Best Practices for FileMaker Hosting at MIT

Best Practices for FileMaker Hosting at MIT

> ⚠ **NOTE: IS&T recommends that IS&T Managed Servers be used for hosting FileMaker databases.**
> Only experienced server administrators should attempt to do so, particularly where databases with sensitive data and/or mission critical functions will be housed. The following web page offers MIT-specific configuration recommendations to help mitigate against security risks in the FileMaker hosting environment. In a changing computing landscape these recommendations in no way offer a guaranteed maintenance or risk-free hosting environment.

The following is a list of best practices for hosting FileMaker databases at MIT if you are not intending to use an IS&T managed FileMaker server (recommended), and includes information on server machine setup, FileMaker Server configuration, and FileMaker database settings. If you are using an IS&T hosted FileMaker server, you will not need to concern yourself with the instructions given here as these tasks will be taken care of for you based on your server needs. For an overview of FileMaker at MIT, including instructions for installing FileMaker Server and more general notes on security, please see FileMaker at MIT. Considering the costs of hardware and ongoing maintenance needs related to any server, an IS&T managed server is very likely the most cost effective option available to DLCs. To find out more about IS&T managed FileMaker servers, please contact filemaker-support@mit.edu before purchasing hardware and preferably before engaging in any new FileMaker development project.

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.

Server Machine

Hardware and physical security

Because securing and maintaining server hardware and FileMaker server software is not a trivial matter, our recommendation is to use IS&T-managed servers whenever possible. If using a non-IS&T hosted server, your server should be server-class physical or virtual machine. If not residing in the MIT data center, server hardware should be kept in a lockable inner office or server closet that is only accessible by authorized personnel; UPS is highly recommended.

Operating system

Use a server-class Windows or Mac OS.

Power settings

Configure server machine to always be on (never asleep or hibernating)

Ports and firewall settings

See FileMaker Server Port Settings at MIT for the port settings required by FileMaker Server.

Backup and recovery

Set up TSM account and exclude the Databases directory:

Win: `C:\Program Files\FileMaker\FileMaker Server\Data\Databases`
Mac: `/Library/FileMaker Server/Data/Databases`

Any non-FileMaker process that accesses the live hosted files runs a risk of file corruption. The FileMaker `Server\Data\Backups` folder may be safely backed up by TSM or your back-up application.

Anti-virus software

Anti-virus software should be completely disabled, or at least set to exclude the live hosted files from scanning (see “Backup and recovery” above).

Indexing software

Turn off Indexing Service (Windows) or Spotlight (Mac). Indexing reduces performance.

Web services

Web services will need to be turned on, even if FileMaker web publishing is not enabled, in order for server administrators to access the FileMaker Server Admin Console.

WIN domain

If the server is deployed on the MIT WIN domain, be mindful of group policies around TSM, antivirus, and other services. Adjustments to these services may need to be made at the group level as changes made locally can be overwritten by the group policy.

Server Maintenance

Before running OS updates, FMS updates, or rebooting the server for any reason, all database files should be closed and then FileMaker Server should be stopped. Once FileMaker Server has been stopped, the machine can be safely rebooted.

FileMaker Server Application

Version

Install the most recent version of FileMaker Server available on the IS&T Software Grid. For a step-by-step guide on installing FileMaker Server, see FileMaker Server Installation and Configuration.

Launching the Admin Console

FileMaker Server settings are configured using the Admin Console. To launch the Admin Console, point a browser to `https://<hostname>.mit.edu:16000`. The items that follow assume you are logged into the Admin Console.

Admin Console access

Restrict Admin Console access, done in the **General Settings pane > Admin Console tab**. Set a username/password (can be set at installation). To allow access to members of a server group, check off **Use external group** and enter the group name. You may also restrict access by IP address.

Only enable Web Publishing if using Web Publishing

Unless using FileMaker to publish databases or data to the web (via WebDirect, the FileMaker Data API, or custom web publishing), do not enable Web Publishing. **Server menu > Edit Deployment > Web Publishing section >** check off **No, do not enable web publishing.**

Note: If using web publishing with solutions that contain sensitive data, extreme care should be taken with the implementation of user accounts and privilege sets such that the sensitive data is never exposed to the web. Further, as a rule, FileMaker should never be used at MIT to store protected data such as social security or credit card numbers.

Email notifications

Enable this to receive error notifications via email if desired. **General Settings pane > Email Notifications tab**. Under **SMTP Information**, enter the appropriate *From* and *Reply-To* information. **SMTP Server Address** = `outgoing.mit.edu`, **port** = `25`, **SMTP Authentication** = `None`. Under *Notification Settings*, check off "**Send email notifications to**" and enter an address. Generally, enable for "**Errors only**". Including Warnings can generate lots of unnecessary notifications.

Auto-start

Enable **FMS auto-start** on system startup/reboot. In the **General Settings pane > Auto Start tab**, check off **Automatically start Database Server** and **Automatically open databases that are in the database folders.** If web publishing is enabled (you should have good reason to do this), check off **Automatically start Web Publishing Engine.**

Disallow ODBC access if not used

Unless using FileMaker as an ODBC data **source**, do not enable ODBC access. **General Settings pane > ODBC/JDBC**, uncheck **Enable ODBC/JDBC.** FileMaker databases may still access external ODBC data sources.

Disconnect idle clients

Set a maximum idle time for FileMaker clients. **Database Server pane > FileMaker Clients tab**; check off **Set maximum idle time allowed for FileMaker clients (minutes)** and enter a value. 240 (4 hours) is a reasonable default setting.

Database cache

To improve performance, increase the memory available to FileMaker Server. **Database Server pane > Databases tab**. Set the **RAM Reserved for Database Cache (MB)** to half of the maximum allowed cache size.

External authentication and Kerberos

Enabling external authentication will allow databases to utilize Moira groups for defining database users and groups, and allow users to access databases using their Kerberos credentials. **Database Server pane > Security tab >** set **Client Authentication** to **FileMaker and external server accounts.** See FileMaker Authentication for more info.

File display filter

Limit the display of files available on the server to only those users are authorized to see. **Database Server pane > Security tab > "List only the databases each user is authorized to access"** radio button.

SSL encryption

Turn on SSL encryption. Database Server pane > Security tab > **Secure connections to FileMaker Server** checkbox, and **Use HSTS for web clients** checkbox. You must stop and restart FileMaker Server for changes to these settings to take effect.

Important: You should also request and install a custom SSL certificate. See FileMaker Server SSL Certificates.

Logging

Database Server pane > Logging tab. Increase the Log Size; 100 MB is a good starting point. Check off **Access**, **Usage statistics**, **Client statistics**, and **Top call statistics**.

Backups

Configure FMS to run backups at least once daily. This is done via the Schedules pane. Backup files are written to the FileMaker `Server\Data\Backups` folder.

FileMaker Files

Implement Kerberos authentication

If the server hosting environment permits, implement Kerberos authentication for all MIT-based, non-full access users. This involves careful planning and multiple steps. For more information, see Configuring FileMaker Databases For Kerberos Authentication.

Full Access and other internal accounts

All database solutions require at least one internally authenticated, full access user account. By default, new databases are given a full access account named 'Admin' with NO password, and are set to auto-login with this account. Before hosting a database, the Admin user account should either be given a strong password, or disabled and a new full access account created.

Strong passwords should be used for all internal FileMaker accounts, whether full access or not.

Privilege sets

The application should have at least two privilege sets, or role levels. Users who are not developing or supporting the system should not be assigned the [Full Access] privilege set.

Sensitive data

PII data (SSN, credit card numbers) should never be stored in FileMaker at MIT. Sensitive data should not be web-enabled.

Disable auto-login

Under **File > File Options**, on the **Open/Close tab**, ensure that **Login using:** is unchecked and that no file credentials are entered.

Hide filename from network

With the database open in FileMaker Pro: under the *Sharing menu*, select **FileMaker Network**, then check off **Don't display in Open Remote dialog.** This must be done before file is hosted with FMS.

Disallow ODBC and WebDirect access if not used

By default, ODBC and WebDirect access are not enabled in new files. For existing solutions, verify settings in FMP client. For WebDirect: **Choose File > Sharing > Configure for WebDirect**, and set to **No Users**. For ODBC: **Choose File > Sharing > Enable ODBC/JDBC**, and set **Enable for ODBC/JDBC** to **Off**.

For more information

Contact filemaker-support@mit.edu.