

FileMaker Server Installation and Configuration

FileMaker Server Installation and Configuration



NOTE: IS&T recommends that [IS&T Managed Servers](#) be used for hosting FileMaker databases.

Only experienced server administrators should attempt to do so, particularly where databases with sensitive data and/or mission critical functions will be housed. The following web page offers MIT-specific configuration recommendations to help mitigate against security risks in the FileMaker hosting environment. In a changing computing landscape these recommendations in no way offer a guaranteed maintenance or risk-free hosting environment.

Note: The information on this page is accurate for FileMaker Server 16. Certain settings and features may differ for prior versions.

On this page:

- [IS&T-Managed FileMaker Hosting](#)
- [Shortlist of Recommended Security Settings](#)
- [Before You Begin](#)
- [Obtaining FileMaker Server](#)
- [Installing and Deploying FileMaker Server](#)
 - [Installation](#)
 - [Deployment Assistant](#)
- [FileMaker Server Admin Console](#)
 - [Accessing the Admin Console](#)
 - [Status Pane](#)
 - [Admin Console Access](#)
 - [Configure Recommended Security Settings](#)
 - [Custom SSL Certificates](#)
- [Other Tasks](#)

IS&T-Managed FileMaker Hosting

As stated above, IS&T strongly recommends use of its [managed FileMaker hosting service](#). To request or inquire about IS&T-managed FileMaker hosting, [fill out this web form](#). Note that with managed hosting, all recommended best practices are handled for you.

If you have determined that you need to run your own FileMaker Server environment, the following information is provided for your reference.

Shortlist of Recommended Security Settings

The following is an overview of essential security-related settings. For a full checklist of best practices, refer to [Best Practices for FileMaker Hosting at MIT](#).

- Enable SSL encryption
- Obtain and install a supported custom SSL certificate. For more information and instructions, see [FileMaker Server SSL Certificates](#)
- Enable option to host password-protected databases only
- Enable option to list only the databases each user is authorized to access
- Do not enable web publishing (WebDirect, custom web publishing, or FileMaker Data API) unless you have reason to
- If using web publishing, take active steps to prevent sensitive data from being exposed to the web
- Do not enable ODBC/JDBC access unless you have reason to

Please follow all recommended [MIT FileMaker Security Guidelines](#) when setting up your server. In addition, please consult the [FileMaker Inc. Security Guidelines](#) for additional considerations for server setup.

Before You Begin

This probably goes without saying, but before you begin you must provision a virtual or physical machine that meets the current minimum specs for FileMaker Server.

To work with FileMaker Server, certain ports must be open and/or available on your server machine in order for FMS to communicate with various types of clients. Port settings should be handled before installing FileMaker Server. For the recommended port settings for FileMaker Server at MIT, see [FileMaker Server Port Settings at MIT](#).

Obtaining FileMaker Server

Starting with version 15, MIT's FileMaker Server licenses are primarily reserved for IS&T's [managed FileMaker hosting service](#), and FileMaker Server is no longer directly available on the IS&T software grid. If you want to run your own FileMaker Server environment, in most cases you will need to purchase your own FileMaker Server license. Education pricing is available. For more information, see [FileMaker Server Licensing at MIT](#).

Installing and Deploying FileMaker Server

Installation

Follow standard procedures for initiating the installation process on your server machine. There are a few gotchas of note:

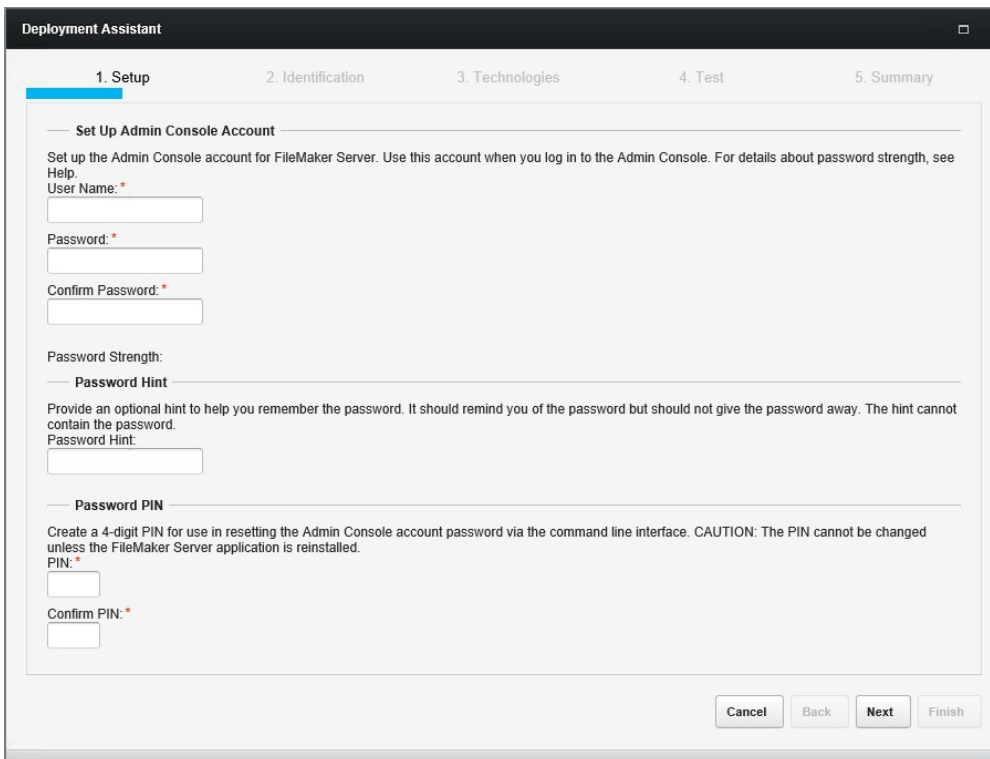
- On Windows, the installer should be extracted to and run from the C:\ root directory.
- When prompted to enter your license information, you must enter the organization name exactly as follows: Massachusetts Institute of Tech
- After installing the software, you may be prompted to register it with FileMaker. Please do not register - the software was already registered via MIT volume site licensing.

Deployment Assistant

Once installation is complete, FileMaker Server will automatically launch the Deployment Assistant. Follow the steps outlined below to configure appropriately.

1. In the Setup screen, enter a User Name and Password for accessing the Admin Console, then click **Next**. The user name and password can be changed later through the Admin Console.

Warning: For security reasons, do not use your Kerberos credentials.



The screenshot shows the 'Deployment Assistant' window with the '1. Setup' tab selected. The window has a dark title bar and a light gray background. At the top, there are five tabs: '1. Setup', '2. Identification', '3. Technologies', '4. Test', and '5. Summary'. The '1. Setup' tab is active and highlighted with a blue bar. Below the tabs, the main content area is titled 'Set Up Admin Console Account'. It contains the following sections: 'Set up the Admin Console account for FileMaker Server. Use this account when you log in to the Admin Console. For details about password strength, see Help.' followed by 'User Name:' with a text input field, 'Password:' with a text input field, and 'Confirm Password:' with a text input field. Below these is a 'Password Strength:' section. Then, a 'Password Hint' section with the text 'Provide an optional hint to help you remember the password. It should remind you of the password but should not give the password away. The hint cannot contain the password.' and a 'Password Hint' text input field. Finally, a 'Password PIN' section with the text 'Create a 4-digit PIN for use in resetting the Admin Console account password via the command line interface. CAUTION: The PIN cannot be changed unless the FileMaker Server application is reinstalled.' followed by 'PIN:' with a text input field and 'Confirm PIN:' with a text input field. At the bottom right of the window, there are four buttons: 'Cancel', 'Back', 'Next', and 'Finish'. The 'Next' button is highlighted.

2. In the Identification screen, enter the Server Name as the fully qualified domain name (FQDN), i.e. <your hostname>.mit.edu. If desired, you can also enter the Server Description and Administrator Contact Information. Then click **Next**. Note that this information will be visible on the Admin Console Start page.

Deployment Assistant

1. Setup 2. Identification 3. Technologies 4. Test 5. Summary

Server Name

FileMaker clients see this name when they use the Launch Center.

Server Name: *

(remaining characters: 41)

Server Description

Users view this description on the Admin Console Start page.

Server Description:

(remaining characters: 174)

Administrator Contact Information

Users view this information on the Admin Console Start page.

Owner:

Email:

Location:

Phone Number:

Cancel Back Next Finish

3. In the Technologies screen, under the ODBC/JDBC heading, unless you plan to allow connections via ODBC so that your hosted solutions may be used as ODBC data sources, select "No, do not enable ODBC/JDBC." You may also opt to enable or disable this feature at a later time as necessary; to do so, in the Admin Console, choose Server > Edit Deployment.

Deployment Assistant

1. Setup 2. Identification 3. Technologies 4. Summary 5. Progress

ODBC/JDBC

ODBC and JDBC are application programming interfaces (APIs) that provide a common language for interacting with a variety of data sources and database services, including FileMaker Server.

Enable ODBC/JDBC on FileMaker Server if you want to use other applications (like spreadsheets, word processors, and reporting tools) to view, analyze, and modify FileMaker data.

Do you want to enable ODBC/JDBC?

☐ Yes, enable ODBC/JDBC

☒ No, do not enable ODBC/JDBC

Web Publishing

Web publishing allows you to publish databases on the internet or an intranet. Enable web publishing if you want to make FileMaker data available in a web browser.

Note: A custom SSL certificate is required to access web publishing technologies over a secure and trusted connection. Obtain a custom certificate from a [Certificate Authority \(CA\) supported by FileMaker](#) and install the certificate.

Do you want to enable web publishing?

☐ Yes, enable web publishing

☒ No, do not enable web publishing

Cancel Back Next Finish

4. Still in the Technologies screen, under the Web Publishing heading, unless you plan to allow web connections to your files (via the FileMaker Data API, WebDirect, or custom web publishing), select "No, do not enable web publishing." You may also opt to enable or disable this feature at a later time as necessary; to do so, in the Admin Console, choose Server > Edit Deployment.
- Note:** FileMaker Server requires a web server in all deployments; the web server hosts the web-based Admin Console application and handles certain data transfer tasks. Turning web services on, which the installation process does for you, is not the same thing as enabling FileMaker web publishing.
- Important:** If you choose to utilize Web Publishing, only non-sensitive data should be accessible to web users. If your database(s)

contain sensitive data, take active steps to prevent sensitive data from being exposed to the web. Please consult the [MIT FileMaker Security Guidelines](#).

- Click **Next** to proceed to the Summary screen.
- Click **Next** to finally run the FileMaker Server deployment using your desired settings.

The screenshot shows the 'Deployment Assistant' window with the 'Summary' tab selected. The progress bar at the top indicates the sequence: 1. Setup, 2. Identification, 3. Technologies, 4. Summary (highlighted), and 5. Progress. The main content area is titled 'Deployment Summary' and contains a table with the following data:

NAME	VALUE
Admin Console User Name	dcad
FileMaker Server Name	dcad-fmp-test-1.mit.edu
ODBC/JDBC	Disabled
Web Server	Disabled
FileMaker WebDirect	Disabled
FileMaker Data API (Trial), expires on September 27, 2018	Disabled
XML	Disabled
PHP	Disabled
Web Publishing	Disabled

At the bottom right, there are four buttons: 'Cancel', 'Back', 'Next', and 'Finish'.

- Click **Finish** to exit the Deployment Assistant and continue to the Admin Console.

The screenshot shows the 'Deployment Assistant' window with the 'Progress' tab selected. The progress bar at the top indicates the sequence: 1. Setup, 2. Identification, 3. Technologies, 4. Test, 5. Summary, and 6. Progress (highlighted). The main content area contains a progress bar and the text: 'Please wait while FileMaker Server is deployed and configured. When deployment completes, click Finish to continue.' Below this is a section titled 'Deployment Results' with a table showing the status of various tasks:

NAME	VALUE
SETUP: PRECONFIGURE WEB SERVER	
Create IIS backup	succeeded
Check to make sure FMI web site exists	succeeded
Create app fmi-test	succeeded
START DEPLOYMENT	
Step 1: Save settings:	
Save administrative configuration settings	succeeded
Step 2: Configure Web Publishing Engine (WPE):	
Stop WPE	succeeded
Configuring JWPC memory	succeeded
Set WPE AutoStart to enabled	succeeded
Add JVM Route to JWPC Server XML file	succeeded
Create CWPC prefs file	succeeded
Update JWPC prefs file	succeeded
Start WPE	succeeded
Update WPE deployment configuration	succeeded
Update mDNS service info	succeeded

At the bottom right, there are four buttons: 'Cancel', 'Back', 'Next', and 'Finish'.

FileMaker Server Admin Console

Accessing the Admin Console

Once FileMaker Server has been installed and deployed, the Admin Console may be accessed by pointing a browser to:

`https://<hostname>.mit.edu:16000`

Status Pane

After authenticating to the Admin Console, you will land on the Status pane. This provides an overview of your FileMaker Server's activities and health.

Note: The Status pane will only display the sections for FileMaker Data API, Web Publishing Engine, and ODBC/JDBC if you elected to enable those functions in the Deployment Assistant. You may revisit these settings in the Admin Console by choosing Server > Edit Deployment. If you do make changes to these settings, you will need to stop and restart FileMaker Server for them to take effect.

Status ?

FileMaker Server 16

IP Addresses18.7.88.46

FileMaker Host Nameist-fmp-test-1.mit.edu

Admin Server Started6/15/17 12:07 PM

Server Version16.0.1.184

DATE	TYPE	DESCRIPTION
Jun 14, 2017 3:23:27 PM	Warning	SECURITY: The default SSL certificate is being used; for better security, import a valid custom SSL certificate

0 Total User Connections clients connected

0 FileMaker Pro

0 FileMaker Go

0 FileMaker WebDirect

1 User Connections client limit

1 Remaining User Connections clients

0 Additional FileMaker Pro and FileMaker Go clients

0 Custom Web Publishing connections currently open

3 Databases hosted out of total 3

1 Schedule is currently enabled

FileMaker Data API

0 FileMaker Data API connections currently open

Web Publishing Engine

Worker Machine: 1

IP Addresses18.7.88.46

Host Namedcad-fmp-test-1.mit.edu

Number of Connections0

0 FileMaker WebDirect connections currently open

FileMaker WebDirect is enabled

ODBC/JDBC

0 XDBC connections currently open

Admin Console Access

In addition to the User Name and Password set via the Deployment Assistant for accessing the Admin Console, you may allow access via an external server group. This is defined on the Admin Console > General Settings pane > Admin Console tab > External Group section. For information on how to use this to enable Kerberos-based authentication to the Admin Console, refer to [Configuring FileMaker Server for Kerberos Authentication](#).

You may also limit access to the Admin Console by IP address; this is done on the same tab in the Restrict Access section.

General Settings ?

Server Information | Email Notifications | **Admin Console** | Startup | ODBC/JDBC | Administrator Groups | Connections

Restrict Access

Restrict Admin Console access either to the current machine or to specific IP addresses. Note: Access from the Master machine is always permitted. When entering multiple addresses, use comma (,) to separate the addresses.

☐ Enable access restrictions

Specify IP Addresses:

Authentication

Change the user name or password of the Admin Console account.

Admin Console User Name: admin

[Change User Name/Password...](#)

External Group

In addition to authenticating with the Admin Console account, allow Admin Console users to login with accounts that are members of the external group. This group must be defined on or accessible by the master machine in the FileMaker Server deployment.

☒ Use external group

Specify External Group:

[Test External Group](#)

Check for Updates

You can enable checking for updates.

☒ Enable FileMaker Server to check for updates

[Revert](#) [Save](#)

Configure Recommended Security Settings

1. In the Admin Console, navigate to the Database Server pane > Security tab.
2. If you intend to use external authentication, including Kerberos-based authentication, as a means to access any of the databases hosted on your server, set Client Authentication to "FileMaker and external server accounts;" otherwise set to "FileMaker accounts only." For more information on external authentication and setting up Kerberos-based authentication for your hosted database(s), see [FileMaker Authentication](#).

Database Server ?

FileMaker Clients | Databases | **Security** | Folders | Logging | Server Plug-Ins | Directory Service

Client Authentication

Specify how FileMaker Server authenticates FileMaker clients.

Amazon	Settings	<input type="checkbox"/>
Google	Settings	<input type="checkbox"/>
Microsoft	Settings	<input type="checkbox"/>

3. Enable SSL encryption. Under SSL Connections, check the boxes for "Use SSL for database connections," and under HTTP Strict Transport Security (HSTS), check the box for "Use HSTS for web clients."

Note: After SSL encryption has been enabled, you must stop and restart FileMaker Server in order for it to take effect.

Database Server ?

FileMaker Clients	Databases	Security	Folders	Logging	Server Plug-Ins	Directory Service
-------------------	-----------	----------	---------	---------	-----------------	-------------------

Client Authentication

Specify how FileMaker Server authenticates FileMaker clients.

FileMaker accounts only

File Display Filter

Filter the list of databases in the Launch Center, based on the FileMaker client account name and password.

☒ List only the databases each user is authorized to access

SSL Connections

Use Secure Sockets Layer (SSL) to encrypt data passed between FileMaker Server and FileMaker Pro, Go, and WebDirect. Restart the FileMaker Server service (Windows) or FileMaker Server background processes (macOS) to apply a change to this setting.

☒ Use SSL for database connections

Warning: The standard FileMaker SSL certificate installed by default on this server is available for test purposes only. A custom SSL certificate is required for production use. Obtain a custom SSL certificate from a [Certificate Authority \(CA\) supported by FileMaker](#).

Click Create Request to create a certificate signing request. Click Import Certificate to import a signed certificate you receive from a CA. Click View Certificate to see detailed information for the current SSL certificate.

Create Request... Import Certificate... View Certificate...

HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) requires that web-client connections use SSL encryption. Enable this setting only when the Web Server is using the default ports (HTTP port 80, HTTPS port 443).

☒ Use HSTS for web clients

Require Password-Protected Databases

Limit FileMaker Server to hosting only databases that require users to enter a password for Full Access privileges. A database that has a Guest account using the Full Access privilege set, a Full Access account with an empty password, or a Full Access account with the password stored in the database using the File Options dialog box "Log in Using" option is insecure and will not be opened.

☒ Host password-protected databases only

Revert Save

- Important:** SSL encryption can be regarded as truly secure (as indicated by the green lock icon displayed in FM clients) only when a custom SSL certificate is obtained and installed; see below for more info.
- Enable the option to "Host password-protected databases only." This will preclude the unintentional hosting of files without passwords. **Note:** By default, newly created FileMaker files have a full-access Admin user account with no password set, and are set to auto-login with this account. As best practice, the Admin account should either be assigned a secure password, or disabled (provided another full-access account exists or is created).

Custom SSL Certificates

SSL allows for the encryption of data passed between FileMaker Server and FileMaker clients, as well as the Admin Console. A critical component of this function is the SSL certificate residing on the server. The FileMaker Server application ships with a self-signed SSL certificate that does not verify the server name. This default certificate is intended only for test purposes, and a custom SSL certificate is required for production use. See [FileMaker Server SSL Certificates](#) for instructions on requesting and installing custom SSL certificates for use with FileMaker Server.

Other Tasks

For more instructions on how to upload your databases and create scheduled tasks to back them up, see Chapter 5 of the [FileMaker Server 16 Installation and Configuration Guide](#) (PDF).

Important: FileMaker Server's backup feature creates a local copy of your databases, stored on the host machine. You should still use another mechanism, such as [TSM](#), to back up those saved files to another secure location, in case of system failure.