FileMaker® Server 16

Installation and Configuration Guide

FileMaker®
An Apple Subsidiary

FileMaker, Inc.
5201 Patrick Henry Drive
Santa Clara, California 95054

For more information, visit our website at http://www.filemaker.com.

Edition: 01

Contents

Chapter 1
Introduction

FileMaker Server® is fast, reliable server software for safely sharing FileMaker information among business teams on iOS, desktops, and the web. FileMaker Server is a dedicated database server that hosts database files created using FileMaker Pro so that data can be shared and modified by FileMaker Pro, FileMaker Go®, and FileMaker WebDirect™ clients, and by other client applications supported by the FileMaker Server Web Publishing Engine.

Before you install, confirm that your machines meet 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 14, 15, and 16
- FileMaker Go 14, 15, and 16
- ODBC (Open Database Connectivity) and JDBC (Java Database Connectivity) client applications using the FileMaker client drivers. The FileMaker ODBC and JDBC drivers are available in the xDBC folder in the installation disk image and on the FileMaker downloads page. See FileMaker ODBC and JDBC Guide and FileMaker Pro Help.
- Web browsers (or other applications) accessing data through the Web Publishing Engine
- Web services (or other applications) accessing data through the FileMaker Data API

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

FileMaker Server can host up to 125 databases at the same time for the following simultaneous client connections:

Client	Supported connections
FileMaker Pro with individual or volume license	Unrestricted
Custom Web Publishing	Unrestricted
ODBC and JDBC	Unrestricted
FileMaker Go, FileMaker WebDirect, and FileMaker Pro as clients with the User Connections License	One connection to use for evaluation purposes You can purchase additional User Connections client connections to use in a production environment.

Note Although FileMaker Server allows an unrestricted number of simultaneous connections for some client types, most operating systems impose their own limits on the number of network connections and open files that a process may use. This operating system limit sets the effective limit on the number of simultaneous client connections.

About the license key

FileMaker software comes with a unique, 35-character license key. Do not lose this license key. Keep the license key in a safe place in case the software ever needs to be reinstalled.

You received an email message with a link to your software download page. Your license key can be found on that page.The license key is customized for your organization. When installing software, enter the organization name exactly as it appears on the software download page.

The license key ensures adherence to the single user license agreement, which generally allows for use of one (1) copy of the Software on one single-machine deployment or on one multiple-machine deployment at a time (refer to your Software License). If the license key is invalid or if another copy of the software installed with that same license key is running on the network, the FileMaker Server software displays an error message.

You can choose to deploy FileMaker Server components across multiple machines that work together to form a single FileMaker Server deployment. You must have a unique license key for each deployment or obtain a volume license for more than one deployment. You must license one copy of FileMaker Server for each deployment.

Updating the FileMaker Server license key

You can enter a new license key for FileMaker Server 16 on the same machine to do the following:

- upgrade from a trial version of FileMaker Server 16
- add support for more FileMaker Go, FileMaker WebDirect, and FileMaker Pro User Connections clients

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

1. From the FileMaker Server Admin Console, choose the **General Settings** > **Server Information** tab. See “Starting Admin Console” on page 36.
2. Click **Change License Key**.
3. Enter the information required, then click **Update**.

Where to go from here

- To install on a single machine, see chapter 2, “Installation quick start.”
- To install using a multiple-machine deployment, see chapter 3, “Deploying FileMaker Server across multiple machines.”
- To move from an existing installation of FileMaker Server, see chapter 6, “Upgrading or moving an existing installation.”

Chapter 2
Installation quick start

This chapter explains how to install FileMaker Server on a single machine. To install on more than one machine, see chapter 3, “Deploying FileMaker Server across multiple machines.”

Before you begin

Here is a list of things you must do before installing FileMaker Server:

- 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 a port for web connections and a port for secure web connections is available on the web server. The default ports are port 80 and 443, though you may specify alternative ports during installation. These ports are used by FileMaker Server even if web publishing is disabled. If the FileMaker Server installer detects existing websites using these ports, the installer prompts you to either specify alternative ports or let it disable those websites.
  - Windows: The FileMaker Server installer enables the IIS web server if it isn’t already enabled, then runs the Microsoft Application Request Routing (ARR) installer, creates its own website in IIS, and configures the website to use the ports specified for web connections.
  - macOS: The web server included in macOS does not need to be enabled. If it is enabled, ensure that no existing website uses port 80 or 443, or be prepared to specify alternative ports during installation. The installer creates a separate web server instance and enables it for FileMaker Server to use on these ports.

    See chapter 7, “Setting up the web server.”
- If your server computer has a firewall, open the necessary ports in the firewall so that FileMaker Server can communicate with administrators and clients:
  - Web connections port: 80 by default, but you may specify a different port during installation. This port is used by Admin Console and for web publishing (HTTP).
  - Secure web connections port: 443 by default, but you may specify a different port during installation. 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 2399 for ODBC and JDBC clients.
  - Ports 1895, 3000, 5013, 5015, 8989, 8998, 9889, 9898, 16001, 16002, 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” on page 22.
- To upgrade from an earlier version of FileMaker Server, see chapter 6, “Upgrading or moving an existing installation.”

- Locate your license key. See “About the license key” on page 7.
- If you are currently running FileMaker Pro on the same machine, you must quit FileMaker Pro before installing FileMaker Server.

Also keep in mind the following:

- 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 installer. Don’t enable antivirus software again until after the Deployment assistant has finished.

  Do not allow antivirus software to scan the folders that contain hosted database files 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, FileMaker, Inc., recommends using a static IP address.
- macOS: Avoid using the macOS Server application to enable any HTTP services while running FileMaker Server. HTTP services provided by macOS Server can interfere with FileMaker Server. See “Using the Apache web server in macOS” on page 57.

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 database files, 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 FileMaker Server Admin Console to schedule backups of databases. See “Backing up databases” on page 38.
- 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.

  See chapter 8, “Optimizing your FileMaker Server deployment.”

Installing FileMaker Server on a single machine

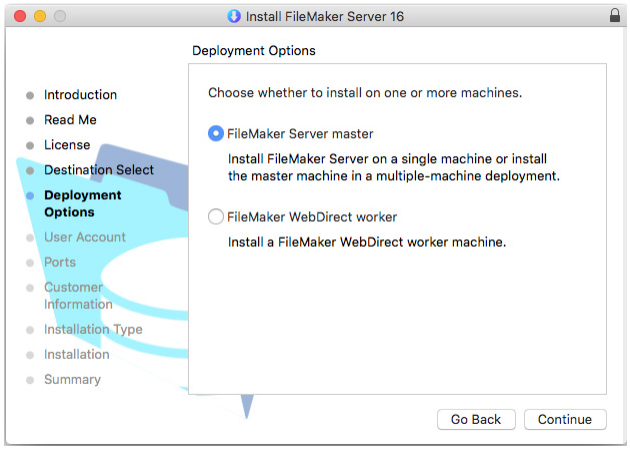
1. Follow your electronic download instructions to download and open the installation disk image, or insert your product DVD.
2. Windows: If you have Bonjour for Windows installed, make sure that it is running before you run the FileMaker Server installer.
3. Double-click the installation icon.

Setup (Windows)

FileMaker Server (macOS)

   - Windows: If a User Account Control alert appears, click **Yes**.
   - macOS: If a security message appears, click **Continue**.
4. Windows: Select a language.
5. To continue with installation, click **Next** (Windows) or **Continue** (macOS).
6. Read the important information displayed. If there is a task you did not do, quit the installer and do the task.
7. Review and accept the end user license agreement.
8. Select the installation destination.

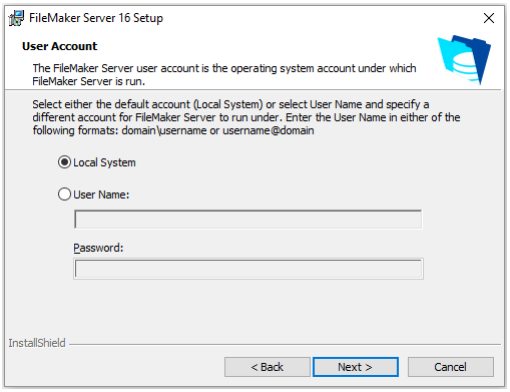
   Note In Windows, you can select a non-default location. See “Installation notes” on page 28.
9. Select **FileMaker Server master**.



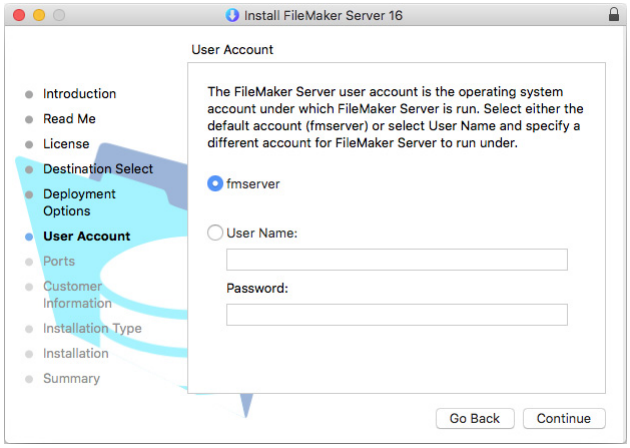
10. Choose an option for the FileMaker Server user account (the account under which you want to run FileMaker Server):

- To use the default account, select **Local System** (Windows) or **fmserver** (macOS).
- To use an existing account on this machine, select **User Name**, enter the account's user name and password. You may want to choose this option if you already have an account that has privileges set as you want—for example, to access network-attached storage.

  If the existing user account you specified does not have sufficient privileges for FileMaker Server to run, the installer displays an error message. See "Installation notes" on page 28.



Windows



macOS

11. Specify the ports that FileMaker Server should use for web connections and secure web connections.

Windows: If the installer detects that the ports required for the web server are currently in use, the installer prompts you to let it disable the website currently using those ports. To continue installation, you must click **Disable Websites**. Or you can click **Cancel**, disable the website manually, then run the installer again.

macOS: If the installer detects that the ports required for the web server are currently in use, the installer lets you know which ports are in use. You can either make the ports available on your system or choose different ports.

12. Enter the user name, organization, and license key information.

13. Click **Install**.

- Windows:

  If you do not have the Microsoft Visual C++ 2015 Redistributable Package (x64) or a minimum update of Java Runtime Environment version 8, the FileMaker Server installer installs them. If you do not have the Microsoft Application Request Routing (ARR) extension for IIS installed, the FileMaker Server installer installs it.

  If you do not have Bonjour for Windows installed, you are prompted to allow the FileMaker Server installer to install it. Follow the onscreen instructions.

  See "Installation notes" on page 28.

- macOS:

  Enter your macOS user name and password, then click **Install Software**.

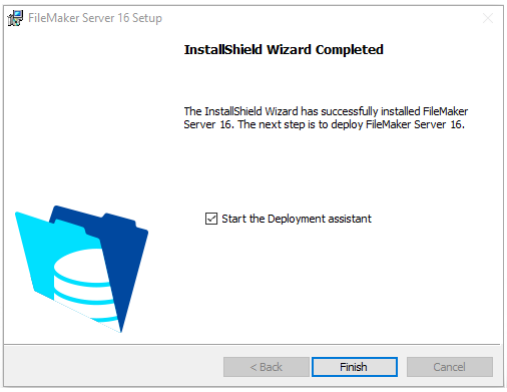
  If you do not have a minimum update of Java Runtime Environment version 8 installed, the FileMaker Server installer installs it. If Bonjour is not running, you are prompted to run it. See “Installation notes” on page 28.

  FileMaker Server begins to install. This process may take several minutes.

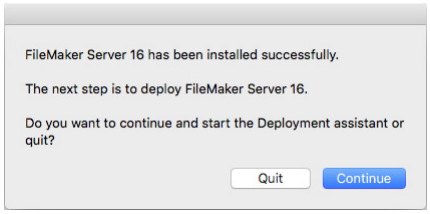
14. After the software has been successfully installed, start the Deployment assistant.

- Windows: In the last step of the installer, select **Start the Deployment assistant**, then click **Finish**.
- macOS: Click **Continue**.

If necessary, see “Deployment assistant doesn’t start after installation on the master” on page 32.



Windows



macOS

You can stop now and start the Deployment assistant later. To deploy FileMaker Server at a later time:

- Windows: For Windows versions with the Start button, click the **Start** button > **All Programs** > **FileMaker Server** > **FMS 16 Admin Console**. For Windows versions with the Windows Start screen, click **FMS 16 Admin Console**.
- macOS: Double-click the **FMS 16 Admin Console** shortcut on the desktop.
- Enter `http://localhost:16001/admin-console` into a web browser.

The Deployment assistant opens in the web browser. It may take a few minutes for Admin Console to start and the Deployment assistant to appear.

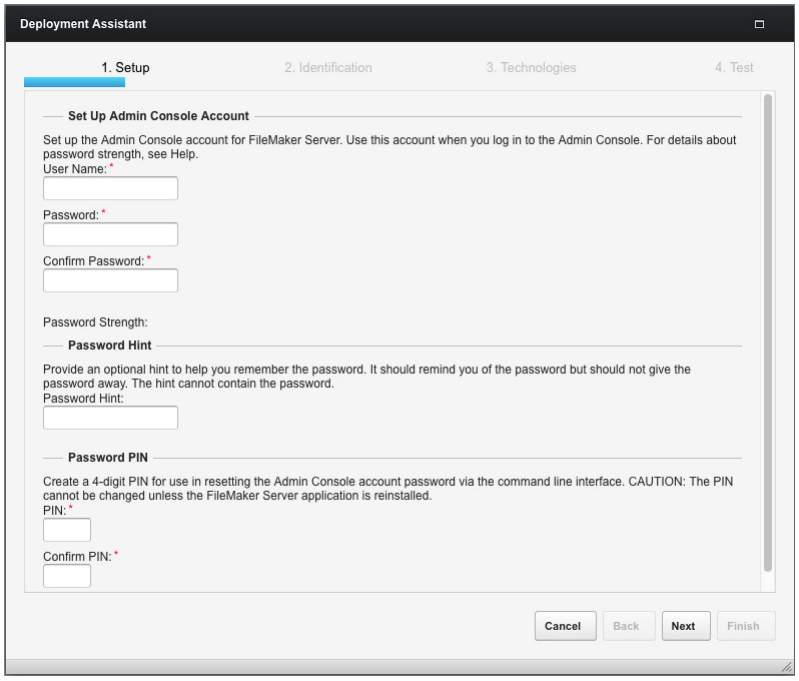
Note If Admin Console and the Deployment assistant do not start, see “Deployment assistant doesn’t start after installation on the master” on page 32.

15. In the first step of the Deployment assistant, assign the user name and password you want to use whenever you log in to Admin Console as the server administrator. The server administrator is responsible for installing and configuring FileMaker Server as well as managing the FileMaker Pro databases hosted on FileMaker Server.

Note User names are not case sensitive. Passwords are case sensitive.

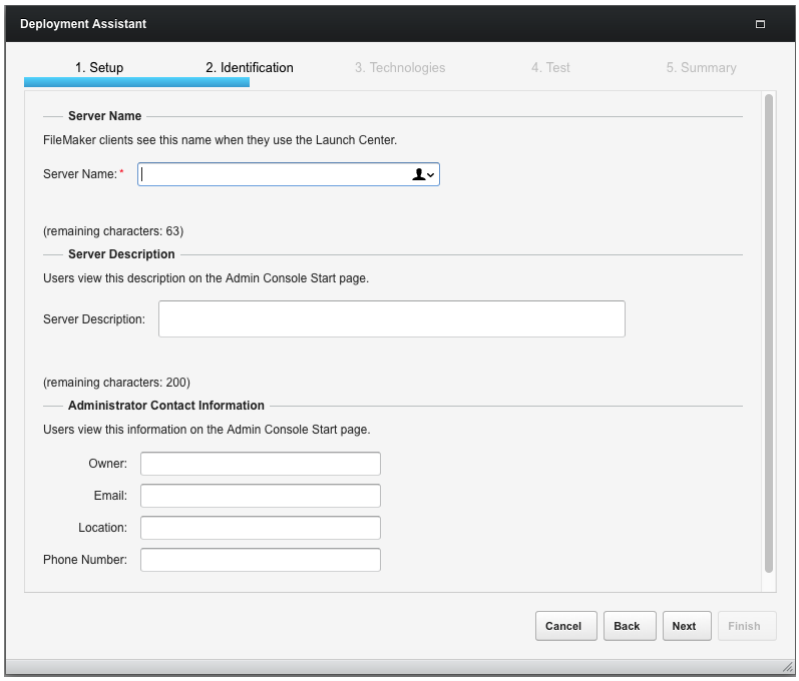
Enter a password hint that will help you remember the password. The hint is displayed on the Admin Console Login page after three failed attempts to enter the user name and password.

Enter a PIN value that can be used to reset the password using the command line interface (CLI).



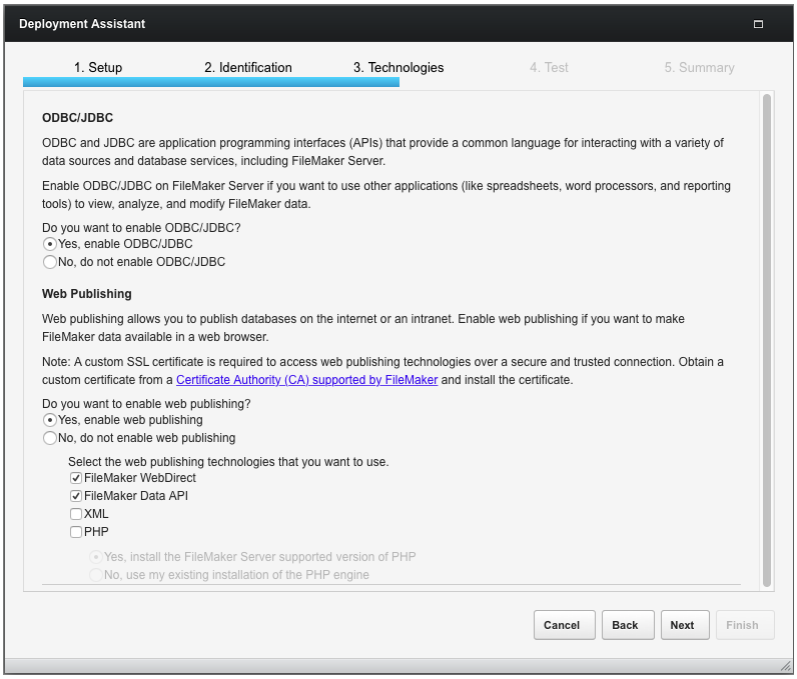
16. Specify a name, description, and contact information for this deployment of FileMaker Server. This information will appear on the FileMaker Server Admin Console Start Page. This information will also be included in the email when the FileMaker Server sends out warning or error notifications (see “Emailing notifications” on page 43).

    Server Name is displayed to FileMaker Pro and FileMaker Go users in the Launch Center.



17. To enable a hosted FileMaker Pro file to be a data source via ODBC and JDBC, click **Yes, enable ODBC/JDBC**.

Important This feature allows clients to use FileMaker files as data sources using ODBC and JDBC. This feature is not needed to host FileMaker Pro databases that access ODBC data sources. See FileMaker Pro Help.



18. To publish FileMaker data on the Internet or an intranet using FileMaker WebDirect, FileMaker Data API, or Custom Web Publishing, click **Yes, enable web publishing**. If you are not enabling web publishing, continue with step 21.

19. Select the web publishing technologies you want to use.

- If you enable the web publishing technologies, use SSL for database connections with a custom SSL certificate installed.
- You can install the FileMaker Server supported version of the PHP engine (see the FileMaker Server system requirements), or you can use your own PHP engine. If you already have a PHP engine installed and choose to use the FileMaker Server supported PHP engine, your currently installed PHP engine is disabled.
- If you use your own PHP engine, you must manually install the FileMaker API for PHP to use PHP publishing. See FileMaker Server Custom Web Publishing Guide.

20. If web publishing is enabled and the Deployment assistant successfully communicates with the web server, you see **The web server test was successful**.

If the Deployment assistant fails to communicate with the web server, see “Deployment assistant reports that the web server test failed” on page 32.

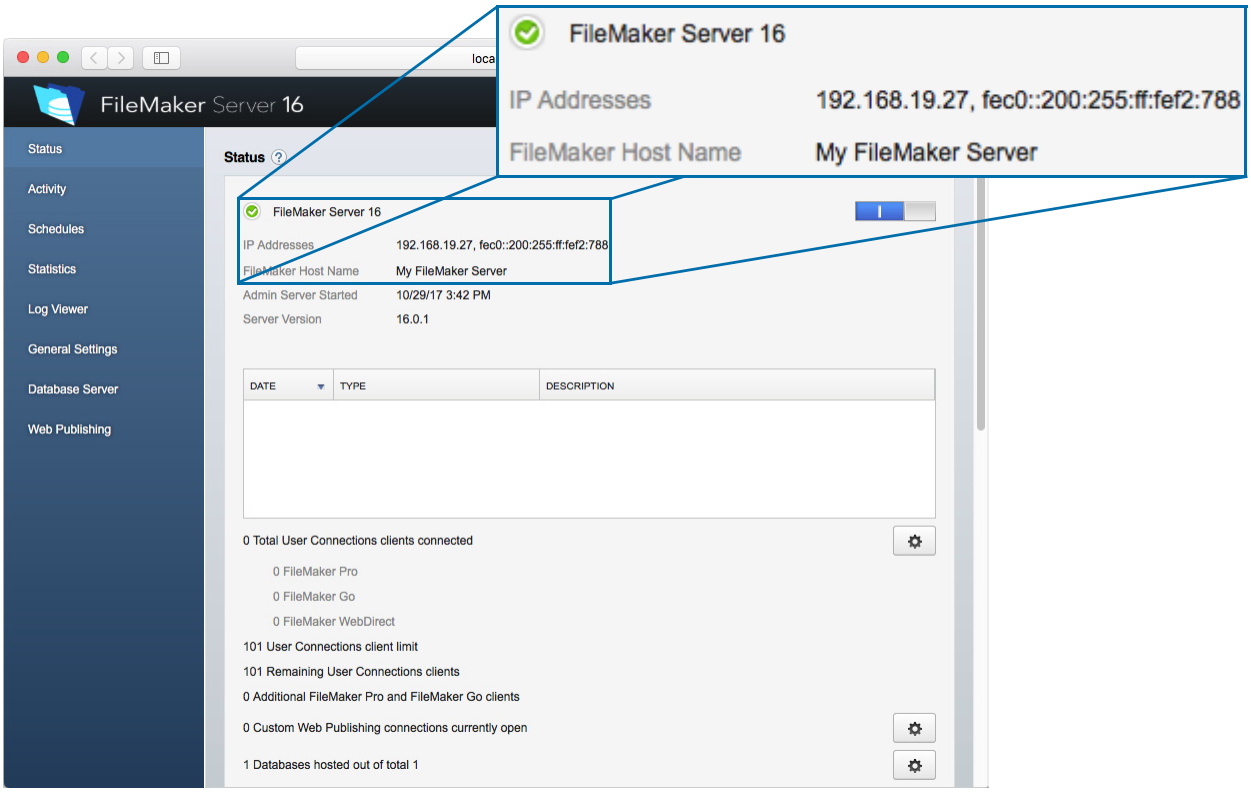
21. A deployment summary appears. Click **Next** to deploy or click **Back** to change any of your choices.

22. FileMaker Server deployment may take a few minutes. When deployment completes, click **Finish** to continue.

23. FileMaker Server Admin Console starts.

If you don't see FileMaker Server Admin Console, open a web browser and enter:
`http://localhost:16001/admin-console`

24. In the FileMaker Server Status pane, note the IP address of the server.



Tip Write down the IP address so that you can start Admin Console from another computer, if needed:

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

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

Next steps

Now that you have deployed FileMaker Server, get started using your new software.

1. Start Admin Console: See "Starting Admin Console" on page 36.

2. Test your installation: See chapter 4, "Testing your deployment."

3. Register your software: See "Customer support and Knowledge Base" on page 75.

4. Administer FileMaker Server: See chapter 5, "Administering FileMaker Server."

5. Upload databases: See "Uploading databases" on page 37.

Chapter 3
Deploying FileMaker Server across multiple machines

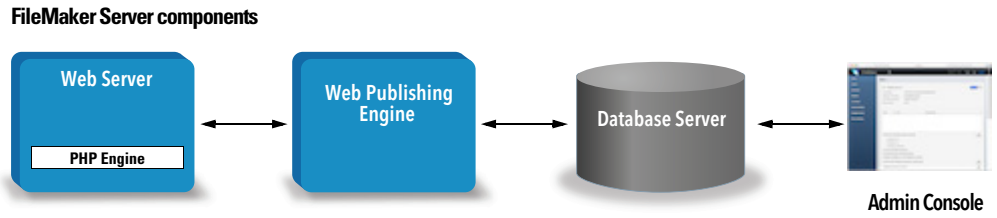
FileMaker Server allows you to add worker machines in a multiple-machine deployment to improve FileMaker WebDirect performance or to enhance the security of server components.

In many environments, a single-machine deployment provides sufficient performance for hosting FileMaker WebDirect solutions. However, if your server regularly has close to 100 FileMaker WebDirect clients, then you can deploy FileMaker WebDirect worker machines to allow additional clients to access FileMaker WebDirect solutions.

If you're not hosting FileMaker WebDirect solutions, you don't gain performance improvements from a multiple-machine deployment. But with a multiple-machine deployment, you can place the most sensitive data residing in the Database Server behind the firewall and give clients access to worker machines placed in front of the firewall.

Master machine components

The diagram below shows the major components of FileMaker Server.



- **Web Server**: in Windows, FileMaker Server requires Internet Information Services (IIS), which is enabled when you install FileMaker Server. In macOS, FileMaker Server uses its own instance of the Apache web server, so you do not need to enable the Apache instance that is installed as part of macOS.
- **Web Publishing Engine**: provides the Custom Web Publishing services and the FileMaker WebDirect services for databases hosted by FileMaker Server.
- **PHP Engine**: for Custom Web Publishing with PHP, FileMaker Server requires a PHP engine to respond to requests from the web server and to process PHP code. FileMaker Server includes a PHP engine and the FileMaker API for PHP. When PHP code calls the FileMaker API for PHP, those calls are interpreted and sent to the Web Publishing Engine.
- **Database Server**: hosts the databases that you share with FileMaker Pro and FileMaker Go users and publish on the web. In a multiple-machine deployment, the machine running the Database Server is called the *master* machine. See the description below.
- **Admin Console:** runs in a web browser on any client computer from which you want to configure and administer FileMaker Server.

In a single-machine deployment of FileMaker Server, these components are installed on one machine. In a multiple-machine deployment, these components are all installed on the master machine.

Worker machine components

In a multiple-machine deployment, you deploy FileMaker WebDirect worker machines that include only two components: a web server and the Web Publishing Engine.

The worker machine does not have an Admin Console. The master communicates with the worker to configure the settings on all machines and monitor the status and activity of all components.

The Web Publishing Engine on a worker machine does not include Custom Web Publishing services or the PHP engine; these components are on the master machine. However, a worker machine can handle these requests from users because it provides routing services.

Important To enhance the security of your database solution, especially when it is available on the Internet, use a firewall with your FileMaker Server deployment. Also use SSL for the web server. See FileMaker Security Guide.

Deployment options

You can first deploy on one machine and then add worker machines to accommodate more FileMaker WebDirect clients if the client load increases over time.

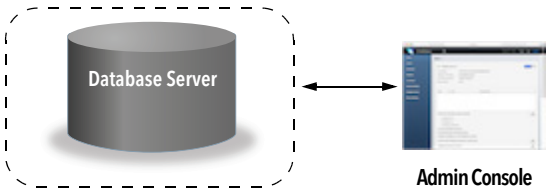
Single-machine deployment

You can deploy FileMaker Server on one machine in two ways: Database Server only or Database Server and Web Publishing Engine. For information on installing FileMaker Server in a single-machine configuration, see chapter 2, “Installation quick start.”

Database Server only

You can install FileMaker Server on one machine with web publishing disabled. With this type of deployment, you can serve FileMaker Pro, FileMaker Go, and ODBC/JDBC clients but not FileMaker WebDirect, FileMaker Data API, or Custom Web Publishing clients.

Benefits: This is the easiest deployment to set up and administer if you don't need web publishing.



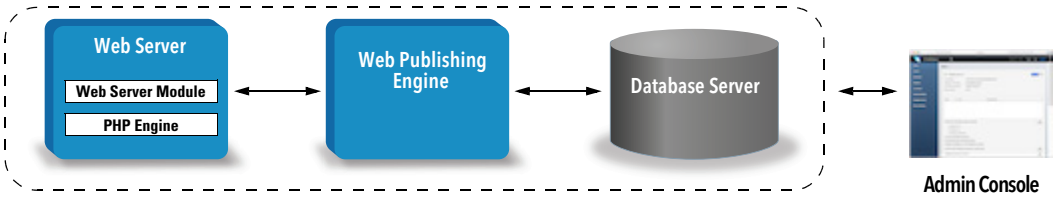
Ports 80 and 443 must be open (or alternative ports specified during installation).
Ports 5003 and 16000 must be open.
Port 2399 must be open to support ODBC and JDBC clients.
Ports 1895, 5013, 16001, 16004, 50003, and 50004 must be available.

Note Even when web publishing is disabled, FileMaker Server requires a web server to host the web-based Admin Console application and to handle some data transfer tasks.

Database Server and Web Publishing Engine

You can install Database Server, the Web Publishing Engine, and all of the associated software components on the same machine as the web server.

Benefits: This is the simplest deployment with web publishing and the one that most FileMaker Server users will use. This configuration is suitable for small deployments (up to 50 FileMaker Pro and FileMaker Go clients combined) and limited web publishing.



Ports 80 and 443 must be open (or alternative ports specified during installation).
Ports 5003 and 16000 must be open.
Port 2399 must be open to support ODBC and JDBC clients.
Ports 1895, 3000, 5013, 8998, 9889, 9898, 16001, 16002, 16003, 16004, 16020, 16021, 50003, and 50004 must be available.

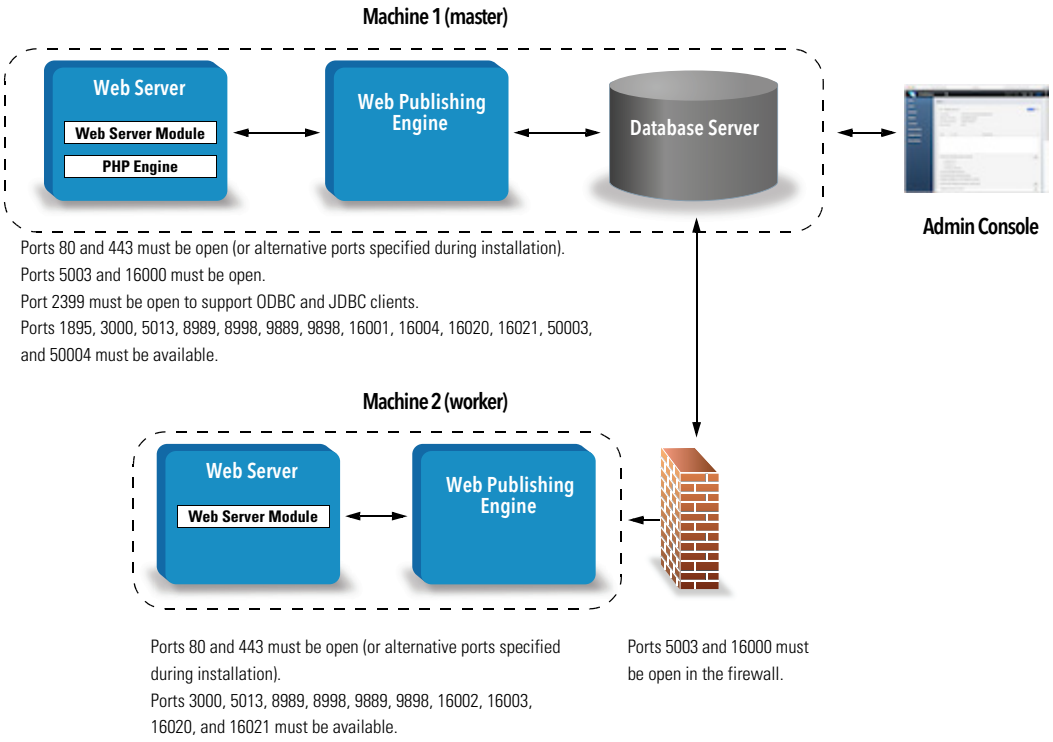
Multiple-machine deployment

You can deploy FileMaker Server on a master machine and then deploy additional FileMaker WebDirect worker machines as needed depending on the number of FileMaker WebDirect clients you want to serve.

Benefits: Under normal circumstances, a single-machine deployment can only accommodate up to 100 FileMaker WebDirect clients. Each worker machine can accommodate an additional 100 FileMaker WebDirect clients.

You can also enhance the security of your deployment by placing the master machine behind a firewall and placing a worker machine in front of the firewall. When a worker machine receives FileMaker Data API and Custom Web Publishing requests, they are proxied through the worker machine to the master machine. FileMaker WebDirect requests are redirected based on the number of worker machines installed.

Tip To best accommodate FileMaker WebDirect clients, consider the design of FileMaker WebDirect solutions. See “Considering database performance” on page 62.



Installing on multiple machines

For a multiple-machine deployment, you install FileMaker Server software on each machine. Install the FileMaker Server software first on the master machine and then on the worker machines. Then use the Deployment assistant on the worker machine to configure the SSL certificate and to connect to a master machine.

Before you begin installing on multiple machines

- Ensure that no existing websites on the master or worker machines use port 80 or 443, or be prepared to enter alternative ports. These ports are used by FileMaker Server on both machines. If the FileMaker Server installer detects an existing website using these ports, the installer prompts you to let it disable that website or to specify alternative ports.
  - Windows: The FileMaker Server installer enables the IIS web server if it isn't already enabled, then runs the Microsoft Application Request Routing (ARR) installer, creates its own website in IIS, and configures the website to use the ports specified for web connections.
  - macOS: The web server included in macOS does not need to be enabled. If it is enabled, ensure that no existing website uses port 80 or 443, or be prepared to specify alternative ports during installation. The installer creates a separate web server instance and enables it for FileMaker Server to use on these ports.

    See chapter 7, "Setting up the web server."
- When you're running FileMaker Server in an environment that uses a firewall, be sure to configure the firewall on each machine to allow FileMaker Server to use ports as indicated in "Ports used by FileMaker Server" on page 22. Restart each machine after configuring the firewall.

- To upgrade from an earlier version of FileMaker Server, see chapter 6, “Upgrading or moving an existing installation.”
- If you already have a single-machine deployment of FileMaker Server 16, you can add a worker machine to your existing deployment. To add a worker machine, install FileMaker Server on the worker (see “Installing on a worker machine” on page 23). Then in the Deployment assistant on the worker machine, connect to the existing server, which becomes the master machine.
- Locate your license key. See “About the license key” on page 7.
- If you are currently running FileMaker Pro on the same machine, you must quit FileMaker Pro before installing FileMaker Server.

Also keep in mind the following:

- If the machine has antivirus software installed, you may need to disable or uninstall it before running the FileMaker Server installer. Don’t enable antivirus software again until after the Deployment assistant has finished.

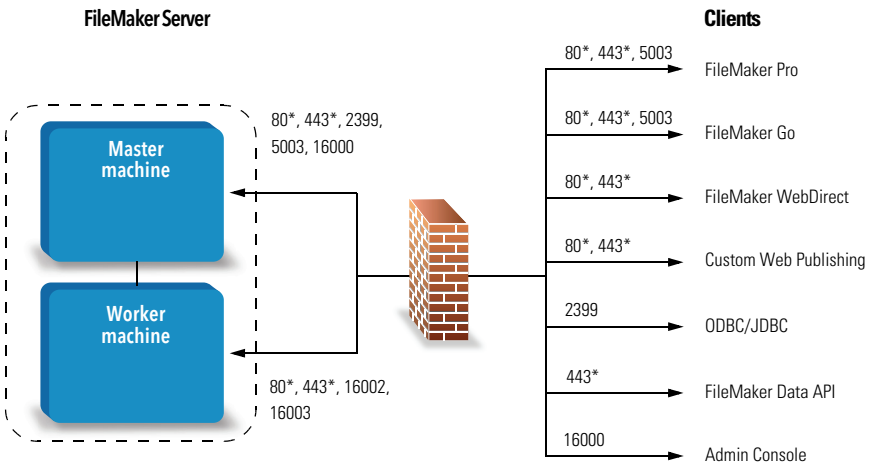
  Do not allow antivirus software to scan the folders that contain hosted database files or the folders that contain files for container fields that store data externally.
- You cannot run two different versions of FileMaker Server on the same machine at the same time.
- Because some DHCP servers cycle IP addresses, FileMaker, Inc., recommends using a static IP address.
- macOS: Avoid using the macOS Server application to enable any HTTP services while running FileMaker Server. HTTP services provided by macOS Server may interfere with FileMaker Server. See “Using the Apache web server in macOS” on page 57.

Ports used by FileMaker Server

When running FileMaker Server in an environment that uses a firewall, be sure to configure the firewall on each machine to allow FileMaker Server to communicate. For a complete list of ports, see the FileMaker Knowledge Base.

Note Not all of the ports listed need to be open to end users or between all machines or end users indicated in the “Used by” column in a FileMaker Server deployment. Ports marked “Available” are used locally on the machine indicated in the “Used by” column; these ports must not be used for anything else but do not need to be opened in a firewall.

The following illustration shows the ports that must be open in a firewall in order for FileMaker clients and Admin Console to communicate with FileMaker Server.



Installing on the master machine

Install FileMaker Server on the master machine first, then on the worker machines. The instructions for installing on the master machine are the same as on a single machine. See “Installing FileMaker Server on a single machine” on page 11.

Installing on a worker machine

After installing FileMaker Server on the master machine, install FileMaker Server on the worker machines. A FileMaker Server deployment can have up to five worker machines. The following process adds one worker machine to a master machine. Follow the same process for each worker machine you want to add to your deployment.

Note If you set up a machine as a worker and want to change it to a master, uninstall and then reinstall FileMaker Server.

1. Follow your electronic download instructions to download and open the installation disk image, or insert your product DVD.
2. Windows: If you have Bonjour for Windows installed, make sure that it is running before you run the FileMaker Server installer.
3. Double-click the installation icon.


Setup (Windows)


FileMaker Server (macOS)

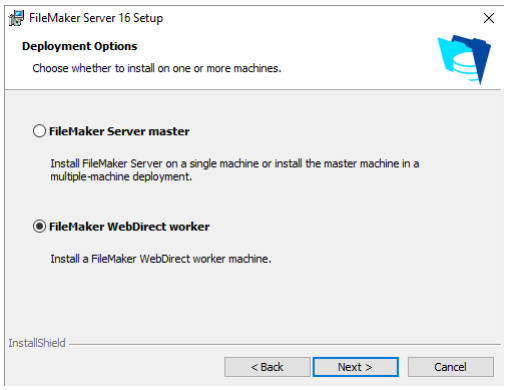
- Windows: If a User Account Control alert appears, click **Yes**.
- macOS: If a security message appears, click **Continue**.

4. Windows: Select a language.

5. To continue with installation, click **Next** (Windows) or **Continue** (macOS).
6. Read the important information displayed. If there is a task you did not do, quit the installer and do the task.
7. Review and accept the end user license agreement.
8. Select the installation destination.

   Note In Windows, you can select a non-default location. See “Installation notes” on page 28.

9. Select **FileMaker WebDirect worker**.



10. Specify the ports that FileMaker Server should use for web connections and secure web connections.

    Windows: If the installer detects that the ports required for the web server are currently in use, the installer prompts you to let it disable the website currently using those ports. To continue installation, you must click **Disable Websites**. Or you can click **Cancel**, disable the website manually, then run the installer again.

    macOS: If the installer detects that the ports required for the web server are currently in use, the installer lets you know which ports are in use. You can either make the ports available on your system or choose different ports.

11. Click **Install**.

- Windows:

  If you do not have the Microsoft Visual C++ 2015 Redistributable Package (x64) or a minimum update of Java Runtime Environment version 8, the FileMaker Server installer installs them. If you do not have the Microsoft Application Request Routing (ARR) extension for IIS installed, the FileMaker Server installer installs it.

  If you do not have Bonjour for Windows installed, you are prompted to allow the FileMaker Server installer to install it. Follow the onscreen instructions.

  See “Installation notes” on page 28.

- macOS:

  If you do not have a minimum update of Java Runtime Environment version 8 installed, the FileMaker Server installer installs it. If Bonjour is not running, you are prompted to run it.

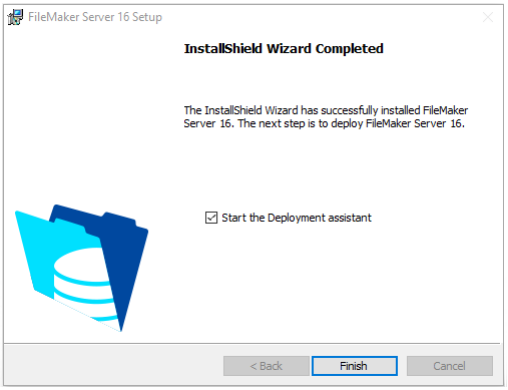
  For information about Java and Bonjour installation, see “Installation notes” on page 28.

  FileMaker Server begins to install. This process may take several minutes.

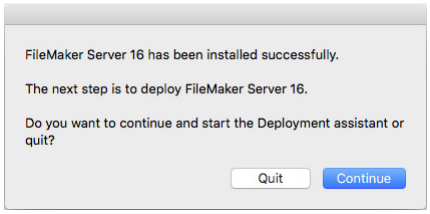
12. After the software has been successfully installed, start the Deployment assistant.

- Windows: In the last step of the installer, select **Start the Deployment assistant**, then click **Finish**.
- macOS: Click **Continue**.

If necessary, see “Deployment Assistant doesn’t start after installation on the worker” on page 33.



Windows

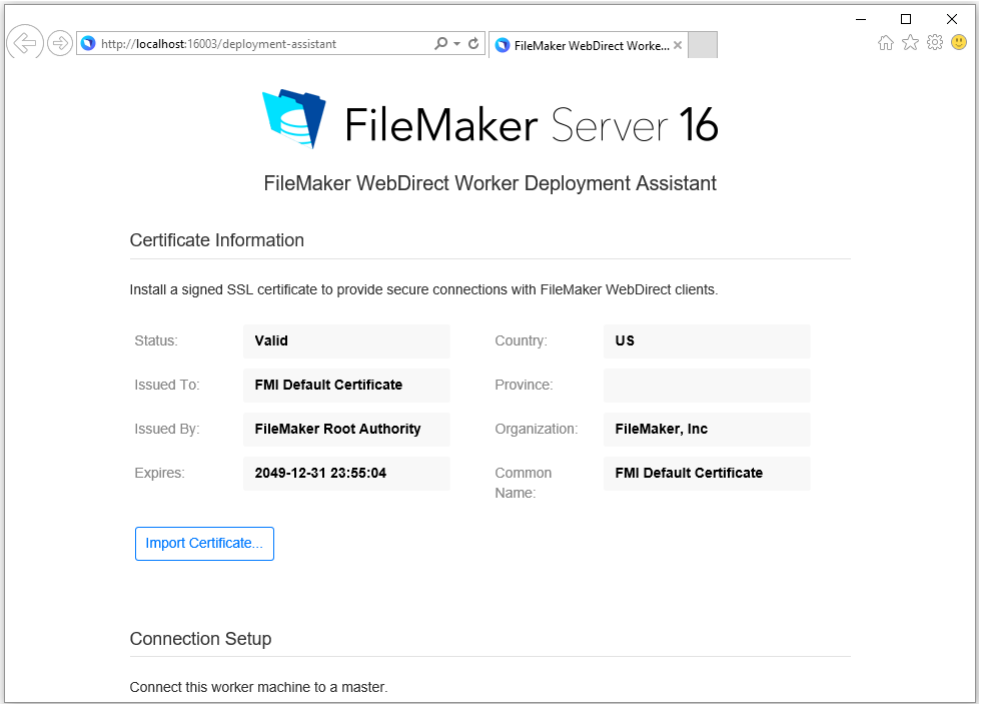


macOS

You can stop now and start the Deployment assistant later. To deploy FileMaker Server at a later time:

- Windows: For Windows versions with the Start button, click the **Start** button > **All Programs** > **FileMaker Server** > **FileMaker WebDirect Worker Deployment Assistant**. For Windows versions with the Windows Start screen, click **FileMaker WebDirect Worker Deployment Assistant**.
- macOS: Double-click the **FileMaker WebDirect Worker Deployment Assistant** shortcut on the desktop.
- Enter `http://localhost:16003` into a web browser on the worker machine.

13. For **Certificate Information**, verify that a signed SSL certificate is installed or click **Import Certificate** to install a signed SSL certificate.

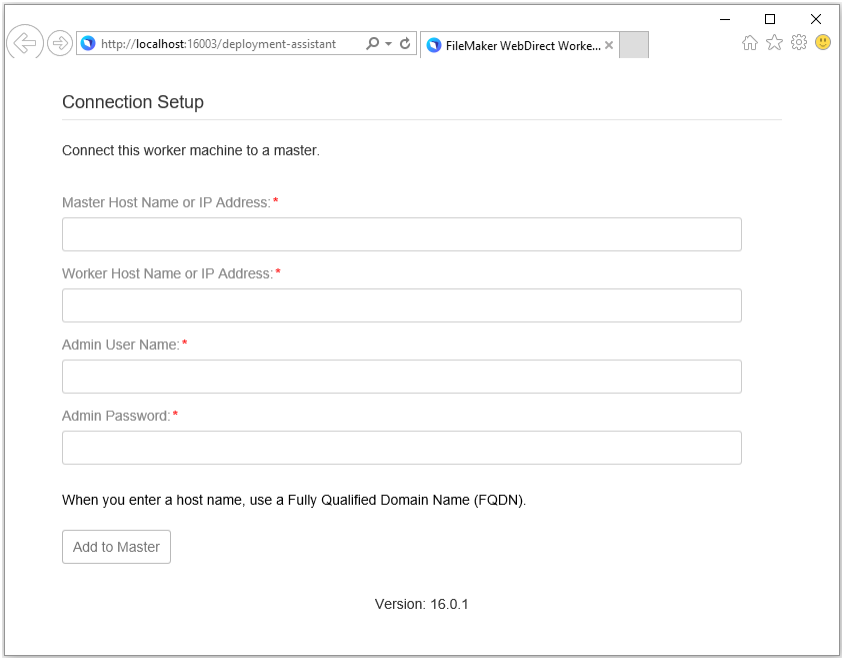


If **Issued To** indicates “FMI Default Certificate,” then you are using the FileMaker default certificate that does not verify the server name. This certificate is intended only for test purposes. A custom SSL certificate is required for production use. See “Requesting an SSL certificate” on page 53.

When you have a custom SSL certificate, click **Import Certificate** to install the custom SSL certificate on the worker machine.

14. For **Connection Setup**, enter:

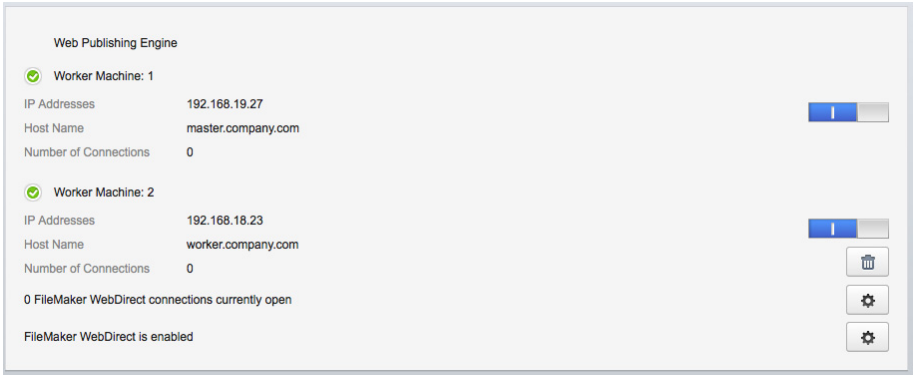
- the master machine's host name or IP address. If you use a host name, it should be the fully qualified host name specified in the custom SSL certificate installed on the master machine.
- the worker machine's host name or IP address. If you use a host name, it should be the fully qualified host name specified in the custom SSL certificate installed on the worker machine.
- the server administrator user name and password that you use to log in to Admin Console on the master machine



Notes

- To change the host name on the master machine, disconnect all worker machines, redeploy the master machine, then enter the new host name when you connect worker machines.
- To change the host name of a worker machine, remove it from the master machine, change the host name, then reconnect it to the master machine.
- If a worker machine is connected to the master machine using an IP address, redirects to the master machine will use an IP address. If a worker machine is connected to the master machine using a fully qualified domain name, redirects to the master machine will use a fully qualified domain name.
- Make sure you have completed the Deployment assistant steps for the master machine before connecting a worker machine. Do not connect a worker machine to a master machine that has been installed but not deployed.

15. Click **Add to Master** to connect the worker machine to the master machine. When you see a message that the worker is successfully connected, the worker has been added to the master machine. You can verify the connection in the **Web Publishing Engine** section of Admin Console on the master machine.



Notes

- If you are using the FileMaker default certificate or a certificate that does not verify the server's host name, you may see an error message. To allow the unverified certificate, select **Connect using the unverified certificate** and click **Add to Master** again.
- If you receive an error saying that the connection timed out, verify that the worker machine has network access to the master machine.

Installation notes

- For information on the versions of supporting software that are required, see the FileMaker Server system requirements.
- Windows: You can install FileMaker Server in a non-default location including a non-boot volume, but not on remote network drives or external removable drives. You cannot install FileMaker Server to a Windows Desktop path, for example [drive]:\Users\[user]\Desktop.

  The path you specify replaces the beginning of the default installation path, \Program Files\FileMaker\
  FileMaker Server. For example, if you specify the My_Path installation folder, the Databases, Scripts, and Extensions folders are installed as follows:
  - \My_Path\Data\Databases
  - \My_Path\Data\Scripts
  - \My_Path\Database Server\Extensions
- macOS: Do not install FileMaker Server on a target volume that is formatted as a Mac OS Extended (Journaled, Case-Sensitive) volume. This format is not supported. Format the volume as Mac OS Extended or Mac OS Extended (Journaled) instead.

- During installation, if you specify a FileMaker Server user account other than the default, the specified account must meet the following requirements:
  - Windows: The account must be either a local user account or a Windows domain account. The account must have the same privileges as the Windows system account for local file access. If you set up additional database or container data folders on remote volumes, the account must also have full permissions to access these remote folders.
  - macOS: The account must be a local user account in macOS and have the same permissions as the fmserver account for local file access (including membership in the daemon group). The account must not be from a directory service (for example, Active Directory or Open Directory). If you set up additional database or container data folders on remote volumes, the account must also have full permissions to access these remote folders.
- Bonjour installation:
  - Windows: Bonjour is optional. If Bonjour is not installed, the server cannot be displayed to FileMaker Pro or FileMaker Go users in the Launch Center.
  - macOS: If Bonjour is not installed and enabled, then you cannot install FileMaker Server.
- FileMaker Server requires the 64-bit version of the Java Runtime Environment on master and worker machines.
- Windows: FileMaker Server requires the Microsoft Application Request Routing (ARR) extension for IIS.
- Windows: Do not uninstall the following while FileMaker Server is installed:
  - IIS URL Rewrite Module
  - Microsoft Application Request Routing
  - Microsoft External Cache for IIS
  - Microsoft Visual C++ 2015 Redistributable Package (x64)

Next steps

Now that you have deployed FileMaker Server, get started using your new software.

1. Start Admin Console: See “Starting Admin Console” on page 36.

2. Test your installation: See chapter 4, “Testing your deployment.”

3. Register your software: See “Customer support and Knowledge Base” on page 75.

4. Administer FileMaker Server: See chapter 5, “Administering FileMaker Server.”

5. Upload databases: See “Uploading databases” on page 37.

Chapter 4
Testing your deployment

Using the FileMaker Server Technology Tests page

The easiest way to test your FileMaker Server deployment is to use the FileMaker Server Technology Tests page.

There are three ways to view the Test page:

- Start Admin Console. Choose **Server** menu > **Open Test Page**.

  If you see a message that a pop-up was blocked, disable pop-up blocking for this website in your web browser.

- Open the Test page by typing the following in a web browser:

  `https://[host]:16000/test`

  where [host] is the IP address or host name of the master machine.

- Open the Start page by typing the following in a web browser:

  `https://[host]:16000`

  Then click the **FileMaker Server Technology Tests** link under the **Troubleshooting** heading on the Admin Console Start Page.

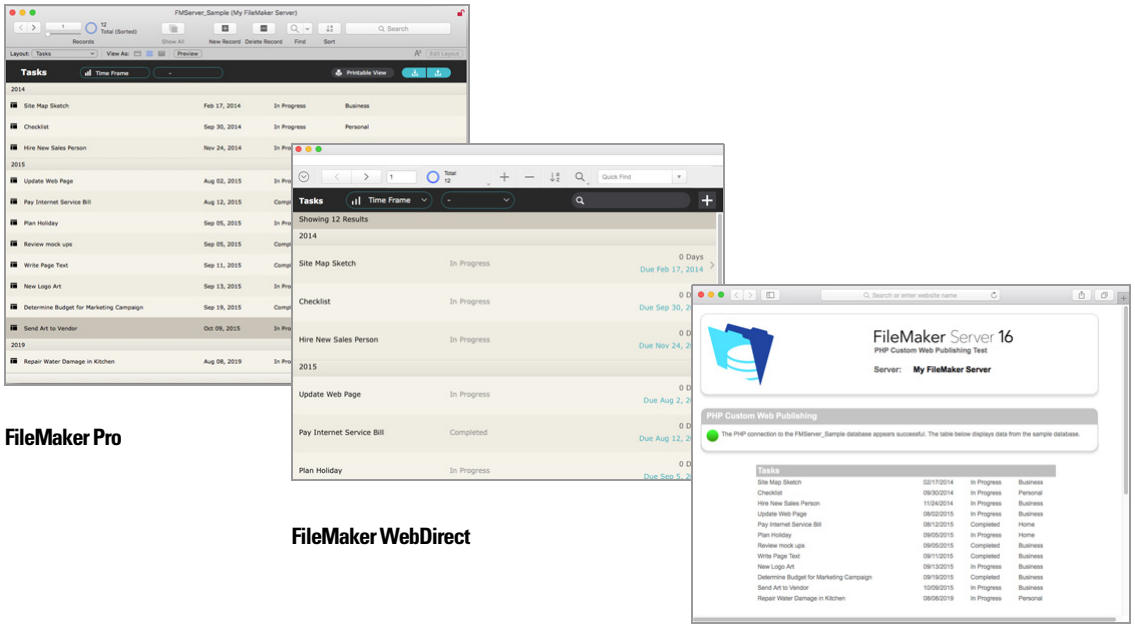
Note You can use the Technology Tests page without logging in to Admin Console.

FileMaker Server Technology Tests page

The tests on the FileMaker Server Technology Tests page access the sample database (FMServer_Sample.fmp12) using FileMaker Pro or one of the web publishing technologies.

To test	Do this
FileMaker Pro	Click **Test FileMaker Pro**. If FileMaker Pro starts and opens the sample database hosted on FileMaker Server, then the Database Server is working and responding to requests from FileMaker Pro clients. You must have FileMaker Pro or FileMaker Pro Advanced installed locally on the machine where you are conducting the test. To perform the same test another way, start FileMaker Pro on another machine, choose **File** menu > **Open Remote**. In the Launch Center, click the **Hosts** tab and select the server you want to test, and select **FMServer_Sample**.
FileMaker WebDirect	Click **Test FileMaker WebDirect**. If another web browser window or tab opens and displays the sample database, then FileMaker WebDirect is working. If successful, this test shows that the Database Server, Web Publishing Engine, and web server are working.
Custom Web Publishing with PHP	Click **Test PHP Custom Web Publishing**. If another web browser window or tab opens and displays a table containing data from the sample database, then Custom Web Publishing with PHP is working. If successful, this test shows that the Database Server, Web Publishing Engine, web server, PHP engine, and FileMaker API for PHP are working.

Successful test pages



Custom Web Publishing with PHP

Troubleshooting

Deployment assistant reports that the web server test failed

If the Deployment assistant cannot communicate with the web server, you will receive an error message.

To confirm web server settings:

1. In the Test step in the Deployment assistant, confirm the **Protocol**, **Host address**, and **Port** for the web server and click **Retry**.

   You may encounter this during initial deployment or when you click **Server** menu > **Edit Server Deployment**.

2. Examine the **Web Server Test Results**.
   - Successful: the result is **Web Server Test Passed**.
   - Unsuccessful: the Deployment assistant could not communicate with the web server. Make sure that you can access the web server using a web browser from the master machine. To try to communicate with the web server again, click **Retry**.
   - Still unsuccessful after retry: you can disable web publishing for now so that you can complete the Deployment assistant. To disable web publishing, click **Back** until you reach the Technologies step, then click **No, do not enable web publishing**.

Deployment assistant doesn't start after installation on the master

If the Deployment assistant doesn't start on the master machine after you run the FileMaker Server installation program, the most common solutions are:

- On the master machine, start the Deployment assistant by double-clicking the **FMS Admin Console** shortcut on the desktop or entering `http://localhost:16001` in a web browser.
- Windows: On the master machine, ensure that IIS is enabled (see chapter 7, "Enabling the IIS web server in Windows"). In IIS Manager, check that the site named FMWebSite has started.
- 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 Start page is not available.

  If you see this message:

  1. Restart the Admin Server process by entering the following command in a command prompt (Windows) or the Terminal application (macOS):

  ```
  fmsadmin restart adminserver
  ```

  2. In Windows, stop and then restart the FileMaker Server service in the **Administrative Tools** > **Services** control panel.

  3. If your server computer has a firewall, make sure all required ports are open in the firewall. (See "Before you begin" on page 9.)

4. If your machine is running slowly, shut down any unnecessary applications.

5. Restart your machine. Open a web browser on the master machine and enter `http://localhost:16001`.

Deployment Assistant doesn't start after installation on the worker

If the Deployment assistant doesn't start on the worker machine after you run the FileMaker Server installation program:

- On the worker machine, start the Deployment assistant by double-clicking the **FileMaker WebDirect Worker Deployment Assistant** shortcut on the desktop or entering `http://localhost:16003` in a web browser.

Admin Console doesn't start after deployment on master machine

The most common solutions are:

- On the Admin Console Start Page, click **Start Admin Console**.
- Open a web browser on the master machine and enter `http://localhost:16001`.

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 port in the URL:

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

  Admin Console always uses an HTTPS connection on port 16000 from remote machines. You can also use `http://[host]/admin-console`, which works because it is redirected to HTTPS on port 16000. See "Starting Admin Console" on page 36.
- If the master machine has a firewall enabled, open the ports required by FileMaker Server to communicate with users and administrators. For open ports required by a single-machine deployment, see "Before you begin" on page 9. Otherwise, see "Before you begin installing on multiple machines" on page 21.

Web browsers display a certificate message

Most web browsers display a certificate error or warning message when you use an HTTPS connection to go to any web page hosted by the FileMaker Server web server. This includes Admin Console, the Start Page, and any FileMaker WebDirect or Custom Web Publishing solution that uses an HTTPS connection. Displaying this message is expected behavior if your FileMaker Server deployment uses the 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" on page 53.

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 begin” on page 9 and “Before you begin installing on multiple machines” on page 21 for information on which ports need to be unblocked in firewalls.

Use FileMaker Pro 14, 15, or 16 and FileMaker Go 14, 15, or 16 to open files that are hosted by FileMaker Server 16. Make sure users have applied the most recent update of their client software.

Apache web server used by FileMaker Server stops responding (macOS)

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

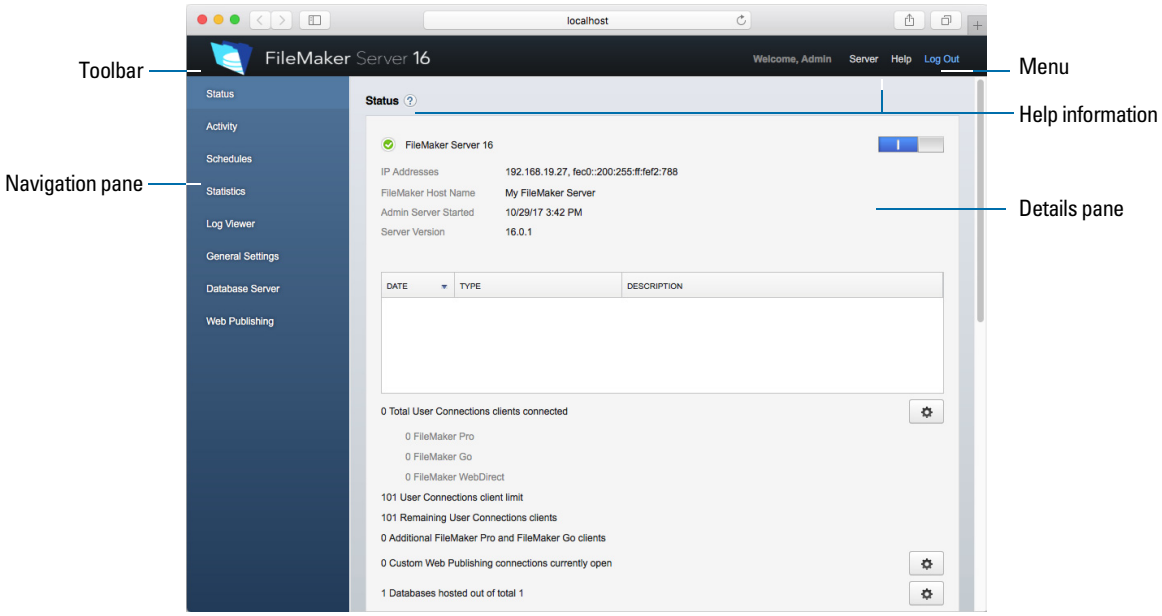
Chapter 5
Administering FileMaker Server

For detailed information about using Admin Console to administer FileMaker Pro databases and clients that are connected to hosted databases, see FileMaker Server Help.

About FileMaker Server Admin Console

FileMaker Server Admin Console is a web-based application that lets you configure and administer FileMaker Server, work with and monitor hosted databases and clients, and track statistical information.

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.



FileMaker Server Admin Console

Note If you click the Back, Forward, or Refresh (or Reload) button in your browser, Admin Console exits and the Login page is displayed. Any unsaved changes in Admin Console are lost, and you must log in again.

Using Admin Console to administer FileMaker Server

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

- configure FileMaker Server application properties
- open—or host—a FileMaker Pro database file, making it available to clients on the network
- view information about the files being hosted, like the number of clients accessing each database

- view database statistics in a table or graph
- 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
- delegate database administration tasks to group administrators, use a Group Launch Center to list the databases used by an administrator group
- 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
- configure Custom Web Publishing settings for XML or PHP

See FileMaker Server Help.

Starting Admin Console

Note To use Admin Console, your remote computer needs only a supported web browser; no additional runtime environments or browser plug-ins are required. See “Requirements for Admin Console” on page 6.

To start Admin Console:

1. Open a web browser and enter:

   `https://[host]:16000`

   where `[host]` is the IP address or host name of the machine running FileMaker Server as a master. This is the address you noted when you installed FileMaker Server.

2. Before the Admin Console Start Page appears, your web browser may require you to respond to a security message. This is normal behavior for the certificate that is included with FileMaker Server. Click the option to continue to go to the Start Page.

   To prevent this message in the future, see “Requesting an SSL certificate” on page 53.

   Tip Bookmark the Start Page in your web browser. Come back to this page to access documentation and other resources.

3. Click **Start Admin Console**.

4. On the Login page, enter the name and password that you chose in the Deployment assistant when you initially deployed FileMaker Server. Click **Log In**.

   Note If your web browser prompts you to save your user name and password, you should decline unless you are sure that access to your web browser is secure.

   Admin Console starts and displays the FileMaker Server Status pane. The following are alternate ways to start Admin Console directly:

To access Admin Console from	Go to
Any computer with network access to the master machine	https://[host]:16000/admin-console http://[host]/admin-console (redirects to HTTPS)
Master machine only	http://localhost:16001/admin-console FMS Admin Console shortcut: ▪ Windows: For Windows versions with the Start button, click the **Start** button > **All Programs** > **FileMaker Server** > **FMS Admin Console**. For Windows versions with the Windows Start screen, click **FMS Admin Console**. ▪ macOS: Double-click the **FMS Admin Console** shortcut on the desktop.

Uploading databases

FileMaker provides two ways to upload databases to FileMaker Server:

- In FileMaker Pro, use **File** menu > **Sharing** > **Upload to FileMaker Server** 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 database files along with any externally stored container field objects. FileMaker Server copies the database files to the specified database folder and sets file permissions and privileges so that you can access the databases after they are uploaded.
- Manually upload database files to FileMaker Server. You must copy the database files and any externally stored container field objects to the proper location. In macOS, change the files' group ownership to belong to the fmsadmin group. 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 Advanced, you can use the database encryption feature to encrypt the contents of a database file. Encryption protects the FileMaker database file and any temporary files that are written to disk. See FileMaker Pro Help.

When you use the database encryption feature, it encrypts the database content by combining the database file's encryption password and a randomly generated, universally unique identifier (UUID), also known as a *salt*. This unique encryption password encrypts the data when it is stored on disk so if someone steals a copy of the database, the database's contents can't be viewed.

Encrypting databases in FileMaker Pro Advanced

In FileMaker Pro, you can restrict user actions while a database is open by setting the user's privileges in the file. To protect the database when it is stored on disk, use the database encryption feature in Developer Utilities (FileMaker Pro Advanced). You can also decrypt or reencrypt a FileMaker database file with Developer Utilities. See FileMaker Pro Help.

To host an encrypted database file on FileMaker Server for FileMaker clients, you can manually upload the database to FileMaker Server or use the **Upload to FileMaker Server** menu command in FileMaker Pro to transfer the file. In either case, you must open an encrypted database using Admin Console or the `fmsadmin` command line interface (CLI). See FileMaker Server Help.

Opening encrypted databases

You can open an encrypted database that is hosted on FileMaker Server by using Admin Console or a CLI command. When you open the encrypted file from Admin Console, the encryption password dialog box displays and you must enter the password. Because you opened the database, FileMaker clients don't need the encryption password to access that database. See FileMaker Server Help.

Note Use the `list` command to check whether a database is encrypted.

Backing up databases

FileMaker, Inc., recommends that you back up your hosted databases. FileMaker Server provides two ways for you to perform database backups:

- **Scheduled backups.** With scheduled backups, you use the Schedule assistant to create a scheduled task that defines which databases are backed up, and how often the databases are backed up. Every time the scheduled task 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 backups.** With progressive backups, FileMaker Server starts by creating a full backup of all hosted databases. After the initial full backup is complete, FileMaker Server subsequently copies just the changed blocks from the hosted file to the backup folder, on a frequency based on what you specify for the save interval setting. Because the subsequent progressive backup copies only the blocks that have changed during the save interval, the progressive backup can run much more quickly than a scheduled backup, with less impact on Server performance.

If your database uses container fields that store data externally, you can specify whether to back up the container file folders. By default the container folders are not backed up. See FileMaker Server Help.

You can use both scheduled backups and progressive backups to ensure a comprehensive backup strategy for your hosted databases. When FileMaker Server backs up an encrypted database, the backup is also encrypted.

Note If you use Time Machine in macOS, exclude FileMaker Server folder items from the Time Machine backup. Use FileMaker Server Admin Console to back up your database files.

Scheduling database backups

Use the FileMaker Server Schedule assistant to create a scheduled task to:

- back up all hosted databases
- back up hosted databases that are in a specified folder
- back up a specified database

To create a scheduled task for backing up databases, choose the Admin Console **Schedules** pane, click , and choose **Create a Schedule**. Then, choose **Back up databases**, and specify whether you want to back up hourly, daily, weekly, or on a custom schedule. You can also select the maximum number of database backups you want to keep for a scheduled backup.

Database backups are saved in the default backup folder or in a folder that you specify. You can specify the default backup folder on the Admin Console **Database Server** > **Folders** tab.

Note If you are backing up a database to a volume that supports Windows ReFS, see “Creating a backup to a Windows ReFS volume” on page 39.

When FileMaker Server backs up a database, it copies the database while it is active. Users can continue to make modifications. When the copy is complete, the database is paused to synchronize backup files with the current database and then the database is resumed. You can set options to verify the backup, save a clone of the database without the data, and send email notifications to clients.

Using progressive backup

To enable progressive backup and specify the folder for progressive backup files, choose the Admin Console **Database Server** > **Folders** tab. For **Progressive Backup Folder**, select **Enable progressive backups**. Enter the number of minutes for **Save interval**, and enter the location of the progressive backup folder.

Specifying backup locations

Although you can specify remote volumes for the additional database folders and the container folders, you can’t specify a backup folder on a remote volume for a scheduled backup or a progressive backup. The backup locations must be on a drive connected directly to the master machine running FileMaker Server.

After the backup files are created, you can copy the backup files to a remote volume.

Creating a backup to a Windows ReFS volume

FileMaker Server can make full backups on any local volume that supports Windows Resilient File System (ReFS); however, the backup process may take more time and require more disk space.

Note Creating backups on remote volumes, including remote ReFS volumes, is not supported. The ReFS volume must be a local volume. See FileMaker Server Help.

When backing up a database, FileMaker Server checks if the backup volume uses ReFS. If the file is not being backed up to a ReFS volume, FileMaker Server checks if the selected databases have changed since the last time that scheduled backup ran. For each scheduled backup task, FileMaker Server creates a full copy of the databases that have changed and creates hard links to the backed up databases without any changes.

Because ReFS doesn't support hard links, FileMaker Server must create a full backup even if the hosted database file is identical to the most recent backup file.

Verifying the integrity of databases

Use the FileMaker Server Schedule assistant to create a scheduled task to:

- verify all hosted databases
- verify hosted databases that are in a specified folder
- verify a specified database

To create a scheduled task for backing up databases, choose the Admin Console **Schedules** pane, click  , and choose **Create a Schedule**. Then, choose **Verify databases**, and specify how often you want to verify the databases.

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 file. 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.

Enabling ODBC data source single sign-on (Windows)

If you work with FileMaker Pro databases hosted by FileMaker Server that access ODBC data from Microsoft SQL Server, you can configure the master machine to enable single sign-on (SSO). ODBC data source single sign-on allows FileMaker Pro clients to use their Windows-authenticated login credentials and permissions to access Microsoft SQL Server without logging in.

To enable ODBC data source single sign-on with FileMaker Server, you must configure the FileMaker Server service on the master machine to log in using the privileged user account. That is, this user account must have the **Impersonate a client after authentication** privilege enabled, and the account must be an Administrator account and configured in Windows Active Directory on the network.

Important Before you can enable ODBC data source single sign-on, your Windows domain administrator must:

- Configure the **Account is trusted for delegation security** setting for each user's Windows user account.
- Configure the **Trust this user for delegation** and **Use Kerberos only** security settings for the privileged user account on the master machine.
- Enable the **Impersonate a client after authentication** privilege for the privileged user account on the master machine.
- Configure the ODBC DSN to use **Windows authentication** on the master machine.
- Configure Microsoft SQL Server to use **Windows authentication**.

To enable ODBC data source single sign-on on the master machine:

1. Open **Control Panel** > **Administrative Tools** > **Services** > **FileMaker Server**, then choose **Action** > **Properties**.
2. On the **Log On** tab, choose **This account**.
3. For **This account**, enter the privileged user account on the master machine, then click **OK**.
4. Open **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Local Policies** > **User Rights Assignments** > **Act as part of the operation system**.
5. On the **Local Security Setting** tab, click **Add User or Group**, then enter the privileged user account you specified earlier for **This account**.
6. Click **OK**, then restart the FileMaker Server service.

Important You must also enable ODBC data source single sign-on in the FileMaker Pro databases hosted by FileMaker Server. See FileMaker Pro Help.

Running server-side scripts

You can create scheduled tasks to run:

- system-level scripts—for example, Windows batch, 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

To create a scheduled task for scripts, choose the Admin Console **Schedules** pane, click  , and choose **Create a Schedule**. Then, choose **System-level script**, **FileMaker script**, or **Script sequence**. The Schedule assistant guides you through the rest of the process.

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, start the Schedule assistant as described above by choosing **System-level Script**. Next, select the script file you want to run.

System-level scripts can perform whatever tasks you need to perform at the operating system level on the master machine.

See FileMaker Server Help.

FileMaker scripts

To schedule a FileMaker script to run, start the Schedule assistant as described above by choosing **FileMaker script**. Next, select the database that contains the script you want to run, then the script.

FileMaker scripts can do simple tasks 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). You use the Script Workspace feature 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, select **Server** for **Show Compatibility** in the Script Workspace. See the script step reference in FileMaker Pro Help.

See FileMaker Server Help.

Script sequences

To create a script sequence, start the Schedule assistant as described above by choosing **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.

See FileMaker Server Help.

Displaying server statistics

You can view a summary of connection statistics and database statistics attributes for FileMaker Server by choosing **Statistics** > **Server** tab. The statistics can help you diagnose performance and client access issues, and prevent certain processes on FileMaker Server from running slowly.

You can view the following information:

- Server statistics in the **Statistics** > **Server** tab. You can view the statistics in a table and graph format. The types of information you can view include 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 in the **Statistics** > **Clients** tab. These statistics are 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
- FileMaker clients as a scheduled task

To send messages to FileMaker clients, choose the Admin Console **Activity** > **Clients** tab, then select one or more clients from the list. Click , then choose **Send Message** or **Send Message to All Clients** to enter the message.

To send messages to FileMaker clients connected to selected databases, choose the Admin Console **Activity** > **Databases** tab and select a folder or database file. Click , then choose **Send Message** (for database files only) or **Send Message to All Clients** to enter the message.

To create a scheduled task for sending messages, choose the Admin Console **Schedules** pane, click , and choose **Create a Schedule**. Then select **Send message**, choose databases whose users will receive the message, create the message, and set up a schedule to deliver it.

Viewing log file entries in Admin Console

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

- To view, sort, filter, and export a snapshot of the log file entries, choose the Admin Console **Log Viewer** pane, select one or more log file modules for **Modules**, and select a date range for **Start** and **End**.
- To filter the log file entries displayed in the Log Viewer pane, select a message type (**All**, **Error**, **Warning**, or **Information**) for **Type**.
- To view the most recently logged events, click **Refresh**.

See FileMaker Server Help.

Emailing notifications

You can configure FileMaker Server to send SMTP email notifications about errors and warnings as well as completion of scheduled tasks. Emails allow for more timely notification of these events, without having to locate the information in system or event logs on the computer running FileMaker Server.

You can send emails:

- when FileMaker Server errors and warnings (optional) occur
- when a scheduled task is finished

Specify your SMTP mail server settings in FileMaker Server, including the SMTP server address, the port number, user name and password, and the list of email addresses that will receive the email messages.

Each email notification type is configured separately in FileMaker Server, allowing for different recipients for each type of email:

- Configure FileMaker Server to send error or warning emails on the Admin Console **General Settings** > **Email Notifications tab**. You can specify a list of email addresses that will receive error or warning emails on this tab. You can also use Secure Sockets Layer (SSL) data encryption and Transport Layer Security (TLS) when FileMaker Server connects to the SMTP email server.
- Enable email notifications when you create a scheduled task with the Schedule assistant. The scheduled task will send email notifications to the email addresses specified in the Schedule assistant. The SMTP server used for email notifications is configured on the **General Settings** > **Email Notifications** tab.

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 command prompt (Windows) and the Terminal application (macOS). 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:

- Windows: [drive]:\Program Files\FileMaker\FileMaker Server\Database Server\fmsadmin.exe
- macOS: /Library/FileMaker Server/Database Server/bin/fmsadmin

Notes

- Windows: If FileMaker Server is installed in a non-default location, the beginning portion of the default path shown above, \Program Files\FileMaker\FileMaker Server, is replaced with the path that was specified during installation. For example: \My_Path\Database Server\
- macOS: 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 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
```

Chapter 6
Upgrading or moving an existing installation

You can upgrade an existing installation of FileMaker Server 14 or 15 to FileMaker Server 16. You can also move an existing installation of FileMaker Server 16 to other machines.

To change the license of an existing deployment of FileMaker Server 16, see “Updating the FileMaker Server license key” on page 7.

The steps listed below outline the process. See the remaining sections for information about each step.

Important You must perform the steps in the following sections in order.

1. Save the settings for your schedules and administrator groups. See “Step 1. Save your schedules and administrator groups” on page 46.
2. Note your existing FileMaker Server settings. See “Step 2. Note your FileMaker Server settings” on page 47.
3. Stop FileMaker Server. See “Step 3. Stop FileMaker Server” on page 47.
4. Make a copy of any database files and shell script files you used with FileMaker Server. See “Step 4. Make a copy of databases, scripts, and plug-ins” on page 47.
5. Uninstall FileMaker Server. See “Step 5. Uninstall FileMaker Server” on page 48.
6. Clear the Java cache and web browser cache to clear information from the previous FileMaker Server install. See “Step 6. Clear the Java cache and web browser cache” on page 49.
7. Install FileMaker Server 16. See “Step 7. Install FileMaker Server 16” on page 49.
8. Move any database files or script files you used with the previous version of FileMaker Server to the proper folders within the FileMaker Server folder structure. See “Step 8. Move files to the proper location” on page 49.
9. Load the settings for your schedules and administrator groups after installation. See “Step 9. Load your schedules and administrator groups” on page 50.
10. Configure FileMaker Server. See “Step 10. Configure your deployment” on page 50.

If you need to upgrade your machine’s operating system, see “Upgrading the operating system on machines running FileMaker Server” on page 50.

Step 1. Save your schedules and administrator groups

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

1. Start FileMaker Server Admin Console.
2. Choose **Server** menu > **Save Schedules and Groups**. By default, the file is saved in your web browser’s download folder.

After you install FileMaker Server, you can then load the settings for your schedules and administrator groups to instantly configure them in the new installation.

Note The default name of the Schedules and Groups settings file matches the version of FileMaker Server:

- For FileMaker Server 14: fms14_settings.settings
- For FileMaker Server 15: fms15_settings.settings
- For FileMaker Server 16: fms16_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 and FileMaker Go users see in the Launch Center).
- Save the schedules and groups settings in a file. See “Step 1. Save your schedules and administrator groups” on page 46.
- Note other settings that you have changed from the defaults and want to reuse in your FileMaker Server 16 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 FileMaker Server Admin Console (see “Starting Admin Console” on page 36). Note the settings in the General Settings, Database Server, and Web Publishing panes.

Step 3. Stop FileMaker Server

1. In the Admin Console **Status** pane, turn off **Web Publishing Engine**.

   Wait until the Web Publishing Engine has stopped.

2. Turn off **FileMaker Server**.

   Wait until the Database Server has stopped.

3. Stop the FileMaker Server service (Windows) or processes (macOS). See FileMaker Server Help.

Step 4. Make a copy of databases, scripts, and plug-ins

Make a copy of any database files, shell script files, and plug-ins you used with FileMaker Server. In a default FileMaker Server installation, they are stored on the master machine in the following folders.

FileMaker Server 14, 15, and 16 files (default installation)

Windows:

- \Program Files\FileMaker\FileMaker Server\Data\Databases
- \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/Scripts/
- /Library/FileMaker Server/Database Server/Extensions/

FileMaker Server 14, 15, and 16 files (non-default installation in Windows)

When you install FileMaker Server in a non-default location in Windows, the beginning portion of the default path, \Program Files\FileMaker\FileMaker Server, is replaced with the path you specified during installation.

User-specified location\Data\Databases

User-specified location\Data\Scripts\

User-specified location\Database Server\Extensions\

Step 5. Uninstall FileMaker Server

After you have noted the settings in your existing installation of FileMaker Server, you can uninstall FileMaker Server.

Important The uninstall process deletes your settings, so be sure to write down any settings that you want to save. See “Step 2. Note your FileMaker Server settings.”

Windows

To uninstall a multiple-machine deployment, uninstall the worker machines first.

To uninstall FileMaker Server:

1. Start Windows.
2. Open **Control Panel**, then click **Uninstall a program** (or **Programs and Features**).
3. Select the FileMaker Server product from the list and click **Change**.
4. When the Installation program starts, click **Next**.
5. Select **Remove**, then click **Next** and **Remove**.
6. If a User Account Control alert appears, click **Yes**.

   Your database files, script files, and plug-ins are not deleted.
7. Click **Finish**.

macOS

To uninstall a multiple-machine deployment, uninstall the worker machines first.

To uninstall FileMaker Server 16:

1. Open the /Library/FileMaker Server folder.
2. Double-click the **FileMaker Server 16 Uninstaller** icon.

3. Click **Yes** to confirm that you want to uninstall FileMaker Server.

To uninstall FileMaker Server 15:

The FileMaker Server 15 uninstaller is included in the FileMaker Server 16 installation disk image. You can find **FMS 15 Uninstaller** in the Extras folder.

Step 6. Clear the Java cache and web browser cache

Even 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 7. Install FileMaker Server 16

To install FileMaker Server, you must use an account with administrative privileges.

- To deploy on a single machine, see chapter 2, “Installation quick start.”
- To deploy across multiple machines, see chapter 3, “Deploying FileMaker Server across multiple machines.”

The FileMaker Server installer and the Deployment assistant prompts you for some of the settings that you noted in “Step 2. Note your FileMaker Server settings” on page 47.

Step 8. 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 16 folder structure. See “Step 4. Make a copy of databases, scripts, and plug-ins” on page 47.

Note You can use FileMaker Pro to transfer .fmp12 databases to your new FileMaker Server deployment. See “Uploading databases” on page 37. To transfer your database files manually, see FileMaker Server Help.

Important If you are using FileMaker Server 16 and you want to transfer settings by loading the Schedules and Groups settings file, make sure you have created a folder structure in the new FileMaker Server 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 macOS. See FileMaker Server Help.

Step 9. Load your schedules and administrator groups

If you are moving from a previous FileMaker Server 14, 15, or 16 installation, you can load the Schedules and Groups settings file after installation. See “Step 1. Save your schedules and administrator groups” on page 46.

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

1. In Admin Console for the new FileMaker Server 16 installation, choose **Server** menu > **Load Schedules and Groups**.
2. Click **Choose File** and navigate to the folder where you saved the Schedules and Groups settings file.
3. Select the Schedules and Groups settings file and click **Choose**.
4. Click **Load** to load the Schedules and Groups settings file into FileMaker Server.
5. Do one of the following:
   - If the Load Successful message appears, no errors occurred.
   - If the Load Schedules and Groups Results dialog box appears, note the errors that occurred so that you can make the necessary corrections, and then click **OK**.

See FileMaker Server Help.

Step 10. Configure your deployment

You can now start Admin Console and configure your FileMaker Server deployment using the settings you noted in “Step 2. Note your FileMaker Server settings” on page 47. 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 chapter 5, “Administering FileMaker Server.”

Upgrading the operating system on machines running FileMaker Server

For a list of supported operating system versions, see the FileMaker Server system requirements.

Applying security updates or minor operating system updates

When applying a security update or minor operating system update—for example, from macOS 10.12.1 to 10.12.2 or using Windows Update—stop the FileMaker Server processes, apply the update, and then restart the machine.

1. Save the settings for your schedules and administrator groups. See “Step 1. Save your schedules and administrator groups” on page 46.
2. Note your existing FileMaker Server settings. See “Step 2. Note your FileMaker Server settings” on page 47.
3. Stop FileMaker Server. See “Step 3. Stop FileMaker Server” on page 47.

4. Make a copy of any database files and shell script files you used with FileMaker Server. Copy the files to an external volume. See “Step 4. Make a copy of databases, scripts, and plug-ins” on page 47.
5. Apply the security update or system update, and then restart the machine.
6. If FileMaker Server wasn’t set up to automatically start, start FileMaker Server manually.

   See “CLI Help” on page 45 for the `fmsadmin start` command or see FileMaker Server Help.
7. Start Admin Console. See “Starting Admin Console” on page 36.
8. Using Admin Console, verify that all FileMaker Server databases are being hosted.
9. Using Admin Console, verify that all FileMaker Server settings, schedules, and groups have been preserved.
10. Review the FileMaker Server Event.log for any error messages, warning messages, or unexpected settings changes.
11. If you find any problems, uninstall FileMaker Server and reinstall it, then restore the files and settings you saved before applying the update. See steps 5 through 11 below for instructions on how to uninstall and restore.

Applying a major system update

When applying a major operating system update—for example, from OS X 10.11 to macOS 10.12 or from Windows Server 2012 to Windows Server 2012 R2—uninstall FileMaker Server, upgrade your operating system, and then reinstall FileMaker Server.

1. Save the settings for your schedules and administrator groups. See “Step 1. Save your schedules and administrator groups” on page 46.
2. Note your existing FileMaker Server settings. See “Step 2. Note your FileMaker Server settings” on page 47.
3. Stop FileMaker Server. See “Step 3. Stop FileMaker Server” on page 47.
4. Make a copy of any database files and shell script files you used with FileMaker Server. Copy the files to an external volume. See “Step 4. Make a copy of databases, scripts, and plug-ins” on page 47.
5. Uninstall FileMaker Server. See “Step 5. Uninstall FileMaker Server” on page 48.
6. Clear the Java cache and web browser cache to clear information from the previous FileMaker Server install. See “Step 6. Clear the Java cache and web browser cache” on page 49.
7. Upgrade your operating system.
8. Install FileMaker Server 16. See “Step 7. Install FileMaker Server 16” on page 49.
9. Move any database files or script files you used with the previous version of FileMaker Server to the proper folders within the FileMaker Server 16 folder structure. See “Step 8. Move files to the proper location” on page 49.

10. Load the settings for your schedules and administrator groups after installation. See “Step 9. Load your schedules and administrator groups” on page 50.
11. Configure FileMaker Server. See “Step 10. Configure your deployment” on page 50.

Chapter 7
Setting up the web server

In all deployments, FileMaker Server uses Internet Information Services (IIS) in Windows or Apache in macOS. The web server serves web publishing clients, hosts the web-based Admin Console application, and handles some data transfer tasks.

This chapter describes the basics of requesting a custom Secure Socket Layer (SSL) certificate, enabling the web server, and configuring additional IIS authentication settings. 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.

Admin Console provides two settings on the **Database Server** > **Security** tab that enable secure connections with clients:

- **Use SSL for database connections** – With this setting, all Database Server client connections use the SSL, except ODBC and JDBC connections.
- **Use HSTS for web clients** – With this setting, web clients are restricted to HTTPS connections.

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

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 FileMaker, 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.

You can request a custom SSL certificate that matches your specific server name or domain name from a trusted certificate authority (CA) supported by FileMaker, Inc., On the **Database Server** > **Security** tab, click the **Create Request** button to create a certificate signing request (serverRequest.pem), which you send to a CA, and a private key (serverKey.pem) that you keep secret. When you receive your signed certificate from the CA, click the **Import Certificate** button and use your private key to import the certificate. See FileMaker Server Help.

Alternately, you can use the CLI `certificate` command to create a certificate signing request and import the custom SSL certificate. See "CLI Help" on page 45.

The custom SSL certificate file is placed in the CStore folder:

- Windows: [drive]:\Program Files\FileMaker\FileMaker Server\CStore\serverCustom.pem
- macOS: /Library/FileMaker Server/CStore/serverCustom.pem

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

See the FileMaker Server Help topic “Securing your data.”

Notes

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

  The Admin Console’s Create Certificate Signing Request dialog box 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. Do not use IIS certificate tools or OpenSSL certificate tools to import a custom SSL certificate for FileMaker Server’s web server component because the Database Server and the web server component must use the same certificate.
- 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, you must 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” on page 45.
- For information about supported certificates, see the FileMaker Knowledge Base.

Enabling the IIS web server in Windows

The IIS web server must be enabled on the master and worker machines in order for FileMaker Server to operate.

If the FileMaker Server installer detects that IIS is not enabled, it will enable IIS. The FileMaker Server installer also installs the Microsoft Application Request Routing (ARR) extension for IIS if it is not present. However, if you need to enable IIS manually, follow the steps below for the supported version of Windows you’re using.

To enable IIS in Windows versions with the Start button:

1. Click the **Start** button > **Administrative Tools** > **Server Manager**.
2. Click **Add Roles**.
3. In the Add Roles wizard, select **Web Server (IIS)**, then click **Next**.
4. Choose the IIS role services to install. Click **Next** to accept the defaults.
5. Add any role services as required.

To enable IIS in Windows versions with the Windows Start screen:

1. On the Windows Start screen, choose **Server Manager**.
2. Click **Manage** menu > **Add Roles and Features**.
3. Select **Role-based or feature-based installation**, then click **Next**.
4. Select the server, then click **Next**.
5. Choose **Web Server (IIS)**, then click **Next**.
6. Choose any additional features, if necessary, then click **Next**.
7. Click **Next**.
8. Choose the IIS role services to install. Click **Next** to accept the defaults.
9. Confirm your selections, then click **Install**.

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

```
http://localhost
```

During installation, the FileMaker Server installer checks whether any existing website is using ports 80 or 443 (the Default Web Site uses port 80 and is enabled when your first enable IIS). If these ports are in use, the installer prompts you to let it stop the website or to specify alternative ports. Then, the installer creates its own separate website named FMWebSite and configures it to use the ports you specify for HTTP and HTTPS. On the master machine, the installer also configures FMWebSite to use port 16000 for Admin Console via HTTPS.

For information about IIS, see the Microsoft website.

Setting up authentication for FMWebSite in IIS

FileMaker Server handles the authentication for password-protected databases that are published via Custom Web Publishing. You can choose whether you want to use IIS website authentication for the FMWebSite site in addition to FileMaker Server authentication.

You can choose from the following configurations:

- **Disable IIS authentication**. You can disable all IIS authentication methods and use anonymous access to the FMWebSite site. This is the simplest configuration. See the next section, “Disabling IIS authentication.”
- **Leave IIS authentication enabled and also enable Basic Authentication**. You can leave the current IIS authentication methods enabled for use with other websites, and use Basic Authentication for the FMWebSite site used by the Web Publishing Engine. You must also set up Windows user accounts that exactly match the user accounts for the web-published FileMaker databases. See “Enabling IIS authentication” on page 56.

Disabling IIS authentication

By default, Windows IIS directory security attempts to authenticate all requests that are made through the IIS web server. The simplest way to use IIS with FileMaker Server is to disable IIS authentication. If you disable all IIS authentication methods and use anonymous access to FMWebSite, then you don’t need to add any Windows user accounts.

To disable IIS authentication:

1. Open **Control Panel**, then choose **System and Security** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In Internet Information Services (IIS) Manager, select the **FMWebSite** site. You may have to expand some of the nodes to see the websites.
3. In the center pane, double-click **Authentication**.
4. In the Authentication pane, do the following:
   - Ensure that **Anonymous Authentication** is enabled.
   - Disable all other authentication methods.

Enabling IIS authentication

If you enable any of the IIS authentication methods for the IIS web server, you must enable Basic Authentication for the FMWebSite site, which connects to the Web Publishing Engine. The Web Publishing Engine uses only Basic Authentication. Other websites on the web server can use the other IIS authentication methods.

In this configuration, you must also create Windows user accounts on the web server host machine that contain user names and passwords. These user names and passwords must exactly match the user names and passwords for all password-protected accounts defined in all FileMaker databases that are published via Custom Web Publishing.

The following steps show how to install Basic Authentication in each supported version of Windows and then how to enable authentication.

To install IIS Basic Authentication in Windows versions with the Start button:

1. Click the **Start** button > **Administrative Tools** > **Server Manager**.
2. Click **Add Roles**.
3. In the Add Roles wizard, select **Web Server (IIS)**, then click **Next**.
4. Select **Web Server** > **Security**. Ensure that **Basic Authentication** is selected.
5. Click **Next** until you reach the end of wizard, then click **Close**.

To install IIS Basic Authentication in Windows versions with the Windows Start screen:

1. On the Windows Start screen, choose **Server Manager**.
2. Choose **Manage** menu > **Add Roles and Features**.
3. Select **Role-based or feature-based installation**, then click **Next**.
4. Select the server, then click **Next**.
5. Choose **Web Server (IIS)**, then click **Next**.
6. Choose any additional features, if necessary, then click **Next**.
7. Click **Next**.

8. Select **Web Server** > **Security**. Ensure that **Basic Authentication** is selected.
9. Click **Next** until you reach the end of wizard, then click **Close**.

To enable IIS authentication:

1. Open **Control Panel**, then choose **System and Security** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In Internet Information Services (IIS) Manager, select the **FMWebSite** site. You may have to expand some of the nodes to see the websites.
3. In the center pane, double-click **Authentication**.
4. In the Authentication pane, do the following:
   - Enable **Anonymous Authentication**.
   - Enable **Basic Authentication**.

Using the Apache web server in macOS

You do not need to enable the Apache web server that is installed with macOS, nor do you need to have the macOS Server application installed. The FileMaker Server installer creates its own instance of the Apache web server on both the master and worker machines and configures this web server to use port 80 for HTTP and port 443 for HTTPS (or the alternative ports you specify). On the master machine, the installer also configures its Apache web server to use port 16000 for Admin Console via HTTPS. If you have enabled the Apache web server that is already installed with macOS, the FileMaker Server installer prompts you to make the ports available or to specify alternative ports before it can continue.

If you have the macOS Server application installed and use it to enable any HTTP services (for example, websites or a wiki), the existing Apache instance may be reenabled after FileMaker Server is installed. To ensure the Apache instance used by FileMaker Server works normally, you may 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 macOS Server application.

Chapter 8
Optimizing your FileMaker Server deployment

This chapter provides tips on selecting the proper hardware, configuring the operating system, identifying issues that help FileMaker Server run efficiently, and monitoring the server's performance. If your company has an IT group, they might be able to provide support and guidance to keep the server running efficiently.

Selecting the right hardware

Before you select hardware for the server, consider how many users are or will be accessing the server. If many users are accessing the database, then the hard drive and processor will probably get heavy usage. A Database Server accessing a great deal of data can take more resources and needs the right equipment.

Consider these key areas when selecting the hardware:

- **Disk subsystem.** The disk subsystem is a type of disk storage that has an integrated collection of disk drives. This subsystem is the most important factor to consider when purchasing hardware for FileMaker Server because it reads and writes data stored in the database. Having a fast and optimized disk subsystem to effectively handle both reading and writing the data has a significant impact on how the database performs. Regardless of the specific drive type you selected, configure the subsystem to support a Redundant Array of Inexpensive Disks (RAID) or reliable Storage Area Network (SAN) for the hosted databases.
- **Processor.** FileMaker Server handles many processor intensive operations, such as finding information, evaluating unstored calculations, and resolving relationships; therefore, the processor you choose is almost as important as the disk subsystem. Because FileMaker Server can take advantage of multiple processors, certain database tasks can be handled by different processors.
- **Network.** The network throughput can be measured using various tools on the system, and the quality of network throughput depends on several factors. These include the type of Network Interface Card (NIC) installed and the network's physical infrastructure. While the network infrastructure may be outside your control, problems happen due to the network configuration, traffic, and routing. Users can connect to and work with databases over a LAN or a WAN connection. Connecting to a FileMaker Server hosted database over the Internet or a WAN requires that several ports be open for TCP.

- **Memory.** The amount of memory a database uses depends on the size of the database, the type of database, the number of users, and the database's complexity. Any one of these factors can require more memory. Another critical factor for FileMaker Server is the cache.

  The maximum allowed database RAM cache size is the smaller positive number of these two formulas:

  - the physical RAM size minus 1024 MB (1 GB)
  - 90% of the physical RAM size

  If Web Publishing is enabled in a single-machine configuration, you should set the database cache to no more than 50% of the maximum.

  You specify the database cache size by selecting the **Database Server** > **Databases** tab in Admin Console.

Note During deployment, FileMaker Server configures memory use based on the physical RAM size. If you add or remove RAM, you need to redeploy so that FileMaker Server can recalculate optimal memory use for its components.

Virtual servers

Virtualization lets you run multiple instances of an operating system and its specific applications or services on the same physical hardware because you can use a software application to divide a server into isolated virtual environments. Some IT departments turn to virtualization to reduce costs and as a way to use the full potential of the hardware.

FileMaker Server has been tested to run in virtual machines. When using FileMaker Server within a virtualized environment, you must monitor the machines to determine the stress being placed upon the physical hardware.

Setting up and configuring the operating system

Keeping the server running reliably and efficiently takes some planning. See the information below for recommendations on how to set up and configure the operating system, either Windows or macOS.

Setting up and configuring Windows

Recommendation	Do this
Update the operating system and other key drivers	Make sure the BIOS, firmware, and drivers are updated, including: ▪ Machine BIOS/Firmware ▪ Disk Controllers, including RAID Controllers ▪ Disk drives ▪ Network Interface Cards (NICs) ▪ Display adapters
Install Windows updates	Check for the latest service patches and updates and install them. See the FileMaker Server system requirements for supported Windows versions and service packs.
Configure the disk subsystem	Configure the disk array into three logical partitions. ▪ On the first partition, install the operating system and FileMaker Server. ▪ On the second partition, store the databases that FileMaker Server will host. ▪ On the last partition, store local backup files and performance logs.
Don't use file sharing	FileMaker Server's database server accesses the FileMaker database files directly and handles the network access by FileMaker clients. File sharing is not needed.
Disable unnecessary services	Disable services that Windows enables by default that FileMaker Server doesn't need to function properly. The FileMaker Server service only needs to access the hard drives and network.
Disable other Windows settings	Consider changing these settings when optimizing the system on which FileMaker Server is going to run: ▪ Disable indexing for the hosted database volume and the backup volume. ▪ Disable **Shadow Copy** (sometimes referred to as Volume Snapshot Service or VSS) on the hosted database volume. ▪ Make the virtual memory swap file a static size so Windows doesn't attempt to adjust it. Use the recommended file size amount.
Configure the Windows firewall	Find out which ports need to be open and configure the firewall on the master and worker machines. See "Before you begin" on page 9 or "Before you begin installing on multiple machines" on page 21.
Configure virus scanning	Do not allow antivirus software to scan the folders that contain hosted database files or the folders that contain files for container fields that store data externally. Antivirus software may cause file corruption if you allow real-time or on-access virus scanning while files are being hosted to users. With real-time scanning, the virus scanner may spend large amounts of time scanning the database files. This scanning places a heavy load on the server's disk, memory, and processor.
Defragment the hard drive	Defragment the hard drive partition containing the live database files (not the backups) routinely; however, don't defragment the partition while files are being hosted. Note Close any live hosted files with Admin Console before defragmenting. See FileMaker Server Help.

Setting up and configuring macOS

Recommendation	Do this
Avoid services that may impact the live, hosted database	Any service or application that allows the live, hosted database files to be copied or accessed in any way may cause database corruption. Sometimes files accessed directly while FileMaker Server is under load become corrupted. To prevent corruption, you must remove processes, services, or applications that attempt to access the hosted files.
Don’t use file sharing	FileMaker Server's database server accesses the FileMaker database files directly and manages the network access by FileMaker clients. File sharing is not needed.
Turn off Spotlight	Spotlight indexing can impact FileMaker Server’s performance. The Spotlight service automatically watches when information is written to the hard drive and indexes the data to allow faster searches for files.
Don’t use Time Machine	Time Machine is an application that automatically backs up files, but doesn’t back up any files that are in use, such as the live FileMaker database files. If you use Time Machine, it doesn’t corrupt the database files if it was configured to back up those files, but can be very CPU intensive. You should add the locations where the databases are stored to the “Do not back up” section of the Time Machine Preferences to avoid problems.
Don’t enable FileVault	FileVault is used to encrypt the entire macOS startup volume. Don’t enable FileVault on your FileMaker Server machine. This requires an additional layer of software and more processor work on any data being moved to or from the hard drive. Instead, use FileMaker Pro Advanced to encrypt databases. See “Encrypting databases” on page 37.
Make sure Dashboard is not running	Dashboard allows special apps called *widgets* to run. Log out or quit Dashboard. (Dashboard does quit when the user logs out.) By not running Dashboard, server resources are not consumed with running widgets.
Configure the firewall	The macOS firewall is disabled by default. You can enable the firewall by opening the System Preferences application. Configure the firewall to allow incoming connections to FileMaker Server. When FileMaker Server is initially deployed, macOS does ask whether the FileMaker Server component is allowed to accept incoming connections.
Disk Permissions and S.M.A.R.T. Status	Because macOS is built on UNIX, the underlying permissions for hosted database files are sometimes set incorrectly. Although the database files are placed in the right location, they can be inaccessible because FileMaker Server can’t modify the permissions. Use FileMaker Pro to upload the database file and to properly set the file permissions. See FileMaker Server Help.
Security	By default when a computer running macOS starts, it immediately opens to the desktop. FileMaker Server doesn’t require anyone to be logged in for it to run.
Configure virus scanning	Do not allow antivirus software to scan the folders that contain hosted database files or the folders that contain files for container fields that store data externally. Antivirus software may cause file corruption if you allow real-time or on-access virus scanning while files are being hosted to users. With real-time scanning, the virus scanner may spend large amounts of time scanning the database files. This scanning places a heavy load on the server’s disk, memory, and processor.

Considering database performance

FileMaker Server's performance can be impacted by the design of hosted databases. When you design your database files, consider the clients that will be using the hosted databases and consider how to simplify the design for those clients.

To improve performance for all clients, you should limit the use of:

- external tables
- complex table relationships
- unstored calculations
- value lists
- script triggers
- the Perform Script on Server script step

For FileMaker Pro clients, you should optimize layout performance, improve search performance, reduce conditional formatting, and disconnect users from the server when they are idle. See FileMaker Pro Help.

For FileMaker WebDirect solutions, limit the number of portals and panel controls, and limit the number of objects displayed in List View and portals. See "Designing a FileMaker WebDirect solution" in FileMaker WebDirect Guide.

For Custom Web Publishing solutions, limit the number of records returned for Find requests and reduce the prevalidation of field data. See FileMaker Server Custom Web Publishing Guide.

To identify performance issues with hosted databases, use the **Top call statistics** setting available in Admin Console. See FileMaker Server Help.

Monitoring FileMaker Server

Monitoring the server is important for recognizing and preventing problems.

- When users report a problem, such as a system crash or very slow performance, you need good monitoring tools to determine what caused the problem.
- By analyzing future hardware needs, taking baseline readings when monitoring a situation, or gaining a better understanding of the server's health, you can prevent future problems.

Monitoring performance in Windows

To monitor FileMaker Server in Windows, you can use a tool called Performance Monitor, also known as *perfmon*. With the perfmon tool, you can examine how applications that are running affect your computer's performance, including the memory used, disk access time, and log statistics on different processes. While some log information shows obvious bottlenecks or stress points, much of the information might require more detailed analysis. With a little experience, you can recognize common stress points.

Note To use perfmon, you must have local Administrators group or equivalent privileges in Windows. See Windows Help and Support.

There are five logs that can help you monitor performance in Windows:

- **Processor.** Logs the processor activity and idle times. Select **% Processor Time** as the primary indicator of processor activity and to display the average percentage of busy time. To view the time the processor is idle, select **% Idle Time**.
- **Network Interface Counter (NIC).** Captures bytes sent and received over each network adapter, the length of the output packet queue (in packets), and the errors for inbound and outbound packets.
- **Memory.** Records the amount of physical memory immediately available for allocation to a process or for system use. The log also records the Cache Bytes for Memory\System Cache, cache faults, page faults, the number of read operations, and the pages written to disk.
- **Process.** Logs statistics on processes, including time, reading and writing rate, page faults, thread count, virtual address space, and the current size, in bytes, of the memory that this process has allocated.
- **Disk.** Captures the disk read time, the disk write time, the percentage of time the disk was idle, the number of outstanding requests, and the split input and output to the disk.

Note The Windows Event Viewer contains the Application log and the System log, which are useful for understanding how the server is performing. These can provide insight into activity at the user, system, and service level.

Reviewing the performance logs

By default the performance logs show you real time statistics of specific counters. To display the performance logs, open **Administrative Tools** > **Performance Monitor**, then navigate to **Monitoring Tools** > **Performance Monitor**.

Monitoring performance in macOS

Monitoring is an important part of any server deployment; FileMaker Server is no exception. The reasons for performing monitoring are planning, resource management, and troubleshooting. macOS has four primary tools that you can use for monitoring server performance: Activity Monitor, the macOS Server application, Top, and System Activity Reporter (SAR).

- Activity Monitor supplies a list of all the processes currently running and information about the overall activity on the computer.
- The macOS Server application, available in the Mac App Store, provides tools to administer services on the operating system and provide a graphical interface for monitoring CPU usage, network traffic, and memory usage. However, be aware of possible conflicts when using macOS Server to enable any HTTP Services (see “Using the Apache web server in macOS” on page 57).
- Top is a command-line program that is part of the UNIX engine for macOS. When running Top, you see a list of the processes that are running on the machine sorted by the process ID.
- SAR is a command-line program installed in macOS by default. It consists of two basic tools, the System Activity Data Collector (SADC) and the System Activity Reporter (sar). It is designed to automatically gather data for an extended time period, then analyze that data later. The data collected by SAR are reports on cumulative statistics counters.

For information about Activity Monitor and macOS Server, see their help systems. For information about command-line tools, open the Terminal application and look at the manual (man page).

Chapter 9
Using a standby server

A standby server is a redundant FileMaker Server installation that can be brought online to replace the primary server. If a hardware or software failure prevents the primary server from hosting databases, you can make the standby server your production server. You can also make the standby server your production server when you want to make scheduled hardware or software upgrades to the primary server.

A standby server is essentially a copy of the primary server, set up so that any changes to the primary server are automatically applied to the standby server. The standby server does not host databases for clients, but is ready to replace the primary server when needed.

When you create the connection between the primary server and the standby server, the database files and external container field objects are securely synchronized from the primary server to the standby server. Any subsequent changes to the primary server databases are saved to progressive backup files, which are incrementally applied to the standby server.

Important Using a standby server is not a replacement for backing up your hosted databases. Although you can use a standby server to recover from potential hardware or software failures, a standby server is not a substitute for a sensible backup and recovery strategy. See “Backing up databases” on page 38.

Standby server requirements

To set up a standby server, you must have two server machines with identical configurations. The two server machines must match in the following ways:

- operating system (Windows or macOS) and operating system version
- FileMaker Server version
- FileMaker Server installation folder
- FileMaker Server user account name
- FileMaker Server login credentials
- physical memory size available on the machine (RAM size)
- deployment configuration (single-machine deployment only)
- ports for web connections (HTTP) and secure web connections (HTTPS)
- whether ODBC/JDBC is enabled
- whether web publishing is enabled
- folders containing files for container fields that store data externally
- default database folder path
- additional database folder paths
- local volumes that contain databases
- progressive backup folder path

- the setting **Enable progressive backups** must be enabled on both the primary server and the prospective standby server
- the FileMaker Server user account must have write permission to the parent folder of the progressive backup folder path

Notes

- The standby server feature is supported only for single-machine deployments. The standby server feature is not supported for FileMaker WebDirect worker machines.
- The standby server feature is not supported for deployments that host FileMaker Data API solutions. FileMaker Data API calls are not forwarded after a switchover operation.
- If your installation uses remote volumes for additional database or container data folders, make sure that the remote volumes are available before using any of the standby commands. To verify a folder is accessible, use the `fmsadmin list files` command.
- In the procedures below, if you are using a container data folder to store container field data externally, be sure to also select the setting to back up that container data folder. For example, if you select the **Enable container data folder 1** setting, then select the **Back up container data folder 1** setting as well. The standby server feature uses progressive backups to copy data, and the backups must include the external container data.

Standby server procedures

The procedures in this section describe how to set up and use a standby server configuration.

To complete these procedures, you must use the FileMaker Server command line interface (see “Using the command line interface” on page 44).

Windows: To run standby commands, open the command prompt window using **Run as Administrator**.

Setting up a standby server

This procedure assumes that you have a FileMaker Server single-machine installation already in production. From the production server, you must be able to open Admin Console and open and close database files. Start this procedure with that production server up and running. That production server will be your primary server.

To set up a standby server for your primary server:

1. Install FileMaker Server on the prospective standby server. During deployment, enter the user name, organization, and license key information that you used for the primary server.

   This procedure assumes that you do not already have a FileMaker Server installation that you want to use as the standby server. If you have a FileMaker Server installation to use as the standby server, then shut down and restart the prospective standby server before continuing to the next step. The prospective standby server must be started after the primary server is already running.

2. Make sure that the prospective standby server configuration matches your primary server configuration. See “Standby server requirements” on page 64. Even though the prospective standby reports a license conflict, you can use Admin Console to configure the settings.

3. Close all databases on the primary server and the prospective standby server.
4. If you have scripts, manually copy the contents of the scripts folder from the primary server to the prospective standby server:
   - In a Windows default installation, copy the \Program Files\FileMaker\FileMaker Server\Data\Scripts\ folder.
   - In macOS, copy the /Library/FileMaker Server/Data/Scripts/ folder.
5. On the primary server, initiate a connection with the standby server using the `standby connect` command:

   `fmsadmin standby connect` *`standbyhost`*

   where *`standbyhost`* is the IP address or host name of the prospective standby server. If you use the host name, the host name must resolve to a single IP address.
6. Enter the user name and password for the Admin Console account that is defined on the primary server.
7. Note the setup code that FileMaker Server returns. In the next step, you will enter this setup code on the standby server. This setup code is valid for one hour.
8. On the standby server, confirm the connection with the primary server using the `standby accept` command:

   `fmsadmin standby accept` *`code`*

   where *`code`* is the setup code that FileMaker Server returned from the `standby connect` command in the previous step.
9. Enter the user name and password for the Admin Console account that is defined on the standby server.
10. On the primary server, complete the connection by responding to the command line prompt. You should see a message that the configuration settings have been transferred to the standby server.
11. Perform the initial file synchronization from the primary server to the standby server. On the primary server, run the `standby update` command:

    `fmsadmin standby update`

    By running the `standby update` command with no arguments, all hosted database files and folders that are hosted on the primary server are updated on the standby server.
12. On the primary server, open the databases that you want to host. As clients use the hosted databases, any changes are written to progressive backup files, which are used to asynchronously transfer incremental file changes to the standby server.

Notes

- With standby commands, you can use the CLI `-y` or `--yes` option to automatically answer yes to all command prompts and the `-f` or `--force` option to ignore any certificate warning messages.
- If a database file is on both the primary server and the standby server when you run the `standby connect` command, the files must be identical or else the command returns an error.

  For example, if your files are on a remote volume and the volume changes the folder timestamp or dates, then FileMaker Server may determine that the files are not identical and the standby connection command returns an error.

  To waive this requirement, use the `--overwrite` option. When this option is used, conflicting databases on the standby server are overwritten when they are updated. Databases that are on the standby server but not on the primary server are not changed.
- When the standby server is initially connected to the primary server, the primary server's license key is transferred to the standby server. If you change the license key on the primary server, the license key is also updated on the standby server. If you receive a license key conflict message, restart the primary server, then restart the standby server.
- After you have defined the standby configuration, do not change the FileMaker Server user account. Changes to the FileMaker Server user account may cause the `standby switchover` command to fail.
- After you have defined the standby configuration, database files synchronize from the primary server to the standby server when they are first opened on the primary server. Opening database files on a primary server may take longer than on a standalone server because the files are synchronized to the standby server before they are opened on the primary server.
- The following folders are synchronized from the primary server to the standby server:
  - Data/Database folder. If you define additional database folders—additional database folder 1 or additional database folder 2—they are also synchronized.
  - Data/Databases/RC_Data_FMS folder, as long as this folder is not a shared network folder such as a SAN target. If you define additional container data folders—container data folder 1 or container data folder 2—they are also synchronized.
  - CStore folder. However, for security reasons, custom SSL certificates are not copied.
- The contents of other folders—for example, the scripts, documents, backup, and HTTPServer folders—are not automatically copied to the standby server. You may either manually copy the folders' contents or use the `standby update` command. See "Updating files and folders on the standby server" on page 72.
- When files are copied from the primary server to the standby server, file attributes are not retained. For example, even if a file is locked on the primary server, it is unlocked on the standby server because the "locked" attribute is not retained when the file is copied. Use FileMaker accounts and privilege sets to secure the database file rather than using the system's file attributes to lock the file.
- If a database is removed from the primary server, the database is not automatically removed from the standby server. To remove the database from the standby server, disconnect the standby server, remove the database, and then reconnect the standby server.

- Once you define a server as a standby server, you cannot configure the standby server's settings directly. Changes that you make to the primary server's configuration settings are saved on the primary server, and are not transferred to the standby server until a switchover procedure (described in "Switching the standby configuration roles") or failover procedure (described in "Using the standby server when the primary server fails" on page 70).

  For security reasons, the settings **Use SSL for database connections** and **Use HSTS for web clients** are not transferred from the primary server to the standby server. Install a custom SSL certificate and configure these settings on the prospective standby server before running the standby connect command.

  In addition, the settings on the following Admin Console tabs cannot be transferred from the primary server to the standby server:

  - **General Settings** > **ODBC/JDBC**
  - **Web Publishing** > **General Settings**
  - **Web Publishing** > **FileMaker WebDirect**
  - **Web Publishing** > **PHP**
  - **Web Publishing** > **XML**
  - **Web Publishing** > **FileMaker Data API**

  To change these settings, disconnect the standby server, change the settings on both servers, and then reconnect the standby server.
- If you installed FileMaker Server on the prospective standby server and opened Admin Console on that machine before opening Admin Console on the primary server, you may receive a license conflict on the primary server that prevents it from acting as the primary server. To resolve this issue:
  - On the prospective standby server, stop FileMaker Server either using Admin Console or the CLI command `fmsadmin stop server`.
  - On the primary server, restart FileMaker Server either using Admin Console or the CLI command `fmsadmin restart server`.
  - On the prospective standby server, start FileMaker Server either using Admin Console or the CLI command `fmsadmin start server`.
  - Follow the procedure described in "Setting up a standby server" on page 65.

Switching the standby configuration roles

When you switch the roles of your primary server and your standby server, you make the standby server your production server and the primary server becomes the standby server. This procedure is called a *switchover*.

Important Running the `standby switchover` command while clients are connected to databases or while scripts are running can cause data loss. Any uncommitted data is lost when you run the `standby switchover` command. Notify clients about a planned switchover in advance, and perform the switchover operation at off-peak times when clients are not connected.

To perform a switchover operation:

1. On the primary server, use the `standby status` command to verify all files:

   ```
   fmsadmin standby status -s
   ```

   Fix any issues that are reported before continuing with the rest of this procedure.

2. On the primary server, use the `pause` command to pause all open databases.

   ```
   fmsadmin pause
   ```

3. On the primary server, use the `standby update` command to update all databases from the primary server to the standby server:

   ```
   fmsadmin standby update
   ```

4. On the primary server, run the `standby switchover` command:

   ```
   fmsadmin standby switchover
   ```

5. After you run the `standby switchover` command, the former standby server becomes the new primary server. On the new primary server, use the `resume` command to resume all paused databases.

   ```
   fmsadmin resume
   ```

Notes

When you run the `standby switchover` command on the primary server:

- The primary server pauses all hosted databases and sends all pending progressive backup files to the standby server.

  Note Only the databases that have been opened on the primary server are synchronized with the standby server. Databases that have never been opened on the primary server are not copied to the standby server, even if those databases are in one of the database folders on the primary server. To copy all the files in a database folder, use the `standby update` command and specify the folder you want to copy. See “Updating files and folders on the standby server” on page 72.

- The standby server applies all the pending progressive backup files that it has received, and then the standby server becomes the production server.
- The former primary server becomes the new standby server.
- In general, hosted databases are resumed for clients to use. However, use Admin Console or CLI commands to verify that databases are open after the switchover operation completes. If the former primary server hosted encrypted database files, the encrypted database files do not automatically open after you switch the roles of your primary and standby servers. You must manually open encrypted database files after completing the switchover. See “Opening encrypted databases” on page 38.
- If the primary server is unable to communicate with the standby server, the switchover operation fails, and the primary server remains the production server.

Using the standby server when the primary server fails

If your primary server fails due to a hardware or software issue, or if the primary server becomes unavailable due to network issues, you can make your standby server the production server in place of the primary server. This procedure is called a *failover*.

To perform a failover operation, run this command on the standby server:

```
fmsadmin standby disconnect
```

When you run the `standby disconnect` command on the standby server:

- The standby server is changed to a standalone server and stops synchronizing with the primary server.
- Because the standby server is no longer communicating with its former primary server, the standby server does not attempt to change the former primary server to a standalone server. It only changes itself to a standalone server. However, if the former primary server is able to communicate with the former standby server and detects that the former standby server is now a standalone server, the former primary server changes itself to a standalone server as well.
- There may be some data loss if the primary server had not fully synchronized with the standby server before the primary server failed.

Important Do not to bring both database servers online after the standby server has switched to a standalone server. When the same database files are simultaneously hosted by two servers, clients may unknowingly commit data to separate copies of the database files.

Setting primary and standby server host names

To minimize the impact to clients, use alias host names instead of direct IP addresses for the primary server and the standby server. By planning the host names for each server, you can make it easier for clients to connect to the production server after switchover and failover operations.

Use the `standby hostnames` command to set the host names that FileMaker clients use to access hosted databases. On the primary server, run this command:

`fmsadmin standby hostnames` *`primaryHost standbyHost`* `[options]`

where *`primaryHost`* is the host name for the primary server and *`standbyHost`* is the host name for the standby server. For `options`, you can use `-w` or `--wait` to set the timeout value.

A network administrator needs to configure the environment's Domain Name System (DNS) to resolve a server host name to both the primary server and standby server addresses.

Disconnecting a standby server

To disconnect a standby server from the primary server:

1. On the primary server, use the `pause` command to pause all open databases:

   ```
   fmsadmin pause
   ```

2. On the primary server, use the `standby update` command to update all databases from the primary server to the standby server:

   ```
   fmsadmin standby update
   ```

3. On the primary server, use the `standby disconnect` command:

   ```
   fmsadmin standby disconnect
   ```

4. On the primary server, use the `resume` command to resume all paused databases:

   ```
   fmsadmin resume
   ```

When you run the `standby disconnect` command on the primary server:

- The primary server removes the standby server from synchronization, then the primary server is changed to a standalone server. The primary server does not need to be restarted after it is changed to a standalone server. Clients can continue to use hosted databases after you resume the paused databases.
- The standby server is removed from synchronization, then the standby server is changed to a standalone server. To prevent both servers from hosting the same databases, the databases on the former standby server are closed, and the **Automatically Open Database Files** setting is disabled on the former standby server.
- If the primary server cannot communicate with the standby server, the primary server still changes to a standalone server and stops sending updates to the standby server. However, the standby server remains as a standby server due to the communication error. To complete the disconnection, run the `standby disconnect` command on the standby server, and the standby server is changed to a standalone server.

Reconnecting a standby server

To reconnect servers that you previously disconnected:

1. Ensure that the prospective primary server is a standalone server by running the `standby status` command, described in “Getting information about the standby configuration” on page 73.
   - If you see the message “Standby server not configured,” then the server is a standalone server.
   - If you see a message that says the server is a primary or a standby server, then run the `standby disconnect` command to change it to a standalone server.
2. Ensure that the prospective standby server is a standalone server by running the `standby status` command, described in “Getting information about the standby configuration” on page 73.
   - If you see the message “Standby server not configured,” then the server is a standalone server.
   - If you see a message that says the server is a primary or a standby server, then run the `standby disconnect` command to change it to a standalone server.

3. After verifying that both servers are standalone servers, follow the procedure described in “Setting up a standby server” on page 65.

Note If a database file is on both the primary server and the standby server when you run the standby connect command, the files must be identical or else the command returns an error. When reconnecting a standby server, you can either delete conflicting databases or use the `--overwrite` option. When this option is used, conflicting databases on the standby server are overwritten when they are updated. Databases that are on the standby server but not on the primary server are not changed.

Updating files and folders on the standby server

In case of an update error or communication failure, you may need to update specific database files or folders. Use the `standby update` command to update files or folders on the standby server. This command can only be run on the primary server. Before running this command, close or pause all open databases using `fmsadmin close` or `fmsadmin pause`.

Format

`fmsadmin standby update [file...] [path...][options]`

Options

- If no file or path is specified, the closed and paused databases located in the default database folder and the additional database folders are updated.
- For *file*, you can specify a database ID or database name to update that database file, including any external container field objects. If the specified file is already up-to-date on the standby server, no updates are transferred. You can specify multiple files, separated by spaces.
- For *path*, you can specify a directory containing database files that you want to update. You can use "*" wildcards, but UNIX regular expressions and other types of wildcards are not supported.

  Note To use "*" wildcards in macOS, enclose the value for *path* in quotation marks. For example: `fmsadmin standby update "/folder/*"`

  The standby server must be able to create the same directory as specified on the primary server. The root volume of the directory must already exist on the standby server. If the volume refers to a remote drive, the drive must be mounted before you run the `standby update` command. The FileMaker Server user account must have write access to the directory.

  The value for *path* cannot include files in reserved folders:

  - the default database folder
  - the additional database folders
  - the container data folders

The value for *path* can include these folders:

- Data/Backups/
- Data/Documents/
- Data/Scripts/
- Database Server/Extensions

- Use the `-r` or `--recursive` option to recursively update folders.

Note To update files that use a filename extension other than .fmp12, you must register the filename extension in Admin Console on the **Database Server** > **Databases** tab before running the standby update command. See FileMaker Server Help.

Getting information about the standby configuration

You can use the `standby status` command to get information about the standby configuration of your server machines. You can run this command on a primary server, a standby server, or a standalone server that is not using a standby configuration.

Example 1

Running standby status on a primary server:

```
fmsadmin standby status -u [admin] -p [pass]
```

Result

```
Primary Server: FMS01 (192.168.1.101) This machine
Standby Server: FMS02 (192.168.1.102)
Last Updated: 10-22-2017 02:55:44 PM
```

Example 2

Running standby status on the standby server:

```
fmsadmin standby status -u admin -p pass
```

Result

```
Primary Server: FMS01 (192.168.1.101)
Standby Server: FMS02 (192.168.1.102) This machine
Last Updated: 10-22-2017 02:55:44 PM
```

Example 3

Running standby status on a standalone server:

```
fmsadmin standby status -u admin -p pass
```

Result

```
Error: 11300 (Server is not connected to standby server)
```

Example 4

To get status information about the updates to individual database files, use the `-s` or `--stats` option.

```
fmsadmin standby status -u admin -p pass -s
```

Result

```
Primary Server: FMS01 (192.168.1.101) This machine
Standby Server: FMS02 (192.168.1.102)
Last Updated: 10-22-2017 02:55:44 PM
ID   File            State          Last Updated              Last Error
1    Contacts.fmp12  Updated        10-22-2017 02:55:44 PM
2    Invoices.fmp12  Update Error   10-21-2017 01:23:14 AM   Permission
Denied
3    Orders.fmp12    Updating       10-22-2017 02:55:43 PM
4    Sales.fmp12     Not Updated
```

Standby server performance considerations

The standby server feature uses progressive backups to communicate changes from the primary server to the standby server. As a result, performance considerations related to progressive backups can also apply to standby server performance.

The setting that most affects primary server performance is the value specified for **Save interval** on the **Database Server** > **Folders** tab. This setting determines how often progressive backups are created. You can specify a **Save interval** value between 1 and 99 minutes. However, to avoid negative performance impact, do not specify a value lower than the default of 5 minutes. If the standby server feature has a negative performance impact on your primary server, then increase the **Save interval** value.

Chapter 10
Additional resources

Product documentation

Online Help is accessible from FileMaker Server Admin Console, **Help** menu > **FileMaker Server Help**.

To access FileMaker Server documentation:

- In Admin Console, choose **Help** menu > **FileMaker Server Product Documentation**.
- Click the links in the FileMaker Server Admin Console Start Page.
- 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 FileMaker Knowledge Base.

To ask questions and get advice from other users, visit the FileMaker Community.

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

Check for software updates

From the FileMaker Server Admin Console Start Page, you can check for software updates. In the Software Update section, click **Check Now**. If an update is available, you can click a link to download the update.

Index

G

H

I

J

L

M

O

P

R

S

T

U

V

W

X