FileMaker Platform Version 15

New Security Features

By:
Steven H. Blackwell

Platinum Member Emeritus
FileMaker Business Alliance

May 10th 2016

VERSION 15 OF THE FILEMAKER PLATFORM BRINGS NEW SECURITY FEATURES

The release today of Version 15 of the FileMaker Platform brings with it a number of new security features, both in FileMaker® Server 15 and in FileMaker® Pro 15. FileMaker® Pro 15 Advanced also has one notable security enhancement.

This White Paper will detail and explain a number of these new features as well as offer some recommendations for their effective use. First however, we should take note that in the past several releases that FileMaker, Inc. has become more conscious about security issues and about equipping all the products with more features to enhance the ***Confidentiality, Integrity, Availability,*** and ***Resilience*** (CIAR) of FileMaker Platform solutions and their deployments. This is a highly welcomed development.

◆**FileMaker Server** is at the center of effective FileMaker Platform deployments. Its significance and importance continue to grow. FileMaker Server 15 has a new feature, *enabled by default*, that imposes restrictions on hosting files based on their security configuration.

Basically speaking there are several scenarios in a file that make the file insecure and vulnerable to a variety of attacks. Some of these can cause real damage to the server and to other hosted files. I described this a couple of years ago in a FileMaker Security BLOG posting (http://fmforums.com/blogs/entry/777-protect-your-filemaker-server-and-files-from-a-vulnerability/).

Here are the scenarios:

- Guest Account enabled and attached to the [Full Access] Privilege Set
- A [Full Access] Account with no password
- A [Full Access] Account with the password stored using the File Options "Log In Using" feature.

By default, FileMaker Server 15 **will not open** such files for hosting. Administrators can authorize the hosting of such files by unchecking an option in the Server Admin Console. **I strongly recommend that they not do so.** Figure 1 shows this option.

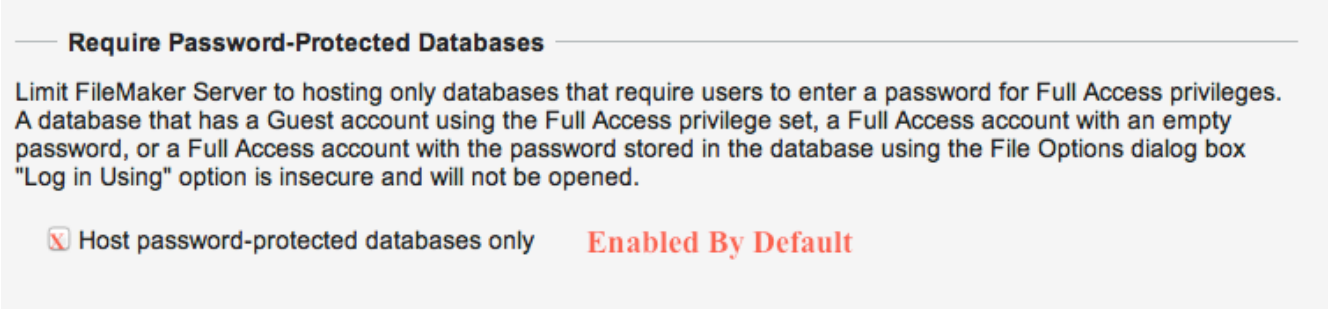


Figure 1. *Hosting Protected Databases Only*

◆**External Application Programming Interfaces** (API's) form an important and significant part of the FileMaker Platform experience. However, many developers are not aware that such API's can serve as attack vectors to cause unexpected and unwanted actions in FileMaker Platform files. Some of these actions can be controlled by settings of bits in the Privilege Sets. The difficulty, however, is that when a user is otherwise authorized to take some actions, either purposefully or inadvertently, these API's can wreak havoc and compromise processes in the files. We saw examples of that in the Two-Factor Authentication discussion several months ago, recounted by Josh Ormond in his BLOG (http://fmforums.com/blogs/entry/1512-a-conversation-about-2-factor-authentication/).

Beginning with Version 15 FileMaker, Inc. has given developers a new method to control the ability of two API's, namely *AppleEvents* and *ActiveX*, to trigger scripts in FileMaker Pro solutions, both stand-alone and hosted. These restrictions *must be specifically enabled* on a Privilege Set by Privilege Set basis. Developers accomplish this in the Extended Privileges section of the file, as shown in Figure 2.

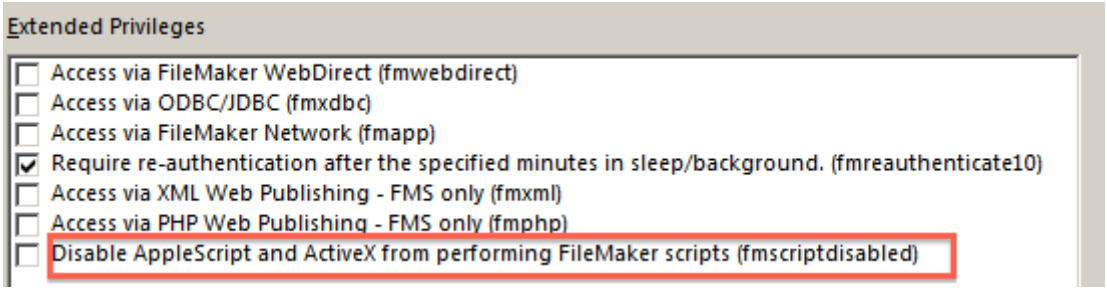


Figure 2. *Toggle the fmscriptdisabled privilege bit.*

Here are some important caveats regarding the use of this new functionality that developers should remember:

- This is a ***version 15 feature only.*** Accessing a file with an earlier version does not afford this protection.
- Developers must *specifically enable* this restriction. I would have preferred for it to have been enabled by default; however, it is a very considerable improvement and enhancement that developers can use.
- It applies only to *scripts* in the file *where it is defined*. It is possible to invoke a script using ActiveX or AppleEvents in another FileMaker Pro file that might impact scripts in the protected file. So always test presumptions here.
- It pertains only to AppleEvents (Macintosh OS) and to ActiveX (Windows OS); it does not control activation of scripts by other API's. *Additionally it does not manage any actions other than scripts that either AppleEvents or ActiveX might call in a particular file.*

◆**FileMaker® Pro 14 introduced the ability to block users from storing credentials in either the KeyChain (Macintosh OS) or the Credentials Manager (Windows OS).** In my view, generally developers should always invoke this option. They do this by leaving the option to store credentials ***unchecked.*** In some instances however, for iOS mobile devices, developers may choose to authorize KeyChain storage. The ubiquity and small form-factor associated with iOS devices seems however to increase the likelihood of their loss or theft. This provides an avenue of unauthorized access to databases, particularly hosted ones, when the device falls into unauthorized hands.

FileMaker Pro 15 adds a new feature to assist in protecting these files when KeyChain or Credentials Manager storage is *authorized* and *enabled.* Developers can require in such instances that users perform an additional validation of their identity assertion by use of the device's *Passcode* or of *TouchID* if that is enabled. This is another reason for having strong passcodes. Developers invoke this new feature in the File Options area as shown in Figure 3. *Note that the storage must first be authorized before the developer can require Passcode use.* ***Also, all elements should be version 15 for this to work correctly. Earlier versions will not work correctly for this feature.***

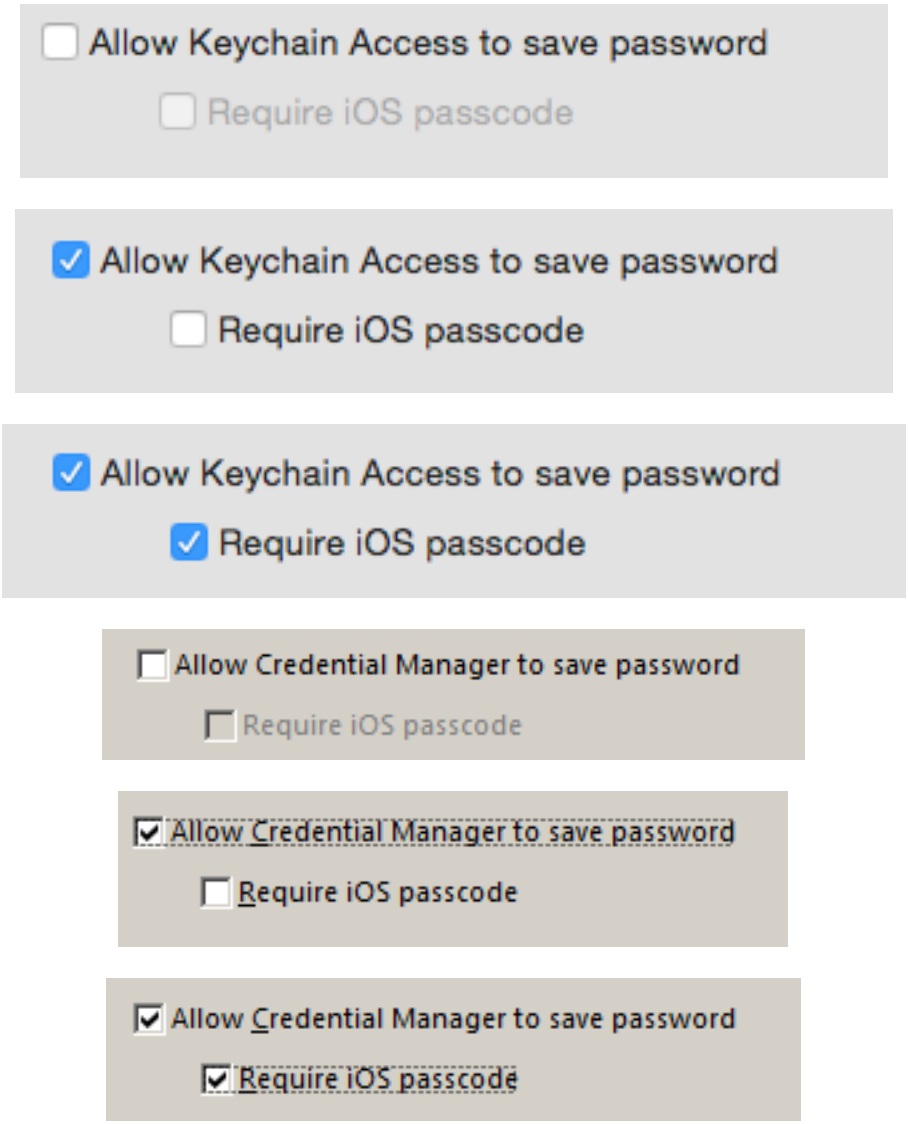


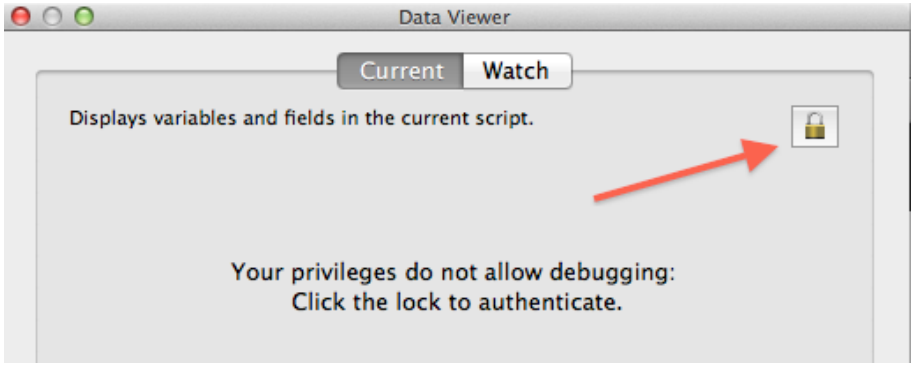
Figure 3. *Require Passcode.*

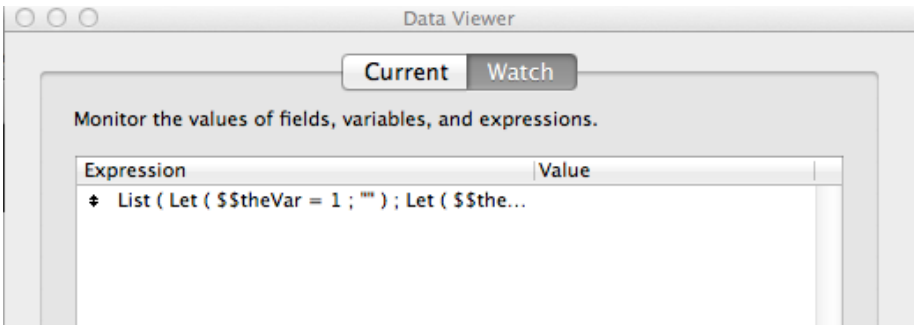
◆**Single SignOn and Credentials Storage.** As noted above, in FileMaker Pro 14, developers could block storage of credentials in the KeyChain or in the Credentials Manager. On the Windows OS, this caused an unexpected issue with Single SignOn when using External Server Authentication with Active Directory. The problem was that Single SignOn failed unless the option to store the credential was enabled. This was an error; it should not have been this way. *In FileMaker Pro 15, this problem has been corrected*. *The credentials*

*toggle does **not** have to be enabled for Single SignOn to work correctly.*

In essence, Single SignOn works correctly with FileMaker® Pro 12 and FileMaker® Pro 13 clients accessing files hosted on FileMaker Server 14. However, Single SignOn ***fails*** in similar circumstances in FileMaker Pro 14 unless developers enabled storage of the credentials. Users do not actually have to store the credentials, but the toggle had to be on for Single SignOn to work.

◆**FileMaker Pro Advanced has a feature called the *Data Viewer*** that is useful for any number of tasks. The Viewer has two different tabs: *Current* and *Watch*. Access to the *Current* tab requires [Full Access] credentials either to have opened the file or to be entered by clicking a lock icon in the *Current* tab window. However, in earlier versions, subordinate level Accounts could open and use the processes in the *Watch* Tab. While there were restrictions a Privilege Set could impose on the breadth of the actions a user with a subordinate Account could undertake, there nevertheless was a vulnerability here. So, in FileMaker Pro 15 Advanced, access to the Watch tab will also require [Full Access] authentication. Figure 4 describes these scenarios.





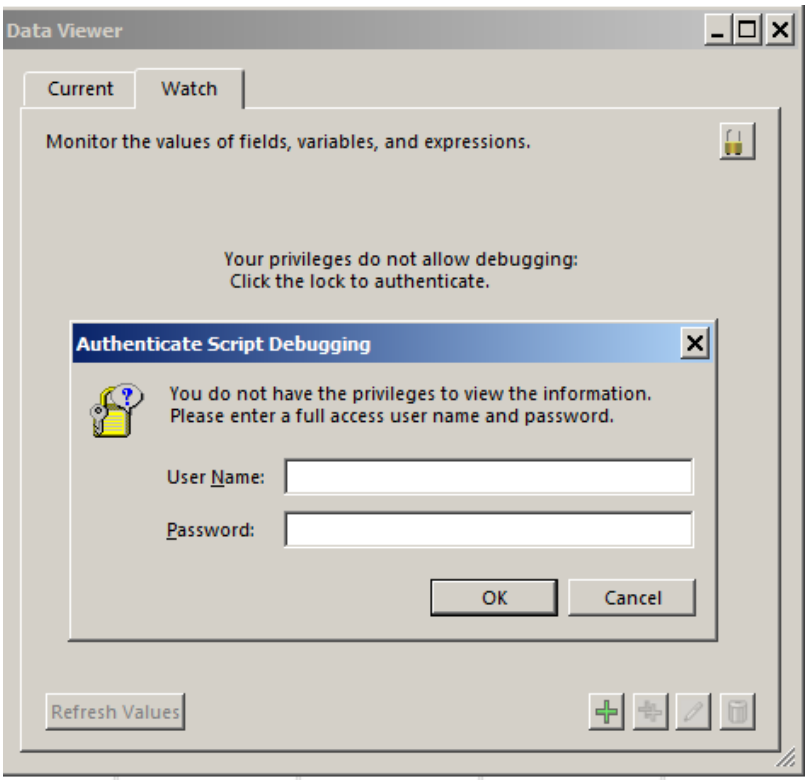


Figure 4. *Data Viewer Tabs. The Watch Tab now requires [Full Access].*

◆**A secure connection** between FileMaker file hosts and FileMaker Platform clients is an important aspect of FileMaker Platform security. Such connections protect data in transit across a variety of networks, particularly public wireless networks such as those found in coffee shops, airports, shopping malls, public parks, *etc*. Additionally, properly verified connections validate that when a user connects to a server that the ***server actually is the device it claims to be.*** This helps to prevent what are called *man-in-the-middle* attacks, where one server impersonates another one.

In Version 15 of the FileMaker Platform, the application displays warnings at various places where insecure connections exist. These are in addition to the familiar lock icons introduced in earlier versions. First, as shown in Figure 5a, *all peer-to-peer connections are insecure by their very nature.*

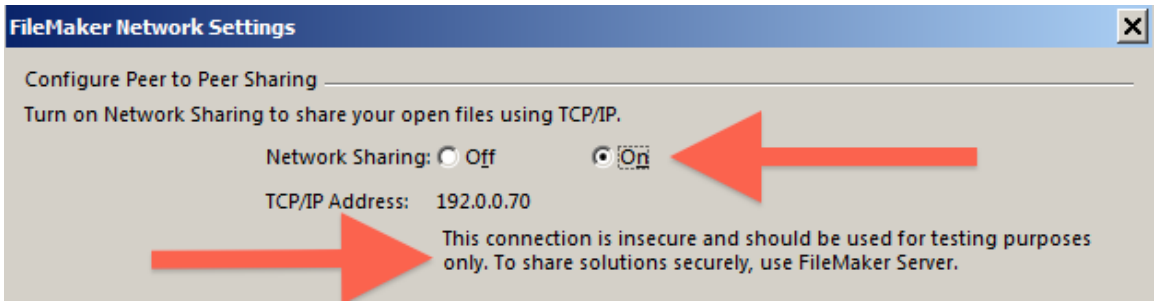


Figure 5a. *Peer-to-peer connections are not secure.*

When a user attempts to employ FileMaker Pro 15 to access a solution hosted by FileMaker Server where the validity of the SSL certificate is in question, FileMaker Pro will display a warning dialog similar to the one shown in Figure 5b. The user can then make decisions about connecting to the file.

Figure 5b. *FileMaker Pro cannot verify SSL certificate.*

◆Finally, with the introduction of FileMaker Server 15, there will be a number of new features related to SSL Certificate management. There is a new capability to create Certificate Signing Requests to send to various Certificate Authorities. Figure 6 shows this new feature.

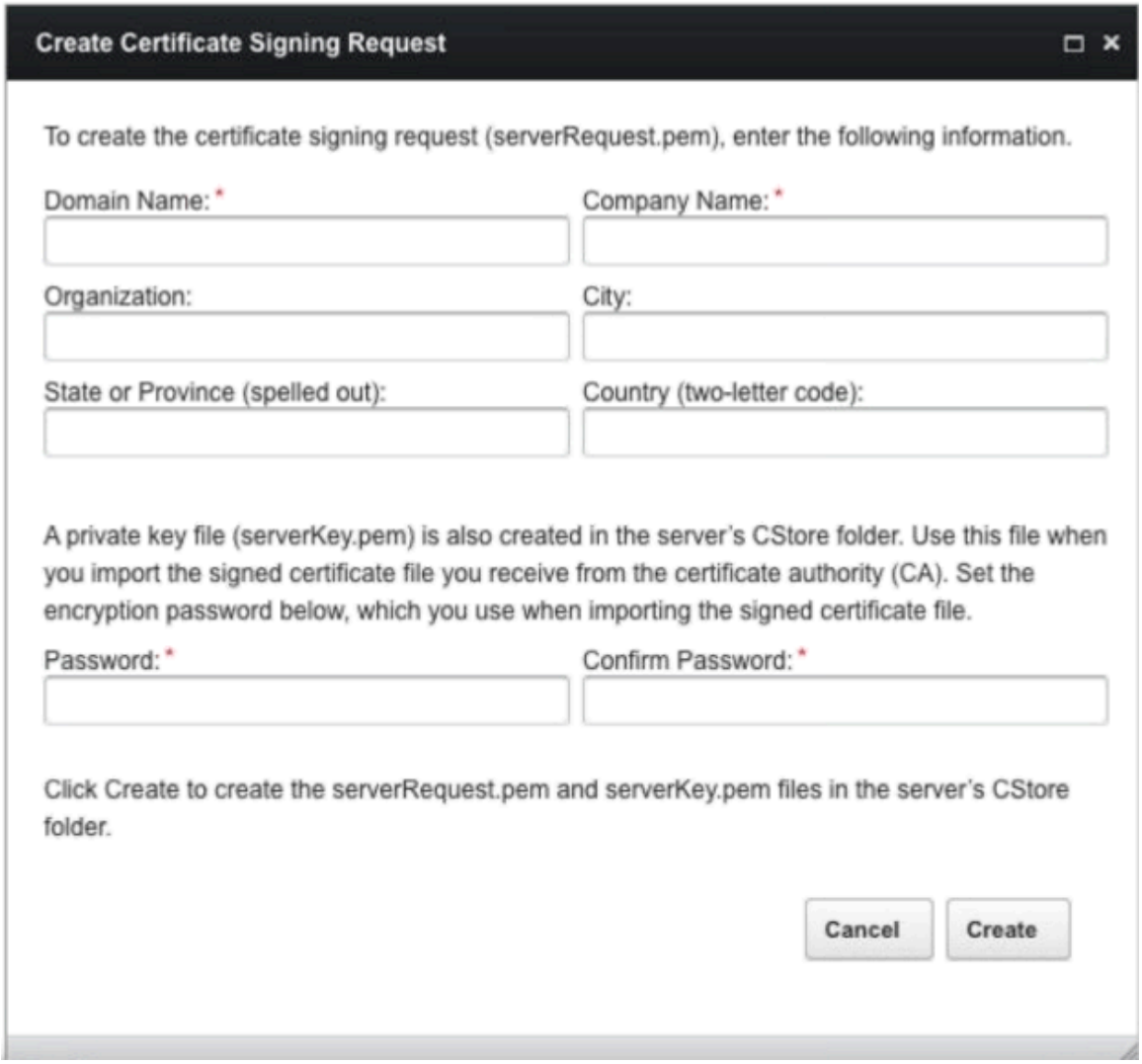


Figure 6. *Certificate Signing Request UI.*

Additionally, FileMaker Server 15 will have support for other elements related to SSL certificates:

- Import Intermediate Certificates
- Wildcard Certificates
- SubjectAlternateName (SAN) Certificates
- New Certificate Vendors
    - DigiCert
    - InCommon

As the security features in the various FileMaker Platform products continue to evolve, I will continue to report on them, including on the FileMaker Security BLOG (http://fmforums.com/blogs/blog/13-filemaker-security-blog/).

♦ACKNOWLEDGEMENTS♦

I would like to acknowledge the assistance of three of my FileMaker Platform colleagues who read and commented on this White Paper before its release. Many thanks to **Barbara R. Levine, Maida Sussman,** and **Wim Decorte** for their help in making this a better paper.