Configuring an SSL Certificate

Last Modified on 10/03/2022 11:27 am EDT

We recommend having your **IT specialist** work through this section to ensure that these critically important steps are completed properly. You may also reference FileMaker's resources on SSL server security:

- FileMaker Server 17 and SSL Certificates: Configuration and Use (https://support.claris.com/servlet/fileField?entityId=ka10H000000bwfr&field=Public_File_1__Body__s)
- Configuring Security for FileMaker 17 and Later (https://support.claris.com/s/article/Configuring-Security-for-FileMaker-17?language=en_US)

aACEsoft requires that you have an SSL certificate purchased and installed onto your copy of FileMaker Server for the purpose of improved security surrounding your system's data. A valid SSL certificate is also required in order to access your hosted aACE system via a convenient “launcher” file.

The FileMaker article on SSL certificate configuration and use (linked above) describes some of the security benefits of using an SSL certificate:

> "SSL protects data in transit across the network by encrypting it. Software known as Packet Sniffers can capture and display all network data. If those data are not encrypted, then whoever uses a packet sniffer can read the unencrypted data, revealing confidential, proprietary information.

> "In addition to protecting the data in transit, SSL also protects and verifies the identity of the FileMaker Server. That is, it confirms that the server is who the server asserts that it is much in the way that the password in the credentials dialog helps validate the identity assertion provided by the FileMaker Pro Advanced Account Name. This helps thwart the man-in-the-middle attacks. In such an exploit, the attacker (sometimes called a Threat Agent) intercepts, relays and sometimes alters communication between two parties who believe they are in direct communication with one another. The man-in-the middle can then inspect and read that intercepted data. The certificate issued to the server helps to validate its identity and to thwart man-in-the-middle attacks. That is one of the reasons for using a fully verified certificate issued by an accepted Certificate Authority."

Enabling Remote Access to Your aACE System

We require that you enable remote access to your hosted aACE system (http://aace5.knowledgeowl.com/help/enabling-remote-access-to-your-aace-system-fms19) before you proceed with configuring your SSL certificate.

Preparing SSL Files

If you do not already have an SSL certificate that was in use by FMS 18, you must create a certificate signing request using your command line interface. Please use the following example command as a template:

```
fmsadmin certificate create "/CN=Server Domain Name/O=Organization/C=Two-Character Country Abbreviation/ST=Two-Character State Abbreviation/L=City" --keyfilepass password
```

In this template command, each bolded item should be replaced by the value relevant to your server or organization. Important details include:

- **Server Domain Name** — This is the fully-qualified domain name directed at your server's *external* IP address. You will enter this URL into FileMaker Client in order to find the files hosted on your server.
  Note: This should *not* be your server's internal domain name that ends in ".local". That will only point to your hosted system from within your server's network.
- **Password** — This can be any password of your choosing. Make sure it is carefully documented, as you will need to use it later to install your new SSL certificate.

Manually type your customized command in your Terminal / Command Prompt — do *not* copy-paste this command because that frequently results in errors.

When you run your customized command, the system will generate a certificate signing request file (i.e. "serverRequest.pem" file) inside the FileMaker Server/CStore folder. (Note: If you need to create a *new* certificate signing request, you must first navigate to the FileMaker Server/CStore folder and remove the existing serverRequest.pem and the serverKey.pem files, then re-run the customized command.)

Provide a copy of the serverRequest.pem file to your preferred certificate authority (e.g. GoDaddy, NameCheap, Comodo, etc). They will prepare your certificate files and send them to you. Note: Some certificate authorities will not allow you to configure the SSL certificate using a certificate signing request or to download CRT files for the certificate (e.g. SquareSpace, etc). If you currently use these providers, you may need to purchase an SSL certificate through a different certificate authority.

Importing SSL Files

After you have the necessary SSL certificate files:

1. In the Admin Console, navigate to **Configuration** > **SSL Certificate**.

2. Click **Import Custom Certificate**, then browse to the correct files:
    - Signed Certificate File: This is usually a .crt file, and is the main certificate file provided by your certificate authority.
    - Private Key File: This file is created by FileMaker Server, typically named “serverKey.pem”. It is kept in the FileMaker Server/CStore folder.
    - Intermediate Certificate File: This is usually a .crt file or a .ca-bundle file, and will typically include the word “bundle” in the file name.
    - Password: Enter the password you created for the SSL certificate.
3. Click **Import**.
   Critical Note: You *must* hold onto the SSL certificate files and securely record the SSL password on the server. Do **not** delete these files and do **not** allow the password to be forgotten. These files must be re-imported the next time you upgrade FileMaker Server or transfer your aACE system to a new server.
4. The system prompts you to stop and restart FileMaker Server for the change to take effect:
    - Coordinate

SSL Certificates and System Performance

Your SSL certificate encrypts and decrypts data during transfers across the network, which may result in a slight performance reduction, although the impact is rarely enough to be noticed during typical use.