





compliance with GDPR:

Limit Full Access accounts and turn off auto-login – by default, a new FileMaker file will have a single full access account with the login ‘Admin’ and no password. This password should be changed as soon as a solution goes into production use with real data. Auto-login can be turned off under File > File Options. FileMaker 16 server by default will not allow you to host and open a file which contains a full access login with no password set.

Use Custom privilege sets – it is prudent to always create custom security privilege sets, rather than relying on the default ‘Data Entry Only’ settings for standard users. As a minimum, you may want to turn off the ability of regular users to routinely print or export data. FileMaker offers full granularity to specify in its security model, which fields and layouts can be accessed by a user and whether new records can be created, modified or deleted in a table. You can also choose a minimum password length and enforce having to change it every X days.


Check Extended privileges – The X in the ‘fmreauthenticateX’ extended privilege controls how many minutes that FileMaker can be left in sleep/background before it requires a user to re-authenticate. 



Make use of Active Directory/OAuth for managing security. Delegating authentication to Active Directory or OAuth provides two obvious benefits: the password can be used across multiple files and centrally managed with strict rules on password length and complexity. As AD is normally managed centrally, there should be a standardised process for leavers to be removed and so it is less likely that accounts will be left active for longer than they should be available.

Limit File Access. By default, one FileMaker file can be linked and referenced within another regardless of the privilege set access level that the user has to the file. This can be

Best Practices I use for development in compliance with GDPR:

restricted to only allow users with full access privileges for 


SSL Encryption in flight. FileMaker Server 16 is now much more explicit when there isn't a properly configured and valid SSL certificate from a supported provider in place. This is essential if you are accessing via a WAN connection.

AES 256 Encryption at rest. It is possible to encrypt FileMaker database files using FileMaker Advanced 16 – this ensures that even if your network and server are compromised, it will be practically impossible to access the data without also having a copy of the encryption key to decrypt the file. We now recommend doing this as standard for any system which includes personal data.

Use secure storage to encrypt container fields. Documents that you have uploaded to container fields can be stored in an encrypted format in an external folder alongside your database files. This is especially prudent if these documents contain personal or sensitive information (i.e. scans of passports for proof of identity, etc).

Encrypt data within fields. In the past, 3rd party plugins were required to encrypt and decrypt field level data within FileMaker. Now with FileMaker 16 there are native functions such as CryptEncrypt/CryptDecrypt. For highly sensitive personal data such as medical information or credit card data there is a good argument for doing this as standard.