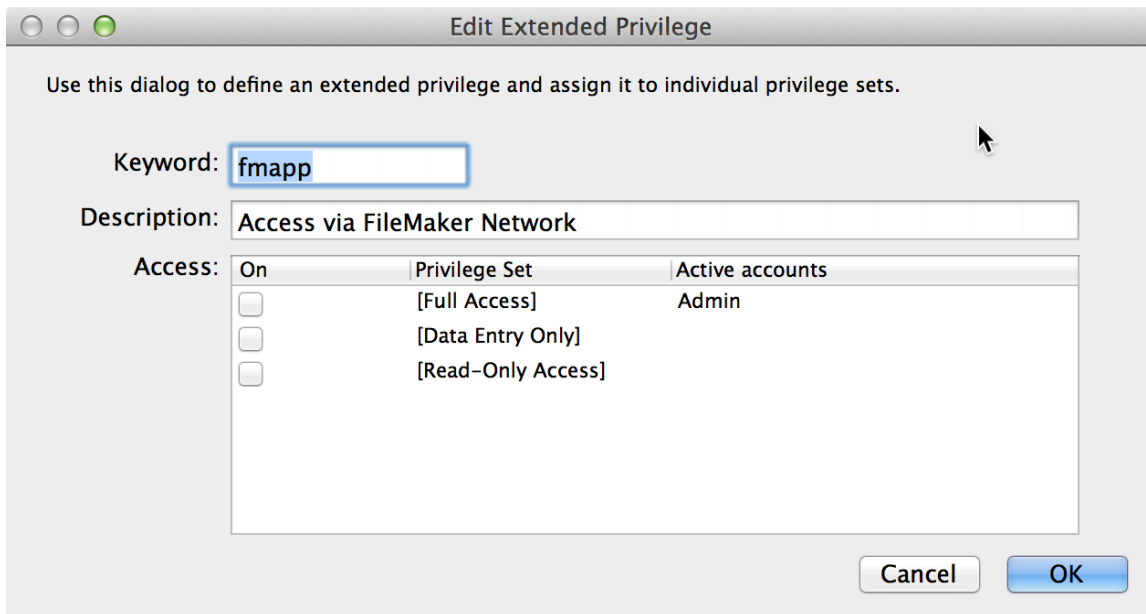


Figure 5. Edit an extended privilege and assign it to individual privilege sets.

Once you enable extended privileges for a privilege set, any accounts attached to that privilege set are able to access the file in the ways the extended privilege specifies.

Important for iPad and iPhone:

If your users will be using iOS devices, you may want to specify the `fmreauthenticate[X]` extended privilege.

FileMaker Go allows multitasking. While using an iOS device, the user can answer a call or move to another app at any time. When this happens, FileMaker Go moves to the background and saves the state of the file.

With the `fmreauthenticate[X]` extended privilege, when FileMaker Go switches to the foreground users must re-enter the account name and password if the specified time limit [X] minutes has elapsed. For example, an extended privilege of `fmreauthenticate10` allows the user up to 10 minutes with FileMaker Go in the background before reauthenticating is required. You can create as many of these extended privileges with different periods as you need and assign them to different privilege sets. Users can attempt to enter their account name and password five times before FileMaker Go closes the file.

You can also create custom extended privileges to simplify your scripts. These custom extended privileges can be used to help you manage the business rules you need to enforce. An example of this might be the ability to run certain reports.

To create your own extended privileges, from the **Extended Privileges** tab, click on **New** and then enter a name and a description. The developer can then test which Extended Privileges a user belongs to by using the `Get(AccountExtendedPrivileges)` function in any calculation dialog.

Learn more about managing extended privileges:

http://fmhelp.filemaker.com/fmhelp_13/en/html/passwords.14.26.html#1029551



Define Other Privileges

Other privileges includes whether the privilege set allows users to:

- Print
- Export
- Manage extended privileges
- Override data validation warnings
- Disconnect user from FileMaker Server when idle
- Modify their own password
- Access menu commands (all, editing only, minimum)

Print includes both printing and saving records as PDF.

Export includes exporting records, saving records as an Excel file, copying records in a found set to the Clipboard, saving a copy of the file, and the use of the data with Apple Events (GetCellValue, Field Contents, Record Value, Table Contents, and Layout Contents). Also a file opened without Export privileges cannot be used as the source of an import.

Please note that **Disconnect user from FileMaker Server when idle** also requires setup. See the [Use Server Idle Timeout](#) section of this guide for the configuration steps for FileMaker Server.

Learn more about other privileges:

http://fmhelp.filemaker.com/fmphelp_13/en/html/passwords.14.25.html#1029402

Setup Accounts or External Server Groups for Authentication

Once you've defined your privilege sets, you can begin to create accounts. Accounts authenticate users who are attempting to open a protected file. Authentication determines and validates the user's identity.

Each database file initially contains two accounts: **Admin** and **Guest**.

The **Admin** account is assigned the **[Full Access]** privilege set, which permits access to everything in a file. This account is fully editable. You can rename it, assign it a password, make the account inactive, or even delete the **Admin** account (although the file will require that there be at least one **[Full Access]** account). Remember, by default, the **Admin** account has no password so it should be changed when you first begin.

The **Guest** account allows users to access your file without supplying any account information. By default, this account is assigned the **[Read-Only Access]** privilege set, but you can assign any privilege set you want to the **Guest** account.

Initially, the **Guest** account is inactive. You can enable the **Guest** account by checking the checkbox in the Active column that corresponds to the **Guest** account (Figure 6). This account is not fully editable. You cannot delete the **Guest** account, change the **Guest** account name, or assign it a password.

To create a new account, click the **New...** button (Figure 6). To edit an existing account, select the account and click the **Edit...** button.



When you create an account, you give it an account name and password and assign a privilege set to the account. Account names are not case sensitive but passwords are case sensitive. Since you should not know the user's password, be sure to check the box **User must change password on next login** (Figure 7). You can also use this to reset users' passwords in the event they forget.

Passwords are stored using a one-way hash, meaning the password can be encrypted but never decrypted. Therefore it is only possible to reset a password and not recover a password.

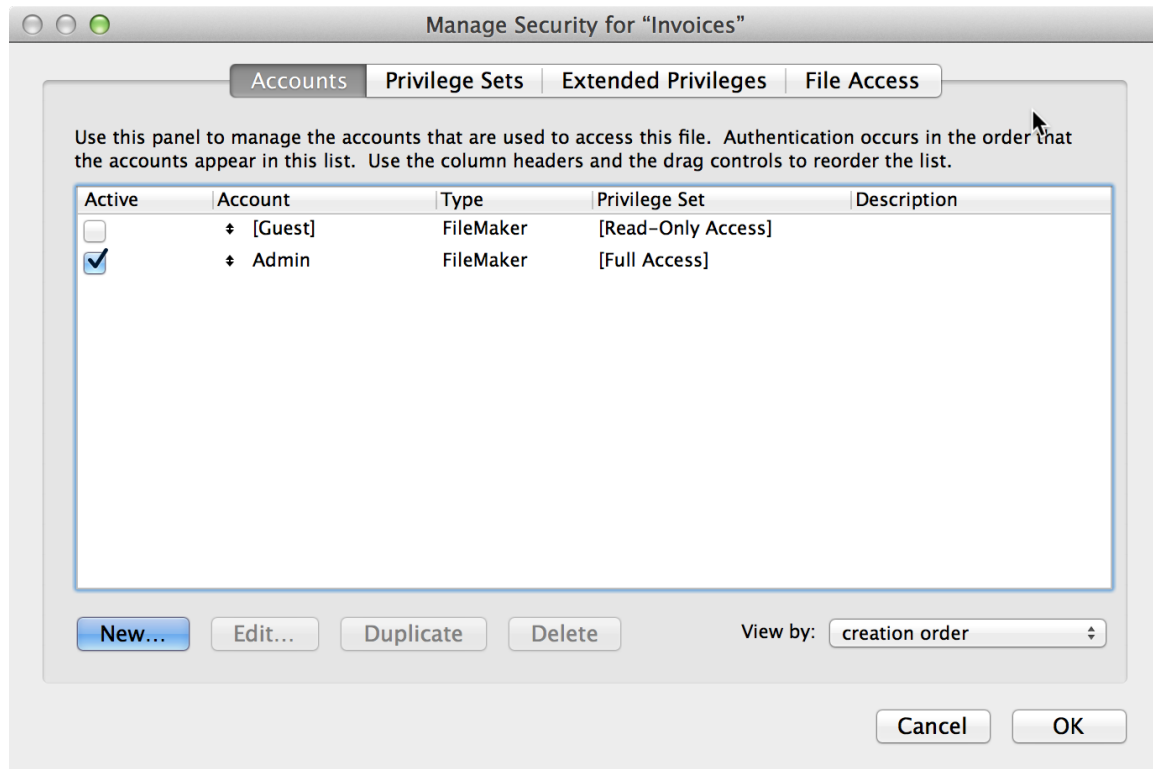


Figure 6. Create, edit and delete accounts.



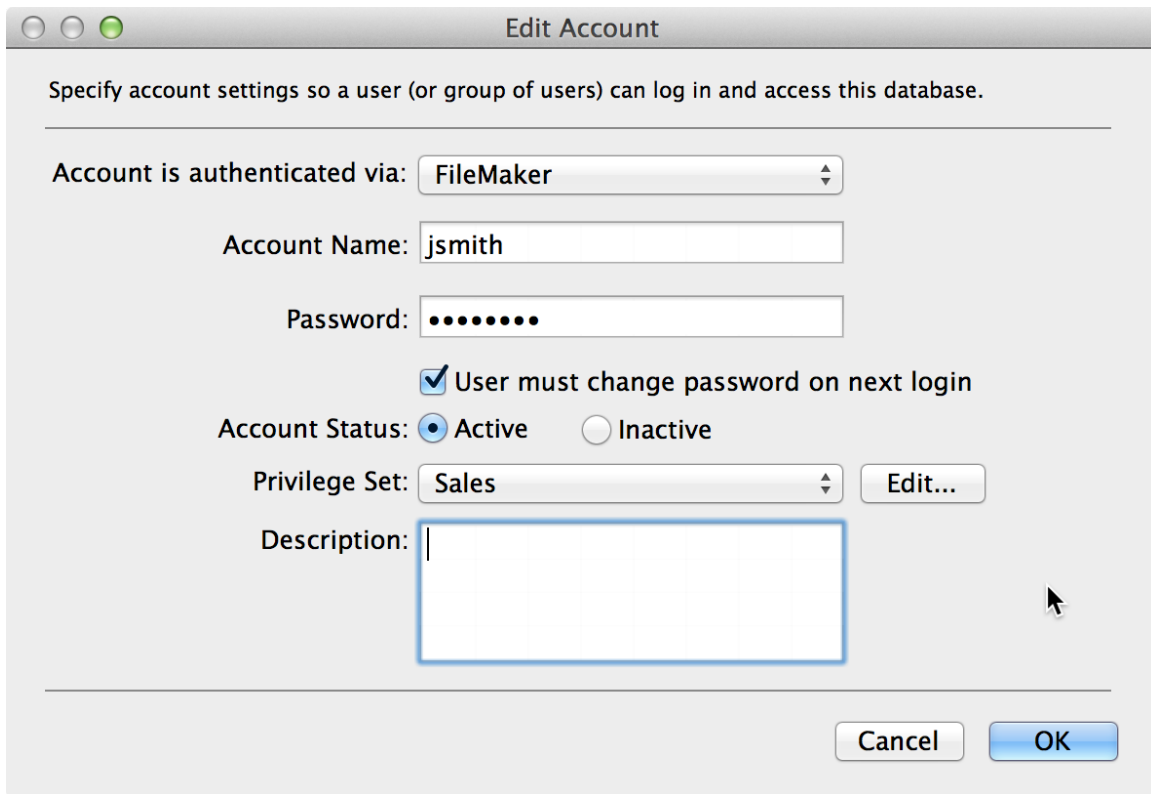


Figure 7. Specify an account name, temporary password and privilege set.

Learn more about creating accounts:

http://fmhelp.filemaker.com/fmphelp_13/en/html/passwords.14.10.html#1028089

If you host files using FileMaker Server, you can create external server accounts that are authenticated by Active Directory or Open Directory. This allows you to use your existing authentication server to control access to databases without having to manage an independent list of accounts in each FileMaker Pro database file.

Alternatively, you can use local Security Groups and Accounts on the server machine hosting FileMaker Server. For more information, please refer to your OS help files.

External authentication is a particularly good idea if:

- Your organization already uses Active Directory or Open Directory.
- Your FileMaker file will be accessed by other files in a multi-file solution.
- Your organization enforces minimum password standards. FileMaker Pro can enforce elementary standards such as password length and frequency of changing password. External Authentication offers more robust password control such as enforcing password complexity requirements.

Additionally, if you host files using FileMaker Server installed on Windows Server OS and use Active Directory for external authentication, your Windows users will enjoy the benefit of Single Sign On.

By using external authentication, there is some risk that someone will gain access to your file by simulating the external authentication environment or mismanaging the groups. It is your responsibility to prevent this by maintaining the security of your external authentication server. One



option to mitigate this risk is to enable database encryption for your solution files, as this would require anyone to first provide the encryption password before sharing the file on FileMaker Server.

In order to use external authentication, you will need to setup external authentication accounts within the file using FileMaker Pro, and you will need to host the file using a FileMaker Server that has been configured for external authentication. See the Enable External Authentication section of this guide for the configuration steps for FileMaker Server.

To implement external authentication for a solution file, follow the steps below (Figure 8):

1. From the **Accounts** tab, click on the **New** button.
2. From the **Edit Account** dialog box, for **Account is authenticated via**, choose **External Server**.
3. For **Group Name**, enter the name of a group that is defined on the external authentication server. Note that group name is case sensitive. If you are using Open Directory, be sure to use the short name format for the Group.
4. Repeat these steps for each external authentication group that you are adding.

Specify account settings so a user (or group of users) can log in and access this database.

Account is authenticated via: External Server

Group Name: SalesReps

Authentication for this account will be handled using the method you designate in FileMaker Server.

Account Status: Active Inactive

Privilege Set: Sales Edit...

Description:

User Data Cancel OK

Figure 8. Accounts can be authenticated via Open Directory or Active Directory.

In the event that the user forgets their password, you will need to use the external authentication server to reset their password.

Learn more about creating accounts that authenticate via an external server:
http://fmhelp.filemaker.com/fmhelp_13/en/html/passwords.14.13.html#1028271



Important information when using external authentication:

With External Authentication turned on, it is possible for an account name and password to be the same for a local FileMaker account and an external account, and also for an external account to belong to multiple groups. When this happens, FileMaker Pro opens the file using the first matching account in the authentication order. Any matching accounts that follow the first one are ignored. Therefore, it's important to set the authentication order for accounts when one or both of the above situations exist. Otherwise, the wrong account may be used to access the file. Authentication order can be viewed and changed under the **Accounts** tab using the **View by** menu (Figure 6). It is a best practice to avoid using a duplicate of an external account and a local FileMaker account so that you do not have to worry about the authentication order.

It is not recommended to create any externally authenticated full access accounts. It is better to maintain a local FileMaker account available for administration purposes in case the file needs to be removed from FileMaker Server for any reason. If there are no local FileMaker accounts, the file will not be able to be opened if it is not hosted.

Authentication and Multi-file Solutions

FileMaker files can be accessed by each other in a multi-file solution. This can be useful, for example, if you have a centrally accessible file of employee contact information that is used by a variety of internal solutions from human resources to sales to operations and more.

When opening one file from another (such as when viewing external data or running a script in an external file), FileMaker will attempt to pass the same credentials the user supplied at login to the second file. If there is a corresponding account and matching password, the user will automatically be logged in to the second file with the privilege set specified by the account. If there is no corresponding account, the user will be presented with an authentication dialog.

You can create accounts manually in multiple files, but doing so can lead to user-entry errors. To better facilitate this process, either automate account creation with scripts or use external authentication. See the [Use scripts, functions and more to enhance security](#) section of this guide for more information on scripts.

It is important that you carefully review the privileges in each file of a multi-file solution. For example, if you are not thorough, a user may be restricted from printing a list in one file by the privilege set for that file, but still be able to print the same list from within another file in a multi-file solution.

Use File Access to Authorize Access to Files

You can control whether other FileMaker Pro files are permitted to access the schema in a file (including its tables, layouts, scripts, and value lists) in your secured solution. When protection is enabled, any use of the protected file through a FileMaker data source, including the file metadata, will first require full access authorization.

Click on the **File Access** tab and check the **Require full access privileges to use references to this file** to ensure that file access is limited. Then, authorize any other files that are part of the solution by clicking **Authorize** and then selecting the files (Figure 9).



Each authorized file is assigned a unique identifier, which the protected file keeps track of, ensuring that the protected file remains protected even if it is renamed or duplicated. Any efforts to bypass authorization, such as by replacing an authorized file with a different one, will be unsuccessful.

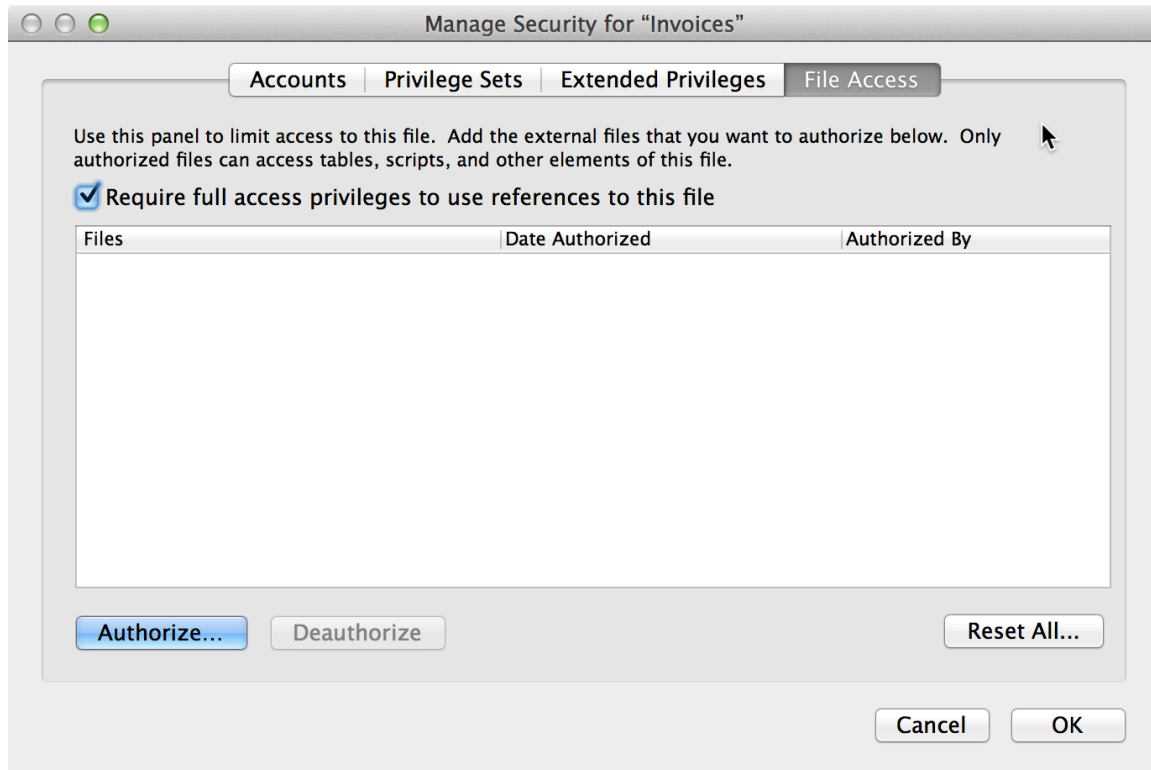


Figure 9. Using File Access to authorize files to access tables, scripts and more.

Learn more about authorizing access to a file:

http://fmhelp.filemaker.com/fmhelp_13/en/html/passwords.14.33.html#1043162

Database Encryption

FileMaker Pro Advanced has the ability to encrypt all of the information stored within a file. This technique is shown in the information security compliance guidelines as **Encryption At Rest**. Using database encryption will protect your solution in the case that someone gains physical access to the file.

Database encryption can be enabled on a file through the Developer Utilities in FileMaker Pro Advanced. Under the Solution Options, check **Enable Database Encryption (or Re-encrypt files)** (Figure 10). **Create Error log for any processing errors** will be enabled by default.



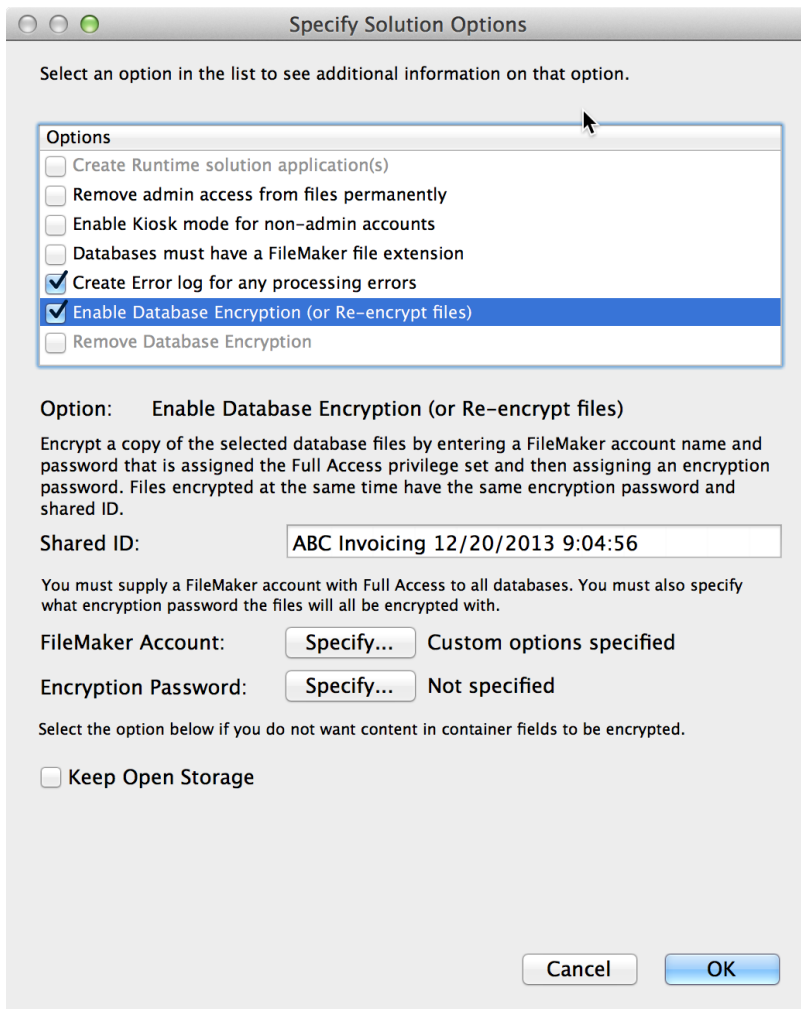


Figure 10. Solution Options under Developer Utilities to enable database encryption for a file.

A local FileMaker account with **[Full Access]** to all files is necessary to enable database encryption. Also necessary are an encryption password and a Shared ID. The password will be used whenever FileMaker Pro or FileMaker Go open a local file, or when FileMaker Server opens a file before hosting. The Shared ID is used by FileMaker to try the same encryption password on another file in the same set, therefore lessening the first user's need to re-type the same password for multi-file solutions.

Learn more about database encryption:

http://fmhelp.filemaker.com/fmphelp_13/en/html/fmpa_tools.24.5.html#1042372

When opening an encrypted file on FileMaker Server, there is an option to save the password. This will allow FileMaker Server to automatically open encrypted files when it is restarted. FileMaker Server uses a two-way AES-256 encryption using a composite key based on information from the machine to encrypt this password and stores it securely on the server.

For help opening encrypted files on FileMaker Server, refer to the FileMaker Server 13 Help Guide, page 103.

https://fmhelp.filemaker.com/docs/13/en/fms13_help.pdf



Use Scripts, Functions and More to Enhance Security

Record deletion, auditing and maintenance are common tasks where security can be enhanced via scripts, functions and more. For example, scripts can be used to:

- Add or delete accounts, reset account passwords, change passwords, enable or disable accounts, and re-login as a different user.
- Archive records when you don't want a user actually to delete records.
- Provide you with information about the user's current session and state for regulatory compliance and auditing purposes.

By default, scripts run with the privilege set of the account currently logged in. This can cause issues if the script tries to perform an action the user does not have the privileges to do. Be sure to test all scripts thoroughly to protect the integrity of your data.

While scripts can improve the user experience of secure solutions, they should not be used as the only security measure. Use scripts in tandem with the options under **Manage Security** to provide the best experience for your users.

For implementation, please familiarize yourself with FileMaker scripting and relational model.

Learn more about scripts to create and manage user accounts:

http://fmhelp.filemaker.com/fmhelp_13/en/html/scripts_ref2.37.27.html#1028418

Learn more about **Get** functions:

http://fmhelp.filemaker.com/fmhelp_13/en/html/func_ref2.32.1.html#1048024

Additionally, if you are in a regulated industry, you may be interested in using the **Database Design Report** feature in FileMaker Pro Advanced to document the schema of your database and publish it to an HTML or XML file.

Learn more about the **Database Design Report**:

http://fmhelp.filemaker.com/fmhelp_13/en/html/fmpa_tools.24.5.html#1027855

Enable or disable plug-ins

In FileMaker Pro, plug-ins can be used to provide additional functionality. Plug-ins can access and modify your solution and connect to other services over the internet. If plug-ins are needed for a solution, be sure to get them from a trusted source.

You can enable or disable the installation of plug-in files to provide additional security and prevent unauthorized plug-ins from being installed using the **Preferences** dialog (see Figure 11). This is a FileMaker Pro preference, not a file-specific preference, and determines if plug-ins may be installed on the user's computer.



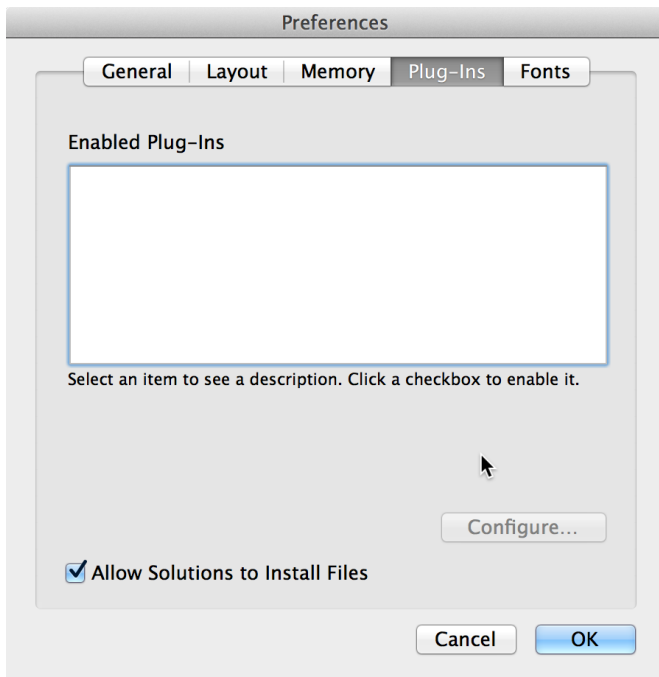


Figure 11. Plug-ins let you add features to your FileMaker Pro file.

Learn more about plug-ins:

http://fmhelp.filemaker.com/fmphelp_13/en/html/preferences.26.5.html#1027768



Security Configuration of FileMaker Server

Several features in FileMaker Server make your data more secure for FileMaker Pro, FileMaker Go, and FileMaker WebDirect clients. The following sections outline the steps to setting up security on your FileMaker Server from the Admin Console.

Install FileMaker Server With All or Some of the Components Behind Your Firewall

A FileMaker Server can contain up to three components:

- Database Server
- Web Publishing Engine
- Web Server

You can deploy them all on one machine or across two machines. When deployed across multiple machines, you can control where each machine is in relation to your firewall.

For example, sensitive data residing in the Database Server can sit behind the firewall, while customers retain access to public, non-sensitive data over FileMaker WebDirect. It's also a good idea for the physical location of the server to be secured (i.e. in a locked room).

When you are done following the installation instructions, you will have access to the FileMaker Server Admin Console (Figure 12).



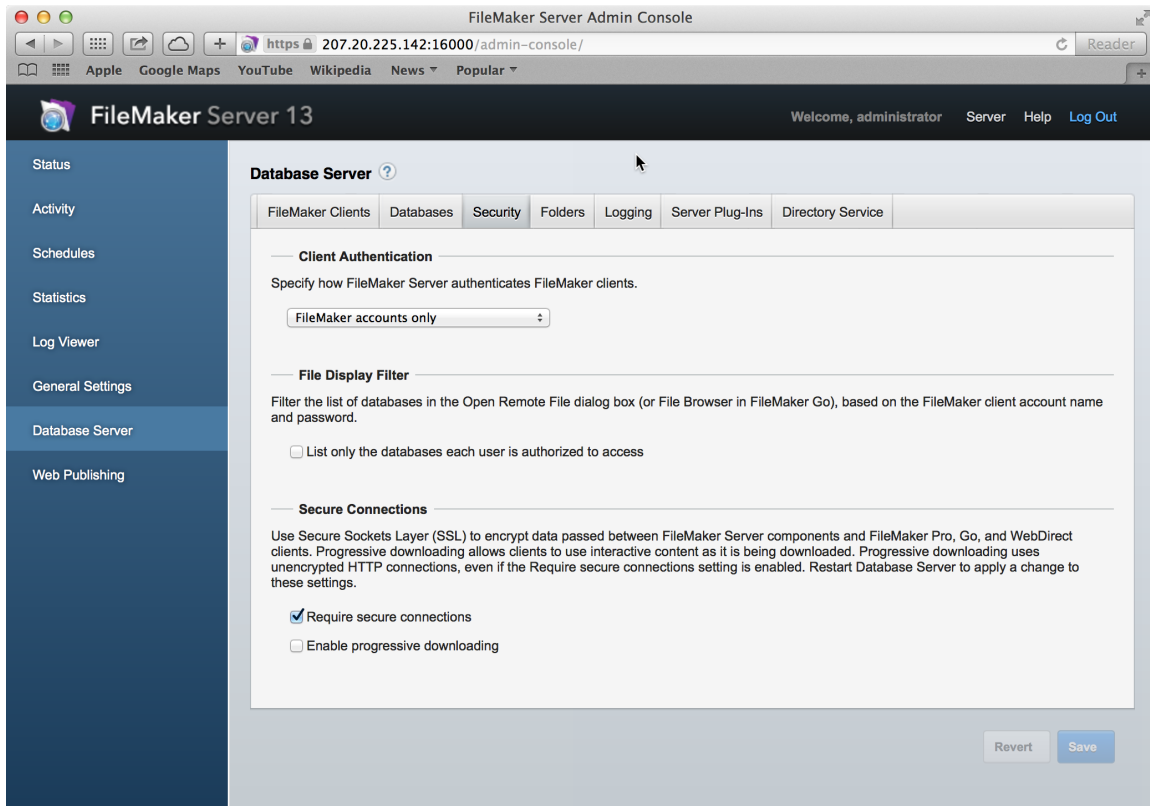


Figure 12. Security tab of the FileMaker Server Admin Console

For installation instructions, read Chapter 1 of the FileMaker Server 13 Getting Started Guide: https://fmhelp.filemaker.com/docs/13/en/fms13_getting_started.pdf

Enable External Authentication

You can use your existing authentication server to control access to files without having to manage an independent list of accounts in each file.

In order to use external authentication, you will need to setup external authentication accounts within the file using FileMaker Pro AND you will need to host the file using a FileMaker Server that has been configured for external authentication. See *Setup Accounts or External Server Groups for Authentication* section of this guide for the configuration steps for FileMaker Pro.

To enable external authentication on FileMaker Server, follow the steps below:

1. Choose the **Database Server > Security** tab.
2. Select **FileMaker and external server accounts** in the **Client Authentication** section.

If you plan on using Active Directory or Open Directory, the server where FileMaker Server is installed must be a member of the domain you plan to use for external authentication.

If you plan on using **Local Security Groups** on the FileMaker Server machine, this machine must not be a member of the domain.

In either case, be sure to test thoroughly. See *Testing Security Settings* section of this guide.



Limit Display of Files

When connecting to a server using **Open Remote** in FileMaker Pro, the **Hosts** tab on FileMaker Go, or navigating to the FileMaker WebDirect home page, FileMaker Server produces a list of files for the user. By default, this list shows all files available on a server. However, you can choose to only show the files that the current user can access. Follow the steps below:

1. Choose **Database Server > Security** tab.
2. Select **List only the databases each user is authorized to access**.

Turn On SSL Encryption

FileMaker Server can encrypt all traffic between the **Database Server** and FileMaker Pro or FileMaker Go clients. It also encrypts all traffic between the Database Server and the Web Publishing Engine and FileMaker WebDirect clients.

To turn on SSL, follow the steps below:

1. Choose **Database Server > Security** tab.
2. Select **Require secure connections**.
3. Choose **Server** menu > **Stop Database Server** (or click on the **Stop Database Server** toolbar icon).
4. Choose **Server** menu > **Start Database Server** (or click on the **Start Database Server** toolbar icon).

With Custom Web Publishing, the connection between the Web Server and the Web Browser is not encrypted. To encrypt the data between the Web Server and the Web Browser, you will also need to enable SSL on your Web Server. Please refer to your Web Server documentation (Apache or IIS).

By default, when SSL encryption is enabled, data in container fields that are configured to allow for streaming will not be streamed. Instead, the full content of the container field will be sent to the user before the user can interact with it.

By checking the **Enable progressive downloading** checkbox, FileMaker Server will allow progressive downloading (streaming) of container data over an unencrypted HTTP connection, even when SSL encryption is enabled.

By default, FileMaker Server creates an SSL certificate that provides an encrypted SSL connection without server name verification. To provide additional security, you can request a signed certificate from a Certificate Authority that matches your specific server name or DNS name to help prevent man-in-the-middle attacks.

To use a signed certificate from a certificate authority, you must use the **fmsadmin** command line interface. The **CERTIFICATE** command is used to create a Certificate Signing Request (CSR) and import a signed certificate matching the server name or domain name system (DNS) name for a fully secure SSL connection with FileMaker Server.

For help with setting up SSL encryption, refer to the FileMaker Server 13 Help Guide, pages 138-139: https://fmhelp.filemaker.com/docs/13/en/fms13_help.pdf



For help with using custom certificates, refer to the FileMaker Server 13 Help Guide, page 191.
https://fmhelp.filemaker.com/docs/13/en/fms13_help.pdf

To test the encryption between the **Database Server** and FileMaker Pro or FileMaker Go clients, use the **Get(ConnectionState)** function. It will return a value of:

- 0 for no network connection for the current file
- 1 for a non-secured connection
- 2 for a secured connection using FileMaker Server's default SSL certificate
- 3 for a secured connection with a fully verified server name in the certificate

For example, you could write a script to run when a file is opened that uses the **Get(ConnectionState)** function that alerts the user if the connection to FileMaker Server is not a secure connection.

Other SSL Options

FileMaker Server can send notifications when errors or warnings are detected or when a scheduled task is completed. To use SSL data encryption when FileMaker Server connects to the SMTP email server, follow these steps:

1. Choose **General Settings > Email Notifications** tab
2. When entering the SMTP information, select **SMTP Authentication** and then select **Use Secure Socket Layer (SSL)**.

For help with setting up SSL encrypted email notifications, refer to the FileMaker Server 13 Help Guide page 44:
https://fmhelp.filemaker.com/docs/13/en/fms13_help.pdf

Additionally, if you are connecting to an external SQL data source, such as Microsoft® SQL Server, MySQL or Oracle, SSL encryption does not extend to the link between FileMaker Server and the external SQL data source. To create an SSL tunnel between FileMaker Server and the external SQL data source, you will either need SSL support from your ODBC driver or you will need to create a point-to-point SSL tunnel by other means.

Lastly, if you would like FileMaker Server to register itself with your organization's LDAP directory service, you can enable SSL in the Directory Service assistant to encrypt this process. This registration is for information and discovery purposes only. It plays no role in the configuration of external authentication. Refer to the FileMaker Server 13 Help Guide, page 66, for more information:
https://fmhelp.filemaker.com/docs/13/en/fms13_help.pdf

Use Server Idle Timeout

You can set the maximum time a FileMaker client can be idle when connected to a file hosted by FileMaker Server. This helps mitigate the risk of your files being accessed via an unattended computer, iPad or iPhone. However, make sure the idle time is long enough to avoid frequent disconnections.

For this to work within FileMaker Pro, you should enable the **Other Privileges** option of **Disconnect user from FileMaker Server when idle** for each privilege set you would like to disconnect when idle.



Because you can set this option on a privilege set basis, certain users will be disconnected while other users always maintain their connections. Note that users logged in with **[Full Access]** privileges will never be disconnected when idle.

To specify the idle time, follow these steps:

1. Choose **Database Server > FileMaker Clients** tab
2. Select **Set maximum idle time allowed for FileMaker clients** and enter the time (in minutes)

Define Administrator Groups

As the server administrator, you can use administrator groups to delegate database administration tasks to other users. You retain exclusive and complete control of FileMaker Server. Group administrators are not allowed to configure FileMaker Server, and you specify which database administration tasks you want to allow group administrators to do. Please note that use of the **Command Line Interface**, specifically the **fmsadmin.exe** service, is constrained; these administrator groups cannot employ the **Command Line Interface** at all.

Additionally, you can use external authentication to validate the credentials of the users in your administrator groups and to support Admin console login.

For help with Administrator Groups, refer to the FileMaker Server 13 Help Guide, pages 52-62: https://fmhelp.filemaker.com/docs/13/en/fms13_help.pdf

Viewing Log File Entries in the Admin Console

As FileMaker Server runs, it logs server activity, and optionally collects client access and other information you may need for regulatory and auditing purposes.

To view, sort, filter and export the log file entries, choose the Admin Console **Log Viewer** pane, select one or more log file modules for **Modules**, and select a date range on the calendars next to **Start** and **End**.

For help with log files, refer to the FileMaker Server 13 Help Guide, pages 125-132: https://fmhelp.filemaker.com/docs/13/en/fms13_help.pdf

Set Up Scheduled or Progressive Backups to a Secure File Location

FileMaker Server offers two types of backups: scheduled and progressive. If you had a user who inadvertently or purposely destroyed the data in your file, you can revert to the backup. Be sure to specify a secure physical location for stored backups.

With a scheduled backup, FileMaker Server will check whether data has changed since the last backup and create a full copy of databases and container data that have changed.

With a progressive backup, FileMaker Server creates two full backups in the progressive backup folder of all hosted databases, then after the specified interval applies any changes to the oldest backup copy.



Backups can only be saved to local disks, therefore other tools are needed to work in tandem to provide offsite backups in the case of disaster recovery.

FileMaker Server creates the directory structure for these backups. Please do not attempt to open or modify these files in place. Never move your backups. Always copy them to another location before opening them.

For help with backup procedures, refer to the FileMaker Server 13 Help Guide, pages 143-147: https://fmhelp.filemaker.com/docs/13/en/fms13_help.pdf

Testing Security Settings

When you think you are completely done setting up the security for your file and the FileMaker Server, it is recommended that you test the security just like you would test any other feature of your solution.

- Set up a test account for each privilege set. Make these active for testing and inactive in your production system.
- Define a checklist of features and functions to test. Go through the checklist with each test account.
- Document your results.
- Repeat testing when new functionality is added.

Continually evaluate your security to make sure it is still protecting your data. This includes verifying that users have the latest, most secure software versions for their operating systems as well as their FileMaker software.

By following these guidelines, you can be confident that you have made your FileMaker solutions inherently secure and you will have documentation to validate that assertion.



Appendix A – Other Considerations

In addition to the guidelines outlined in this document, depending on your internal or regulatory requirements (COBIT, HIPAA, ISO, PCI, NIST, FIPS, etc.), there may be additional steps you need to take.

- You may need to encrypt all network traffic. Turn on SSL on FileMaker Server and then also configure SSL (outside of the FileMaker Platform) between:
 - FileMaker Server Database Server and external database(s)
 - FileMaker Server's web server (Apache or IIS) and web browsers accessing a Custom Web Publishing website
- You may have minimum password standards to meet. In this case, it is best to use an external authentication server.
- You may need an audit trail. If your needs are simple, you can build this with FileMaker Pro using tables and scripts. If your needs are more complex, consider using a commercially available audit plug-in.

It is up to you to fully understand your security compliance requirements and to take the appropriate steps.



Appendix B – Quick Reference Guide for Day-to-Day Operations

If you want to...	Go here...
Manage accounts, privileges, extended privileges or file access	FileMaker Pro or FileMaker Pro Advanced: File menu > Manage > Security
Immediately stop someone from accessing any data	FileMaker Server or FileMaker Server Advanced: Choose Clients and then select a client in the Connected Clients list. For Actions , select Disconnect . Click Perform Action . For Message , type a message if you choose. For Delay time , enter 0 to immediately disconnect. Click Send Message FileMaker Pro or FileMaker Pro Advanced: File menu > Manage > Security . Go to Accounts . Uncheck Active . If the user has access via an external authentication group, rather than deactivate access for the entire group, remove the user from the external authentication group. In an emergency, you can prevent access to everyone by closing the file.
Force a user to change their password	FileMaker Pro or FileMaker Pro Advanced: File menu > Manage > Security Go to Accounts . Select the Account and click Edit . Check User must change password on next login Note: You can also write a script to force more than one user to take this action. If the user has access via external authentication, manage this using your Active Directory or Open Directory server.
View FileMaker Server log files	FileMaker Server or FileMaker Server Advanced: Log Viewer pane



Appendix C – Types of Encryption Used by FileMaker

FileMaker encrypts data in different ways depending on the type of data. For example passwords use a one-way hash because they should never be decrypted, where SSL uses a two-way hash because data will need to be decrypted on the other end. Below lists the different ways FileMaker can encrypt data, and the hash and cipher type that it uses.

Option	Hash Type	Cipher Type
Account Password Storage	One way	AES-256
Database Encryption	Two way	AES-256
SSL (Between FileMaker Server and FileMaker Pro, FileMaker Go, FileMaker Web Publishing Engine, and between Web Server and Web Browser for FileMaker WebDirect and Admin Console)	Two way	AES-256
Secure Storage (Database Encryption Disabled)	Two way	AES-128
Secure Storage (Database Encryption Enabled)	Two way	AES-256



Appendix D – Process for Installing a Custom Certificate for SSL

Outlined below is the process for installing a custom certificate with FileMaker Server for all SSL connections.

1. Create a Certificate Signing Request (CSR) from the command line with the command

```
fmsadmin certificate create serverAddress.com
```

This will generate two files in the CStore directory where FileMaker Server installed: `serverRequest.pem` and `serverKey.pem`. `serverRequest.pem` is the CSR, and `serverKey.pem` contains a private key used to generate the CSR.

2. Provide `serverRequest.pem` to a Certificate Authority (CA) and purchase a Certificate.
3. Copy the certificate from the CA onto your server.
4. Import the certificate from the command line with the command

```
fmsadmin certificate import /path/certificate.cer
```

5. FileMaker Server will create `serverCustom.pem` in the CStore folder if the certificate is successfully imported. Copy this file to a safe location in case FileMaker Server needs to be reinstalled on the same machine.

The `fmsadmin certificate create` command allows you to provide extra information about your server into the CSR. To learn more about this command, refer to the FileMaker Server 13 Help Guide, pages 191-193:

https://fmhelp.filemaker.com/docs/13/en/fms13_help.pdf



© 2014 FileMaker, Inc. All rights reserved. FileMaker and FileMaker Go are trademarks of FileMaker, Inc., registered in the U.S. and other countries. The file folder logo and FileMaker WebDirect are trademarks of FileMaker, Inc. All other trademarks are the property of their respective owners. Product specifications and availability subject to change without notice.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, AND FILEMAKER, INC., DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR THE WARRANTY OF NON-INFRINGEMENT. IN NO EVENT SHALL FILEMAKER, INC., OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS, PUNITIVE OR SPECIAL DAMAGES, EVEN IF FILEMAKER, INC., OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY. FILEMAKER MAY MAKE CHANGES TO THIS DOCUMENT AT ANY TIME WITHOUT NOTICE. THIS DOCUMENT MAY BE OUT OF DATE AND FILEMAKER MAKES NO COMMITMENT TO UPDATE THIS INFORMATION.

