# Preparing the Server (FMS 17)

Last Modified on 10/27/2020 4:19 pm EDT

Use the following guidelines to ensure you are ready for installing FMS 17.

## Server Specifications

### Dedicated Server

Do **not** use the machine for any other purpose (e.g. email server, remote access, etc). Your aACE server should be used for the *sole purpose* of hosting aACE and not for any other service that could be hosted on another computer.

Note: If your aACE server was not previously configured in accordance with these instructions (e.g. the server hosted any FileMaker system other than aACE, offsite backups were installed but not configured properly, additional user accounts existed, etc.), we require that *prior* to installing FMS 17 you restore the machine back to its factory default state by performing a factory reset.

### Multiple Accounts

Do **not** create multiple user accounts on your server; only install FMS/aACE on a machine with a single administrator account. If there are security or other concerns, virtualization software such as VMware can be used, so long as that computer instance only has FMS running with a single user account.

Note: FMS manages its own communication with the respective clients (i.e. FileMaker Pro, FileMaker Go, and FileMaker WebDirect) and does not utilize any Microsoft or Apple server technologies (e.g. file sharing, network drives, user accounts, etc). As such, turning on any of these services can significantly slow your server.

### Technical Specifications

Your server must meet the technical specifications for FMS 17, available on the FileMaker web site (https://support.claris.com/s/answerview?language=en_US&anum=000026030).

### Backup Requirements for Self-Hosted Systems

If your system is self-hosted, we require *at minimum* either an offsite backup solution or else a dedicated, physical hard drive mechanism for backups (e.g. RAIDs or USB drive, internal or external).

Note: If your system is hosted in a cloud (e.g. Amazon Web Services, Google Cloud Platform, Microsoft Azure, etc), we do not require dedicated backup drives; these data centers include built-in redundancy.

### Mac Mini and Mac Pro Servers

If your aACE server is a Mac Mini or a Mac Pro which is *not* hooked up to a display (i.e. “headless"), remote access applications such as LogMeIn are likely to have issues displaying the user interface. As a preventative measure, we recommend the use of an HDMI dummy plug (https://www.amazon.com/Headless-Display-Emulator-Headless-1920x1080-generation/dp/B06XT1Z9TF/ref=pd_bxgy_147_img_2/142-6839987-1156967). Simply plugging one into your server’s HDMI slot will prevent any problems with displaying the user interface.

Note: If your aACE server is not a Mac Mini or Mac Pro or is not headless, then the HDMI dummy plug is not required.

### Google Cloud Virtual Machines

If your aACE server is a virtual machine hosted on the Google Cloud Platform (GCP), you must complete an additional step before screen-sharing applications such as LogMeIn or GoToAssist will function properly:

1. From the GCP portal, navigate to **Compute Engine** > **VM Instances**, then click on your aACE server virtual machine and click **Edit**.
2. Under the 'Display device' section, mark the flag **Turn on display device**.
   Note: This can be done either by shutting down the instance and editing the settings, or while you are creating the new virtual machine.
3. Turn on your virtual machine, then access the virtual machine using Microsoft Remote Desktop.
4. On the machine, locate the Windows PowerShell application, right-click it, and select **Run as Administrator**.
5. Enter the following command:

   ```
   googet install google-compute-engine-driver-gga
   ```

7. At the prompt, agree to install the driver and all dependencies.
8. To ensure the change takes effect, restart the virtual machine.

## Default Server Settings

All automatic 'check for updates' features *must be disabled*. You can find specific instructions

on this step here (http://aace5.knowledgeowl.com/help/disabling-automatic-software-updates).

In addition, your aACE server must *not* be allowed to enable its screensaver or sleep mode automatically:

- Mac
  - Navigate to System Preferences > Energy Saver, then set both **Computer sleep** and **Display sleep** to "Never".
  - Navigate to System Preferences > Desktop & Screen Saver > Screen Saver, then set **Start after** to "Never".
- PC
  - Navigate to Control Panel > Hardware > Power Options > Edit Plan Settings, then set **Turn off the display** and **Put the computer to sleep** to "Never".

**Default Browser**

- Mac
  - You may leave your default browser set to Safari or download an alternative (i.e. FireFox or Chrome).
- PC
  - Mozilla FireFox (https://www.mozilla.org/en-US/firefox/new/) *must* be installed and set as the server's default browser before proceeding.

**Windows Defender Firewall**

- PC
  - Navigate to Control Panel > System and Security > Windows Defender Firewall, then click the **Turn Windows Defender Firewall on or off** button. Check the radio buttons **turn off** Windows Defender Firewall for both **Private network settings** and **Public network settings**.

## Network Configuration

Note: We recommend having your **IT specialist** work through this section to ensure that these critically important steps are completed properly.

Your server's network must be configured to include the following:

- A static external IP address
- A fully-qualified domain name (Recommended: aace.mydomain.com) directed at your server's IP address
  - Using the same service you used to purchase your domain name, you will need to

create an "A" DNS record in order for the "aace" subdomain to forward traffic to your server's external IP address.

- A valid SSL certificate purchased through your preferred certificate authority (such as GoDaddy, NameCheap, Comodo, etc.).
    - At a later step in the process, this SSL certificate will be configured (or keyed) for your server's fully-qualified domain name, then it will be installed onto your server. Please make sure you are either familiar with the keying process using your preferred certificate authority or have access to that certificate authority's documentation on the subject.

Your server's network / firewall must have the following ports open to / forwarded from all incoming traffic:

- TCP 80
- TCP 443
- TCP 5003

Note: FileMaker uses a proprietary network protocol and communicates on these ports: 5003, 80 (HTTP - important for download of container data), and 443 (HTTPS - important for upload of container data). Additional port requirements (https://fmhelp.filemaker.com/docs/17/en/fmsinstall/#before) can be found on the FileMaker Support web site.

## Installers, Licenses, and Credentials

Obtain the following elements prior to the server setup:

- The login credentials to the server's single user account
  Note: You will need to enter this name and password several times throughout the process.
- A valid SSL certificate for your server's fully-qualified domain name (e.g. aace.mydomain.com)
  Note: If you have purchased an SSL certificate, but have not yet associated it with your fully-qualified domain name, you will be guided on creating a certificate signing request during a later step.
- A valid FileMaker 'LicenseCert.fmcert' file
  Note: This contains the key for your FileMaker Server 17 license. Note: If you are familiar with the installation process for FMS 16 or earlier, note that the FMS 17 installation process looks to this file instead of prompting you to enter your license key.
- Valid FileMaker Pro licenses for all users
- A basic understanding of the FileMaker Server Command Line Interface (CLI).

Note: See FileMaker's help guide on Using the CLI (https://fmhelp.filemaker.com/help/16/fms/en/index.html#page/fms/command_line.html). Most commands required during the server setup will prompt you to enter the Admin Console's username and password. When you obtain these credentials in Step 2, be sure to store them for use later.

- Remote access with LogMeIn
  Note: In the server's browser, download the aACEsoft LogMeIn installer (http://logmein.aacesoft.com). Once you have installed LogMeIn on your server, have aACE Software or your FileMaker developer confirm remote access to the server.
- Remote access to your server with a secondary method
  Note: In addition to LogMeIn, we recommend either of these tools:
  - Microsoft Remote Desktop (https://support.microsoft.com/en-us/help/17463/windows-7-connect-to-another-computer-remote-desktop-connection)
  - GoToAssist — The installer can be provided by aACE Software or your FileMaker developer.
- FileMaker software installers (http://www.filemaker.com/support/downloads/), including:
  - FileMaker Server 17
  - FileMaker Pro 17 Advanced
  - FileMaker Pro 16 Advanced (if needed)
- Your aACE system, including:
  - A ZIP archive containing your aACE files
  - The "management" password to your copy of aACE