FileMaker - MIT Security Guidelines

FileMaker - MIT Security Guidelines

> ⚠ **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 FileMaker platform includes a very robust set of security features. FileMaker supports individual user accounts and employs modern hashing methods for the protection of passwords. FileMaker Server may also be configured for SSL encryption of the data transmission between server and FileMaker clients. For these reasons, IS&T recommends that users of shared FileMaker database applications implement a client/server configuration, and follow FileMaker security best practices.

To get the full benefit of the security available with FileMaker, shared databases should be hosted on FileMaker Server. Some file-level measures can also be taken; implementing these in conjunction with Server protections will protect your databases with a greater level of security.

Security Best-Practices Checklist

Here is a checklist to help you apply security best practices to your FileMaker files.

Applies to Local and Hosted FileMaker Files

- Do not store PIRN in any FileMaker database
- Implement Kerberos authentication for all non-full access MIT users
- Always use strong passwords for internally-authenticated accounts
- Disable auto-login of the default Admin account
- Add a strong password to the default Admin account; alternatively, deactivate this account and create a new Full Access account with a strong password
- Use privilege sets to create roles and give each user an individual account, not a shared one
- Keep your list of active user accounts up-to-date; de-activate accounts for any users who should no longer have access
- Convert all files to the current file format (.fmp12) so that they may be opened with the most recent version of FileMaker Pro
- Files in version 6 and earlier (.fp5 format) must be converted to current version by way of FileMaker Pro 11
- Avoid storing inactive FileMaker files locally
- Take an inventory of the data in your files
- Never use the peer-to-peer file sharing configuration
- **Host your FileMaker files on an IS&T-managed server**

Applies to Hosted FileMaker Files and FileMaker Server

- Require that all databases hosted on your server are password-protected
- Provide users with opener files, or add the files to users' Favorites list in the FileMaker Launch Center
- If using WebDirect or custom web publishing, take active steps to prevent sensitive data from being exposed to the web
- Enable SSL encryption in FileMaker Server
- Obtain and install a custom SSL certificate on the server
- Hide hosted filenames from the network
- Implement a robust backup and recovery procedure
- Require a password for the FileMaker Server Admin console
- Remember that users who have FileMaker Server Admin Console access can make local copies of databases
- Physically secure your server and backup media
- Use a Server OS firewall to allow access only to authorized users
- If using the External SQL Sources (ESS) feature to connect to the MIT Data Warehouse, do not store warehouse usernames or passwords, or share warehouse passwords
- If connecting to the Data Warehouse, do not import warehouse data into local FileMaker tables unless you have good reason to
- Use encrypted connections when connecting to external systems like the Data Warehouse

See also:

FileMaker Security

For help with security of FileMaker databases, contact IS&T filemaker-support.