Configuring FileMaker Databases For Kerberos Authentication

Configuring FileMaker Databases For Kerberos Authentication

It is possible to implement Kerberos-based external authentication for hosted FileMaker databases at MIT. Doing this requires modifying settings at both the server and database level, as well as creating Moira lists that function as access control lists.

This article covers the various tasks and configurations necessary in order to implement Kerberos authentication with FileMaker at MIT. For more information on FileMaker authentication in general, see FileMaker Authentication.

On this page:

Important Security Considerations

While it has many advantages, use of external authentication with FileMaker carries its own set of considerations, particularly with regards to security. Before getting started, it is extremely important to be mindful of the following:

1. In order to commit changes made in the Manage Security dialog in FileMaker databases (when editing accounts and privilege sets), you must enter the credentials of an internally authenticated full access account. As such, **even when employing external authentication, you must still maintain at least one internal full access FileMaker account**. Please refer to FileMaker Authentication for recommendations on setting up password-secured, full access FileMaker accounts.
2. **It is generally not recommended to use external authentication for full access accounts in FileMaker**, as this practice carries potential security risks. If an illegitimate user gains physical access to a FileMaker file with an external full access account, they may easily spoof the external group and gain entry to the file. If you choose to employ an external full access account, securing the server and any backup locations is of paramount importance. In addition, as noted above, remember that external full access accounts cannot be used to commit changes made in the Manage Security dialog; this must be done with an internal full access FileMaker account.
3. The use of Moira lists for FileMaker access control requires responsible Moira list management. Moira list setup is described in detail later on in this article, but understand these key points before starting your implementation:
   - A unique, dedicated Moira list should be created for **each privilege set within each FileMaker database application**. For example, if you manage two FileMaker databases, and each one has three active privilege sets, you will need to create six Moira lists.
   - **Do not** reuse Moira lists across multiple FileMaker applications. It's very rare that the users and privilege sets would be identical between databases.
   - **Do not** use Moira lists created for FileMaker access control for any other purpose, such as an office email list.

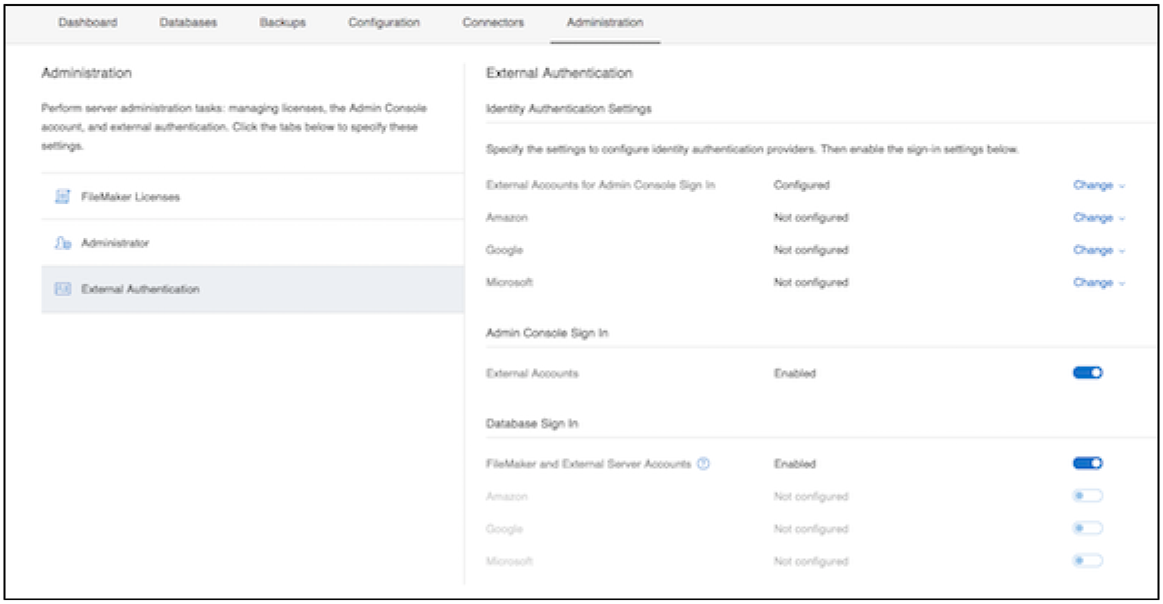
Server Configuration

MIT WIN domain

When hosted with FileMaker Server, FileMaker databases may be set up to use external authentication, allowing authentication via local server groups and/or LDAP. At MIT, when a FileMaker server is added to the win.mit.edu domain, it has access to MIT's LDAP directory service, thereby allowing for Kerberos-based external authentication. All IS&T-managed FileMaker servers are part of the MIT WIN domain, so if your DLC engages with IS&T for your FileMaker hosting needs (which we strongly recommend), this capability comes automatically. If your DLC manages its own Windows-based FileMaker server, you can add your server to the WIN domain to leverage this capability. IS&T is currently unable offer any support or guidance on Macintosh-based FileMaker servers.

FileMaker Server configuration

If you intend to use external authentication as a means for access to any of the databases hosted on your server, you must enable the external authentication option within the FileMaker Server application. In the FileMaker Server Admin Console 17, navigate to the **Administration Tab.** Under External Authentication, enable external accounts for Admin Console and FileMaker and External Server Accounts for Database Sign In.



Administration

Perform server administration tasks: managing licenses, the Admin Console account, and external authentication. Click the tabs below to specify these settings.

External Authentication

Identity Authentication Settings

Specify the settings to configure identity authentication providers. Then enable the sign-in settings below.

External Accounts for Admin Console Sign In — Configured
Amazon — Not configured
Google — Not configured
Microsoft — Not configured

Admin Console Sign In

External Accounts — Enabled

Database Sign In

FileMaker and External Server Accounts — Enabled
Amazon — Not configured
Google — Not configured
Microsoft — Not configured

Database Configuration

There are several steps involved in setting up external authentication for a specific FileMaker database application (which may itself be comprised of one or more FileMaker files).

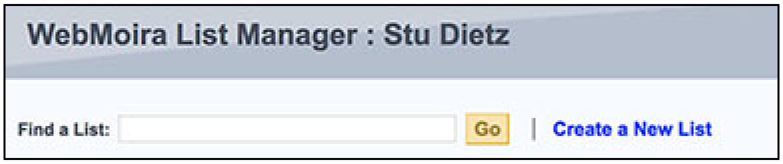
Database roles and privilege sets

The first step is to identify the various database user roles, or privilege sets, that may be assigned to users who will be accessing the database via external authentication. Privilege sets are defined in FileMaker by going to **File > Manage > Security > Privilege Sets** tab. Please refer to FileMaker documentation) for more information on the creation of privilege sets.

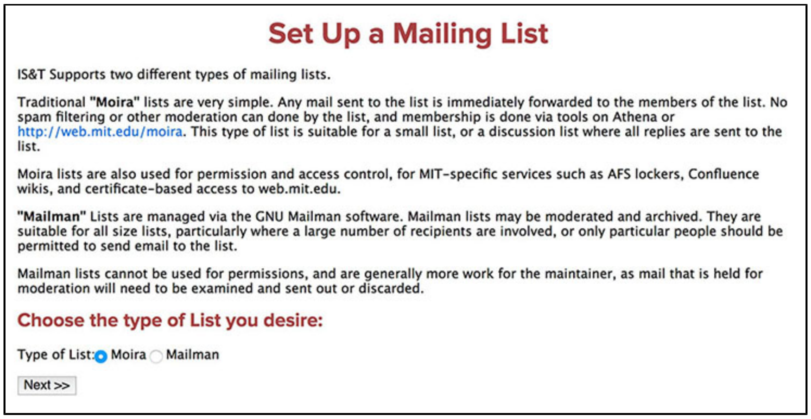
Moira list setup

For each privilege set identified above, you will need to create a Moira list that will function as an access control list defining all of the users with that particular privilege set. The following steps will guide you through this process; repeat all steps in full to create a Moira list for each privilege set.

1. Go to WebMoira.
2. Click **Create a New List**.



3. You will land on the *Mailing List setup screen*. Note that while this Moira list may be used as a mailing list, we do not intend to actually use it for that purpose. For *Type of List*, choose Moira, and click **Next**.



Set Up a Mailing List

IS&T Supports two different types of mailing lists.

Traditional **"Moira"** lists are very simple. Any mail sent to the list is immediately forwarded to the members of the list. No spam filtering or other moderation can done by the list, and membership is done via tools on Athena or http://web.mit.edu/moira. This type of list is suitable for a small list, or a discussion list where all replies are sent to the list.

Moira lists are also used for permission and access control, for MIT-specific services such as AFS lockers, Confluence wikis, and certificate-based access to web.mit.edu.

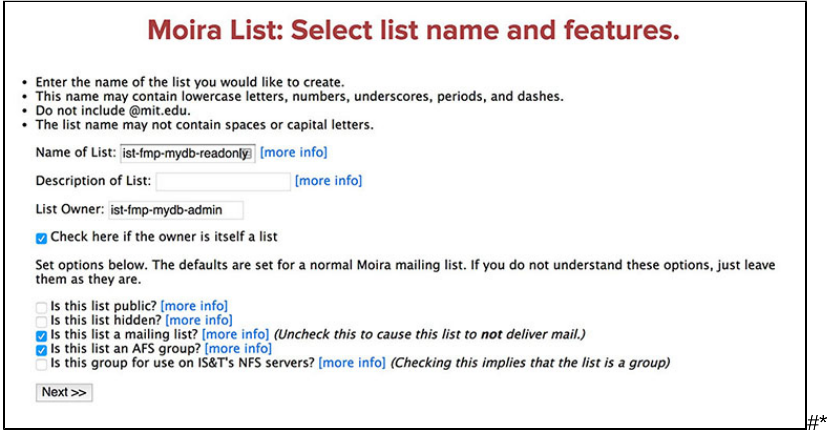
"Mailman" Lists are managed via the GNU Mailman software. Mailman lists may be moderated and archived. They are suitable for all size lists, particularly where a large number of recipients are involved, or only particular people should be permitted to send email to the list.

Mailman lists cannot be used for permissions, and are generally more work for the maintainer, as mail that is held for moderation will need to be examined and sent out or discarded.

Choose the type of List you desire:

Type of List: ● Moira ○ Mailman

4. You will then land on the *Moira List configuration screen*.



Moira List: Select list name and features.

- Enter the name of the list you would like to create.
- This name may contain lowercase letters, numbers, underscores, periods, and dashes.
- Do not include @mit.edu.
- The list name may not contain spaces or capital letters.

Name of List: ist-fmp-mydb-readonly [more info]

Description of List: [more info]

List Owner: ist-fmp-mydb-admin

☑ Check here if the owner is itself a list

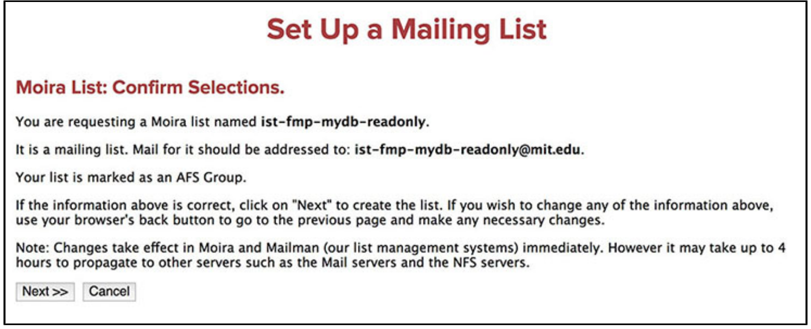
Set options below. The defaults are set for a normal Moira mailing list. If you do not understand these options, just leave them as they are.

☐ Is this list public? [more info]
☐ Is this list hidden? [more info]
☑ Is this list a mailing list? [more info] *(Uncheck this to cause this list to **not** deliver mail.)*
☑ Is this list an AFS group? [more info]
☐ Is this group for use on IS&T's NFS servers? [more info] *(Checking this implies that the list is a group)*

#* For list name, the recommended naming convention is `dlcname-fmp-dbname-privsetname`; for example, `ist-fmp-mydb-readonly`.

- For list owner, enter the MIT Kerberos account username or existing Moira list name for the person(s) who will manage the list membership. If the owner is itself a list, check the box indicating so.
  Note: In general, we recommend creating a separate Moira list specifically for managing membership of these database access lists, with naming convention `dlcname-fmp-dbname-admin` (or something similar). Admin lists such as these should be configured to be self-owned, but otherwise would have the same settings as described here.
- Check off the box for **Is this list an AFS group**. This is the setting that turns the list into an access control list.
- The remaining settings can be left as-is. However, if you would like to hide the list name and membership from public view on WebMoira, check off **Is this list hidden?**
- Then click **Next.**

5. In the *Confirm Selections screen*, ensure the information you entered is correct, and then click **Next.**



Set Up a Mailing List

Moira List: Confirm Selections.

You are requesting a Moira list named **ist-fmp-mydb-readonly**.

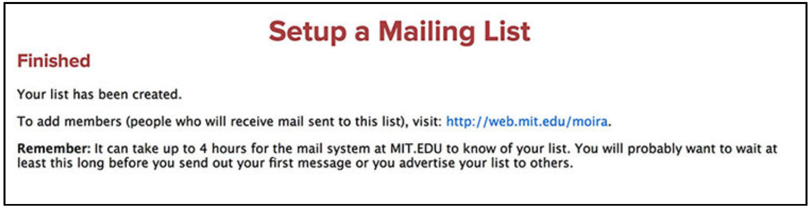
It is a mailing list. Mail for it should be addressed to: **ist-fmp-mydb-readonly@mit.edu**.

Your list is marked as an AFS Group.

If the information above is correct, click on "Next" to create the list. If you wish to change any of the information above, use your browser's back button to go to the previous page and make any necessary changes.

Note: Changes take effect in Moira and Mailman (our list management systems) immediately. However it may take up to 4 hours to propagate to other servers such as the Mail servers and the NFS servers.

6. In the final confirmation screen, click on the WebMoira link to return to the WebMoira list manager page.



Setup a Mailing List

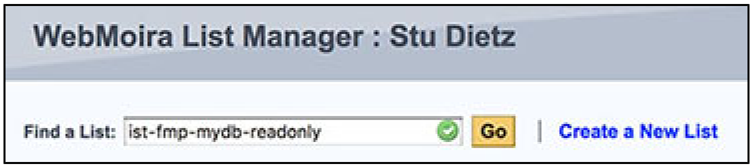
Finished

Your list has been created.

To add members (people who will receive mail sent to this list), visit: http://web.mit.edu/moira.

Remember: It can take up to 4 hours for the mail system at MIT.EDU to know of your list. You will probably want to wait at least this long before you send out your first message or you advertise your list to others.

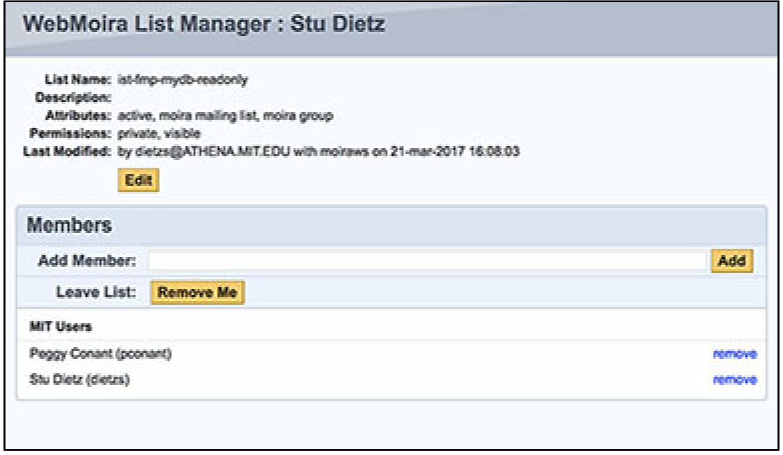
7. Back on the *WebMoira list manager page*, type your new list name into the **Find a list** box, and click **Go**.



WebMoira List Manager : Stu Dietz

Find a List: ist-fmp-mydb-readonly

8. Finally, populate the list membership with the individual database users with the selected privilege set.



WebMoira List Manager : Stu Dietz

List Name: ist-fmp-mydb-readonly
Description:
Attributes: active, moira mailing list, moira group
Permissions: private, visible
Last Modified: by dietzs@ATHENA.MIT.EDU with moiraws on 21-mar-2017 16:08:03

MIT Users

Peggy Conant (pconant) remove
Stu Dietz (dietzs) remove

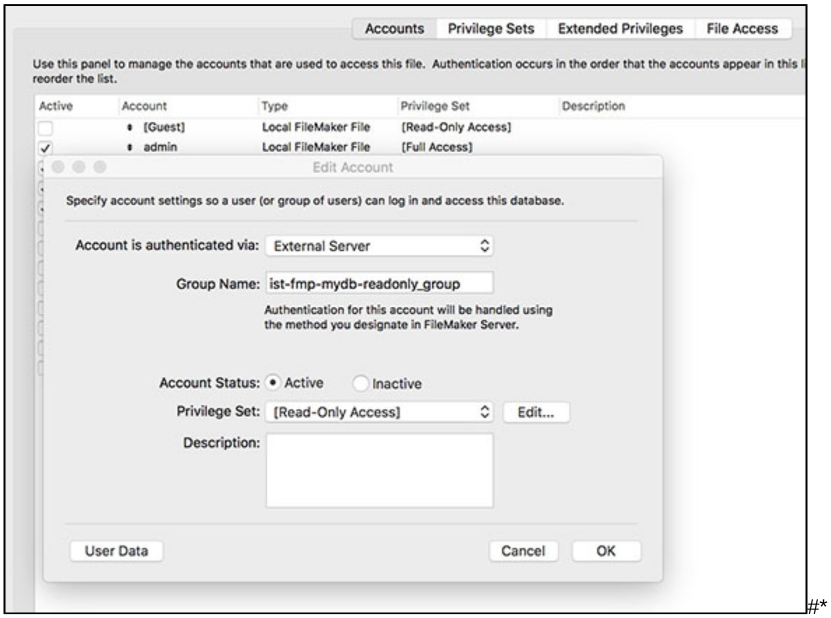
9. **Note**: When a user should no longer be able to access your database (such as when they leave MIT), be sure to remember to remove them from the appropriate Moira list.

Database security settings

Now that we've set up our Moira list(s) for each active privilege set in our FileMaker database, the final step is to create corresponding external account(s) in the database. The following steps will guide you through this process; repeat all steps in full to create an external account for each privilege set/Moira list.

Note: If your FileMaker database application is comprised of multiple files, you will also need to repeat this entire process for each FileMaker file.

1. Open the FileMaker database file with a full access account, and choose **File > Manage > Security > Accounts** tab.
2. Click **New** to create a new account.
3. You will then land on the *Edit Account* screen.



Use this panel to manage the accounts that are used to access this file. Authentication occurs in the order that the accounts appear in this l
reorder the list.

Active	Account	Type	Privilege Set	Description
□	[Guest]	Local FileMaker File	[Read-Only Access]	
✓	admin	Local FileMaker File	[Full Access]	

Edit Account

Specify account settings so a user (or group of users) can log in and access this database.

Account is authenticated via: External Server

Group Name: ist-fmp-mydb-readonly_group

Authentication for this account will be handled using the method you designate in FileMaker Server.

Account Status: ● Active ○ Inactive

Privilege Set: [Read-Only Access]

Description:

#* For *Account is authenticated via*, select **External Server**. The *Account Name* field label will then change to *Group Name*.

- For *Group name*, enter the name of the Moira list, **followed by the suffix "_group"**. For example, `ist-fmp-mydb-readonly_group`.
- Select the corresponding privilege set.
- Then click **OK** to finish creating the external account.

When finished creating an external account for each privilege set/Moira list, click **OK** at the bottom right of the Manage Security dialog, and enter the credentials for an internal full access account to commit the security changes.

Example use case

Let's say that I work in IS&T and I have two FileMaker databases: one called MyDB and another called MyOtherDB. Both databases require an internally authenticated full access account for use by the developer and/or database administrator. For all other users, MyDB employs two active privilege sets called Data Entry and Read Only, and MyOtherDB also employs two privilege sets called Data Entry and Limited Data Entry. The Kerberos authentication setup for these databases would be as follows:

1. MyDB
   - Privilege set: Data Entry. Moira list: `ist-fmp-mydb-dataentry`. FileMaker external account: `ist-fmp-mydb-dataentry_group`.
   - Privilege set: Read Only. Moira list: `ist-fmp-mydb-readonly`. FileMaker external account: `ist-fmp-mydb-readonly_group`.
2. MyOtherDB
   - Privilege set: Data Entry. Moira list: `ist-fmp-myotherdb-dataentry`. FileMaker external account: `ist-fmp-myotherdb-dataentry_group`.
   - Privilege set: Limited Data Entry. Moira list: `ist-fmp-myotherdb-limited`. FileMaker external account: `ist-fmp-myotherdb-limited_group`.

Note that we have created a unique Moira list for each privilege set within each database. In this case, two databases with two privilege sets each means four total Moira lists. Even though both databases have a privilege set called Data Entry, we still need to create separate "Data Entry" Moira lists. This is because it's unlikely that the exact same users should be able to access both applications. Even if that were the case, it's still best to create separate lists to allow for more explicit access control should the users or needs ever change in the future.

Finally, a note on Moira list ownership/management: If I were the sole FileMaker database administrator in IS&T, it might be perfectly acceptable for me to be the owner of each of the four Moira lists. However, if multiple individuals in my group need to be able to manage these access lists, then I would create an additional self-owned Moira list called `ist-fmp-acladmin` (i.e. access control list admin) to define the individuals who can manage the four access lists. I would then change the owner of the four Moira lists above to be `ist-fmp-acladmin`.

User Login

Using Kerberos to login to FileMaker

Any users who are a member of a Moira list with an associated external account in FileMaker as described above will now be able to authenticate to the FileMaker database with their Kerberos username and password. They will also have the privilege set associated with the particular Moira list.

Note: If a user is a member of multiple Moira lists with corresponding external accounts in FileMaker, they will authenticate to FileMaker with whichever external account is listed first (from top to bottom) in the **File > Manage > Security > Accounts tab**.

Windows and Single Sign-On

It's common for Windows users at MIT to have their local machine be on the MIT WIN domain. When such a user logs in to their machine, they enter their Kerberos credentials to authenticate to win.mit.edu. In this setup, when a user first opens a hosted FileMaker database with external authentication enabled, the database will automatically attempt to log them in based on membership of any external groups available via the server. Hence, if the user is a member of any Moira lists (or local server groups on the FileMaker server machine) which match an external account defined in the database, they will be automatically logged in with that account. This approximates the single sign-on experience. To bypass this behavior and always get prompted for FileMaker credentials, the user must hold down the Shift key while opening the database.

There is no equivalent single sign-on behavior for Mac users.

Additional Resources

More information on External Authentication can be found in FileMaker's in-depth guide.

For any questions related to FileMaker at MIT, please contact filemaker-support@mit.edu.