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

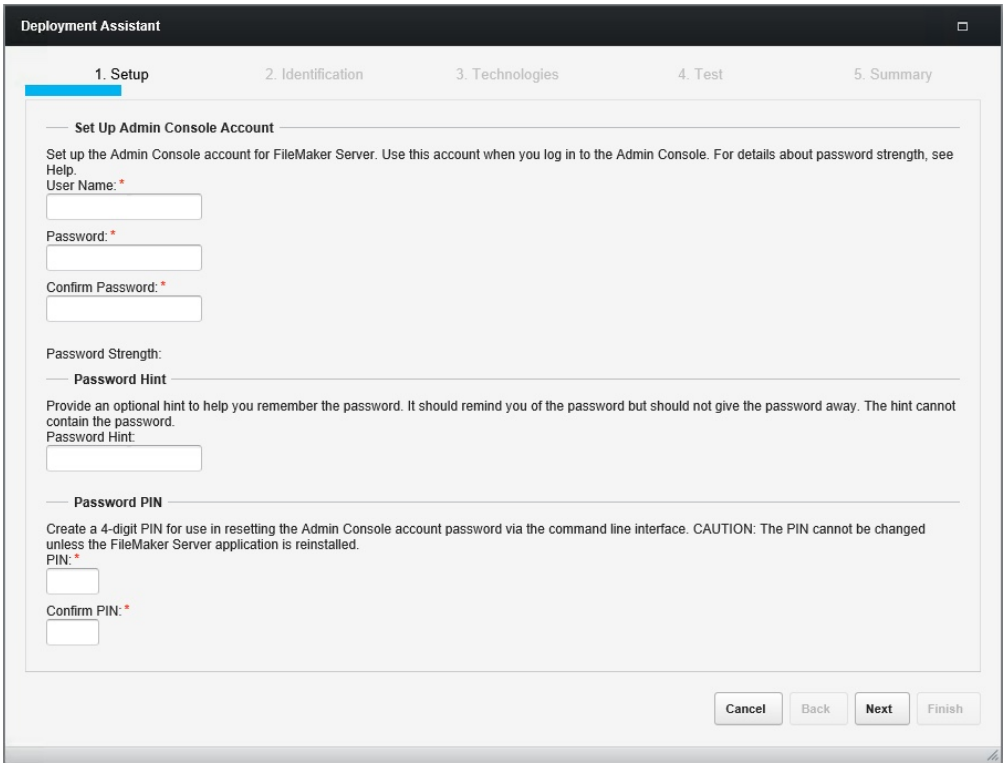
Follow standard procedures for initiating the installation process on your server machine. There are a few gotchas of note:

- 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.

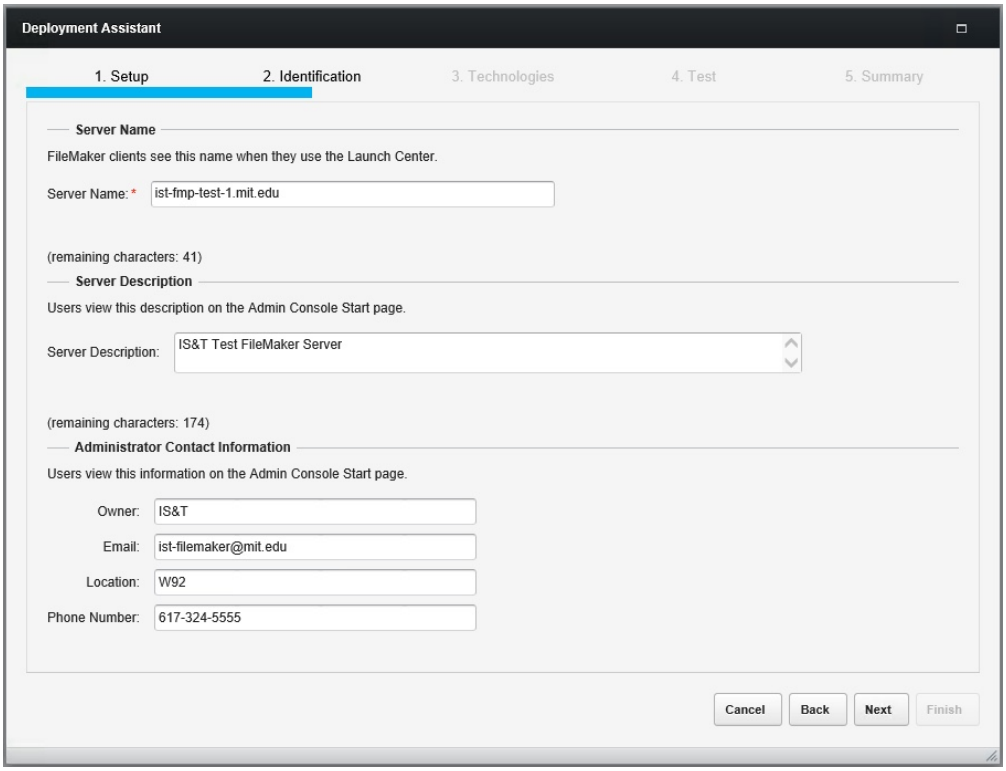
Deployment Assistant

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

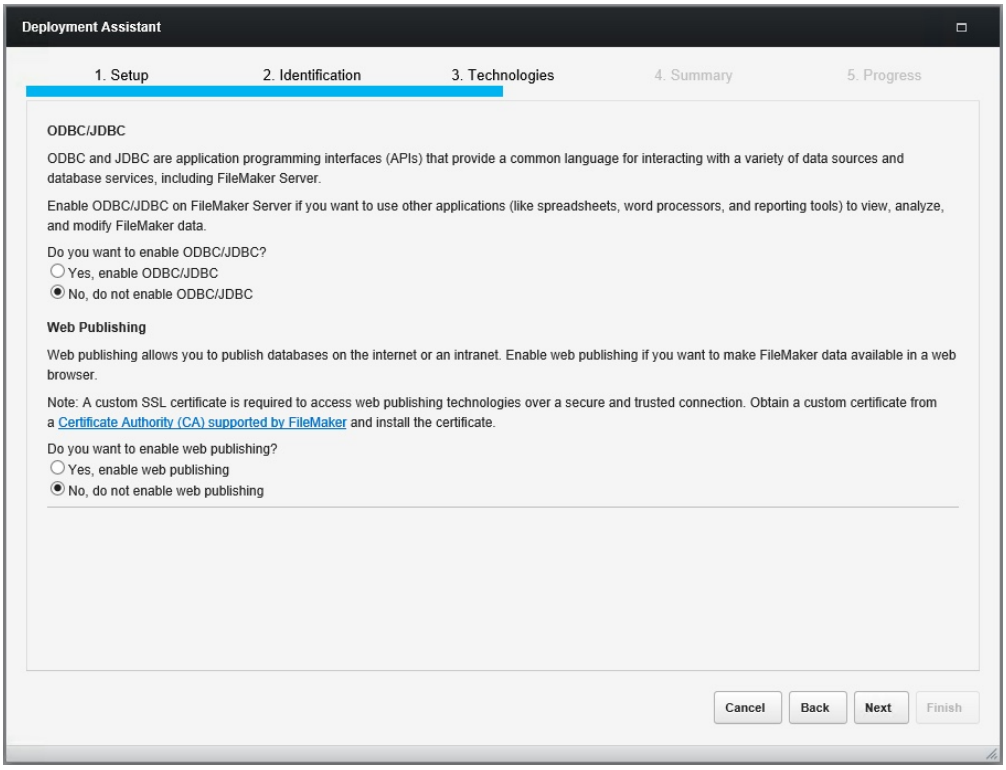
1. In the Setup screen, enter a User Name and Password for accessing the Admin Console, then click **Next**. The user name and password can be changed later through the Admin Console.
   Warning: For security reasons, do not use your Kerberos credentials.



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.



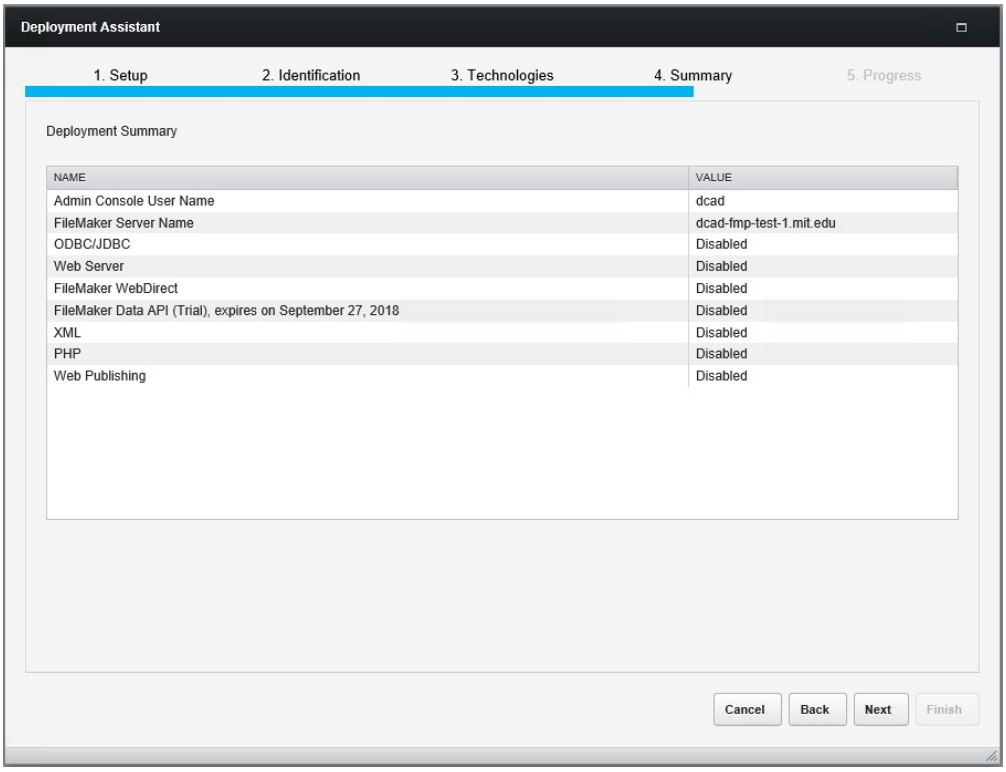
3. In the Technologies screen, under the ODBC/JDBC heading, unless you plan to allow connections via ODBC so that your hosted solutions may be used as ODBC data sources, select "No, do not enable ODBC/JDBC." You may also opt to enable or disable this feature at a later time as necessary; to do so, in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



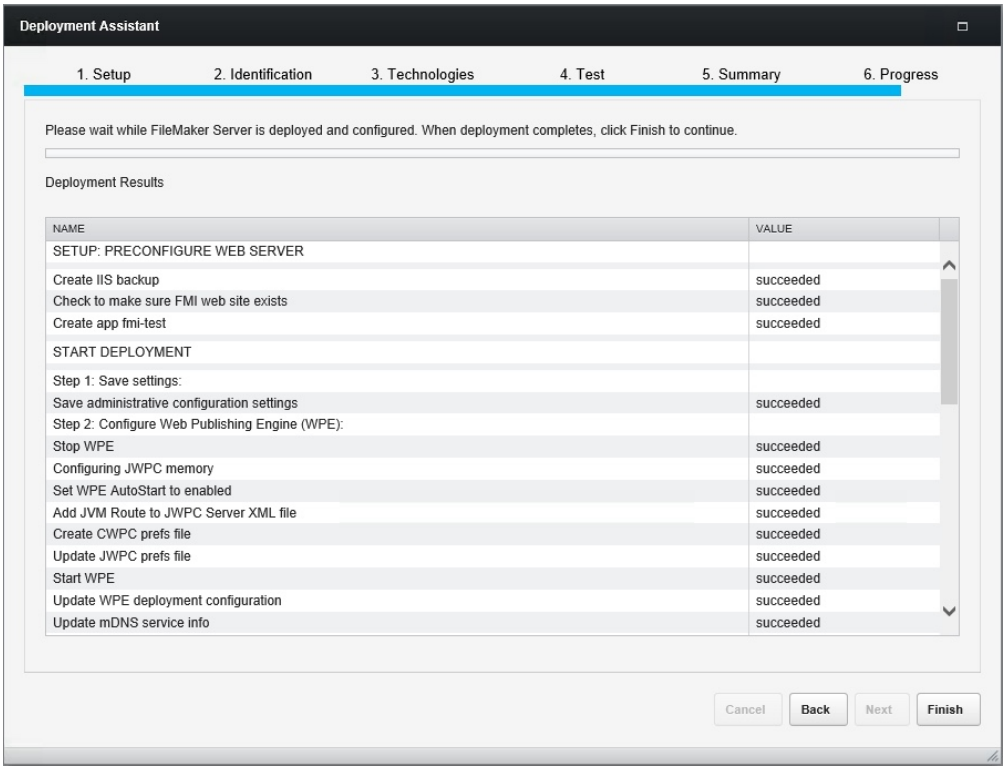
4. Still in the Technologies screen, under the Web Publishing heading, unless you plan to allow web connections to your files (via the FileMaker Data API, WebDirect, or custom web publishing), select "No, do not enable web publishing." You may also opt to enable or disable this feature at a later time 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.

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



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



FileMaker Server Admin Console

Accessing the Admin Console

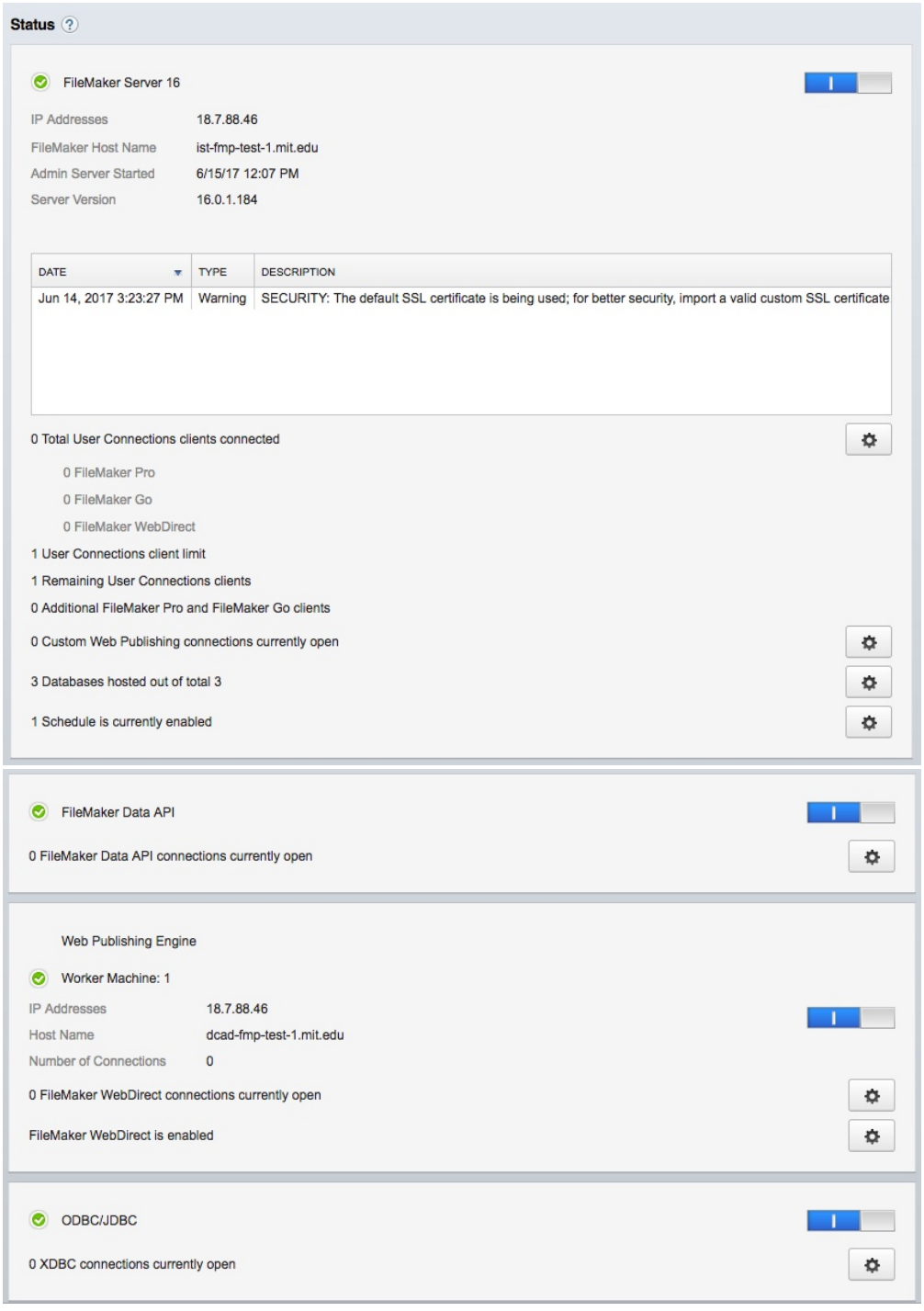
Once FileMaker Server has been installed and deployed, the Admin Console may be accessed by pointing a browser to:

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.

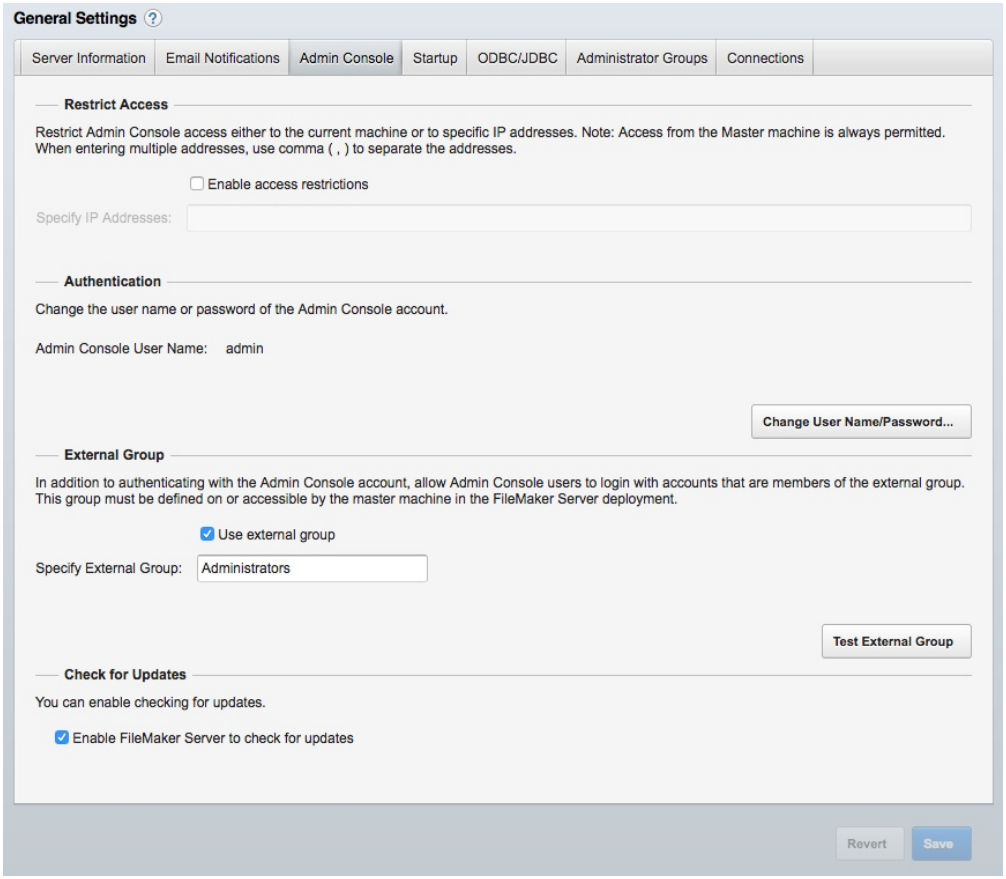
Note: The Status pane will only display the sections for FileMaker Data API, Web Publishing Engine, and ODBC/JDBC if you elected to enable those functions in the Deployment Assistant. You may revisit these settings in the Admin Console by choosing Server > Edit Deployment. If you do make changes to these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



Admin Console Access

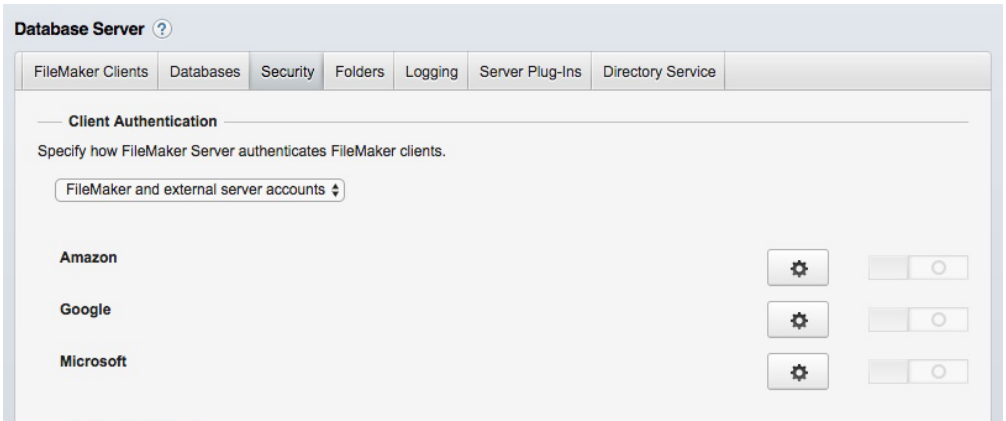
In addition to the User Name and Password set via the Deployment Assistant for accessing the Admin Console, you may allow access via an external server group. This is defined on the Admin Console > General Settings pane > Admin Console tab > External Group section. For information on how to use this 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.

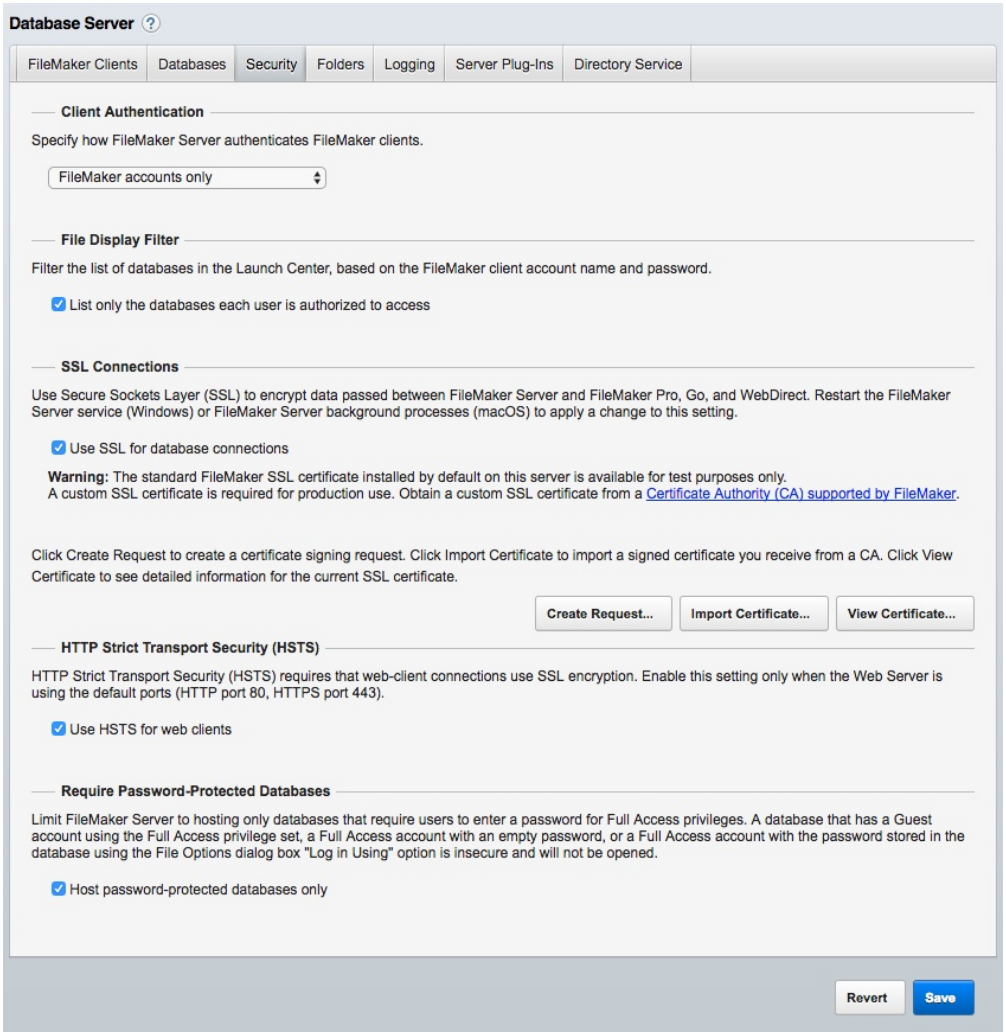


Configure Recommended Security Settings

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.



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.



4. **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.
5. 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.