FileMaker Server SSL Certificates

FileMaker Server SSL Certificates

> ⚠ **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.

Note: The information on this page is accurate for FileMaker Server 17. Certain settings and features may differ for prior versions.

Overview

SSL allows for the encryption of data passed between FileMaker Server and FileMaker clients, as well as the web browser-based FileMaker Server Admin Console. A critical component of this function is the SSL certificate residing on the server. The FileMaker Server application ships with a self-signed SSL certificate that does not verify the server name. This default certificate is intended only for test purposes, and a custom SSL certificate is required for production use.

Instructions for Enabling SSL and Installing a Custom SSL Certificate

Instructions for configuring FileMaker Server to use SSL and requesting and installing a custom SSL certificate are provided here with the caveat that this process is best done by someone with server administration experience.

Some notes before we begin:

- If you are using IS&T's managed hosting service, you do not need to worry about this process; it is all handled for you.
- The following assumes that your server machine has already been set up with FileMaker Server installed and configured. Refer to Installing and Configuring FileMaker Server for more information on that process.
- These instructions are for Windows servers only; the various file paths and FileMaker CLI commands will differ for Macintosh servers.

Configuring FileMaker Server for SSL

1. In the FileMaker Server Admin Console > Configuration>General Settings > Server Information, the Server Name should be entered with the fully qualified domain name (FQDN), i.e. <your hostname>.mit.edu.

Request and Instal a Custom SSL Certificate

With FileMaker Server 17, the process for requesting a certificate must be done through the command line interface. Importing a certificate can still be managed through the Admin Console. Instructions below will lead you through all the steps of making the request as well as importing the requested certificate.

Request an SSL Certificate for FileMaker Server 17 Using the Command Line Interface

1. While logged into your server, open a command prompt as an administrator and run the following command to run the command from within FileMaker Server.

```
cd “C:\Program Files\FileMaker\FileMaker Server\Database Server”
```

2. Run the following command, using your own values for the <fqdn> and <secret>:

```
fmsadmin certificate create <fqdn> --keyfilepass <secret>
```

EXAMPLES:

```
fmsadmin certificate create dcdd.mit.edu --keyfilepass mYsuPerSecretPassphrase
or
fmsadmin certificate create
"/C=US/ST=MA/L=Cambridge/O=MassachusettsInstituteofTechnology/CN=dcdd-fmp.mit.edu" --keyfilepass
mYsuPerSecretPassphrase
```

3. Two files, serverKey.pem and serverRequest.pem, will have been generated by the above command in the following folder: C:\Program Files\FileMaker\FileMaker Server\CStore\.
4. Send an email to mitcert@mit.edu with serverRequest.pem file attached. Explicitly request a Comodo Elite SSL certificate for use with your FileMaker Server machine and include the hostname.
5. The custom certificate will be returned via email, generally within a day or two. The email will contain links to multiple formats of your new certificate. Download the signed certificate file labeled "X509 Certificate only, Base64 encoded," and the intermediate certificate file labeled "X509 Intermediates/root only, Base64 encoded." The resulting certificate files will be named <your FQDN>_cert.cer and <your FQDN>_interm.cer, respectively, with dots in the FQDN replaced with underscores. Copy the files to the FileMaker Server\CStore directory (path noted above).

Import and Bind the Certificates Using FileMaker 17 Server Console

1. Log into the FileMaker Server Console>>Configuration>>SSL Certificate
2. Select the Import Custom Certificate button and provide the requested files and your secret password as prompted and shown here before performing the Import with the Import button.

> Signed Certificate File: yourDomainName.crt provided by the CA.
>
> Private Key File: serverKey.pem located in /FileMaker Server/CStore/.
>
> Private Key Password: <secret> specified during CSR creation.

3. After you complete the import, you will need to close all files and stop and restart FileMaker Database Server. Go to Databases and select option to close all databases. Go to Configuration>>General Settings and choose the option to Stop Database Server.
4. To stop and restart the FileMaker service, open the Windows Services Manager (via Control Panel > Administrative Tools > View local services) and restart the FileMaker Server service.
5. Return to the FileMaker Server Admin Console (note that you will need to log back in after restarting the FileMaker Server service). In the Database Server pane > Security tab, under SSL Connections, the Information note should now read "The custom SSL certificate installed on this server originated from a certificate authority supported by FileMaker." This confirms that the certificate has been properly installed and that SSL is ready for production use.
6. Make a backup of the serverRequest.pem and serverKey.pem files located in the FileMaker Server\CStore directory, along with the two certificate files and documentation of your encryption key password, and place these in a separate location on the server outside of the FileMaker Server directory. Should you need to reinstall FileMaker Server for any reason, you can install the existing certificate; see Installing an Existing Certificate below for more information.

If You Already Have an Existing Certificate

If you have a server with an existing custom SSL certificate and need to re-install FileMaker Server for any reason, such as when migrating to a new version of FileMaker Server or migrating to a new server machine, you can bypass the certificate request process as follows:

1. If you haven't already (as described above), make a backup of the serverRequest.pem and serverKey.pem files located in the FileMaker Server\CStore directory, along with the two certificate files, and have your encryption key password handy.
2. Perform the FileMaker Server migration, whether it be uninstalling and reinstalling FileMaker Server on the same machine or installing FileMaker Server on a new machine.
3. Copy the original serverRequest.pem and serverKey.pem files to the FileMaker Server\CStore directory.
4. Proceed with the instructions above, starting at the Import Certificate step.

Note: SSL certificates requested for FileMaker Server 14 cannot be re-used for v15 and up. If you are upgrading from FileMaker Server 14, you will need to request a new certificate rather than use your existing one. Follow the above steps for requesting and importing certificates.

Other Resources

The list of SSL certificates that are supported by FileMaker Server is available here. Note that MIT's certificate provider is InCommon, and InCommon provides the Comodo Elite SSL certificate which is supported by FileMaker.

Refer to FileMaker Server Help for more detail on requesting and installing SSL certificates for use with FileMaker Server.

For an overview on FileMaker network security and SSL, refer to http://help.filemaker.com/app/answers/detail/a_id/14176/.