Claris

Claris FileMaker Server 19 Deployment Guide for Linux

Introduction

About FileMaker Server

Claris™ FileMaker Server™ is a dedicated database server that hosts databases created using Claris FileMaker Pro™ so that data can be shared and modified by FileMaker Pro, Claris FileMaker Go®, and Claris FileMaker® Data API Engine.

FileMaker Server 19 in Linux is available only as an electronic download. It includes product software and a link to an electronic license certificate that contains a license key needed for installation.

For information about installing on Windows and macOS, see FileMaker Server Installation and Configuration Guide.

FileMaker Server for Linux requirements

FileMaker Server for Linux has the following requirements:

- Supported Linux distribution: CentOS version 7.7
- The following Linux packages:
  - wget: Retrieves the FileMaker Server for Linux installer from the web
  - unzip: Unzips the FileMaker Server for Linux software package

  For more information, see Installing FileMaker Server.

Before you install, confirm that your machine meets the minimum requirements. See the FileMaker Server system requirements.

Requirements for Admin Console

FileMaker Server Admin Console is a web-based application that lets you configure and administer FileMaker Server. You can use Admin Console on machines that have network access to FileMaker Server and a supported web browser.

Supported client applications

FileMaker Server supports the following client applications:

- FileMaker Pro Advanced 18 and FileMaker Pro 19
- FileMaker Go 18 and 19
- ODBC (Open Database Connectivity) and JDBC (Java Database Connectivity) client applications using the FileMaker client drivers. The FileMaker ODBC and JDBC drivers are available on the Downloads and Resources page. See FileMaker ODBC and JDBC Guide and FileMaker Pro Help.
- web users accessing data via the FileMaker Server Web Publishing Engine using FileMaker WebDirect
- web services or applications accessing data through the Claris FileMaker Data API

Make sure users have applied the most recent update of their client software.

For additional information about supported clients and licensing requirements, see the FileMaker Server system requirements.

Notes

- Becuase of to Java licensing changes, FileMaker Server no longer installs a Java Runtime Environment (JRE), needed for using Custom Web Publishing and FileMaker WebDirect. To use web-related services, you must install either OpenJDK or

Oracle JRE. After enabling the Web Publishing Engine on the master machine in Admin Console, follow the onscreen instructions that appear. For details and installation steps, search for "JDK" in the Knowledge Base.

About the license certificate

FileMaker Server uses a license certificate to set the license key. Do not lose this license certificate. Keep a copy of the license certificate in a safe place in case the software needs to be reinstalled.

You received an email message with a link to your software download page. Information about your license certificate is on that page.

The license certificate ensures adherence to the end user license agreement. If the license key is invalid or if too many installations of the software with that same license key are running on the network, the FileMaker Server software displays an error message.

Updating the FileMaker Server license key

You can import a new license certificate for FileMaker Server 19 on the same machine to do the following:

- upgrade from a trial version of FileMaker Server 19
- add support for more FileMaker Go, FileMaker WebDirect, and FileMaker Pro users or connections
- increase the FileMaker Data API annual limit

To change the FileMaker Server license key of an existing deployment:

1. Download the new license certificate from your software download page.
2. Open Admin Console and click the **Administration** > **FileMaker Licenses** tab. See Starting Admin Console.
3. Click **Import License Certificate**.
4. Click **Browse** to choose the new license certificate, and enter your organization name.

Where to go from here

- To install FileMaker Server, see Installing FileMaker Server.
- To move from an existing installation of FileMaker Server to another operating system, see Moving an existing installation.

Installing FileMaker Server

Before you install FileMaker Server

This section includes important information you need before installing FileMaker Server for Linux.

- FileMaker Server requires a web server in all deployments. The web server serves web publishing clients, hosts the web-based Admin Console application, and handles some data transfer tasks. FileMaker Server requires that port 80 is available for web connections and port 443 is available for secure web connections. These ports are used by FileMaker Server even if web publishing is disabled. If the FileMaker Server for Linux installer detects existing websites using these ports, you must disable those websites and make the ports available.

  See Setting up the web server.

- In the server computer's firewall, open the necessary ports so that FileMaker Server can communicate with administrators and clients:
  - The *web connections port*, port 80. This port is used by Admin Console and for web publishing (HTTPS).
  - The *secure web connections port*, port 443. This port is used by Admin Console and for web publishing (HTTPS) if SSL connections are used.
  - Port 5003 for FileMaker clients.

- Port 16000 for server administrators using Admin Console.
- Port 16002 must be open on the master machine, open in the firewall, and available on the worker machines.
- Port 2399 for ODBC and JDBC clients.
- Ports 1895, 3000, 5013, 5015, 8989, 8998, 9889, 9898, 16000, 16003, 16004, 16020, 16021, 50003, and 50004 must be available on the machine, but not open in the firewall.

See Ports used by FileMaker Server.

- To move a FileMaker Server installation to another operating system, see Moving an existing installation.
- Locate your license certificate. See About the license certificate.
- If you are currently running FileMaker Pro on the same machine, quit before installing FileMaker Server. On a FileMaker Server machine, FileMaker Pro is for testing purposes only.
- Server security is important. Review the topic "Securing your data" in FileMaker Server Help and the information in the FileMaker Security Guide.
- If the machine has antivirus software installed, you may need to disable or uninstall it before running the FileMaker Server for Linux installer. Don't enable antivirus software again until after the FileMaker Server for Linux installer has finished.

  Do not allow antivirus software to scan the folders that contain hosted databases or the folders that contain files for container fields that store data externally.
- You cannot run two different versions of FileMaker Server on the same machine at the same time.
- Because some DHCP servers cycle IP addresses, use a static IP address.

Considering performance

For best performance, run FileMaker Server on a dedicated machine reserved for use as a database server. When FileMaker Server is hosting many clients or a large number of databases, it uses a high level of processor, hard disk, and network capacity. Other processor-intensive software or heavy network traffic on the same machine will cause FileMaker Server to run more slowly and degrade the performance for FileMaker clients.

To improve performance:

- Avoid installing FileMaker Server on a machine that is a user's primary workstation.
- Avoid using the machine running FileMaker Server as an email, print, or network file server.
- Do not use system or third-party backup software to back up databases hosted by FileMaker Server. Instead, use Admin Console to schedule backups of databases. See Backing up databases.
- Disable screen savers and sleep (or hibernate and standby) mode on the server. These features reduce performance or suspend access to hosted databases.
- Use a fast hard disk, multiple-disk RAID system, or reliable Storage Area Network (SAN) for the hosted databases.
- Turn off operating system indexing services or any third-party file indexing software. These features reduce performance.

Installing FileMaker Server

This section describes how to install FileMaker Server from the Linux command line interface (CLI).

FileMaker Server 19 on Linux is available only as an electronic download. It includes product software and a link to an electronic license certificate that contains a license key needed for installation.

FileMaker Server supports installation only on the master machine. To deploy FileMaker Server for Linux in a multiple-machine environment, connect to Windows and macOS worker machines. See FileMaker Server Installation and Configuration Guide.

Step 1. Install the Linux packages and license certificate

Install the required Linux packages using the following CLI commands:

1. `sudo yum install wget [-y]`
2. `sudo yum install unzip [-y]`

For more information, see FileMaker Server system requirements for Linux.

Install the FileMaker Server for Linux installer license certificate file. Place the license certificate in one of the following locations:

- the default downloads folder: /Users/*[user]*/Downloads
  where *[user]* is the name of the user with administrative privileges
- the FileMaker Server for Linux installer folder: The folder where the FileMaker Server for Linux installer is located
- the LicenseFile folder on the machine where FileMaker Server is installed: /opt/FileMaker/FileMaker Server/CStore/LicenseFile

See About the license certificate.

Step 2: Download FileMaker Server

Download and unzip the FileMaker Server for Linux installer package:

1. Download the FileMaker Server for Linux installer using the link to the software download page you received in an email message. Enter the command:
   `wget [url]`
   where *[url]* is the download link from the email message.
2. Unzip the FileMaker Server for Linux installer package file. Enter the command:
   `unzip [installer]`
   where *[installer]* is the name of the installer package.

Step 3: Install FileMaker Server

1. Identify the name of the FileMaker Server for Linux installer. Enter the command:
   `ls -la`
2. Run the FileMaker Server for Linux installer. Enter the command:
   `sudo yum install [name] [-y]`
   where *[name]* is the FileMaker Server for Linux installer name and *[-y]* is an optional parameter.
3. To verify the installation, check that FileMaker Server processes and the Apache server are running. Enter the commands:
   - `ps -A | grep fm`
   - `ps -A | grep httpd`

   If the Apache server and FileMaker Server processes are running, the installation is complete.

Uninstalling FileMaker Server

Enter the following CLI commands to uninstall FileMaker Server for Linux.

1. Disconnect all FileMaker Server clients:
   `fmsadmin disconnect client`
2. Close all FileMaker databases:
   `fmsadmin close`
3. Stop FileMaker Server:
   `sudo service fmshelper stop`

4. Uninstall FileMaker Server:
   `sudo yum erase filemaker_server`

Important: The uninstall process deletes your settings, so be sure to write down any settings that you want to save. See FileMaker Server settings.

Next steps

- Change the default user name and password: see Changing default credentials.
- Start Admin Console: see Starting Admin Console.
- Configure Admin Console: see Configuring Admin Console.
- Test your installation: see Testing your deployment.
- Administer FileMaker Server: see Administering FileMaker Server.
- Upload databases: see Uploading databases.
- Get support: see Customer Support and Knowledge Base.

Testing your deployment

Testing overview

To test your FileMaker Server deployment, open a hosted database using FileMaker WebDirect or FileMaker Pro.

Using FileMaker WebDirect

1. Open Admin Console and click the **Connectors** > **Web Publishing** tab. See Starting Admin Console.
2. Verify that the Web Publishing Engine is running and FileMaker WebDirect is enabled.
3. For **FileMaker WebDirect**, click **Open Launch Center**.
4. In the Launch Center, select **FMServer_Sample**.

If FMServer_Sample opens, then your FileMaker Server deployment is working correctly.

Using FileMaker Pro

1. Open FileMaker Pro from any networked machine that can reach the machine where FileMaker Server is installed.
2. In the Hosts dialog box, choose the server you want to test, and select **FMServer_Sample**.

If FileMaker Pro opens the sample database hosted in FileMaker Server, then the Database Server is working and responding to requests from FileMaker Pro clients.

Note: Test using a FileMaker Pro client running on a different machine, not the machine where FileMaker Server is installed.

Troubleshooting

Admin Console doesn't start after installation on the master

If Admin Console doesn't start on the your machine after you run the FileMaker Server installation program, the most common solutions are:

- Start Admin Console either by:
  - entering `https://127.0.0.1:16000/admin-console` into a web browser.
  - using a desktop shortcut. To start Admin Console using a desktop shortcut: Double-click Claris FileMaker Server Admin Console on the desktop.
- When you open the URL `https://127.0.0.1:16000/admin-console` in a web browser, if the web browser displays a

message like "Can't Open the Page," then the browser may be enforcing HTTP Strict Transport Security (HSTS) for local host URLs. To correct the issue, clear the browser history.

- If the Admin Server process does not respond within 60 seconds to the FileMaker Server installation program, the following message appears: "The FileMaker Server Admin Console is not available".

  If you see this message:

  1. Restart the Admin Server process by entering the following command on the command line:

     ```
     fmsadmin restart adminserver
     ```

  2. If your server computer has a firewall, make sure all required ports are open in the firewall. (See Before you install FileMaker Server.)
  3. If your machine is running slowly, shut down any unnecessary applications.
  4. Restart your machine. Open a web browser on the master machine and enter `https://127.0.0.1:16000/admin-console`.

Cannot start Admin Console from a remote machine

If you cannot start Admin Console from a remote machine but you can from the master machine, the most common solutions are:

- Ensure that you're using the correct URL:

  `https://[host]:16000/admin-console`

  where `[host]` is the IP address of the server.

  See Starting Admin Console.
- If the master machine has a firewall enabled, open the ports required by FileMaker Server to communicate with users and administrators. See Before you install FileMaker Server.

Web browsers display a certificate message

Web browsers may display a certificate error or warning message when you use an HTTPS connection to go to any webpage hosted by the FileMaker Server web server. This includes Admin Console, a FileMaker WebDirect solution, or a Custom Web Publishing solution that uses an HTTPS connection. Displaying this message is expected behavior if your FileMaker Server deployment uses the default SSL certificate provided with FileMaker Server.

- To proceed to the desired page, users can click the option in the web browser to continue.
- To prevent this error message, see Requesting an SSL certificate.

Clients cannot see databases hosted by FileMaker Server

- The firewall settings on the master machine may be blocking the display of databases to clients. See Before you install FileMaker Server for information on which ports need to be unblocked in firewalls.
- Use supported clients to open files that are hosted by FileMaker Server 19. See the FileMaker Server system requirements.
- Make sure users have applied the most recent update of their client software.

Apache web server used by FileMaker Server stops responding

Ensure that no other websites or HTTP services use the ports required by the FileMaker Server web server. For example, if you have the FileMaker Server application installed and use it to enable HTTP services such as websites or a wiki, the existing Apache instance installed may be reenabled after FileMaker Server is installed.

To ensure the Apache instance used by FileMaker Server works normally, you need to configure any other HTTP services to use different ports from the ports that FileMaker Server uses, disable other HTTP services, or uninstall the FileMaker Server

application.

Administering FileMaker Server

Admin Console overview

Admin Console is a web-based application that lets you configure and administer FileMaker Server, work with and monitor hosted databases and clients (client applications), and track statistical information. You can administer Admin Console using the FileMaker Server CLI and the Admin API. See CLI Help, Using the command line interface, and the FileMaker Admin API Guide.

To administer FileMaker Server, use Admin Console on the computer where FileMaker Server is running or on any computer that has network access to the master machine running FileMaker Server. To secure remote administration, Admin Console uses Secure Sockets Layer (SSL) technology to encrypt HTTPS connections from other computers.

Admin Console supports many FileMaker Server administration tasks. You can:

- configure FileMaker Server application settings
- open—or host—a FileMaker Pro database, making it available to clients on the network
- view information about the files being hosted, like the number of clients accessing each database
- send messages to connected clients
- close a hosted FileMaker Pro database, making it unavailable to clients
- download a hosted FileMaker Pro database to your local system
- disconnect a selected client from all hosted databases
- pause or resume hosted databases
- create scheduled tasks to back up, verify, and clone hosted databases
- create scheduled tasks to run system scripts, FileMaker scripts, and script sequences that contain both system scripts and FileMaker scripts
- start or stop the Database Server
- start, stop, or remove a FileMaker WebDirect worker machine
- start or stop the Web Publishing Engine
- start or stop the FileMaker Data API Engine
- configure settings for ODBC and JDBC
- configure settings for FileMaker Data API
- configure settings for FileMaker WebDirect

For detailed information, see FileMaker Server Help.

Starting Admin Console

You can start Admin Console either using a web browser or the FileMaker Server Admin Console desktop shortcut.

To use Admin Console, your remote computer needs a supported web browser; no additional runtime environments or browser plug-ins are required. See Requirements for Admin Console.

1. Initialize Admin Console:
   - using a web browser
     Open a web browser and enter:

     ```
     https://[host]:16000/admin-consoleonsole
     ```

where `[host]` is the IP address or host name of the machine running FileMaker Server.

Note: You can get the host name or IP address using the `nmcli` command.

- using the FileMaker Server for Linix shortcut: Double-click Claris FileMaker Server Admin Console on the desktop.

2. Before the Admin Console **Sign In** page opens, your web browser may require you to respond to a security message. This is normal behavior for the default SSL certificate that is included with FileMaker Server. Click the option to continue to go to the **Sign In** page.

   To prevent this message in the future, see Requesting an SSL certificate.

   Tip: Bookmark the **Sign In** page in your web browser. Come back to this page to sign in to Admin Console or to open Server Help.

3. On the Admin Console **Sign In** page, enter `admin` for the user name and password, then click **Sign In**. Admin Console starts and displays the **Dashboard** page.

4. On the the **Administrator** tab, change the Admin Console account user name and password. If your web browser prompts you to save your user name and password, decline unless you are sure that access to your web browser is secure. For details, see FileMaker Server Help.

Alternative ways to start Admin Console

You can start Admin Console directly using the following:

To access Admin Console from	Go to
Any computer with network access to the master machine	`https://[host]:16000/admin-console` where `[host]` is the IP address of the server.
Master machine only	`https://127.0.0.1:16000/admin-console` From an FMS Admin Console shortcut: Double-click Claris FileMaker Server Admin Console on the desktop.

Configuring Admin Console

This section details how to configure Admin Console using the UI. Alternatively, you can configure Admin Console using the FileMaker Server CLI or the Admin API. See CLI Help and FileMaker Admin API Guide.

1. On the Admin Console **Sign In** page, enter `admin` for the user name and password, then click **Sign In**. **Note:** If you want to change the default user name and password, see Changing default credentials.

2. On the Admin Console **Security Settings** page, decide whether to import an SSL certificate.

   Because data security is important, FileMaker Server asks you to import an SSL certificate when you first open Admin Console.

   - If you have a custom SSL certificate to import, follow the instructions to import the SSL certificate.
   - If you don't have a custom SSL certificate to import, close Admin Console and request a custom SSL certificate from a trusted CA, or continue without importing an SSL certificate. (Open Admin Console and click the **Configuration** > **SSL Certificate** tab to import a custom SSL certificate later.)

3. If you want to allow technologies such as FileMaker WebDirect, FileMaker Data API, and ODBC and JDBC to access hosted databases, enable the settings on the corresponding tabs in Admin Console.

To enable	Go to Admin Console tab
FileMaker WebDirect	**Connectors** > **Web Publishing**
FileMaker Data API	**Connectors** > **FileMaker Data API**
ODBC and JDBC	**Connectors** > **ODBC / JDBC**

See FileMaker Server Help.

Changing default credentials

When you installed FileMaker Server for Linux, a default user name, password, and hardcoded four-digit security code was created for you. To change the default credentials, use one of the following:

- In Admin Console, use the **Administrator** tab. See FileMaker Server Help.
- In the Linux CLI, enter:
  `fmsadmin resetpw -p [pass] -z 1234`

  where *[pass]* is the new password, and `1234` is the default code.

Uploading databases

FileMaker provides two ways to upload databases to FileMaker Server:

- In FileMaker Pro, use **File** menu > **Sharing** > **Upload to Host** to transfer FileMaker Pro databases from your computer's file system to FileMaker Server if both computers are on the same network. FileMaker Pro uploads databases along with any externally stored container field objects. FileMaker Server copies the databases to the specified database folder and sets file permissions and privileges so that you can access the databases after they are uploaded.
- Manually upload databases to FileMaker Server. Copy the databases and any externally stored container field objects to the proper location. See FileMaker Server Help.

Note: If any of your databases require a plug-in, see FileMaker Server Help to manage plug-ins.

Encrypting databases

In FileMaker Pro, you can use the Database Encryption feature to encrypt the contents of a database. Encryption protects the FileMaker database and any temporary files that are written to disk. See FileMaker Pro Help.

To host an encrypted database on FileMaker Server for FileMaker clients, you can manually upload the database to FileMaker Server or use the **Upload to Host** menu command in FileMaker Pro to transfer the file.

When you use FileMaker Pro to upload encrypted files to the Secure folder, FileMaker Pro asks you for the encryption password so that FileMaker Server can automatically open the files on the server after they are uploaded. If you upload encrypted files to a folder other than the Secure folder or if you manually upload encrypted files, they must be opened on the server using Admin Console or the `fmsadmin` command line interface (CLI). See FileMaker Server Help.

Tip: Use the CLI command to check whether a database is encrypted.

Backing up databases

FileMaker Server provides the following ways to perform database backups.

Backup type	Description
Automatic	FileMaker Server creates an automatic backup of hosted databases once a day.
On-demand	Click **Back Up Now** on the **Backups** page to create an on-demand backup at any time.
Scheduled	Use the **Backups** > **Backup Schedules** tab to create a backup schedule that defines which databases are backed up and how often they are backed up. Every time the schedule runs, FileMaker Server checks whether the selected databases have changed since the last backup. FileMaker Server creates a full copy of the databases that have changed and creates hard links to the backed-up databases that have not changed.
Progressive	FileMaker Server starts by creating a full backup of all hosted databases. After the initial full backup is complete, the Database Server only copies the changes from the hosted file to the progressive backup folder. Progressive backups can run more quickly than a backup schedule, with less impact on server performance. Progressive backups keep two copies of the backup files: a timestamped copy that is available for you to use as a backup, and an in-progress copy that gets updated with the accumulated changes.

Use a combination of these backup types to create a comprehensive backup strategy for your hosted databases. See FileMaker Server Help.

Understanding startup restoration

FileMaker Server creates a restoration log for hosted databases. At startup, before databases are opened for client access, FileMaker Server validates database entries. If databases were not properly closed, startup restoration uses the restoration log to restore the files to their last consistent state.

Startup restoration is not a replacement for database backups. But it may help resolve database integrity issues that occur due to server power loss, hardware failures, or software issues. See FileMaker Server Help.

By default, the restoration log is written to the following folder:

```
/opt/FileMaker/FileMaker Server/Data/Restoration
```

For best results, use the FileMaker Admin API to change the restoration log folder location to a separate disk drive. See FileMaker Admin API Guide.

Hosting databases connected to ODBC data sources

FileMaker Server can host FileMaker Pro databases that are connected to external SQL data sources. In FileMaker Pro, you can work with the ODBC data in much the same way that you work with data in a FileMaker database. For example, you can add, change, delete, and search external data interactively.

See FileMaker Server Help for information on using ODBC and JDBC with FileMaker Server and accessing external ODBC data sources.

Note: You do not need to enable the OBDC/JDBC data source feature of FileMaker Server to host FileMaker Pro databases that access an external SQL data source via ODBC.

Running server-side scripts

You can create scheduled tasks to run:

- system-level scripts—for example Perl, VBScript, and AppleScript
- FileMaker scripts in databases hosted by FileMaker Server
- script sequences that combine a FileMaker script with an optional pre-processing system-level script and an optional post-processing system-level script

See FileMaker Server Help.

System-level scripts

Script files must be placed in the Scripts folder on the master machine in your FileMaker Server deployment. To schedule a system-level script to run, create a scheduled script and specify the type **System Script**. Next, select the script file you want to run.

System-level scripts can perform operating system level tasks on the master machine.

FileMaker scripts

To schedule a FileMaker script to run, create a scheduled script and specify the type **FileMaker Script**. Next, select the database that contains the script you want to run, then the script.

FileMaker scripts can do simple or complex tasks. For example, you can write a FileMaker script to remove duplicate records or to validate the format of phone numbers. You can schedule these scripts to run during off hours, perhaps before a daily backup.

Scripts can incorporate conditional decisions (if-else statements) and perform repetitive tasks (loop statements). Use the Script Workspace in FileMaker Pro to build scripts by selecting from a list of supported FileMaker Pro commands, called *script steps*, and specifying options (if necessary).

To find out if a FileMaker script step is supported from a FileMaker Server schedule, choose **Server** for **Show Compatibility** in the Script Workspace. See the script step reference in FileMaker Pro Help.

Script sequences

To create a script sequence, create a scheduled script and specify the type **Script Sequence**. Next, select the database that contains the FileMaker script you want to run, then the script. Next, select an optional pre-processing system-level script, an optional post-processing system-level script, or both.

Viewing system statistics

The Admin Console **Dashboard** page displays statistics related to CPU usage, memory usage, network throughput, and disk throughput. These statistics can help you diagnose system hardware issues that may be affecting system performance.

Viewing server and client statistics

To see a summary of connection and database statistics for FileMaker Server, open the server statistics log (Stats.log) and client statistics log (ClientStats.log). These statistics can help you diagnose performance problems and identify client access issues. You can view:

- the percentage of times FileMaker Server retrieved data from the cache (RAM) rather than the hard disk, percentage of cache unsaved, the amount of data read from disk, data written to disk, and client call times
- client connection information collected during remote calls made by each FileMaker client, all Web Publishing Engine (WPC) clients, and all ODBC and JDBC clients

See FileMaker Server Help.

Sending messages to FileMaker clients

You can send messages to notify FileMaker Pro, FileMaker Go, and FileMaker WebDirect clients about important events such as server shutdowns, database maintenance, or deadline reminders. You can send messages to:

- all FileMaker clients or selected FileMaker clients connected to hosted databases
- FileMaker clients connected to any database or selected databases hosted by FileMaker Server

See FileMaker Server Help.

Downloading log files in Admin Console

FileMaker Server tracks activity, client access, and other information as it operates and stores this information in log files.

To download log files, open Admin Console and click the **Configuration** > **Logging** tab.

See FileMaker Server Help.

Emailing notifications

You can configure FileMaker Server to send SMTP email notifications about errors. Specify your SMTP mail server settings in Admin Console, including the SMTP server address, the port number, user name and password, and the list of email addresses that will receive the email messages.

See FileMaker Server Help.

Using the command line interface

FileMaker provides the tool `fmsadmin` for administering FileMaker Server via the command line interface (CLI). You must be logged on to the computer running FileMaker Server, either directly or using remote desktop software, to use the CLI. The CLI is available via the Linux command promp. CLI commands can also be used in a script or batch file.

Command line interface files

The CLI executable `fmsadmin` is located in the folder: /opt/FileMaker/FileMaker Server/Database Server/bin/fmsadmin

Note: A symbolic link to `fmsadmin` is also installed: /usr/bin/fmsadmin

Command line interface commands

The general format for `fmsadmin` commands is:

```
fmsadmin command [options]
```

The following example authenticates with the Admin Console user name *admin* and the password *pword*, and closes all open databases without prompting you to confirm:

```
fmsadmin close -y -u admin -p pword
```

> **Important:** CLI commands can include the Admin Console name and password. If a command is used interactively, the user name is visible but the password is not. If a command in a script or batch file must include a name and password, be sure that only the password owner can view the script or batch file.

CLI Help

In the CLI, use the `help` command to see Help pages that list what commands and options are available and how to use them:

```
fmsadmin help
```

Moving an existing installation

Overview

You can migrate data from an existing FileMaker Server installation that's on another operating system to a Linux machine.

The steps below outline the data migration process and assume that you've already installed FileMaker Server on your Linux machine. To install FileMaker Server, see Installing FileMaker Server.

See the remaining sections for information about each step.

Important: After you move your data, unistall FileMaker Server from the previous machine to prevent duplicating the same license. For more information on removing FileMaker Server, see Unistalling FileMaker Server. To change the license of an existing deployment of FileMaker Server 19, see Updating the FileMaker Server license key.

1. Save the settings for your schedules.
2. Note your existing FileMaker Server settings.
3. Make a copy of any databases and shell script files you used with FileMaker Server.
4. Clear the Java cache and web browser cache to clear information from the previous FileMaker Server installation.
5. Move any databases or script files you used with the previous version of FileMaker Server to the proper folders within the FileMaker Server folder structure.
6. Load the settings for your schedules after installation.
7. Configure FileMaker Server.

Step 1. Save your schedules

You can save the settings for your schedules that are configured in the current installation.

1. Open Admin Console and click the **Configuration** > **Script Schedules** tab.
2. Click **Save or Load** and choose **Save All Schedules**. By default, the file is saved in your web browser's download folder.

After you install FileMaker Server, you can load the *schedule settings file* to instantly configure them in the new installation.

Note: The default name of the schedule settings file matches the version of FileMaker Server:

- FileMaker Server 18: fms18_settings.settings
- FileMaker Server 19: fms19_settings.settings

You cannot specify a different name when you save the file in Admin Console, but you can change the filename using your operating system tools after you save the file.

Step 2. Note your FileMaker Server settings

Make a note of your existing FileMaker Server settings because you will have to reenter your settings manually later. Some examples are:

- Note the name of your FileMaker Server installation (the name FileMaker Pro users see in the Hosts dialog box and FileMaker Go users see in the Launch Center).
- Save the schedule settings in a file. See Step 1. Save your schedules.
- Note other settings that you have changed from the defaults and want to reuse in your FileMaker Server 19 deployment.
- If you are using a custom SSL certificate, save a copy of the serverCustom.pem and serverKey.pem files stored in the CStore folder so that you can import your custom SSL certificate later.

Where to note settings for FileMaker Server

Before moving an existing installation of FileMaker Server to another machine, start Admin Console (see Starting Admin Console). Make a note of the settings in the configuration tabs:

- For FileMaker Server 18 and 19, note the settings on the Configuration, Connectors, and Administration tabs.
- For earlier versions, note the settings on the General Settings, Database Server, and Web Publishing tabs.

Step 3. Make a copy of databases, scripts, and plug-ins

Make a copy of any databases, shell script files, and plug-ins you used with FileMaker Server and copy them to the

corresponding directory on your Linux machine. In a default FileMaker Server installation, they are stored on the master machine in the following folders.

FileMaker Server files on Windows and macOS

Windows:

- \Program Files\FileMaker\FileMaker Server\Data\Databases
- \Program Files\FileMaker\FileMaker Server\Data\Secure
- \Program Files\FileMaker\FileMaker Server\Data\Scripts
- \Program Files\FileMaker\FileMaker Server\Database Server\Extensions

macOS:

- /Library/FileMaker Server/Data/Databases
- /Library/FileMaker Server/Data/Secure
- /Library/FileMaker Server/Data/Scripts
- /Library/FileMaker Server/Database Server/Extensions

FileMaker Server files on Linux

Linux:

- /opt/FileMaker/FileMaker Server/Data/Databases
- /opt/FileMaker/FileMaker Server/Data/Secure
- /opt/FileMaker/FileMaker Server/Data/Scripts
- /opt/FileMaker/FileMaker Server/Database Server/Extensions

Step 4. Clear the Java cache and web browser cache

After you uninstall FileMaker Server, the Java cache may retain pointers to FileMaker Server components that have been uninstalled. In addition, your web browser may retain cached versions of artwork and HTML files that have been uninstalled.

Clear the Java cache and web browser cache to clear information from the previous FileMaker Server install.

Step 5. Move files to the proper location

Move the script files and plug-ins you used with the previous version of FileMaker Server to the proper folders within the FileMaker Server 19 folder structure. See Step 4. Make a copy of databases, scripts, and plug-ins.

Note: You can use FileMaker Pro to transfer .fmp12 databases to your new FileMaker Server deployment. See Uploading databases. To transfer your databases manually, see FileMaker Server Help.

Important: If you are using FileMaker Server 19 and you want to transfer settings by loading the schedule settings file, make sure you have created a folder structure in the FileMaker Server for Linux installation that is identical to the source server installation. Copy the databases, scripts, and other solution files from the source installation to the new FileMaker Server installation, and set the appropriate permissions in Linux. See FileMaker Server Help.

Step 6. Load your schedules

If you are moving from a previous FileMaker Server 18 or 19 installation, you can load the schedule settings file after installation. See Step 1. Save your schedules.

Important: Whenever you load a schedule settings file, all existing schedules in the new FileMaker Server installation are deleted and replaced by the schedules in the schedule settings file. You cannot merge the schedule settings from multiple FileMaker Servers.

1. Open Admin Console for the new FileMaker Server 19 installation and click the **Configuration** > **Script Schedules** tab.
2. Click **Save or Load** and choose **Load All Schedules**.
3. Click **Browse** and navigate to the folder where you saved the schedule settings file.
4. Select the schedule settings file and click **Choose**.
5. Click **Load** to load the schedule settings file into FileMaker Server.
6. Read the message to see how many schedules loaded successful.
7. Open the LoadSchedules.log file in the Logs folder for detailed information about errors that may have occurred and make any necessary corrections.

See FileMaker Server Help.

Step 7. Configure your deployment

You can now start Admin Console and configure your FileMaker Server deployment using the settings from Step 2. Note your FileMaker Server settings. See FileMaker Server Help.

As part of the configuration, be sure to import your custom SSL certificate, if you are using SSL.

For information about uploading databases, scheduling backups, and performing other regular tasks, see Administering FileMaker Server.

Setting up the web server

Web server overview

In all deployments, FileMaker Server uses Apache in Linux. The web server serves web publishing clients, hosts the web-based Admin Console application, and handles some data transfer tasks.

This section describes the basics of requesting a custom Secure Socket Layer (SSL) certificate, and enabling the web server. For information about configuring the web server, see the documentation for the web server.

Requesting an SSL certificate

FileMaker Server uses SSL technology to encrypt HTTPS connections between the web server and users' web browsers for Admin Console, FileMaker WebDirect, FileMaker Data API, and Custom Web Publishing. The Database Server can also use SSL encryption for connections with FileMaker Pro clients, FileMaker Go clients, and the Web Publishing Engine.

SSL uses digital certificates to certify the ownership of the public key used to encrypt data. FileMaker Server provides a standard SSL certificate signed by Claris International Inc., that does not verify the server name. This certificate is used by all FileMaker Server components that use SSL. However, because this certificate doesn't verify the server name, most web browsers will warn users of a problem with the website's security certificate. For some web browsers, certificate issues can affect performance and functionality as well. The FileMaker default certificate is intended only for test purposes.

A custom SSL certificate is required for production use. If your server does not have a custom SSL certificate, Admin Console will display security warnings.

When you import a custom SSL certificate, FileMaker Server enables all Database Server client connections to use SSL, and web clients are restricted to HTTPS connections.

For information about using secure connections, see FileMaker Server Help.

You can request a custom SSL certificate that matches your specific server name or domain name from a trusted certificate authority (CA) supported by Claris International Inc. Use the CLI `certificate` command to create a certificate signing request (serverRequest.pem), which you send to a CA, and a private key (serverKey.pem), which you keep secret. See Using the CLI certificate command. When you receive your signed certificate from the CA, open Admin Console and click the **Configuration** > **SSL Certificate** tab to import the certificate.

The custom SSL certificate file is placed in the CStore folder:/opt/FileMaker/FileMaker Server/CStore/serverCustom.pem

After updating the custom SSL certificate, restart the Database Server.

When the Database Server starts, if it is unable to find a custom SSL certificate, it will use the default server.pem file.

See FileMaker Server Help for information about securing your data.

Notes

- FileMaker Server supports using a single-domain certificate, a wildcard certificate, or a subject alternative name (SAN) certificate.

  The CLI `certificate` command can create a request for a single-domain certificate or a wildcard certificate. To use a SAN certificate, contact a CA to create the certificate signing request.
- Use FileMaker methods to import the custom SSL certificate: either the Admin Console import certificate feature or the CLI `certificate` command.
- The custom SSL certificate must use base-64 encoding.
- FileMaker Server does not support validation using a certificate revocation list (CRL validation).
- If you are using a multiple-machine deployment, request custom SSL certificates for the master machine and the worker machines. Import a custom SSL certificate on each machine.
- To remove an imported certificate, use the CLI command `fmsadmin certificate delete`, and restart FileMaker Server to apply the change. See CLI Help.
- For information about supported certificates, see the Knowledge Base.

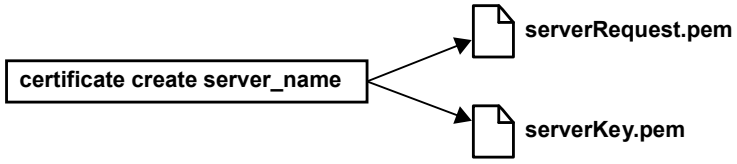
Using the CLI certificate command

Use the CLI `certificate` command to create a signed certificate matching the server name or domain name system (DNS) name for a fully secure SSL connection with FileMaker Server.

FileMaker Server ships with a default certificate that is installed on the Database Server and a root certificate that ships with the FileMaker Pro and FileMaker Go software. If you are using this certificate, make sure that the server certificate is installed on the machine running the Database Server, and the client certificate is installed on the FileMaker Pro and FileMaker Go client computers.

You can use the `certificate` command and request a signed certificate from a CA that matches your specific server name or DNS name. A CA issues digital certificates that contain a public key and the identity of the owner. When you create the certificate request, a private key is generated that corresponds to the public key.

- Use the `certificate create` command to create the certificate request file that you send to the CA (serverRequest.pem), plus an encrypted private key file that is used by the `certificate import` command (serverKey.pem).



The `certificate create` command creates two output files:

- the encrypted private key file: serverRequest.pem
  Submit the serverRequest.pem file to the CA using the process provided by the CA.
- the encrypted private key file: serverKey.pem
  The `certificate import` command combines this file with the certificate file returned to you by the CA.

Note: Use an encryption password for a private key when creating a server request. For example: `certificate create --keyfilepass exampleSecretPassphrase`

- Use the `certificate import` command to create a custom server .pem file. This custom server .pem file combines the certificate file that you receive from the CA with the encrypted private key file created by the `certificate create` command.

Note: To write information to the serverkey.pem file, you must have administrator privileges. If you don't have administrator privileges, Linux generates an error. To prevent this error, authenticate as sudo to run commands as the superuser.

Format

```
fmsadmin certificate create server_name

fmsadmin certificate create subject

fmsadmin certificate import certificate_file
```

Options

`server_name | subject`

`server_name` or `subject` is required for the `certificate create` command.

`server_name` is the value used by clients to open hosted files with the FileMaker Network protocol, fmnet.

For example, if FileMaker Pro clients use `fmnet:/salesdbs.mycompany.com/sales` to open the hosted database Sales, then use the following command with salesdbs.mycompany.com as the `server_name`:

```
fmsadmin certificate create salesdbs.mycompany.com --keyfilepass exampleSecretPassphrase
```

`subject` may be used to include more information than the server name. (Some certificate authorities require additional information.) `subject` uses the same syntax as the argument in the `openssl req [-subj arg]` command:

- `subject` is not case sensitive.
- `subject` must be formatted as `/type0=value0/type1=value1/type2=...`, where each `type=value` pair is an attribute type and a value specifying a relative distinguished name.
- Use the backslash character (\) to escape special characters.
- Use double quotation marks to enclose the subject string if it includes space characters.

For example, to use the DNS common name salesdbs.mycompany.com and the country value US, use the following command:

```
fmsadmin certificate create /CN=salesdbs.mycompany.com/C=US --keyfilepass exampleSecretPassphrase
```

The following example shows additional attributes that may be specified using the subject option:

```
fmsadmin certificate create "/CN=ets-srvr.filemaker.com/O=FileMaker DBS
Test/C=US/ST=California/L=Santa Clara" --keyfilepass exampleSecretPassphrase
```

Options

`certificate_file`

`certificate_file` is required for the `certificate import` command.

`certificate_file` is the full pathname to the custom SSL certificate file that you received from the CA. You may use an absolute pathname or a relative pathname.

For example, if the certificate file is c:\Documents\signedCertificate.crt, then use the following command:

```
fmsadmin certificate import c:\Documents\signedCertificate.crt
```

The `certificate import` command combines the signed certificate file with the serverKey.pem file and creates a file called serverCustom.pem. The serverCustom.pem file is created in the CStore folder:/opt/FileMaker/FileMaker Server/CStore/serverCustom.pem

To use the `certificate import` command You must have read and write access permissions to the CStore folder.

After using the `certificate import` command, you must restart the Database Server. After restarting, if the Database Server is unable to find serverCustom.pem, it will use the default server.pem file.

To verify the web server is running, enter the following in a web browser on the web server host machine:

```
https://127.0.0.1
```

During installation, the FileMaker Server for Linux installer checks whether any existing website is using ports 80 or 443. If these ports are in use, the installer prompts you to make these ports available. Then, the installer creates its own separate website named FMWebSite and configures it to use port 80 for HTTP and port 443 for HTTPS. On the master machine, the installer also configures FMWebSite to use port 16000 for Admin Console via HTTPS.

Additional resources

Product documentation

- FileMaker Server Help is available on each page of Admin Console. Scroll to the bottom of the page and click **Help**.
- FileMaker Server documentation is accessible on each page of Admin Console. Scroll to the bottom of the page and click **Documentation**.
- On the web, go to the Product Documentation Center.

Customer Support and Knowledge Base

- For help with installation, launch, or reinstallation, visit Support.
- For tips, technical advice, and more information about FileMaker Server, visit the Knowledge Base.
- To ask questions and get advice from other users, visit the Claris Community.

Note: Information in the Knowledge Base and the Claris Community may not be available in all languages.

Check for software updates

Check for software updates on the Admin Console **Configuration** > **General Settings** tab. When a software update is available, for **Server Version**, click the link to download the update.

Legal information

Claris International Inc.
5201 Patrick Henry Drive
Santa Clara, California 95054

Edition: 01