THE SUPPORT GROUP

FileMaker Security Best Practices

Create separate user accounts

- Each of your FileMaker users should have their own individual accounts.

Manage user privileges appropriately

- Each user's access should be consistent with their roles and responsibilities within the database.

Specify password standards

- User passwords should be strong and automatically reset on a regular basis.

Assign passwords to default accounts

- Since FileMaker creates unprotected default accounts when a new file is created, you have to be sure to assign a password to each default account.

Control file access

- Use FileMaker's manage security dialog to help you efficiently manage file access across multi-file systems.

Automate the audit process

- Auto enter fields can be used to easily document user log in, record creation and record modification events within a file.

Encrypt sensitive information

- FileMaker offers built-in encryption functions so be sure to take advantage of as many of the features as necessary.

Secure your data in flight

- An SSL certificate for FileMaker Server will secure your data as it's transferred between the server and client.

Schedule regular database backups

- It's important to establish regular partial and full backups of your database with both local and remote storage.

Boston • Los Angeles • New York • San Francisco
www.supportgroup.com