Configuring an SSL Certificate (FMS 17)

Last Modified on 07/25/2019 1:07 pm EDT

Note: 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 help guide on improving server security via SSL for additional information on the subject.

We require 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 allow access to your hosted aACE system via a convenient, easy-to-use “launcher” file.

Confirming Network Configuration

Before configuring your SSL certificate, please take a moment to confirm that your server's network configuration includes:

- A static external IP address
- A fully-qualified domain name directed at your server's IP address (for example, "aace.mydomain.com")

Also confirm that your server’s network / firewall has the following ports open to / forwarded from all incoming traffic:

- TCP 80
- TCP 443
- TCP 5003

Preparing SSL Files

If you do not already have an SSL certificate that was in use by FMS 16, you must create a certificate signing request using your command line interface. Please use the following example command as a template. Each of the bold items represents a value relating to your server or organization.

```
fmsadmin certificate create "/CN=Server Domain Name/O=Organization/C=2-Chara
cter Country Abbreviation/ST=2-Character State Abbreviation/L=City" --keyfil
epass password
```

Please note the following details about these variable values:

- **Server Domain Name**: This is the fully-qualified domain name directed at your server's **external** IP address. This will be the URL that you will enter 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", as 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.

In your Terminal / Command Prompt, *manually type* your customized command — copy-pasting the command often results in errors.

When you run the customized command, the system will generate a "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 .PEM file to your preferred certificate authority (e.g. GoDaddy, NameCheap, Comodo, etc). They will prepare and send your certificate files.

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**.
4. The system prompts you to stop and restart FileMaker Server for the change to take effect:
    - Navigate to Configuration > General Settings > Server Information section, then click the Stop Database Server link.
    - Restart FileMaker Server at the Admin Console login screen by clicking the Start Database Server button.
