Adding oAuth to the External Authentication Alphabet Soup

FileMaker Developer Conference 2017

Session ADV002

Submitted by
Wim Decorte
Senior Technical Architect
Soliant Consulting, Inc.

With more than a little assistance from
Steven H. Blackwell
President & CEO
Management Counseling Services

April 7, 2017

Why read this document?

This is a long document but do not let that discourage you. The bulk of it is a very detailed step-by-step on how to set up FileMaker Server to take advantage of the new External Authentication providers.

It took us a while to figure out how to get all the moving parts clicking together and we hope that we can get you through that learning curve very quickly. The terminology and steps on the Azure, Google and Amazon pages are not always intuitive and it can be confusing at first to find your way and know what to configure there and what pieces of information that FileMaker Server requires. This guide will help with that.

In addition to the detailed how-to, we have also tried to provide some background and overall perspective and links to other relevant documentation.

If you have any comments or suggestions, feel free to contact me by email: wdecorte@soliantconsulting.com

External Authentication / Federated Identity Management

Back in 2004 when the FileMaker 7 product line was launched it came with support for External Authentication, or in more modern terms: support for Federated Identity Management.

External Authentication (EA) allows developers to choose something other than FileMaker to determine who the user is and once the user is identified, FileMaker will trust that authentication and will then apply the proper authorization through the privilege set.

So who does FileMaker trust to do the authentication? Ever since it was introduced the authentication could be provided by these three providers:

- Windows Active Directory (AD)
- Apple's Open Directory (OD)
- Operating System (local) accounts & groups on the FileMaker Server

In the FileMaker 16 product line, three more identity providers are added:

- Microsoft Azure Active Directory
- Amazon
- Google

With those, users can use their existing Microsoft accounts, gmail accounts and Amazon store accounts to access your FileMaker solutions. This document will describe how these new providers works and how to set it up. And why you would want to and what to watch out for.

Authentication is not to be confused with Authorization of course. Authentication covers the "who are you" part of log-in process whereas Authorization takes care of "what are you allowed to do". This document only discusses authentication. FileMaker 16 has new features in the authorization department too; you will find those described in the white paper 'New Security Features Version 16'[1]

Why use External Authentication?

The main reason for using EA is to leverage an existing identity management structure. If the accounts already exist outside of FileMaker then there is no need to create and manage separate identities and their credentials in FileMaker.

When identities can be managed in one place only it has an obvious security benefit. If an account is disabled in say Active Directory then it automatically trickles down to the FileMaker solution and that account can not be used anymore to gain access to FileMaker. That happens automatically without any modification to the FileMaker solution. Similarly, adding accounts or moving accounts in and out of roles (groups) can all be managed in one central place outside of FileMaker.

Those trusted identity management systems can also offer tools that FileMaker does not provide natively. Notably, they offer multi-factor authentication mechanisms, the ability to restrict logins to particular time frames and locations for instance.

Back in 2004, Steven H. Blackwell and I wrote a very detailed 60-page Technology Brief[2] that explains how EA works with the three traditional providers (AD,OD, Local). That document has been updated over the years through version 9 of FileMaker. And while it has not been updated since then, the core concepts have not changed at all and EA still functions today as it is described in that document. The screenshots are out of date but still meaningful. I will defer to that document for a full explanation of how EA works with the traditional three and in this document we will concentrate on the three new providers.

---

[1] Blackwell, Steven H. *New Security Features Version 16,* http://fmforums.com/files/file/90-new-security-features-version-16/

[2] Decorte, Wim and Blackwell, Steven H. *Server External Authentication*. (FileMaker, Inc. Santa Clara, CA. 2007), http://fmforums.com/files/file/89-external-server-authentication/

The Alphabet Soup: EA, SSO, LDAP, AD, OD, OAuth,…

There are quite a few acronyms in play here so let's run through them quickly.

EA = External Authentication. This is the most common term used for the use of federated identities in the FileMaker product line.

SSO = Single Sign On. SSO is an edge case of EA. SSO happens when a user is already authenticated against the identity provider and gains access to another system without being challenged for credentials; the logon happens automatically and in the background. Note that using features of the operating system like Keychain (Mac) or Credential Manager (windows) are not considered SSO. In the FileMaker product line, SSO is only possible in an all Windows line-up:

- User is logged into a Windows machine with an AD account
- FileMaker Server runs on Windows, on a member server in that same AD domain

LDAP = Lightweight Directory Access Protocol. As the name implies it is a protocol, a language if you will to speak to Directory Services. Much like HTTP is a protocol to speak to a web server. All things LDAP are entirely irrelevant for authentication into a FileMaker solution. FileMaker Server has a Directory Services tab in its admin console and FileMaker Pro has an LDAP config area but those are **NOT** used at all in authenticating users. Those features only serve to find a FileMaker Server on the network. That LDAP feature is very seldom used in our experience but very often misunderstood to be part of the authentication process. It is not.

AD = Active Directory. The default Windows Directory Service.

OD = Open Directory. The default Mac Directory Service.

IP = Identity Provider, when used in the context of identity management, a service/system that stores and manages identities and provices authentication services.

I&AM / IAM = Identity & Access Management. A general catch-all phrase that covers the concept of identity management. This is a term that used very explicitly in the Amazon documentation.

OAuth[3] = Open Authorization. An industry standard protocol that uses tokens between systems to authenticate users between those systems.

FIM = Federated Identity Management. Same concept as EA. When two systems 'agree' so that one system trusts the other's authentication mechanism and delegates the identity management then those two systems have formed a federation[4] around that identity management.

---

[3] https://oauth.net/2/

[4] as in "joining together separate entitities"

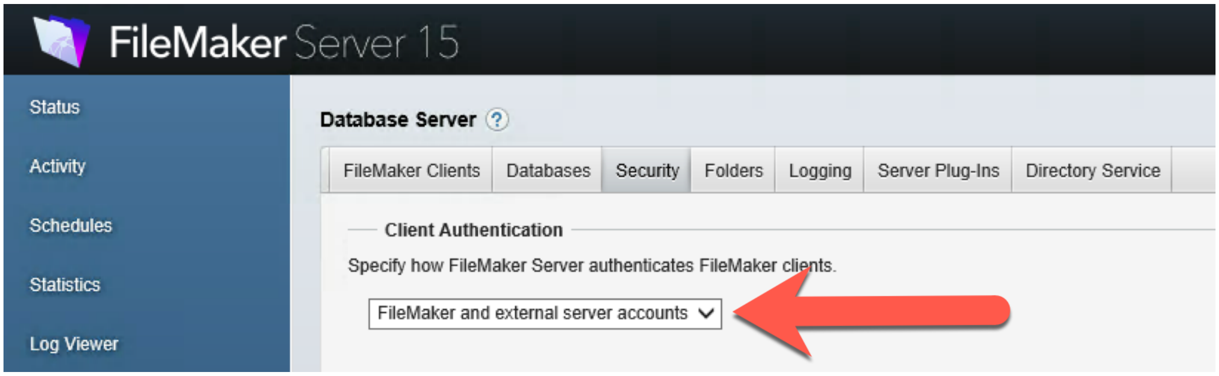
Old vs. New

The main difference between the three traditional identity providers and the new ones, is that original ones depend on and work off how the Operating System of the FileMaker Server machine is configured.

As such they depend on the authentication protocol used by operating system in the negotiation with their respective identity providers. On both Windows and Mac for instance that is often the Kerberos[5] protocol when Active Directory or Open Directory is involved.

In the traditional model FileMaker Server just hands off the authentication request to the operating system and waits for the operating system to come back with confirmation that the user is genuine and a list of groups that the user belongs to.

In the admin consoles for FileMaker Server 15 and earlier versions, that is reflected by a simple selection to use 'FileMaker and External Accounts'. There is no futher configuration that needs to be done in FileMaker Server.

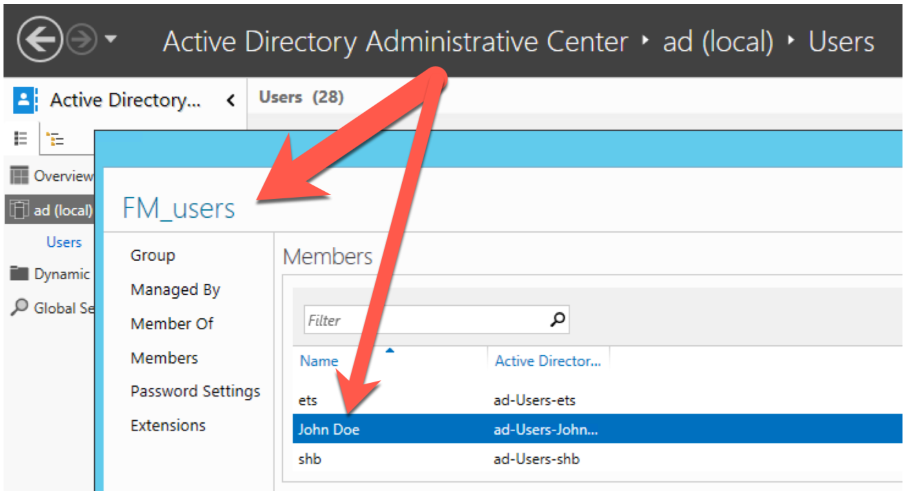


Client Authentication

Specify how FileMaker Server authenticates FileMaker clients.

FileMaker and external server accounts

As mentioned before, the traditional EA mechanism works entirely on the concept of groups. In the example below there is a group named "FM_users" in Active Directory and a user named "John Doe" is a member of that group.

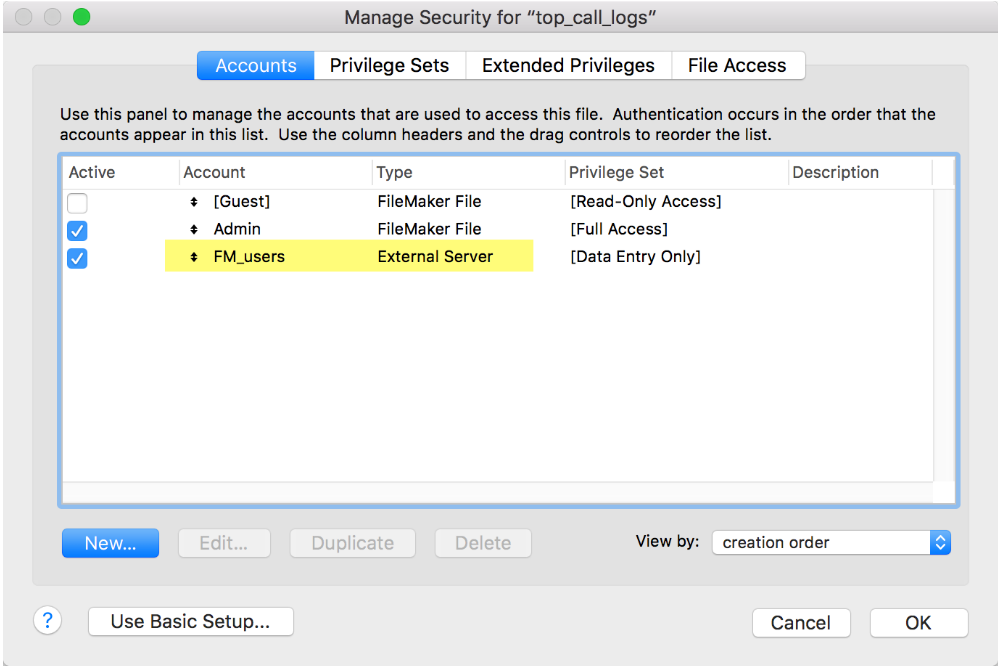


Name	Active Director...
ets	ad-Users-ets
John Doe	ad-Users-John...
shb	ad-Users-shb

---

[5] https://web.mit.edu/kerberos/

In the FileMaker solution we have an ‘external server account named to match the group name in Active Directory:

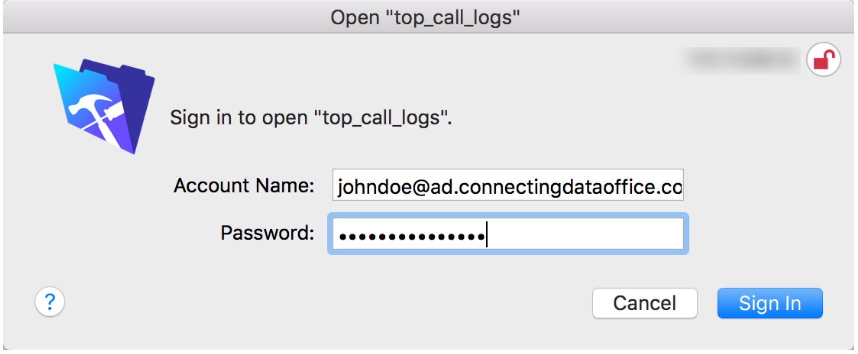


Use this panel to manage the accounts that are used to access this file. Authentication occurs in the order that the accounts appear in this list. Use the column headers and the drag controls to reorder the list.

Active	Account	Type	Privilege Set	Description
☐	[Guest]	FileMaker File	[Read-Only Access]	
☑	Admin	FileMaker File	[Full Access]	
☑	FM_users	External Server	[Data Entry Only]	

View by: creation order

And when John Doe logs into the solution:



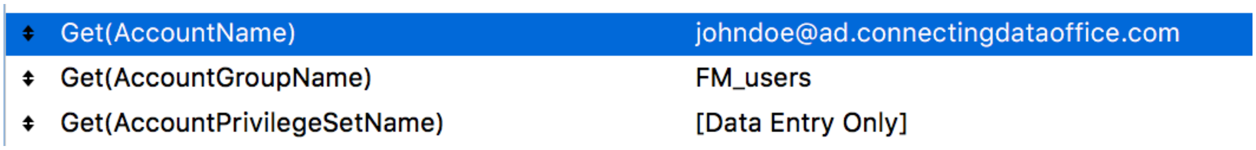
Sign in to open "top_call_logs".

Account Name: johndoe@ad.connectingdataoffice.co

Password: •••••••••••••••

FileMaker Server hands the logon request off to Windows, Windows in turn talks to the AD to verify the John Doe identity and returns a list of AD groups that John Doe belongs to. Since the FM_users group is one of those groups and there is a match in the groups set up in FileMaker, John Doe is granted acess to the FileMaker solution with the privilege set attached to the FM_users account in FM.

Using the Get() functions we can get the relevant information about the user:



Get(AccountName)	johndoe@ad.connectingdataoffice.com
Get(AccountGroupName)	FM_users
Get(AccountPrivilegeSetName)	[Data Entry Only]

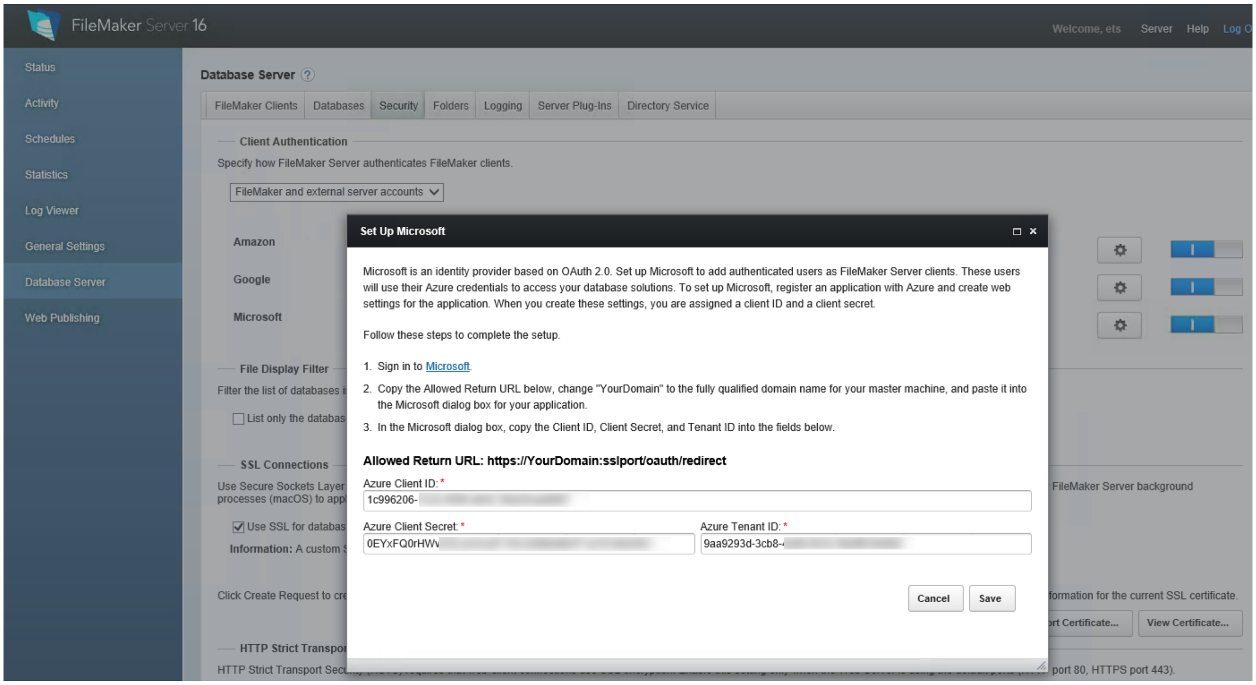
Although we do not have an individual account for John Doe in the FileMaker solution the Get(AccountName) will properly return the AD account that was used to log in.

Note

The Get(AccountGroupName) is new in FileMaker 16 and a very welcome addition to our arsenal.

That was the 'Old'. And everything we talked about so far works just fine in 16 as it has since FileMaker 7. The newly added providers however work slightly differently.

The three new providers (Azure, Amazon, Google) use the OAuth2 protocol to communicate with the identity provider and do the authentication dance. There is no hand-off of the authentication request to the operating system. Because there is no handoff to the operating system, everything needs to be configured in the FileMaker Server admin console. Below is an example of the configuration to have Microsoft Azure AD take care of the identity verification. As you can see in the screenshot when you toggle the option for 'FileMaker and External Accounts' you will have the option to choose one or more of the additional identity providers and the gear icon gives you the setup dialog to plug in all the relevant configuration details to make sure that FileMaker Server and the chosen provider can communicate properly.



Specify how FileMaker Server authenticates FileMaker clients.

FileMaker and external server accounts

Microsoft is an identity provider based on OAuth 2.0. Set up Microsoft to add authenticated users as FileMaker Server clients. These users will use their Azure credentials to access your database solutions. To set up Microsoft, register an application with Azure and create web settings for the application. When you create these settings, you are assigned a client ID and a client secret.

Follow these steps to complete the setup.

1. Sign in to Microsoft.
2. Copy the Allowed Return URL below, change "YourDomain" to the fully qualified domain name for your master machine, and paste it into the Microsoft dialog box for your application.
3. In the Microsoft dialog box, copy the Client ID, Client Secret, and Tenant ID into the fields below.

Allowed Return URL: https://YourDomain:sslport/oauth/redirect

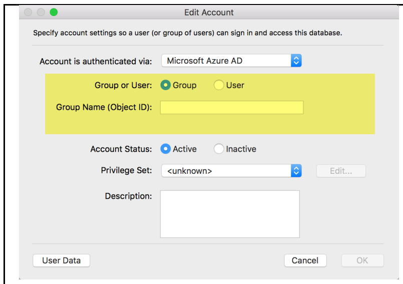
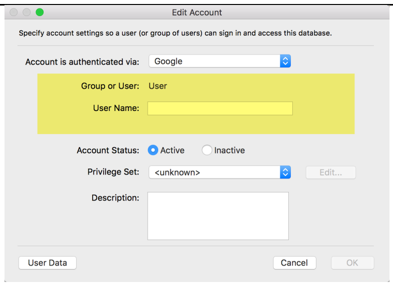
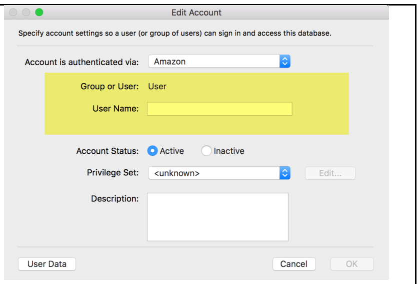
Azure Client ID: * 1c996206-[redacted]

Azure Client Secret: * 0EYxFQ0rHWv[redacted]

Azure Tenant ID: * 9aa9293d-3cb8-[redacted]

Another major difference is that two of the three new providers (Google and Amazon) only work for individual accounts. You can not set up groups in Google or Amazon and use those in the FileMaker solution. To some extent this negates one of the big benefits of using External Authentication: you do need to maintain individual account names in the FileMaker solution when using Google or Amazon.

The implementation for Microsoft Azure AD does offer both choices: add individual accounts to FileMaker or use Azure AD groups. That makes Auzre AD the implementation that is easiest to manage.

 Edit Account Specify account settings so a user (or group of users) can sign in and access this database. Account is authenticated via: Microsoft Azure AD Group or User: ● Group ○ User Group Name (Object ID): Account Status: ● Active ○ Inactive Privilege Set: <unknown> Description:	 Edit Account Specify account settings so a user (or group of users) can sign in and access this database. Account is authenticated via: Google Group or User: User User Name: Account Status: ● Active ○ Inactive Privilege Set: <unknown> Description:	 Edit Account Specify account settings so a user (or group of users) can sign in and access this database. Account is authenticated via: Amazon Group or User: User User Name: Account Status: ● Active ○ Inactive Privilege Set: <unknown> Description:
Microsoft Azure AD: both groups and invidivual users.	Google: only individual users	Amazon: only individual users

In the next sections we will go through the setup for each of the providers.

The OAuth dance

Before we get into the detailed setup, a quick word on the OAuth2 protocol that lies underneath all of this. Understanding the OAuth flow can help us make sense on how the configuration needs to be done and where to look for the information that is needed to complete the setup. Gaining some familiarity with these basics will certainly help in understanding the documentation that Microsoft, Google and Amazon have available on the subject[6].

The single most important aspect to the flow is that the actual login, the authentication is done on a a web site by the authentication provider. Not inside FileMaker. The external provider maintains the 'identity', the information about the user and its credentials. As we have seen earlier, in FileMaker you do have to maintain a matching account name or group name.

---

[6] See: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-protocols-oauth-code and https://developers.google.com/identity/protocols/OAuth2

Some common elements

There are some common elements to the configuration of all three OAuth services. We will discuss them here instead of repeating them for all three of them.

The 'app'

Microsoft Azure and Google require you to set up an 'app' on their side. Amazon requires either an app or a security profile. To avoid confusion I will not use 'app' for the FileMaker side of things but will use the term 'solution' for the FileMaker file (or files) that contains your business logic and data.

The app on the Azure / Amazon / Google side is basically just a placeholder. We need just the most basic configuration, enough so that it can give information like the 'Client ID' and 'Client Secret' that we need to input in the FileMaker Server configuration.

Those 'apps' will never be accessed directly by your clients, they are just required as passthroughs for FileMaker Server. However most of the documentation on Azure / Amazon / Google is based on the assumption that users will access the app. As such that documentation can be somewhat misleading and irrelevant for our purposes.

Redirect url

When Azure, Google or Amazon has authenticated the user it needs to know where to send the reply to so that FileMaker can complete the process. They a need a url that they can send that notification to. That url is sometimes also referred to as 'Reply url' or 'Allowed Return url'.

The url has to be the fully qualified domain name of your FileMaker Server or the Master machine in a multi-machine deployment. The url has the endpoint **`/oauth/redirect`** appended to the domain name.

The url has to use HTTPS. If you use a non-default HTTPS port (the default is 443) then you need to include the port as part of the url. If you use the default HTTPS port you can safely omit the port number.

In the examples below, my FileMaker Server is available on https://xxxxxxxx.soliant.cloud and uses the default SSL port. That makes the redirect url: https://xxxxxxxx.soliant.cloud/oauth/redirect.

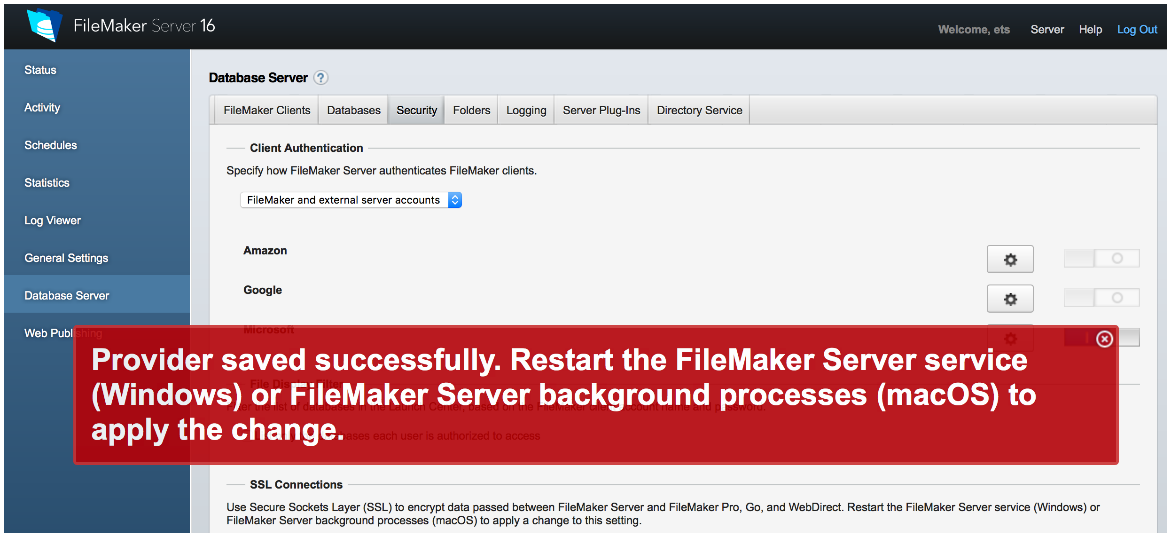
Important!

This means that the FileMaker Server (master) machine needs to be reachable from the internet on the configured address and HTTPS port. The server also needs to be able to reach Azure / Google / Amazon. The FileMaker Server machine therefore needs both incoming and outgoing internet access. Depending on the deployment environment that will mean setting up the proper DNS configuration, firewall rules and port forwarding.

It also implies that there is a custom SSL certificate installed in FileMaker Server to cover the domain name.

FileMaker Server restart

When you save the FileMaker Server configuration you will be prompted to restart the main FileMaker Server service. So do this process when you have a maintenance windows that users do not need to work in the hosted solutions. Without the restart, the authentication will not work.



Specify how FileMaker Server authenticates FileMaker clients.

FileMaker and external server accounts

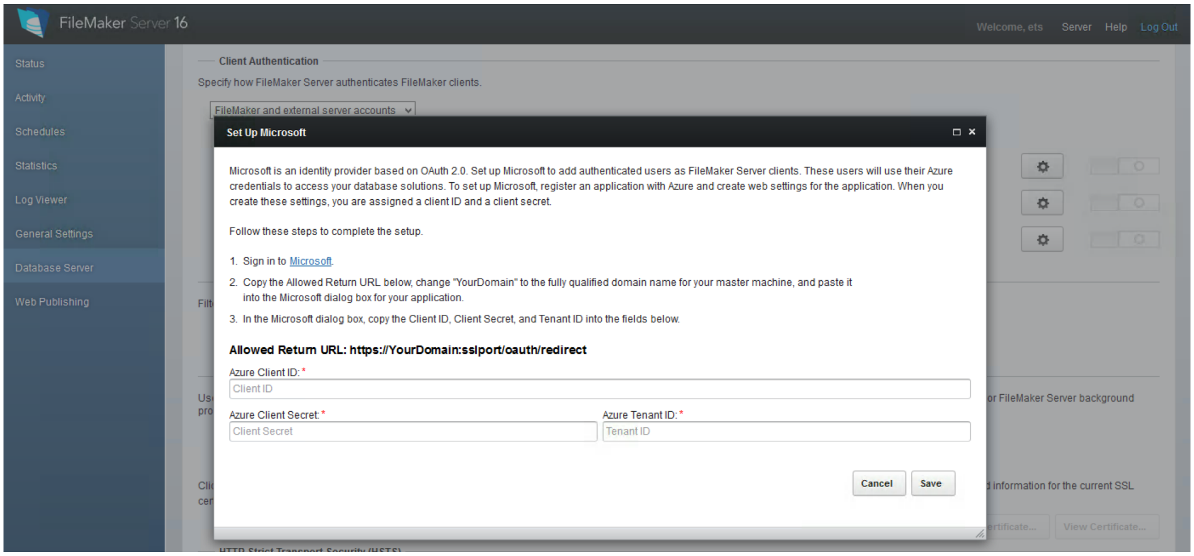
Provider saved successfully. Restart the FileMaker Server service (Windows) or FileMaker Server background processes (macOS) to apply the change.

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.

Microsoft Azure AD

Let's start with the Microsoft Azure AD setup. It is the most intricate one but it is also the most rewarding because it is the only one of the three that offers group authorization.

In the FileMaker Server admin console with 'FileMaker and External Accounts' enabled, click the gear icon to enable the Microsoft provider. This brings up the configuration window that outlines the steps to take to collect the necessary information and do the setup on the Microsoft Azure side.



Client Authentication

Specify how FileMaker Server authenticates FileMaker clients.

FileMaker and external server accounts

Set Up Microsoft

Microsoft is an identity provider based on OAuth 2.0. Set up Microsoft to add authenticated users as FileMaker Server clients. These users will use their Azure credentials to access your database solutions. To set up Microsoft, register an application with Azure and create web settings for the application. When you create these settings, you are assigned a client ID and a client secret.

Follow these steps to complete the setup.

1. Sign in to Microsoft.
2. Copy the Allowed Return URL below, change "YourDomain" to the fully qualified domain name for your master machine, and paste it into the Microsoft dialog box for your application.
3. In the Microsoft dialog box, copy the Client ID, Client Secret, and Tenant ID into the fields below.

Allowed Return URL: https://YourDomain:sslport/oauth/redirect

Azure Client ID: * Client ID

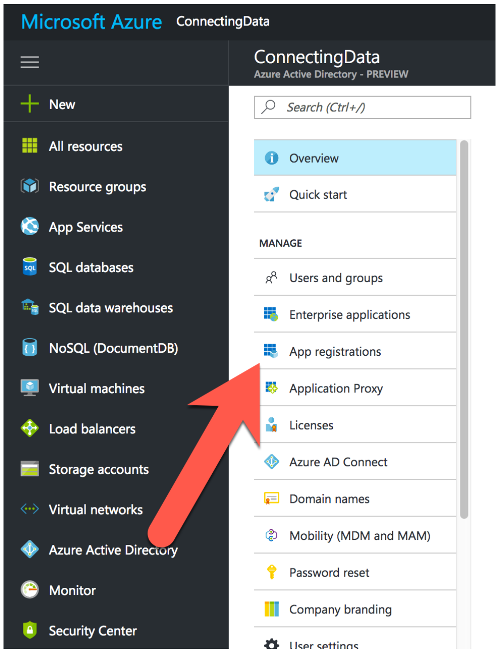
Azure Client Secret: * Client Secret

Azure Tenant ID: * Tenant ID

The link listed under #1 will take you to a Microsoft web site that explains the basics of registering an app to your Azure Active Directory. It is very easy though to get bogged down in that explanation, specially around the concept of an Azure app. As mentioned before we do need to set up an app in Azure, but it is largely just a placeholder to make sure the OAuth flow can complete. The Azure app has no other functional use.

Before we go through the steps listed in FileMaker Server, let's go over to the Azure side of things and make sure everything there is set up correctly.

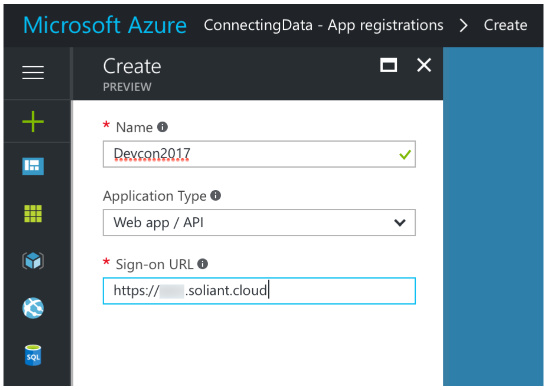
All of this assumes that you already have an Azure account. If you don't have an Azure account yet then go to https://azure.microsoft.com and set one up. Once you are all set, point your browser to portal.azure.com and log into your Azure account. From the menu on the left click on Azure Active Directory and then on the 'App registrations' option.



For the purpose of this guide we will set up an app named 'Devcon2017'. Click the 'Add' button in App registrations and fill in the details as below. The name can be whatever you want but you may want to pick a meaningful name because it will be exposed to the user at some point the first time the user logs in.

Important!

If your FileMaker Server hosts multiple solutions then pick a name that is not going to cause confusion. This setup covers the whole FileMaker Server and all the solutions it hosts. Only one Azure app is linked to a whole FileMaker Server, no matter how many different solutions it hosts. In other words; all solutions on one FileMaker Server share the same one Azure app.



* Name: Devcon2017

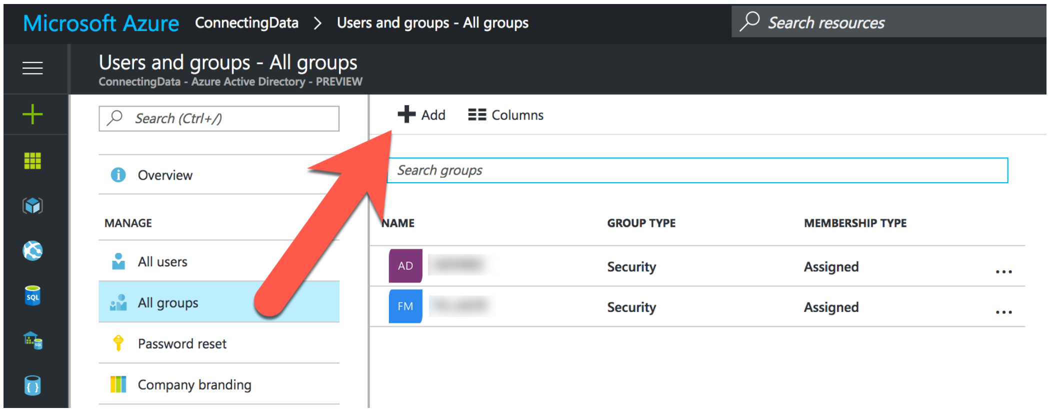
Application Type: Web app / API

* Sign-on URL: https://[redacted].soliant.cloud

Choose 'Web app / API' for the type of app. The 'sign-on URL' is irrelevant at this point. Fill in anything you like, it does not even have to be a working URL. This is not the reply url that we mentioned before, that part comes later.

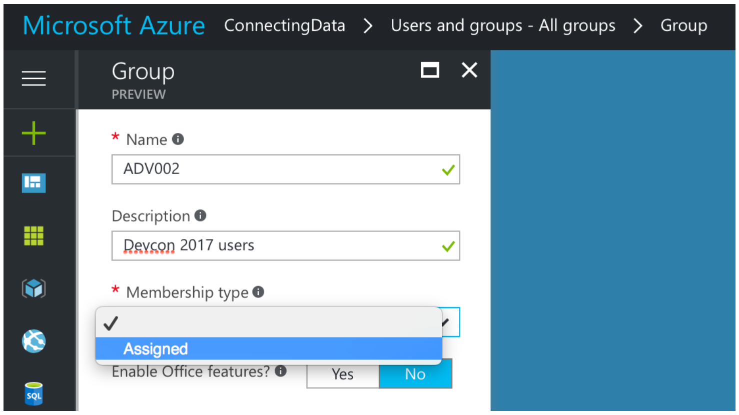
Now that we have an app in Azure we will add a user and a group to the Azure Active Directory. If you do not plan on using the group authentication for Azure AD in FileMaker then you can go straight to setting up the user and skip the group setup.

Click on 'Azure AD' in the left menu and choose 'Users and groups', then 'All groups' and click the 'Add' button.



NAME	GROUP TYPE	MEMBERSHIP TYPE
AD [redacted]	Security	Assigned
FM [redacted]	Security	Assigned

Fill in the details. Avoid any spaces or special characters in the group name. For type, pick 'Assigned'. Turn off the Office features.



* Name: ADV002

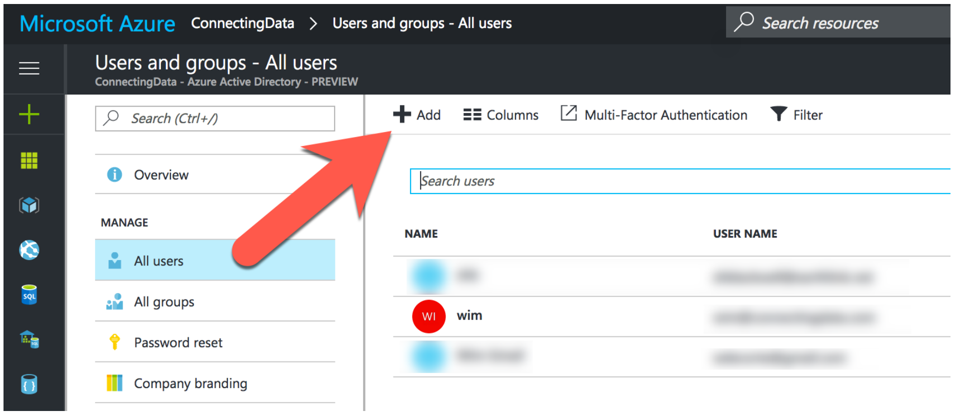
Description: Devcon 2017 users

* Membership type: Assigned

Enable Office features? Yes [✓ No]

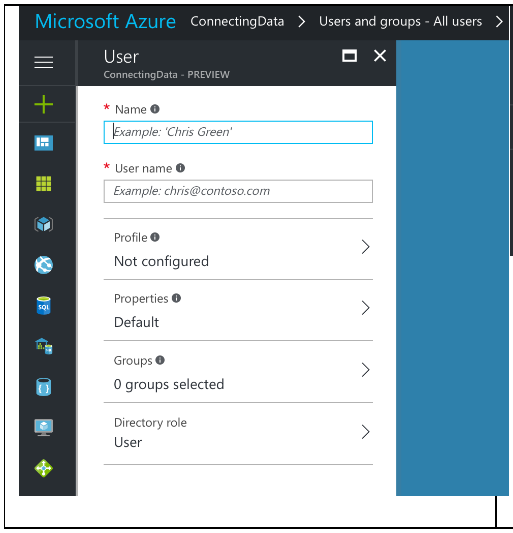
With a group in place we can now add a user.

Click on Azure AD in the menu on the left then on 'Users and groups' and then on 'All users'. Click the 'Add' button.


Microsoft Azure
ConnectingData > Users and groups - All users
Search resources
Users and groups - All users
ConnectingData - Azure Active Directory - PREVIEW
Search (Ctrl+/)
Overview
MANAGE
All users
All groups
Password reset
Company branding
Add
Columns
Multi-Factor Authentication
Filter
Search users

NAME	USER NAME
[redacted]	[redacted]
WI wim	[redacted]
[redacted]	[redacted]

The 'Name' can be anything you want and is usually the long name or full name of the user. It is NOT the name that will be used for authenticating the user. The second field 'User name' is what the user will be using to log in. That has to be an email address.



Microsoft Azure ConnectingData > Users and groups - All users >

User
ConnectingData - PREVIEW

* Name
Example: 'Chris Green'

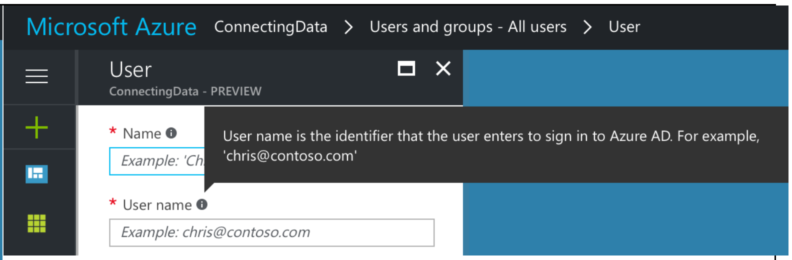
* User name
Example: chris@contoso.com

Profile
Not configured

Properties
Default

Groups
0 groups selected

Directory role
User



Microsoft Azure ConnectingData > Users and groups - All users > User

User
ConnectingData - PREVIEW

* Name
Example: 'Ch

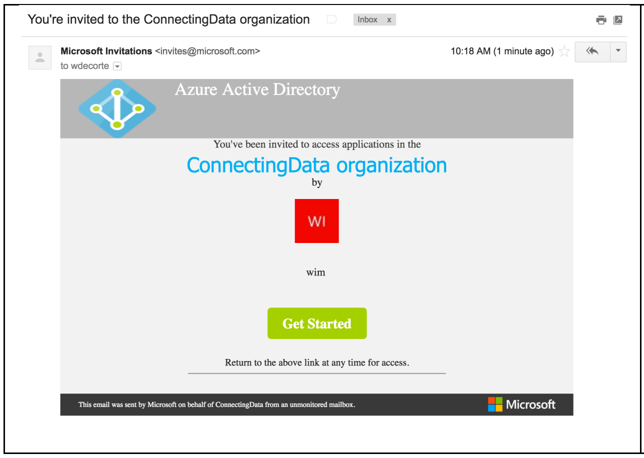
User name is the identifier that the user enters to sign in to Azure AD. For example, 'chris@contoso.com'

* User name
Example: chris@contoso.com

'Properties' and 'Profile' do not need to be set or changed.

Under 'Groups' you can select the group that we just created or any other group to which the user should belong. If you are not planning to use the group authentication for Azure in FileMaker then you do not need to add the user to any group.

It is important to note that the user account that you add to Azure AD has to be linked to a Microsoft account. If the email address is not recognized as having a matching Microsoft account, an invite will be sent out to the email address of the user.



You're invited to the ConnectingData organization Inbox x

Microsoft Invitations <invites@microsoft.com>
to wdecorte
10:18 AM (1 minute ago)

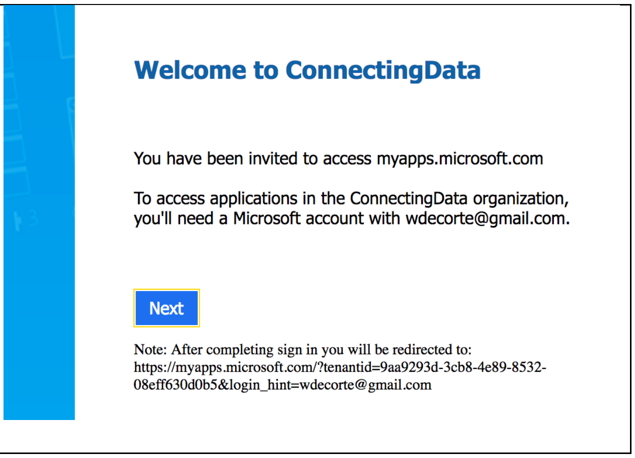
Azure Active Directory

You've been invited to access applications in the
ConnectingData organization
by
WI
wim

Get Started

Return to the above link at any time for access.

This email was sent by Microsoft on behalf of ConnectingData from an unmonitored mailbox. Microsoft



Welcome to ConnectingData

You have been invited to access myapps.microsoft.com

To access applications in the ConnectingData organization, you'll need a Microsoft account with wdecorte@gmail.com.

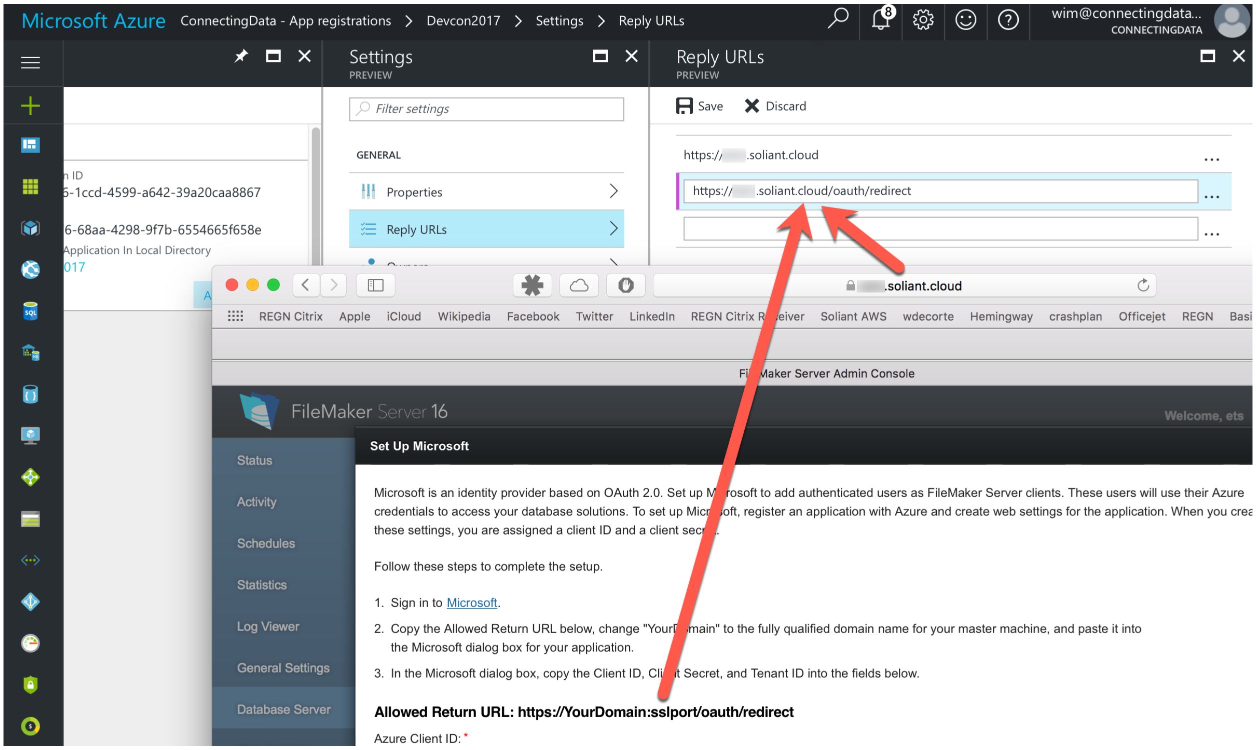
Next

Note: After completing sign in you will be redirected to: https://myapps.microsoft.com/?tenantid=9aa9293d-3cb8-4e89-8532-08eff630d0b5&login_hint=wdecorte@gmail.com

That user will have to complete the set up on the Microsoft side before they can log into the FileMaker solution.

There is one more Azure setting that needs to be completed. In Azure, click on 'Azure AD' > 'App registrations' > your app. Over on the right hand side you will see an entry for 'Reply URLs'.

This is where you enter what the FileMaker Server instructions describe in step #2 for the 'Allowed return URL' and what we discussed in the 'common elements' section. Enter that url here.



Set Up Microsoft

Microsoft is an identity provider based on OAuth 2.0. Set up M[illegible]rosoft to add authenticated users as FileMaker Server clients. These users will use their Azure credentials to access your database solutions. To set up Micr[illegible]oft, register an application with Azure and create web settings for the application. When you crea these settings, you are assigned a client ID and a client secr[illegible].

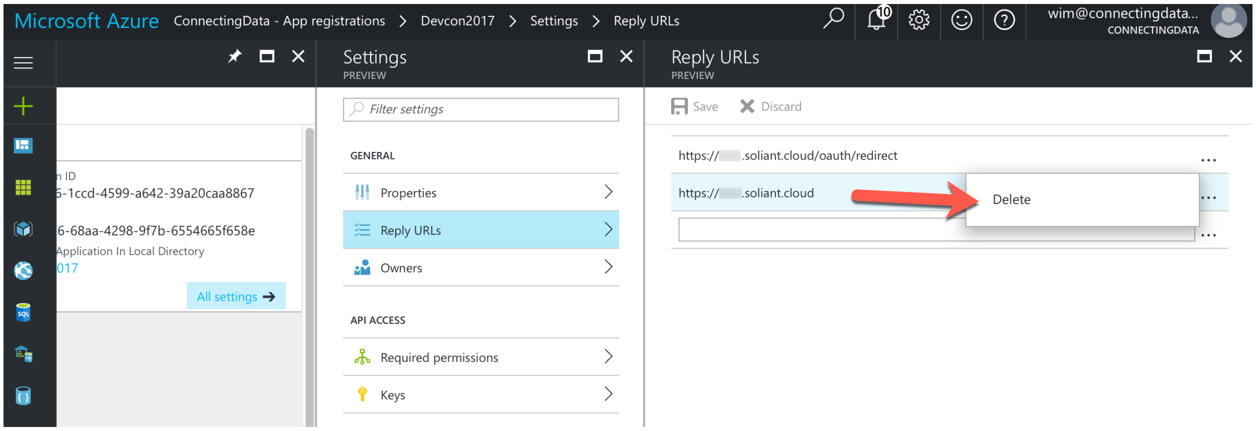
Follow these steps to complete the setup.

1. Sign in to Microsoft.
2. Copy the Allowed Return URL below, change "Your[illegible]main" to the fully qualified domain name for your master machine, and paste it into the Microsoft dialog box for your application.
3. In the Microsoft dialog box, copy the Client ID, Cli[illegible]t Secret, and Tenant ID into the fields below.

Allowed Return URL: https://YourDomain:sslport/oauth/redirect

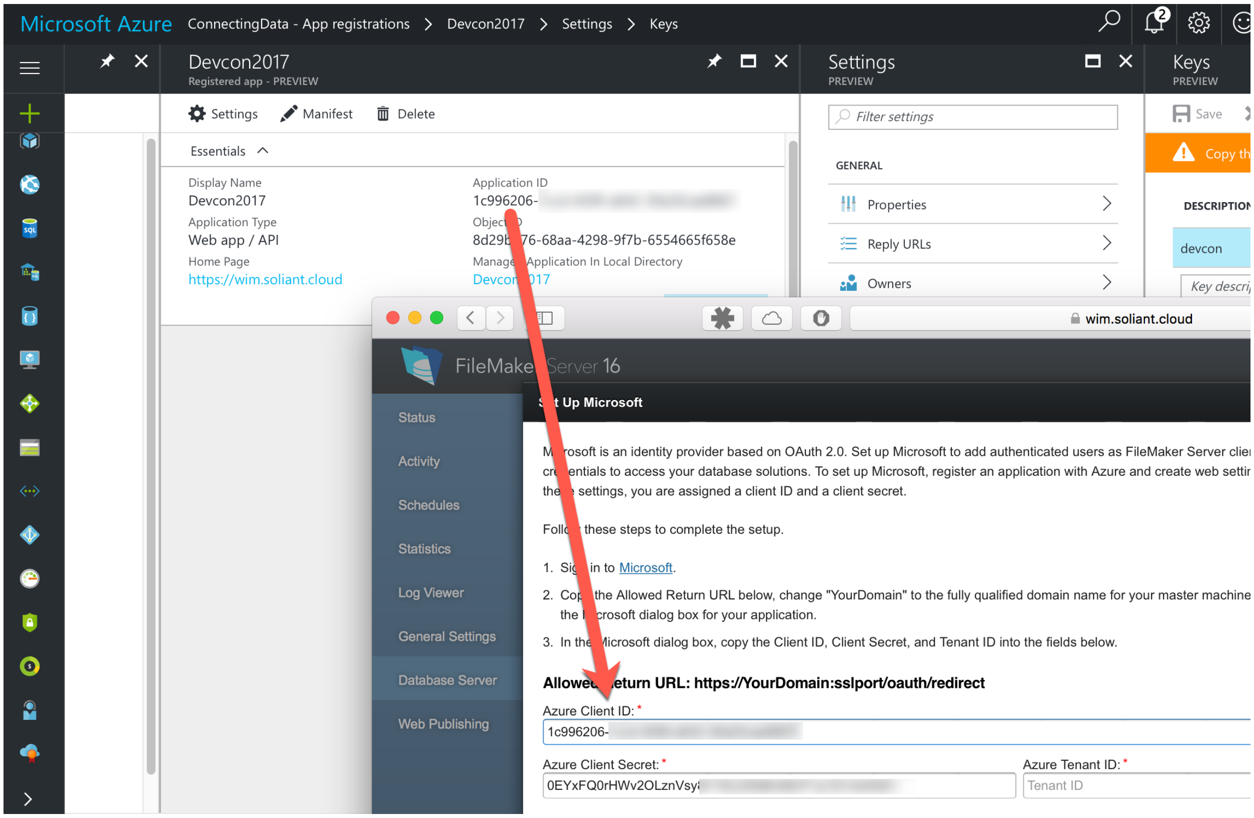
Azure Client ID: *

Before we leave the 'Reply URLs' configuration area; Azure had already helpfully created an entry for whatever we typed in as the 'Sign-on URL' at the start when we created the Azure app. You can safely delete that entry.



At this point, everything in Azure is ready. We need to take some of the Azure information and add them to the FileMaker Server configuration. This is the most confusing part of the setup because things are labeled differently in the FileMaker Server screens than they are in Azure.

The first field in FileMaker Server is called ‘Azure Client ID’. This is what Azure actually calls the ‘Application ID’. In Azure AD click on your app in ‘Registered apps’. Azure will display some IDs, from those copy the Application ID and paste it into the FileMaker Server admin console.



Display Name
Devcon2017

Application Type
Web app / API

Home Page
https://wim.soliant.cloud

Application ID
1c996206-[redacted]

Object ID
8d29bb76-68aa-4298-9f7b-6554665f658e

Managed Application In Local Directory
Devcon2017

Set Up Microsoft

Microsoft is an identity provider based on OAuth 2.0. Set up Microsoft to add authenticated users as FileMaker Server clie credentials to access your database solutions. To set up Microsoft, register an application with Azure and create web settir these settings, you are assigned a client ID and a client secret.

Follow these steps to complete the setup.

1. Sign in to Microsoft.
2. Copy the Allowed Return URL below, change "YourDomain" to the fully qualified domain name for your master machine the Microsoft dialog box for your application.
3. In the Microsoft dialog box, copy the Client ID, Client Secret, and Tenant ID into the fields below.

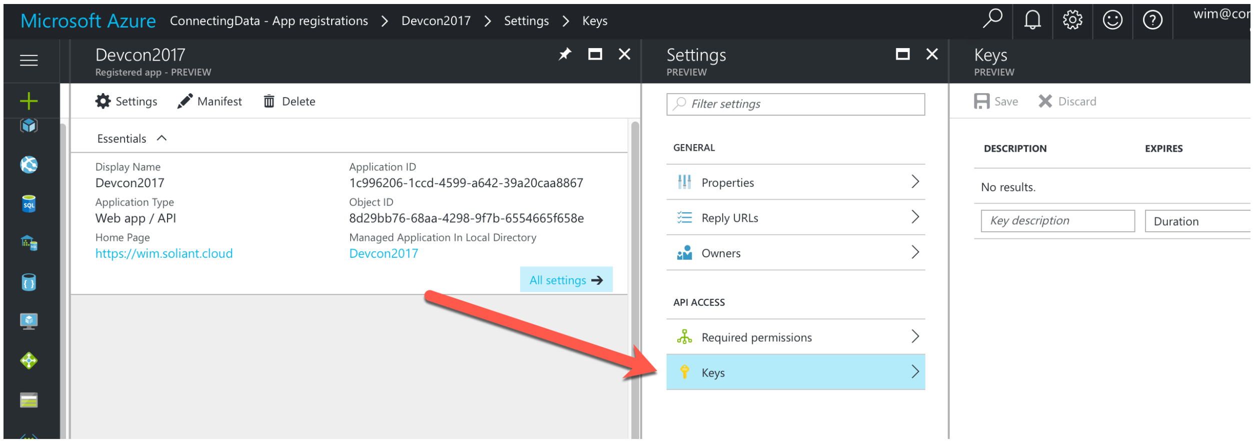
Allowed Return URL: https://YourDomain:sslport/oauth/redirect

Azure Client ID: *
1c996206-[redacted]

Azure Client Secret: *
0EYxFQ0rHWv2OLznVsy[redacted]

Azure Tenant ID: *
Tenant ID

The next field in the admin console is named ‘Azure Client Secret’. That is a key that you have to generate in your Azure app. With your app in Azure still selected, click on ‘Keys’



Display Name
Devcon2017

Application Type
Web app / API

Home Page
https://wim.soliant.cloud

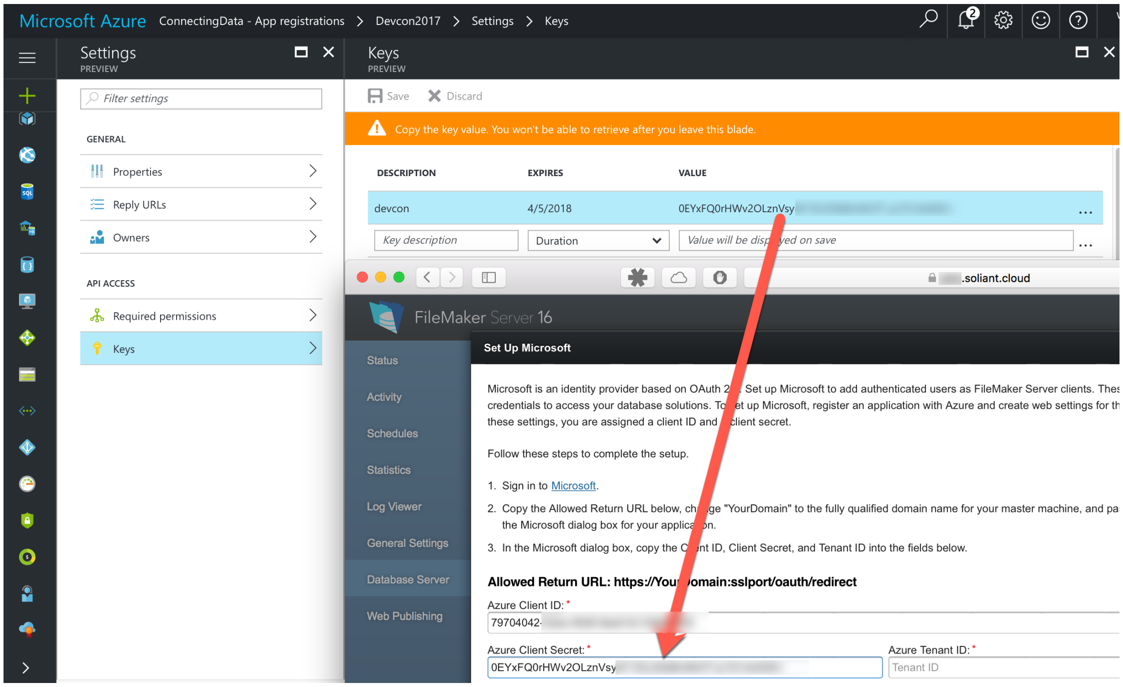
Application ID
1c996206-1ccd-4599-a642-39a20caa8867

Object ID
8d29bb76-68aa-4298-9f7b-6554665f658e

Managed Application In Local Directory
Devcon2017

DESCRIPTION	EXPIRES
No results.	
Key description	Duration

Create a key by filling in a description and a duration. When you save the key entry the actual key will be shown, copy it and paste it into the 'Azure Client Secret' field in the admin console.



Copy the key value. You won't be able to retrieve after you leave this blade.

DESCRIPTION	EXPIRES	VALUE
devcon	4/5/2018	0EYxFQ0rHWv2OLznVsy[redacted]
Key description	Duration	Value will be displayed on save

Set Up Microsoft

Microsoft is an identity provider based on OAuth 2. Set up Microsoft to add authenticated users as FileMaker Server clients. Thes credentials to access your database solutions. To set up Microsoft, register an application with Azure and create web settings for th these settings, you are assigned a client ID and a client secret.

Follow these steps to complete the setup.

1. Sign in to Microsoft.
2. Copy the Allowed Return URL below, change "YourDomain" to the fully qualified domain name for your master machine, and pa the Microsoft dialog box for your application.
3. In the Microsoft dialog box, copy the Client ID, Client Secret, and Tenant ID into the fields below.

Allowed Return URL: https://YourDomain:sslport/oauth/redirect

Azure Client ID: *
79704042-[redacted]

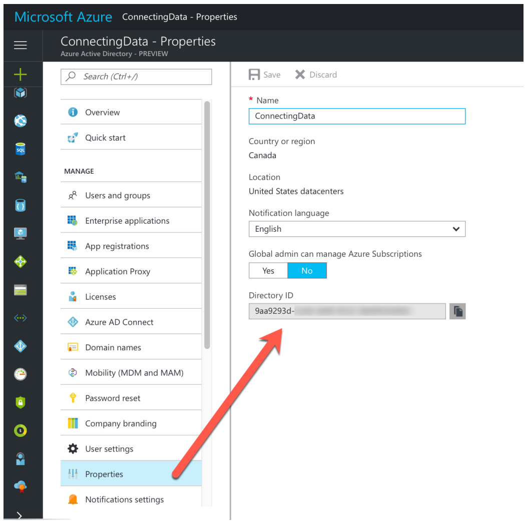
Azure Client Secret: *
0EYxFQ0rHWv2OLznVsy[redacted]

Azure Tenant ID: *
Tenant ID

Important!

Mind the warning in orange on the Azure web page; as soon as you leave that 'Keys' pane in the Azure interface the key will not be shown again and can not be retrieved. If you did not copy the key in time you will have to generate another one.

The last setting we need is what FileMaker Server calls the 'Azure Tenant ID'. In Azure that is the 'Directory ID'. Select 'Azure AD' from the left menu in Azure and choose 'Properties'. The Directory ID is listed at the bottom of that page.



* Name
ConnectingData

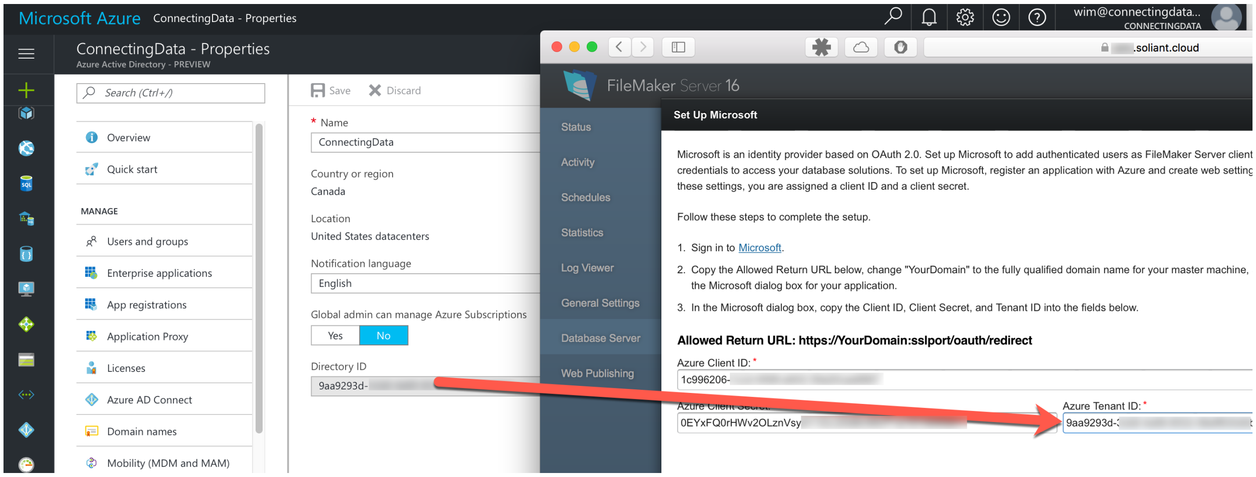
Country or region
Canada

Location
United States datacenters

Notification language
English

Global admin can manage Azure Subscriptions
Yes [✓ No]

Directory ID
9aa9293d-[redacted]



* Name: ConnectingData

Country or region: Canada

Location: United States datacenters

Notification language: English

Global admin can manage Azure Subscriptions: Yes [✓ No]

Directory ID: 9aa9293d-[redacted]

Set Up Microsoft

Microsoft is an identity provider based on OAuth 2.0. Set up Microsoft to add authenticated users as FileMaker Server client credentials to access your database solutions. To set up Microsoft, register an application with Azure and create web setting these settings, you are assigned a client ID and a client secret.

Follow these steps to complete the setup.

1. Sign in to Microsoft.
2. Copy the Allowed Return URL below, change "YourDomain" to the fully qualified domain name for your master machine, the Microsoft dialog box for your application.
3. In the Microsoft dialog box, copy the Client ID, Client Secret, and Tenant ID into the fields below.

Allowed Return URL: https://YourDomain:sslport/oauth/redirect

Azure Client ID: * 1c996206-[redacted]

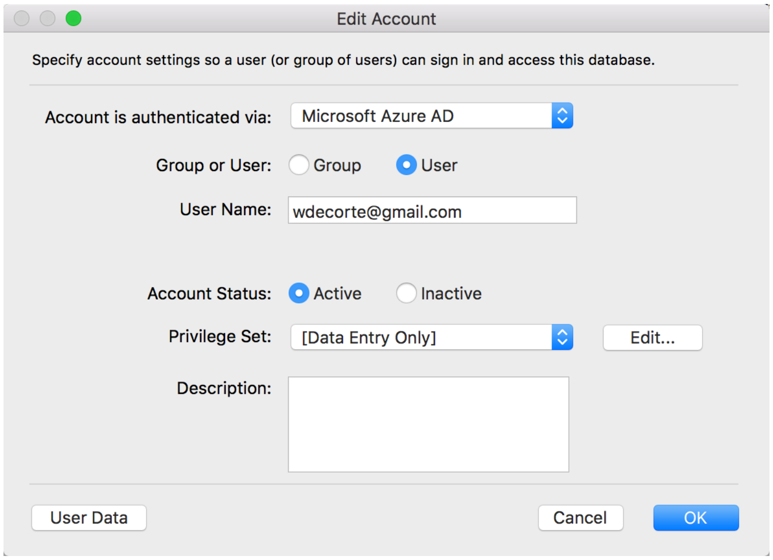
Azure Client Secret: 0EYxFQ0rHWv2OLznVsy[redacted]

Azure Tenant ID: * 9aa9293d-[redacted]

That is all the set up that is needed on Azure and in FileMaker Server When you save and close the settings FileMaker Server will need a restart before users can be authenticated.

The last steps are all about configuring the FileMaker solution to allow users to use their Microsoft accounts.

In the FileMaker soluiton go to Manage > Security and add an account with authentication via 'Microsoft Azure AD'. Select 'User' instead of the default 'Group'. For 'User Name' type in the email address for the Azure AD's user.



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

Account is authenticated via: Microsoft Azure AD

Group or User: ○ Group ● User

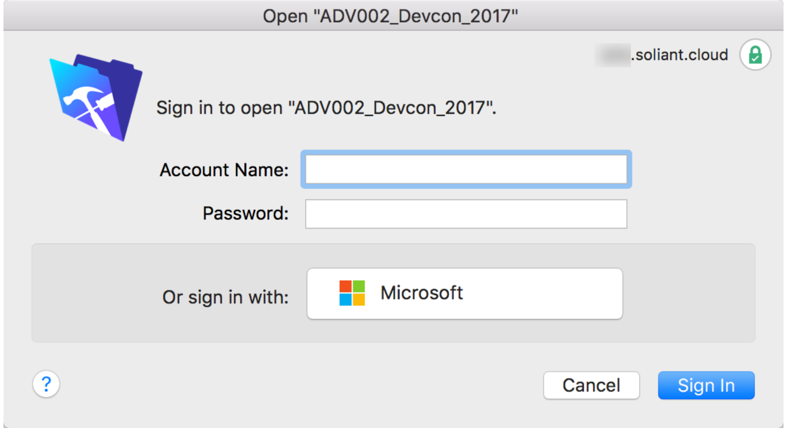
User Name: wdecorte@gmail.com

Account Status: ● Active ○ Inactive

Privilege Set: [Data Entry Only]

Description:

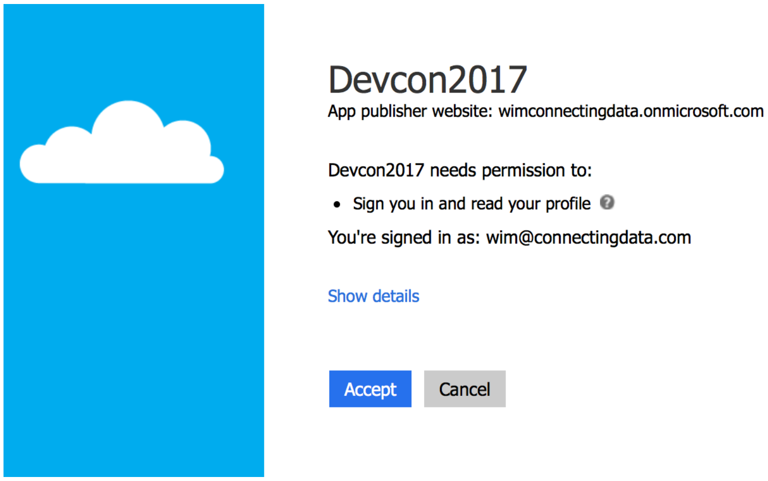
Save the account. When you open the file, the login dialog will show an option to log in with a Microsoft account:



Sign in to open "ADV002_Devcon_2017".

The top two fields are for regular FileMaker accounts; those entry fields are not where the user woud input the Microsoft account credentials.

The first time a user logs into the FileMaker solution with their Microsoft account they will be prompted by Microsoft to accept the app's requested privileges. As hinted at before, this is where the Azure app name is exposed to the user and the app covers all FileMaker solutions hosted on the FileMaker Server; so pick an Azure app name that does not cause confusion for the users of the various solutions.


Devcon2017

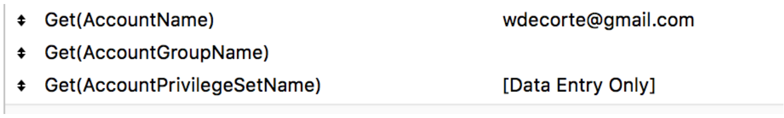
App publisher website: wimconnectingdata.onmicrosoft.com

Devcon2017 needs permission to:

- Sign you in and read your profile

You're signed in as: wim@connectingdata.com

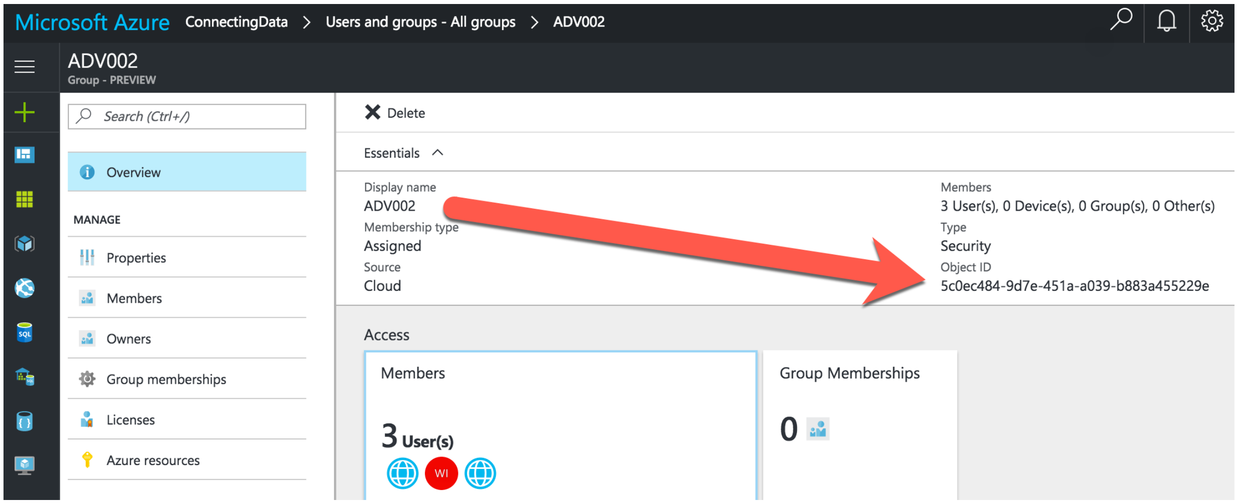
Once all the formalities are out of the way the user will be logged into the FileMaker solution and will be identified by the Microsoft account name:



Get(AccountName)	wdecorte@gmail.com
Get(AccountGroupName)	
Get(AccountPrivilegeSetName)	[Data Entry Only]

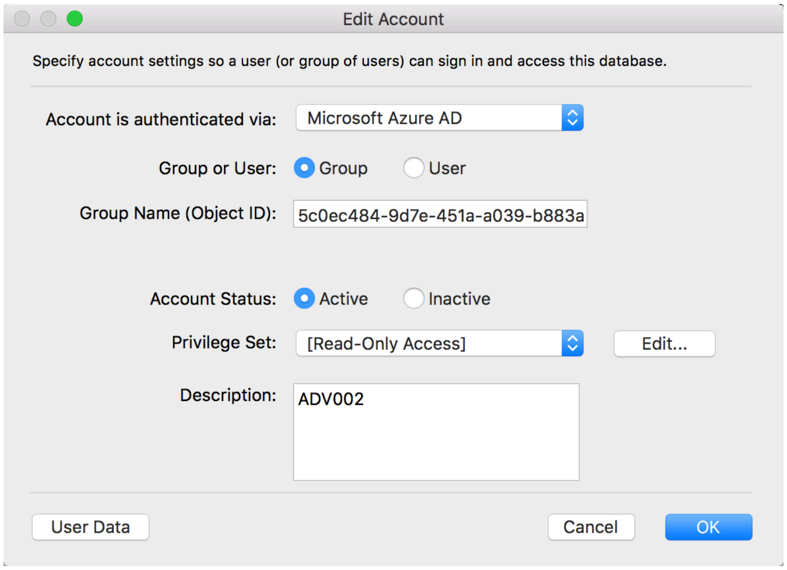
Note that the Get(AccountGroupName) is empty. That is because we set the account in FileMaker to be a 'User' account and not a 'Group' account. When you set up individual Azure AD user accounts in FileMaker, then no group information is retrieved from Azure.

Since we have a group in our Azure AD, let's add an account to the FileMaker solution that uses the Azure AD group. First, log into Azure and select the group that you want to add to FileMaker. Copy the Object ID.



Display name: ADV002
Membership type: Assigned
Source: Cloud
Members: 3 User(s), 0 Device(s), 0 Group(s), 0 Other(s)
Type: Security
Object ID: 5c0ec484-9d7e-451a-a039-b883a455229e

In FileMaker add an account, select 'Microsoft Azure AD' and make sure 'Group' is selected. In the Group Name field, paste the Object ID that was copied from Azure. Only the Object ID is used to identify the group, not the actual group name.

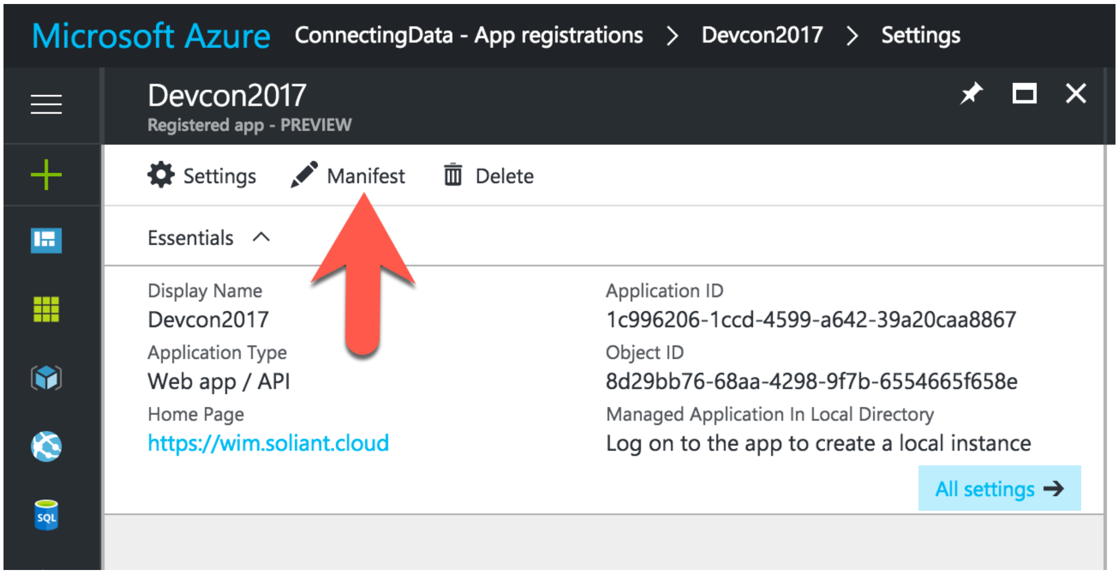


Specify account settings so a user (or group of users) can sign in and access this database.

Account is authenticated via: Microsoft Azure AD
Group or User: ● Group ○ User
Group Name (Object ID): 5c0ec484-9d7e-451a-a039-b883a
Account Status: ● Active ○ Inactive
Privilege Set: [Read-Only Access]
Description: ADV002

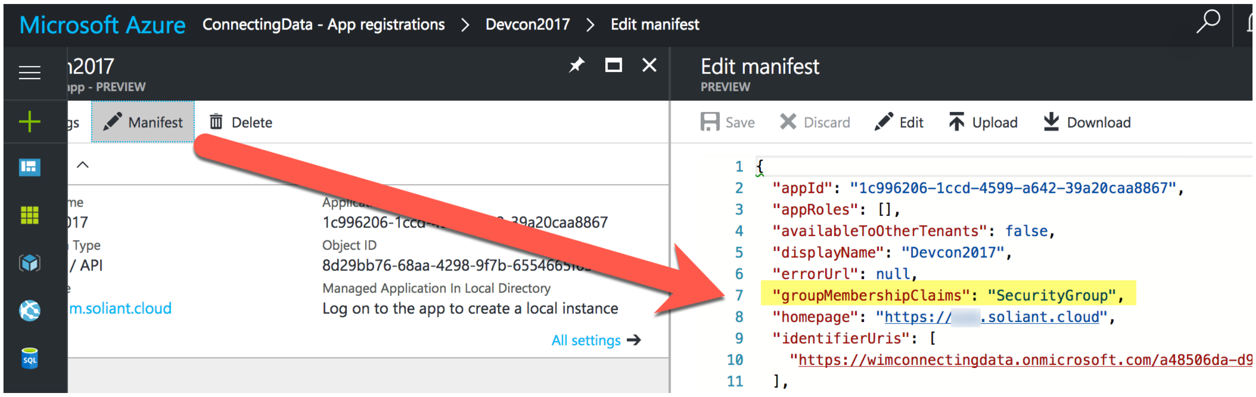
There is one more change to make in the Azure app. By default Azure apps are not configured to allow group authentication.

In Azure AD, click on ‘App registrations’ and click on your app. Click the ‘Manifest’ button.



Display Name
Devcon2017
Application Type
Web app / API
Home Page
https://wim.soliant.cloud
Application ID
1c996206-1ccd-4599-a642-39a20caa8867
Object ID
8d29bb76-68aa-4298-9f7b-6554665f658e
Managed Application In Local Directory
Log on to the app to create a local instance

In the manifest, change the ‘groupMembershipClaims’ from ‘null’ to ‘SecurityGroup’



```
{
  "appId": "1c996206-1ccd-4599-a642-39a20caa8867",
  "appRoles": [],
  "availableToOtherTenants": false,
  "displayName": "Devcon2017",
  "errorUrl": null,
  "groupMembershipClaims": "SecurityGroup",
  "homepage": "https://[redacted].soliant.cloud",
  "identifierUris": [
    "https://wimconnectingdata.onmicrosoft.com/a48506da-d9
  ],
```

Save the manifest. Now if a user that belongs to this group logs into FileMaker, the Get() values will reflect this:

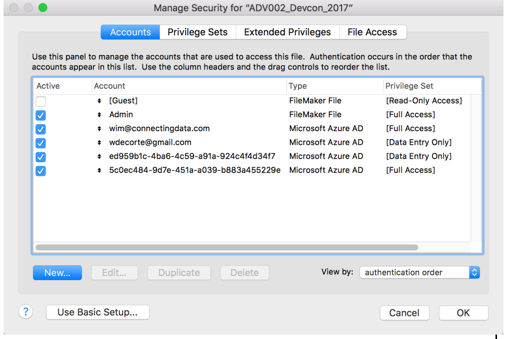
Get(AccountName)	wdecorte@gmail.com
Get(AccountGroupName)	5c0ec484-9d7e-451a-a039-b883a455229e
Get(AccountPrivilegeSetName)	[Full Access]

With this, the FileMaker solution, FileMaker Server and Azure AD are all set up properly. Any user that belongs to the Azure AD and that has a matching individual or group account in a FileMaker solution can log into the solution with their Microsoft account.

Before we move on to the next OAuth provider, a quick word on the importance of the authentication order.

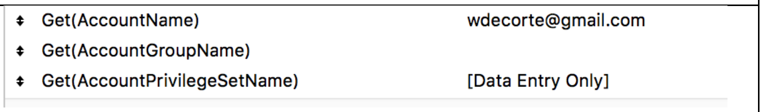
Since Azure AD authentication supports both individual accounts and groups; it is possible that a user is set up in the FileMaker solution as a member of one or more groups and / or with an individual account. That means that the authentication order comes into play.

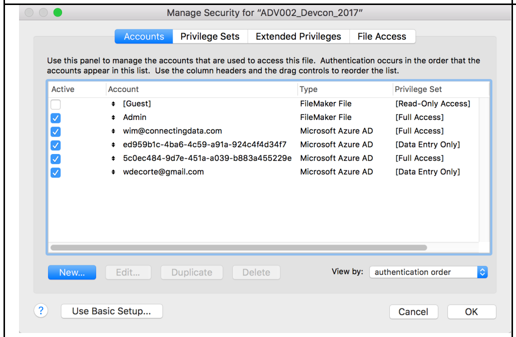
To illustrate the effects of the authentication order, we have the ‘wdecorte@gmail.com’ set up as an individual account in FileMaker and we also have two Azure group accounts, and wdecorte@gmail.com belongs to both groups. The screenshots below show the ‘accounts’ section of FileMaker’s ‘Manage Security’ dialog, with ‘view by’ set to ‘authentication order’ (see the dropdown at the lower right). For each different authentication order setting we logged into the FileMaker solution with the email address and captured the Get() functions to see what they would return.

<table>
<tr><th>Authentication setup</th><th>Results in</th></tr>
<tr>
<td>


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 list. Use the column headers and the drag controls to reorder the list.
<table>
<tr><th>Active</th><th>Account</th><th>Type</th><th>Privilege Set</th></tr>
<tr><td>☐</td><td>[Guest]</td><td>FileMaker File</td><td>[Read-Only Access]</td></tr>
<tr><td>☑</td><td>Admin</td><td>FileMaker File</td><td>[Full Access]</td></tr>
<tr><td>☑</td><td>wim@connectingdata.com</td><td>Microsoft Azure AD</td><td>[Full Access]</td></tr>
<tr><td>☑</td><td>wdecorte@gmail.com</td><td>Microsoft Azure AD</td><td>[Data Entry Only]</td></tr>
<tr><td>☑</td><td>ed959b1c-4ba6-4c59-a91a-924c4f4d34f7</td><td>Microsoft Azure AD</td><td>[Data Entry Only]</td></tr>
<tr><td>☑</td><td>5c0ec484-9d7e-451a-a039-b883a455229e</td><td>Microsoft Azure AD</td><td>[Full Access]</td></tr>
</table>

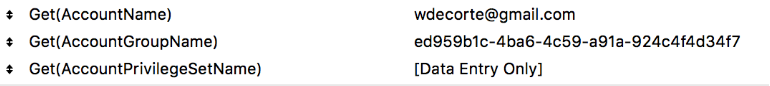
View by: authentication order

The individual account is higher in the authentication order than the two group accounts.
</td>
<td>

<table>
<tr><td>Get(AccountName)</td><td>wdecorte@gmail.com</td></tr>
<tr><td>Get(AccountGroupName)</td><td></td></tr>
<tr><td>Get(AccountPrivilegeSetName)</td><td>[Data Entry Only]</td></tr>
</table>

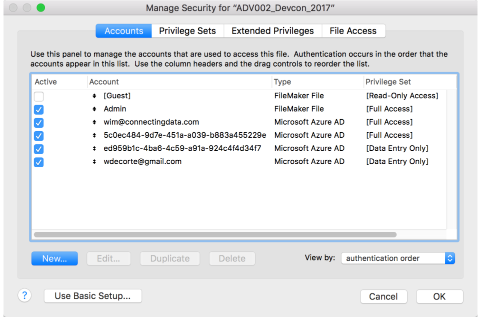
The email address is recognized as the account name, the account group name is empty. This is normal since the individual account is recognized first and it is not a group account.
</td>
</tr>
<tr>
<td>


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 list. Use the column headers and the drag controls to reorder the list.
<table>
<tr><th>Active</th><th>Account</th><th>Type</th><th>Privilege Set</th></tr>
<tr><td>☐</td><td>[Guest]</td><td>FileMaker File</td><td>[Read-Only Access]</td></tr>
<tr><td>☑</td><td>Admin</td><td>FileMaker File</td><td>[Full Access]</td></tr>
<tr><td>☑</td><td>wim@connectingdata.com</td><td>Microsoft Azure AD</td><td>[Full Access]</td></tr>
<tr><td>☑</td><td>ed959b1c-4ba6-4c59-a91a-924c4f4d34f7</td><td>Microsoft Azure AD</td><td>[Data Entry Only]</td></tr>
<tr><td>☑</td><td>5c0ec484-9d7e-451a-a039-b883a455229e</td><td>Microsoft Azure AD</td><td>[Full Access]</td></tr>
<tr><td>☑</td><td>wdecorte@gmail.com</td><td>Microsoft Azure AD</td><td>[Data Entry Only]</td></tr>
</table>

View by: authentication order

The group starting with ‘ed’ is higher in the authentication order than the other group account and in the individual account.
</td>
<td>

<table>
<tr><td>Get(AccountName)</td><td>wdecorte@gmail.com</td></tr>
<tr><td>Get(AccountGroupName)</td><td>ed959b1c-4ba6-4c59-a91a-924c4f4d34f7</td></tr>
<tr><td>Get(AccountPrivilegeSetName)</td><td>[Data Entry Only]</td></tr>
</table>

The email address is recognized as the account name, the account group name starts with ‘ed’, matching the highest group in the list that the account is a member of.
</td>
</tr>
</table>



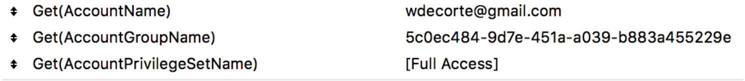
Manage Security for "ADV002_Devcon_2017"

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 list. Use the column headers and the drag controls to reorder the list.

Active	Account	Type	Privilege Set
☐	[Guest]	FileMaker File	[Read-Only Access]
☑	Admin	FileMaker File	[Full Access]
☑	wim@connectingdata.com	Microsoft Azure AD	[Full Access]
☑	5c0ec484-9d7e-451a-a039-b883a455229e	Microsoft Azure AD	[Full Access]
☑	ed959b1c-4ba6-4c59-a91a-924c4f4d34f7	Microsoft Azure AD	[Data Entry Only]
☑	wdecorte@gmail.com	Microsoft Azure AD	[Data Entry Only]

View by: authentication order

The group starting with '5c is higher in the authentication order than the other group account and in the individual account.



Get(AccountName)	wdecorte@gmail.com
Get(AccountGroupName)	5c0ec484-9d7e-451a-a039-b883a455229e
Get(AccountPrivilegeSetName)	[Full Access]

The email address is recognized as the account name, the account group name starts with '5c, matching the highest group in the list that the account is a member of.

It is clear then that Azure AD returns both the account name and all groups that the user belongs to. FileMaker stops at the first match of either a group or individual account in the FileMaker list of accounts, evaluated in authentication order..

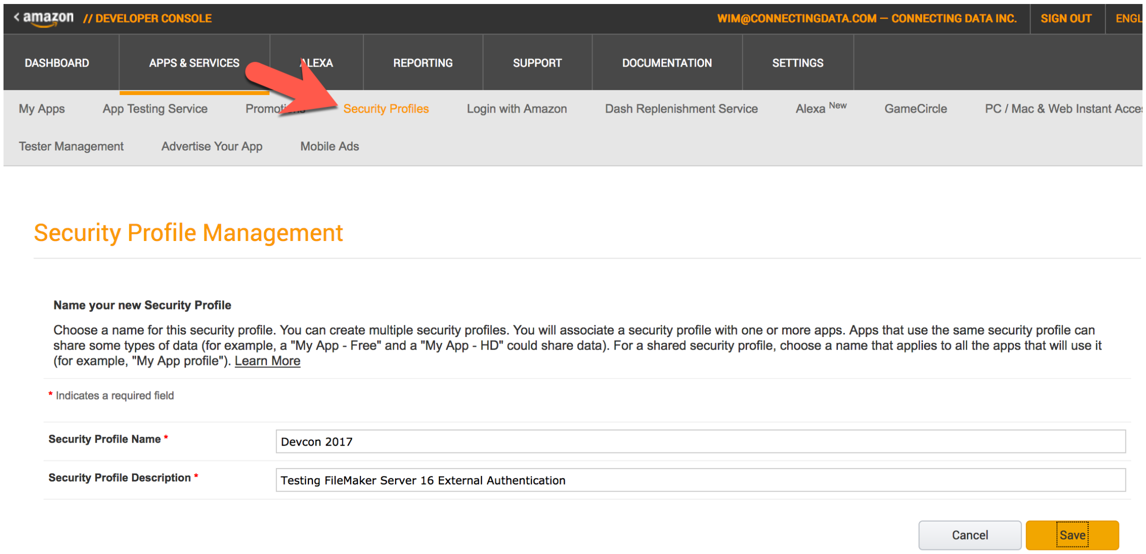
This is very similar to the behavior of the traditional external authentication mechanism. If users will belong to multiple groups in Azure AD, evaluate the authentication order carefully so that the users are assigned the proper privilege set for their role.

Amazon

Amazon offers a service named ‘Login with Amazon’. That is where we need to set up a security profile and use that profile’s information in the FileMaker Server admin console.

This section assumes that you have an Amazon developer account. Use it to log into developer.amazon.com. If you don’t have a developer account, you can set one up from that web site.

Once logged in, click on the menu item for ‘Services & APIs’ and on ‘Security Profiles’ in the submenu, then click the button to add a new security profile. Give the profile a name and a description:



Security Profile Management

Name your new Security Profile

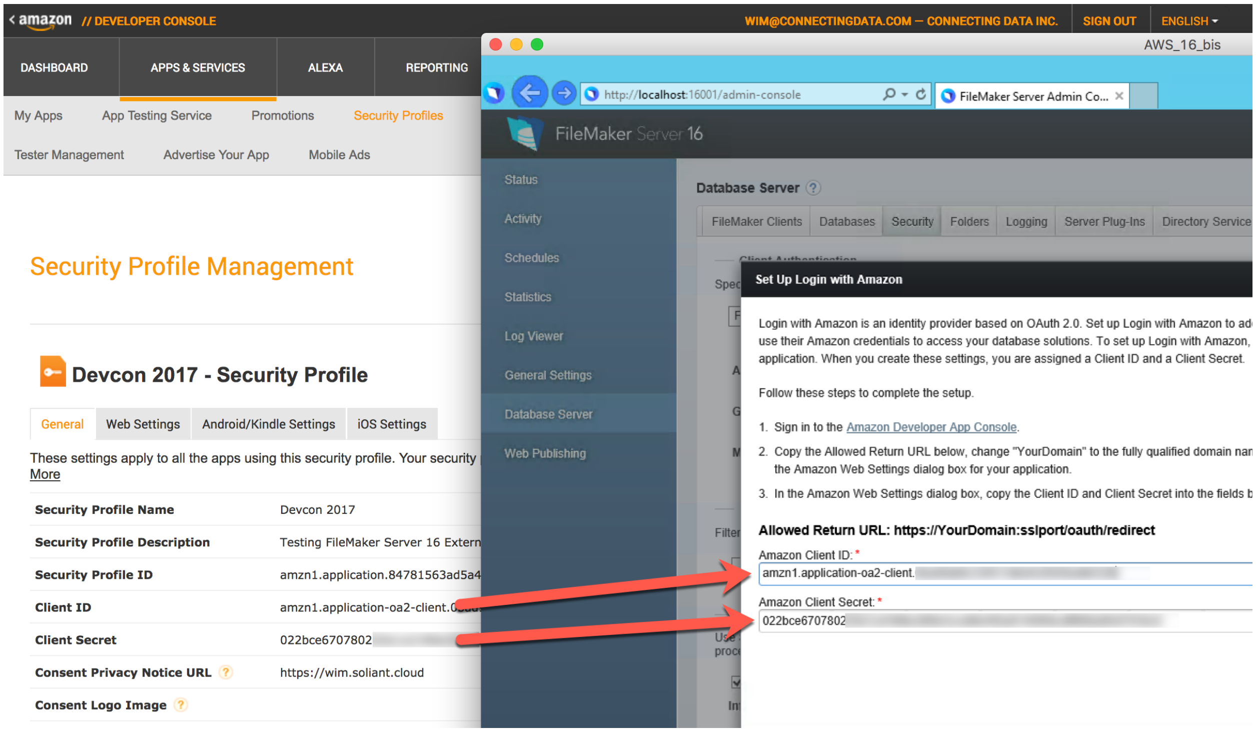
Choose a name for this security profile. You can create multiple security profiles. You will associate a security profile with one or more apps. Apps that use the same security profile can share some types of data (for example, a "My App - Free" and a "My App - HD" could share data). For a shared security profile, choose a name that applies to all the apps that will use it (for example, "My App profile"). Learn More

* Indicates a required field

Security Profile Name *: Devcon 2017

Security Profile Description *: Testing FileMaker Server 16 External Authentication

When you save the profile you will see a client id and a client secret for the new profile: Copy both pieces of information over to the Amazon settings in the FileMaker Server admin console:



Security Profile Management

Devcon 2017 - Security Profile

These settings apply to all the apps using this security profile. Your security
More

Security Profile Name	Devcon 2017
Security Profile Description	Testing FileMaker Server 16 Extern
Security Profile ID	amzn1.application.84781563ad5a4
Client ID	amzn1.application-oa2-client.0
Client Secret	022bce6707802[redacted]
Consent Privacy Notice URL ?	https://wim.soliant.cloud
Consent Logo Image ?	

Set Up Login with Amazon

Login with Amazon is an identity provider based on OAuth 2.0. Set up Login with Amazon to ad
use their Amazon credentials to access your database solutions. To set up Login with Amazon,
application. When you create these settings, you are assigned a Client ID and a Client Secret.

Follow these steps to complete the setup.

1. Sign in to the Amazon Developer App Console.
2. Copy the Allowed Return URL below, change "YourDomain" to the fully qualified domain nar
   the Amazon Web Settings dialog box for your application.
3. In the Amazon Web Settings dialog box, copy the Client ID and Client Secret into the fields b

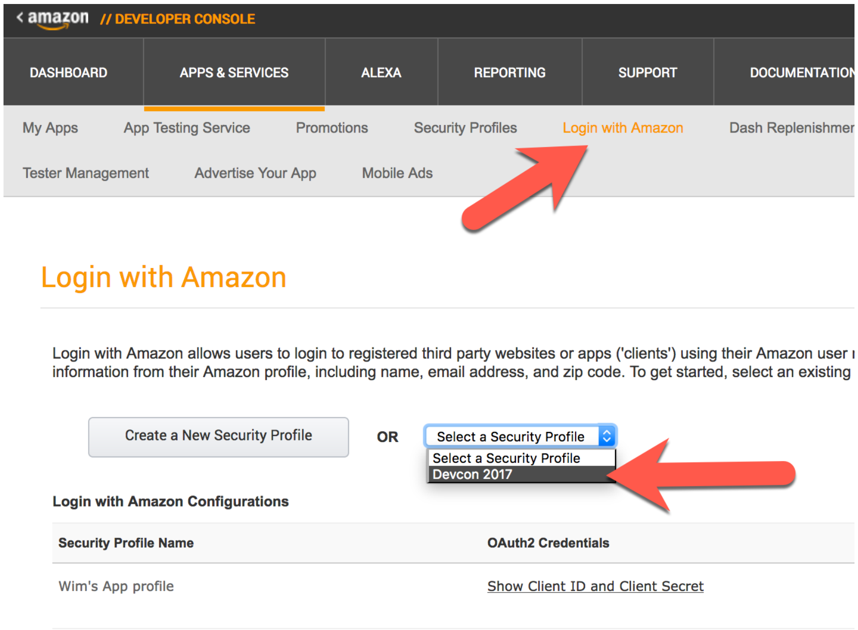
Allowed Return URL: https://YourDomain:sslport/oauth/redirect

Amazon Client ID: *
amzn1.application-oa2-client.[redacted]

Amazon Client Secret: *
022bce6707802[redacted]

Save the settings in FileMaker Server and restart the service.

Back on the Amazon web site, click on the 'Login with Amazon' menu item and choose the newly created security profile:



Login with Amazon

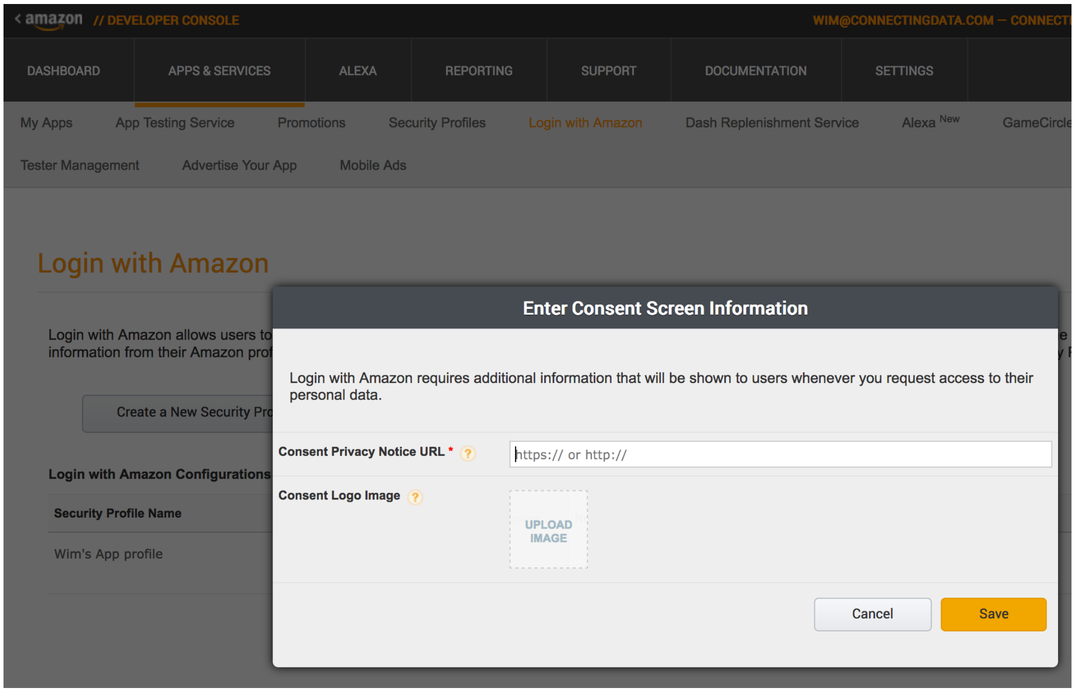
Login with Amazon allows users to login to registered third party websites or apps ('clients') using their Amazon user
information from their Amazon profile, including name, email address, and zip code. To get started, select an existing

Create a New Security Profile
OR
Select a Security Profile
Select a Security Profile
Devcon 2017

Login with Amazon Configurations

Security Profile Name	OAuth2 Credentials
Wim's App profile	Show Client ID and Client Secret

You will be asked to provide some additional information, including a url where your privacy information will be available. That url will be show to the user as part of the login page later. For now you can fill in any old URL. This is not the important Redirect URL.



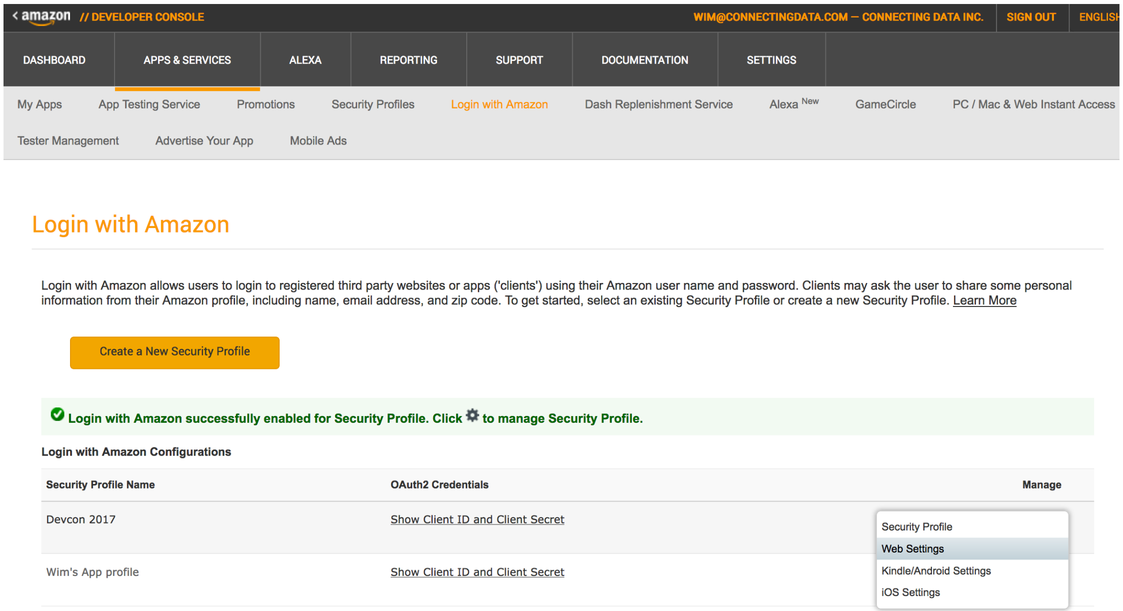
Enter Consent Screen Information

Login with Amazon requires additional information that will be shown to users whenever you request access to their personal data.

Consent Privacy Notice URL * https:// or http://

Consent Logo Image

‘Login with Amazon’ will now be enabled for that security profile. We still need to give it the redirect URL back to FileMaker Server so choose ‘web settings’ from the profiles menu:



Login with Amazon

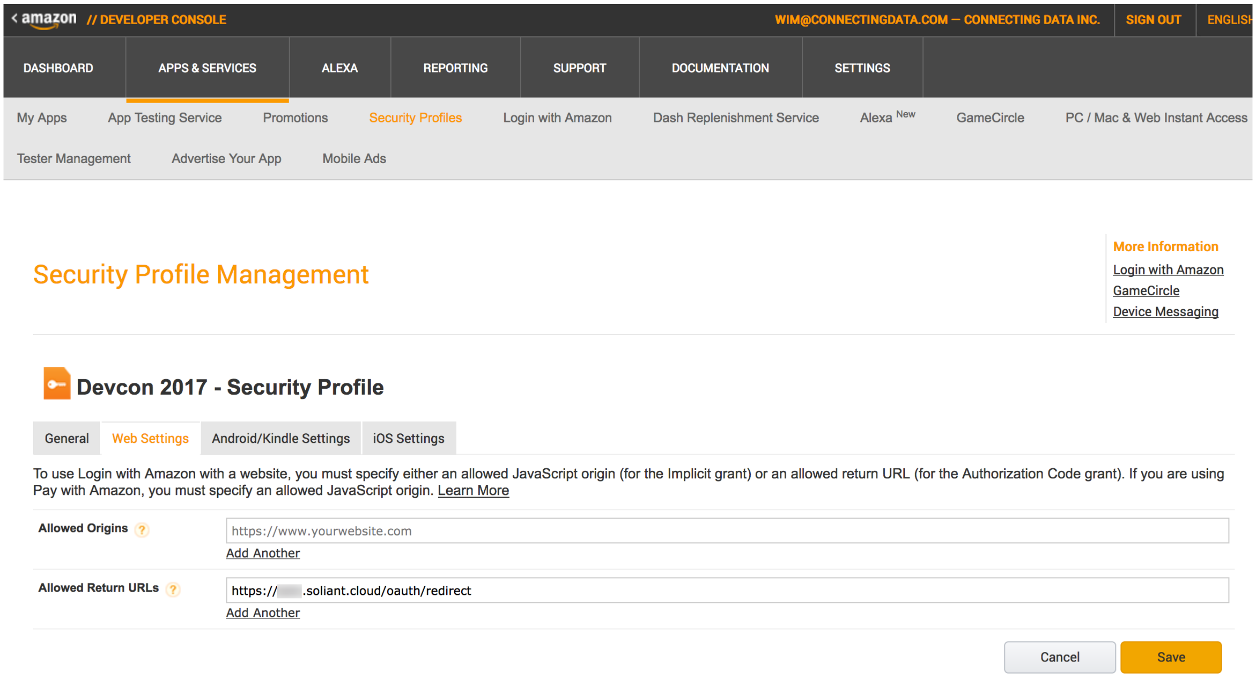
Login with Amazon allows users to login to registered third party websites or apps ('clients') using their Amazon user name and password. Clients may ask the user to share some personal information from their Amazon profile, including name, email address, and zip code. To get started, select an existing Security Profile or create a new Security Profile. Learn More

✓ **Login with Amazon successfully enabled for Security Profile. Click ⚙ to manage Security Profile.**

Login with Amazon Configurations

Security Profile Name	OAuth2 Credentials	Manage
Devcon 2017	Show Client ID and Client Secret	
Wim's App profile	Show Client ID and Client Secret	

In the ‘Allowed Return URLs’ enter the redirect url for your FileMaker Server: “https://” + fully qualified doman name of your filemaker server machine or master machine + SSL port if you don’t use the default port 443 + “/oauth/redirect”, and save the settings.



Security Profile Management

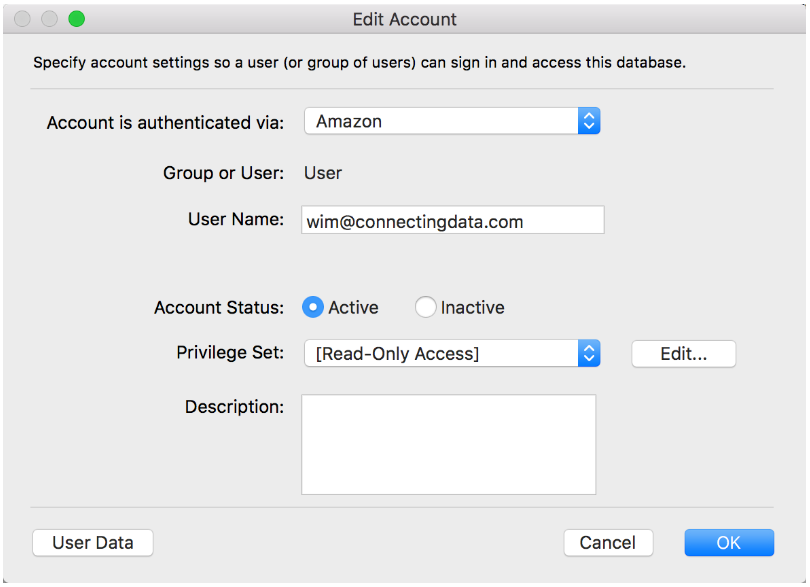
Devcon 2017 - Security Profile

To use Login with Amazon with a website, you must specify either an allowed JavaScript origin (for the Implicit grant) or an allowed return URL (for the Authorization Code grant). If you are using Pay with Amazon, you must specify an allowed JavaScript origin. Learn More

Allowed Origins: https://www.yourwebsite.com

Allowed Return URLs: https://[redacted].soliant.cloud/oauth/redirect

Now in the FileMaker solution we add a account with an email address that is registered as an Amazon account and we set ‘authentication via Amazon’.



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

Account is authenticated via: Amazon

Group or User: User

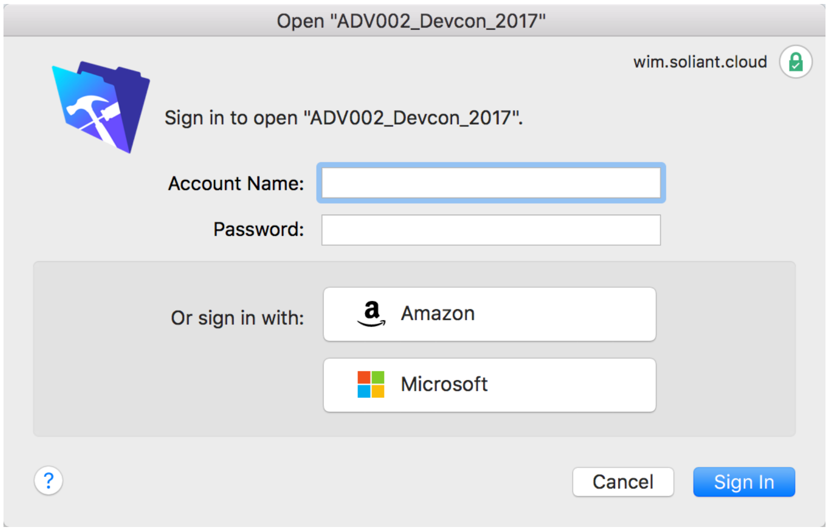
User Name: wim@connectingdata.com

Account Status: ● Active ○ Inactive

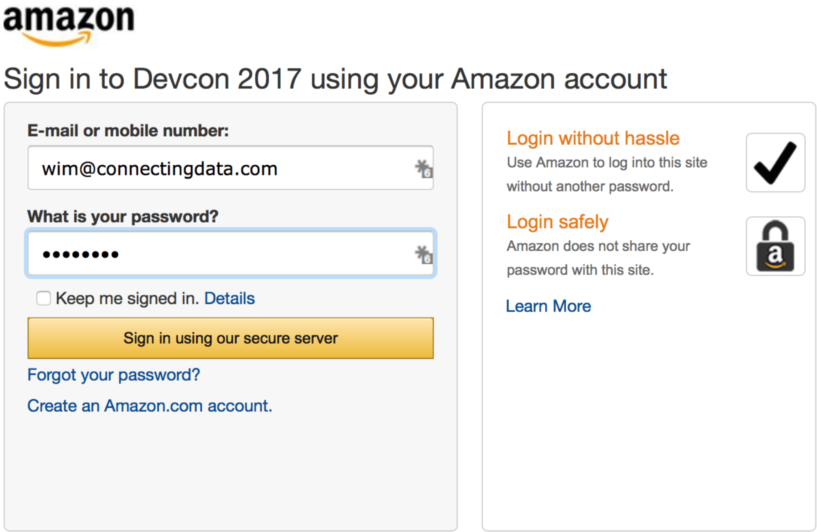
Privilege Set: [Read-Only Access]

Description:

When logging in the user can now click on the “Amazon” button.



This will launch the default browser or open a new tab if the browser is already running and will show the Amazon login page, with the name of the selected profile in the title:



Sign in to Devcon 2017 using your Amazon account

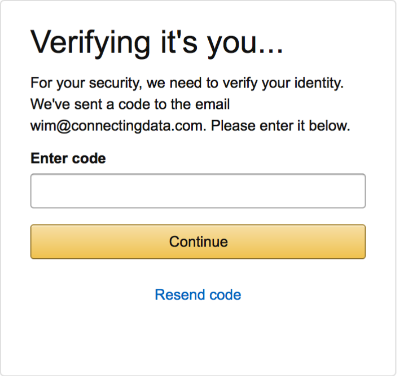
E-mail or mobile number: wim@connectingdata.com

What is your password? ••••••••

☐ Keep me signed in. Details

Sign in using our secure server
Forgot your password?
Create an Amazon.com account.
Login without hassle
Use Amazon to log into this site without another password.
Login safely
Amazon does not share your password with this site.
Learn More

In the example used for this document, the account is also set up for multi-factor authentication so next step is to input the code that was sent to the email:

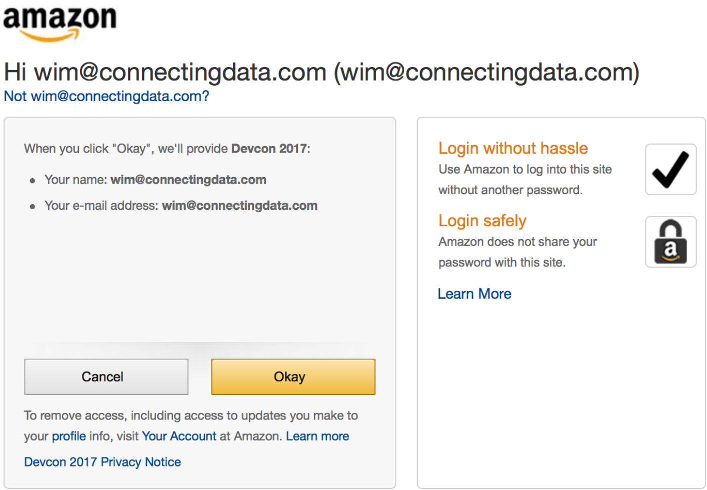


Verifying it's you...

For your security, we need to verify your identity. We've sent a code to the email wim@connectingdata.com. Please enter it below.

Enter code

When that code is verified and it is the very first time that this account is used for this profile the user is asked for confirmation that the profile's requirements are acceptable:



Hi wim@connectingdata.com (wim@connectingdata.com)

Not wim@connectingdata.com?

When you click "Okay", we'll provide **Devcon 2017**:

- Your name: **wim@connectingdata.com**
- Your e-mail address: **wim@connectingdata.com**

To remove access, including access to updates you make to your profile info, visit Your Account at Amazon. Learn more

Devcon 2017 Privacy Notice

Login without hassle
Use Amazon to log into this site without another password.

Login safely
Amazon does not share your password with this site.

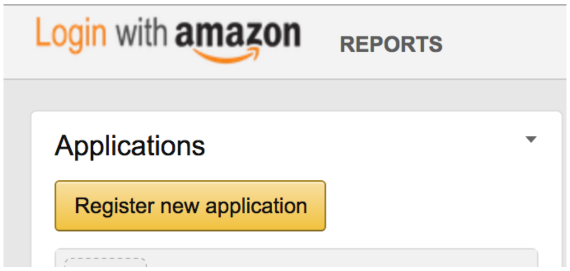
Learn More

If the user agrees and clicks 'Okay' then the user is logged into the FileMaker solution and the Get() functions reflect the account.

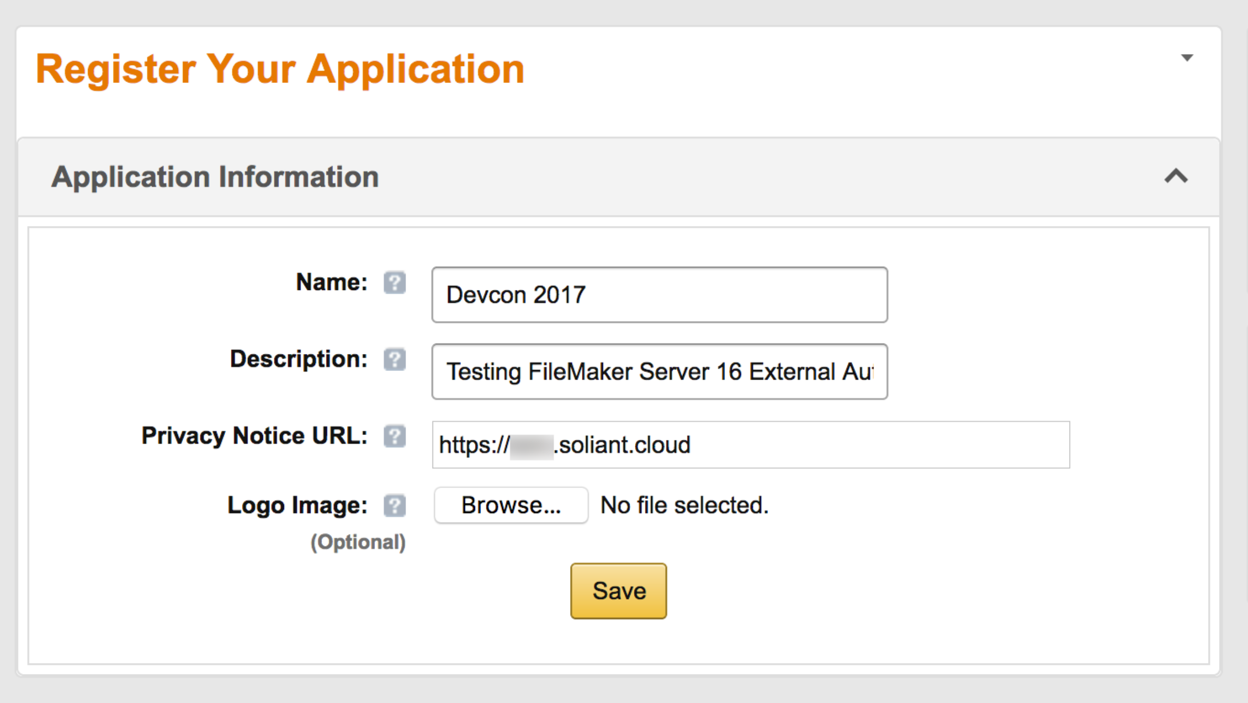
Get(AccountName)	wim@connectingdata.com
Get(AccountGroupName)	
Get(AccountPrivilegeSetName)	[Read-Only Access]

As expected, the Get(AccountGroupName) is empty because there is no notion of a group with the Amazon accounts.

There is another way to use Amazon accounts and that approach is more 'app' based like Azure's is. The starting point for this approach is 'https://sellercentral.amazon.com' and once there and logged in with your Amazon developer account, click the button to register a new application.



Give it a name, description and a privacy notice url (that url can be any url, the app will not be used except for FileMaker Server authentication so there is no user-facing aspect to this application).



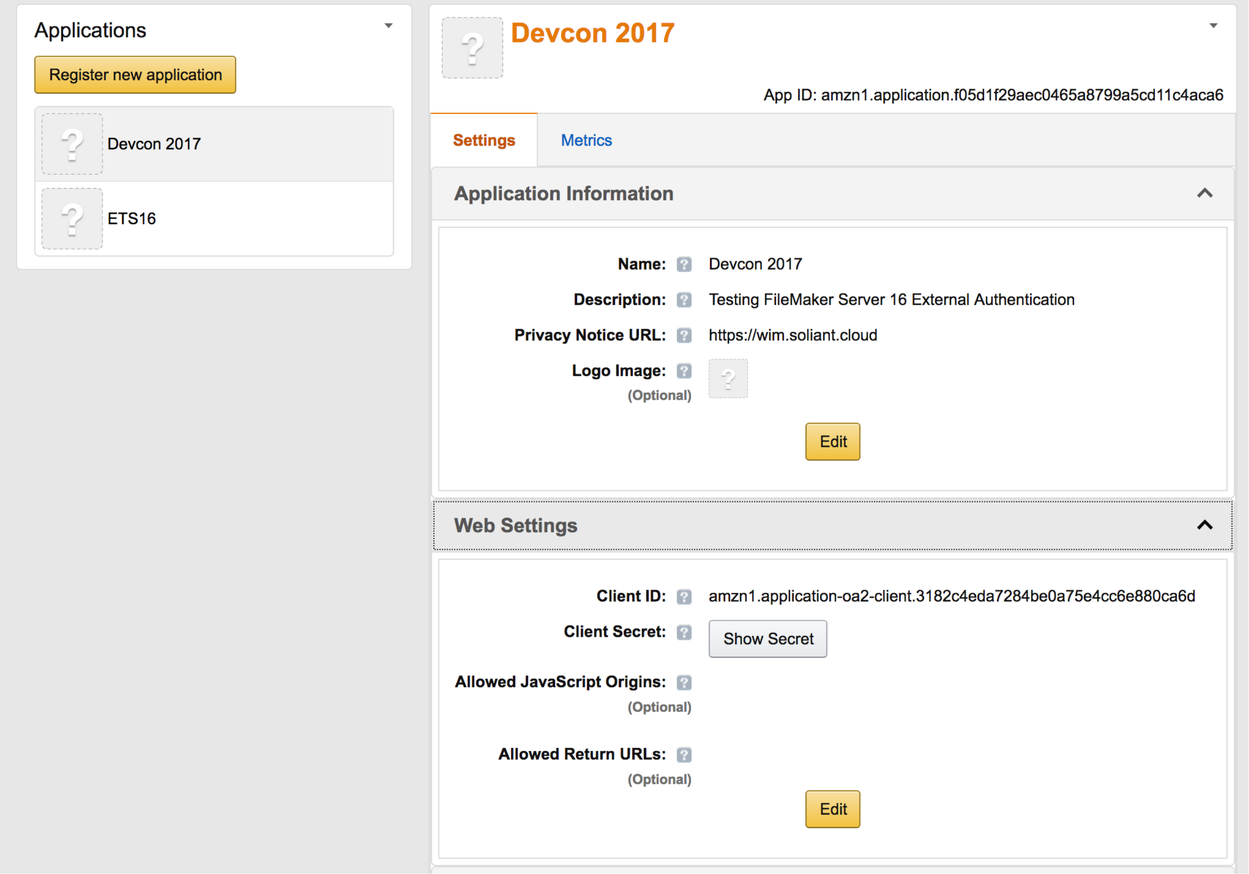
Name: Devcon 2017

Description: Testing FileMaker Server 16 External Au

Privacy Notice URL: https://[redacted].soliant.cloud

Logo Image: (Optional) No file selected.

After you click Save the interface will update as below. Expand the 'Web Settings'



App ID: amzn1.application.f05d1f29aec0465a8799a5cd11c4aca6

Application Information

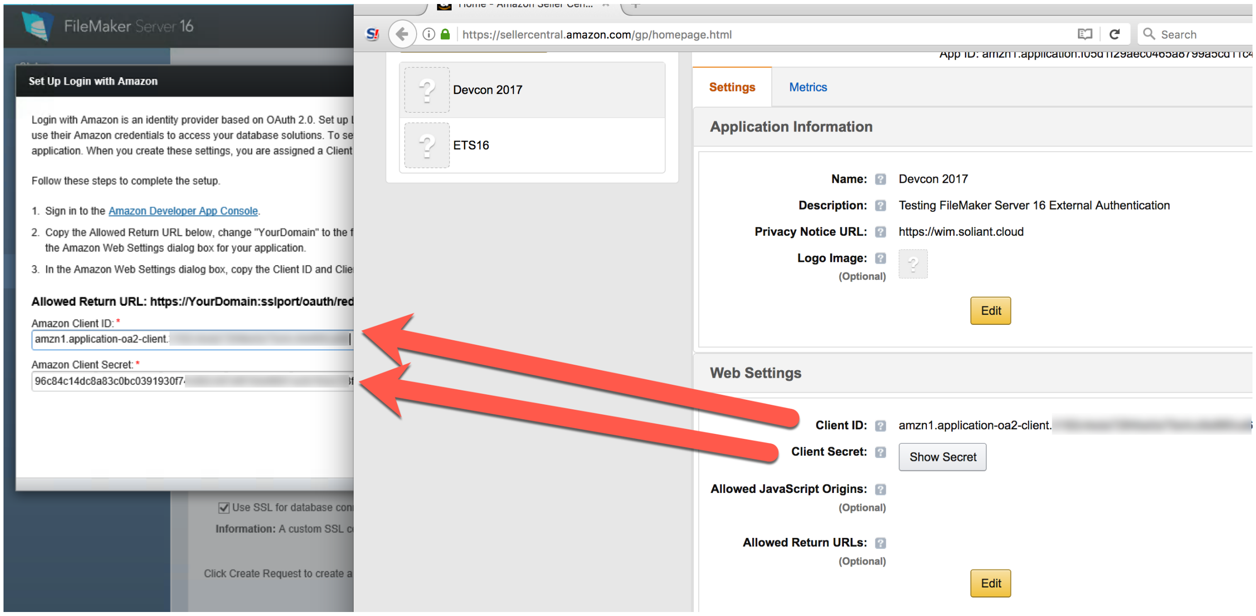
Name: Devcon 2017
Description: Testing FileMaker Server 16 External Authentication
Privacy Notice URL: https://wim.soliant.cloud
Logo Image: (Optional)

Web Settings

Client ID: amzn1.application-oa2-client.3182c4eda7284be0a75e4cc6e880ca6d
Client Secret: Show Secret
Allowed JavaScript Origins: (Optional)
Allowed Return URLs: (Optional)

Open the FileMaker Server admin console and click the gear icon next to Amazon to bring up the setup window.

Copy the client id and the secret:



Set Up Login with Amazon

Login with Amazon is an identity provider based on OAuth 2.0. Set up l
use their Amazon credentials to access your database solutions. To se
application. When you create these settings, you are assigned a Client

Follow these steps to complete the setup.

1. Sign in to the Amazon Developer App Console.
2. Copy the Allowed Return URL below, change "YourDomain" to the f
   the Amazon Web Settings dialog box for your application.
3. In the Amazon Web Settings dialog box, copy the Client ID and Clie

Allowed Return URL: https://YourDomain:sslport/oauth/red

Amazon Client ID: *
amzn1.application-oa2-client.[redacted]

Amazon Client Secret: *
96c84c14dc8a83c0bc0391930f7[redacted]

☑ Use SSL for database con
Information: A custom SSL c
Click Create Request to create a

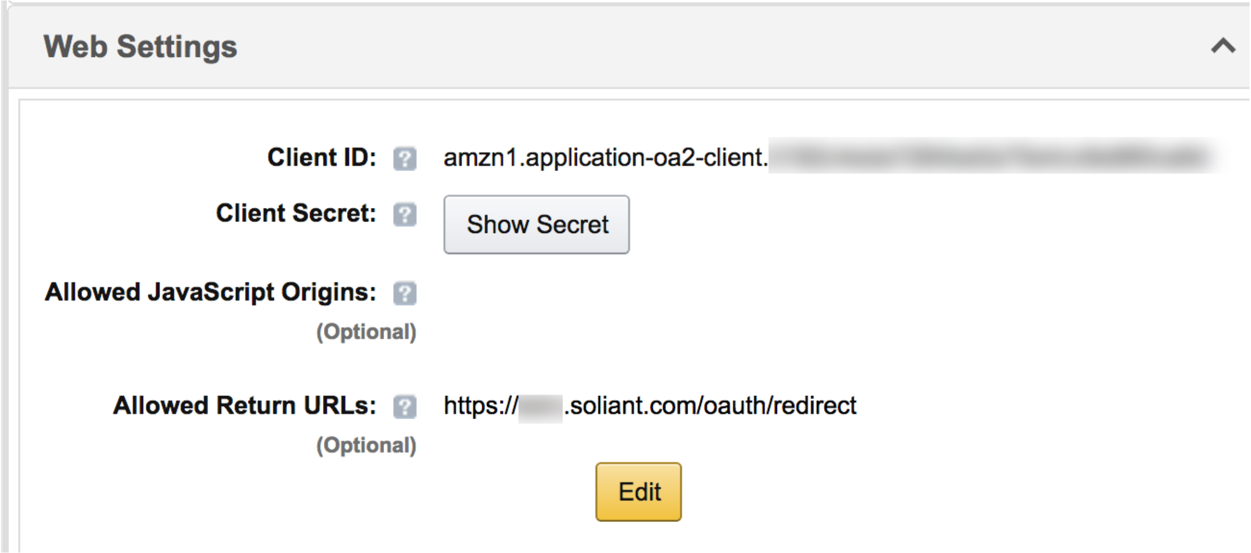
Application Information

Name: Devcon 2017
Description: Testing FileMaker Server 16 External Authentication
Privacy Notice URL: https://wim.soliant.cloud
Logo Image: (Optional)

Web Settings

Client ID: amzn1.application-oa2-client.[redacted]
Client Secret: Show Secret
Allowed JavaScript Origins: (Optional)
Allowed Return URLs: (Optional)

And in the Amazon settings, enter the ‘Allowed Return URLs’ with the “https://” + fully qualified doman name of your filemaker server machine or master machine + SSL port if you don’t use the default port 443 + “/oauth/redirect”



Web Settings

Client ID: amzn1.application-oa2-client.[redacted]

Client Secret:

Allowed JavaScript Origins: (Optional)

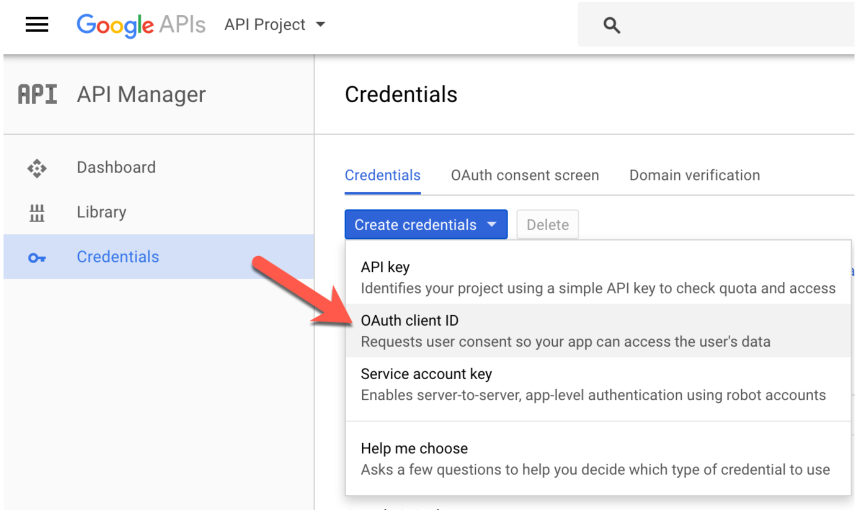
Allowed Return URLs: (Optional) https://[redacted].soliant.com/oauth/redirect

Save all the settings in Amazon and save the settings in the FileMaker Server admin console and restart FileMaker Server

The user will also be able to log into FileMaker with an Amazon account.

Google

To start using Google accounts to log into a FileMaker solution, start at https://console.developers.google.com/apis/credentials/ and click on the ‘Create Credentials’ button, and choose ‘OAuth Client ID’ to set up a new ‘app’.



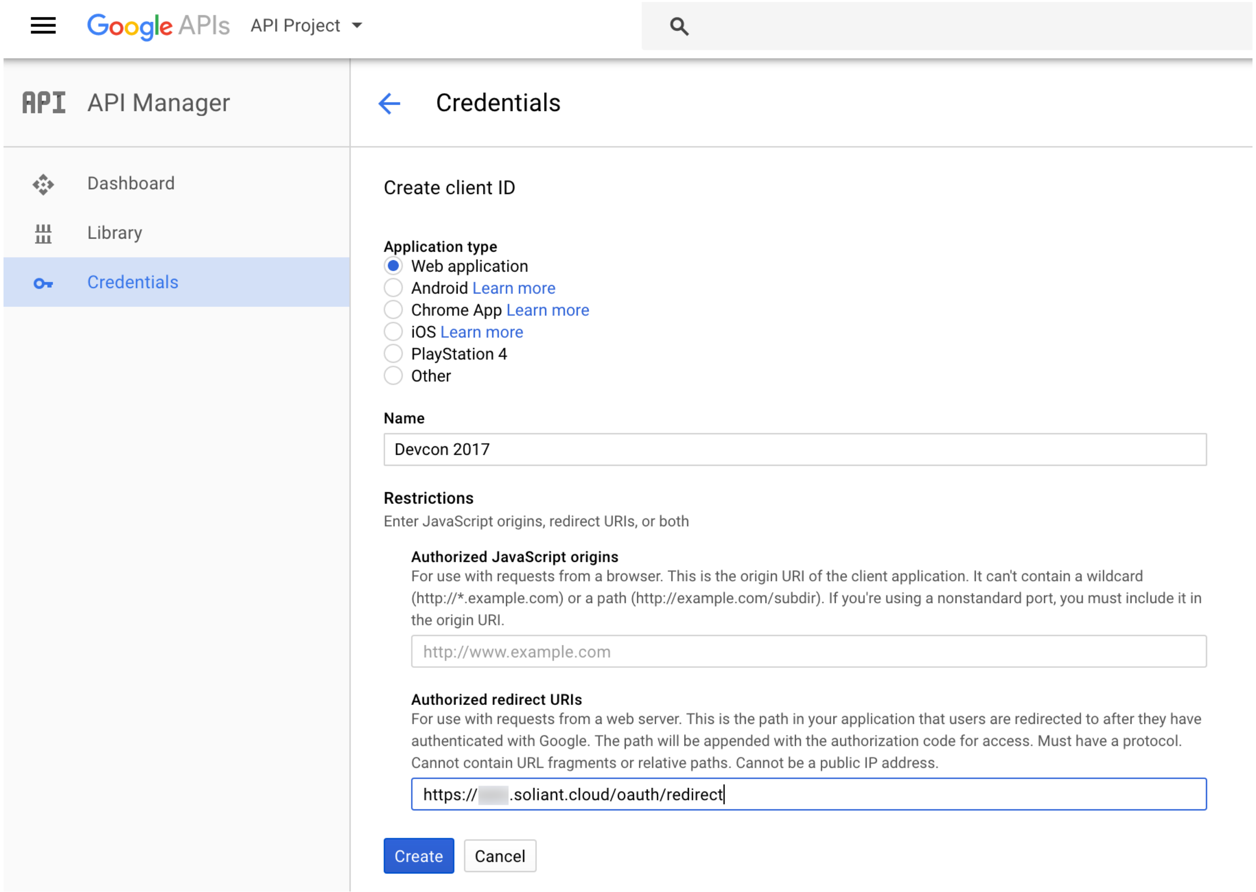
API key
Identifies your project using a simple API key to check quota and access

OAuth client ID
Requests user consent so your app can access the user's data

Service account key
Enables server-to-server, app-level authentication using robot accounts

Help me choose
Asks a few questions to help you decide which type of credential to use

Choose ‘web application’, provide a name to your app and fill in the redirect URL for your FileMaker Server:



Credentials

Create client ID

Application type
- ● Web application
- ○ Android Learn more
- ○ Chrome App Learn more
- ○ iOS Learn more
- ○ PlayStation 4
- ○ Other

Name
Devcon 2017

Restrictions
Enter JavaScript origins, redirect URIs, or both

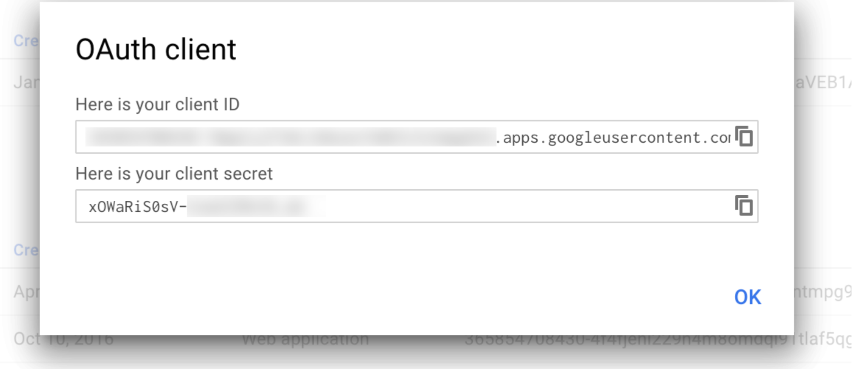
Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

http://www.example.com

Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

https://[redacted].soliant.cloud/oauth/redirect

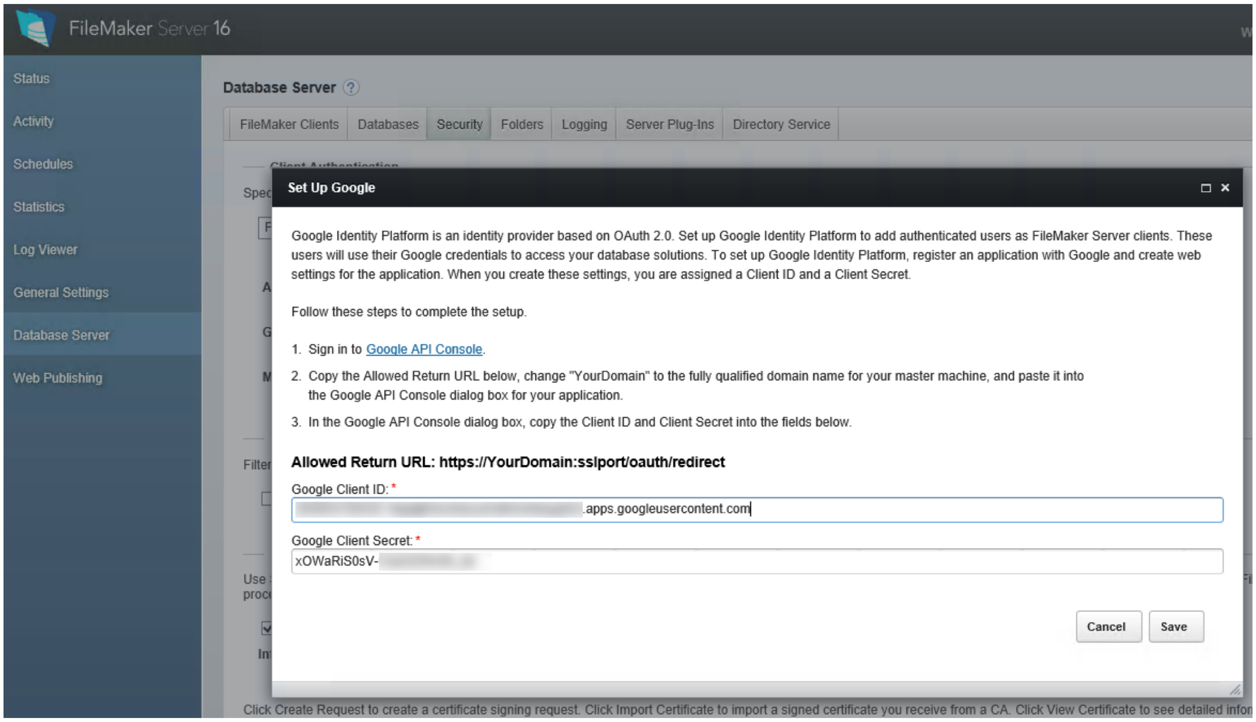
After you click ‘Create’, Google will present you with the client ID and the client secret. Copy thse over to your FileMaker Server settings for Google:



OAuth client

Here is your client ID
[redacted].apps.googleusercontent.com

Here is your client secret
xOWaRiS0sV-[redacted]



Google Identity Platform is an identity provider based on OAuth 2.0. Set up Google Identity Platform to add authenticated users as FileMaker Server clients. These users will use their Google credentials to access your database solutions. To set up Google Identity Platform, register an application with Google and create web settings for the application. When you create these settings, you are assigned a Client ID and a Client Secret.

Follow these steps to complete the setup.

1. Sign in to Google API Console.
2. Copy the Allowed Return URL below, change "YourDomain" to the fully qualified domain name for your master machine, and paste it into the Google API Console dialog box for your application.
3. In the Google API Console dialog box, copy the Client ID and Client Secret into the fields below.

Allowed Return URL: https://YourDomain:sslport/oauth/redirect

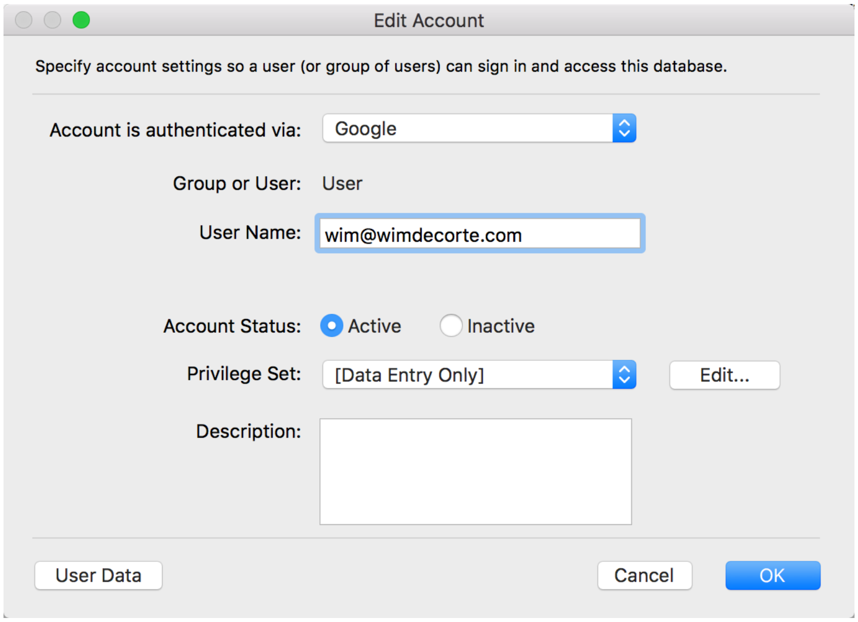
Google Client ID: * [redacted].apps.googleusercontent.com

Google Client Secret: * xOWaRiS0sV-[redacted]

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 infor

Save the settings in FileMaker Server and restart FileMaker Server.

In the FileMaker solution we add an account that will be authenticated via Google:



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

Account is authenticated via: Google

Group or User: User

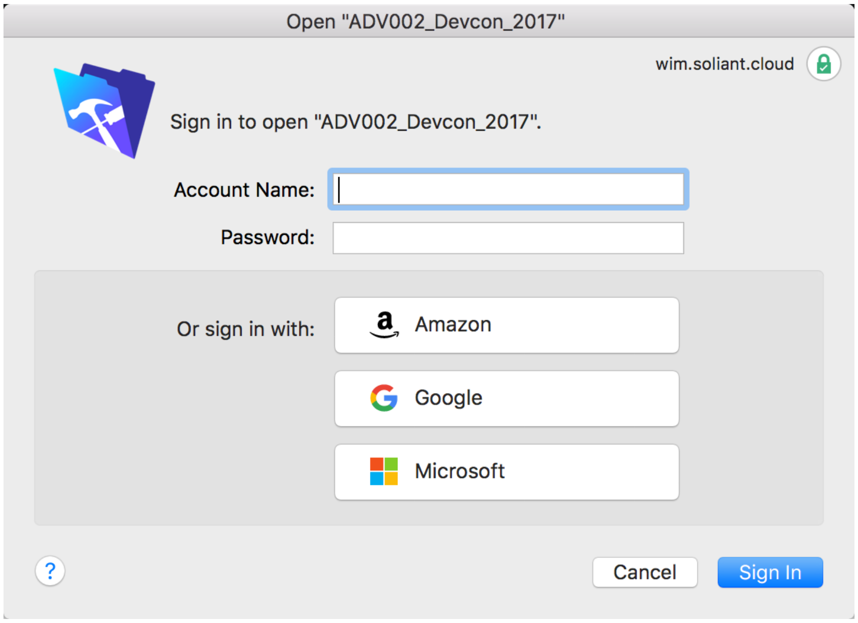
User Name: wim@wimdecorte.com

Account Status: ● Active ○ Inactive

Privilege Set: [Data Entry Only]

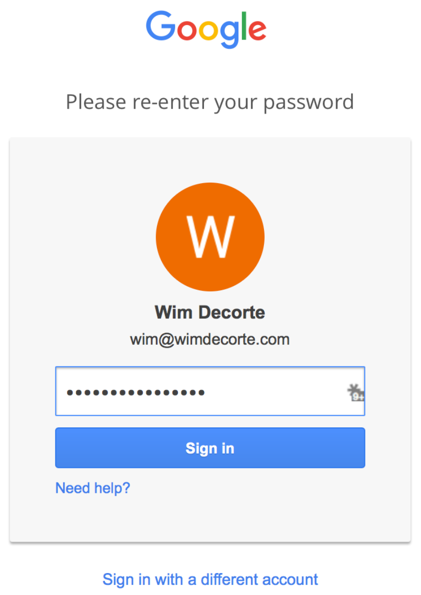
Description:

The login window will now also show the Google button.


Open "ADV002_Devcon_2017"

Sign in to open "ADV002_Devcon_2017".

When we click it we are taken to a Google login page: may need to retake screenshots after completely logging out of Safari


Please re-enter your password

Wim Decorte
wim@wimdecorte.com

and once we log in there we end up in the FileMaker solution with the Get() functions properly reflecting the account used:

Get(AccountName)	wim@wimdecorte.com
Get(AccountGroupName)	
Get(AccountPrivilegeSetName)	[Data Entry Only]

Note

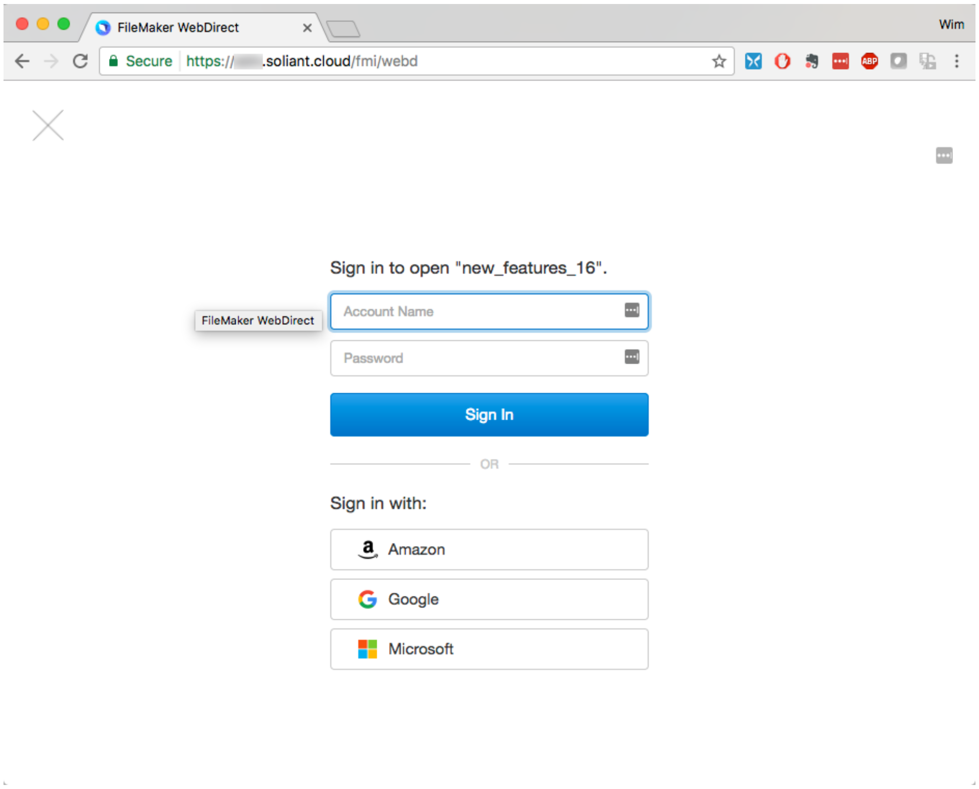
Unlike the Azure and Amazon login pages, the Google one does not display the app name, nor does it ask for consent the very first time an account is used to log into a new app.

FileMaker Go and FileMaker WebDirect

Since all the configuration happens on FileMaker Server and in the FileMaker files, there are no issues using these three identity providers in solutions on FileMaker Go and WebDirect.

When you select a file from the normal WebDirect launch screen you will see a login page with the provider buttons added to it.

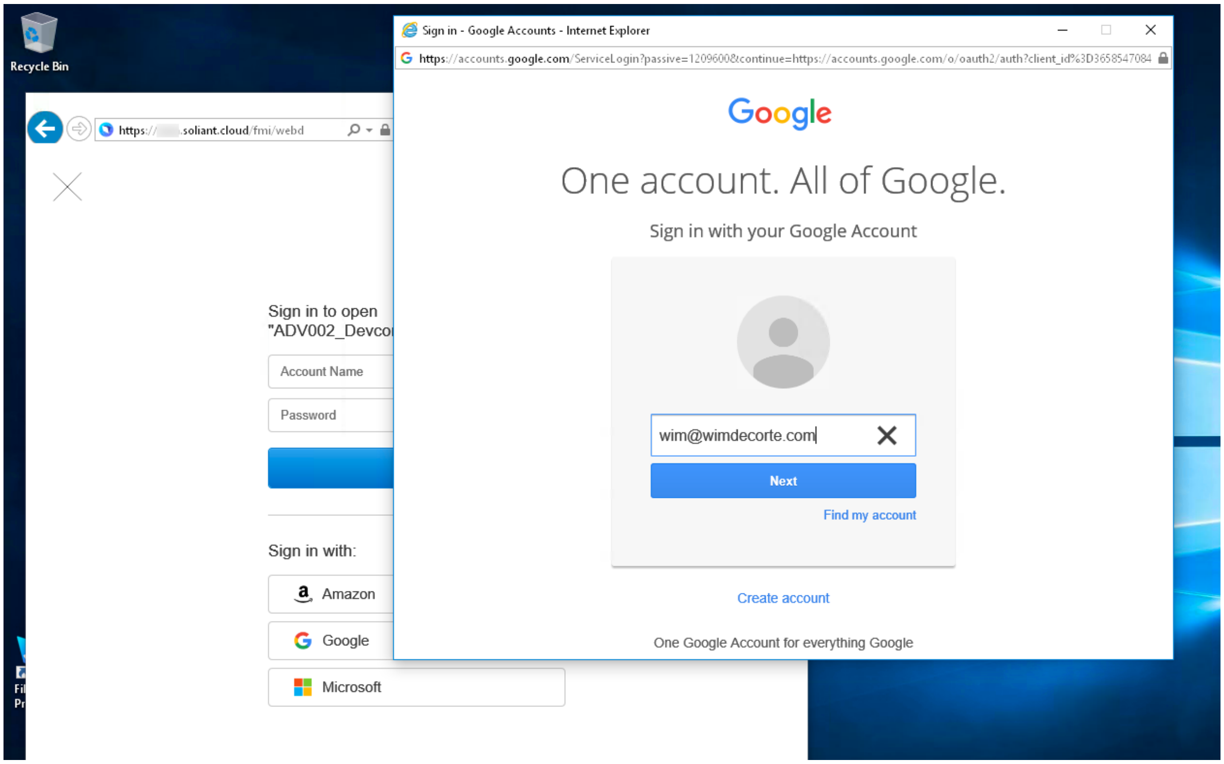
In Chrome on Mac:



Sign in to open "new_features_16".

Sign in with:

In IE on Windows:


Sign in - Google Accounts - Internet Explorer

https://accounts.google.com/ServiceLogin?passive=1209600&continue=https://accounts.google.com/o/oauth2/auth?client_id%3D3658547084

https://[redacted]soliant.cloud/fmi/webd

One account. All of Google.

Sign in with your Google Account

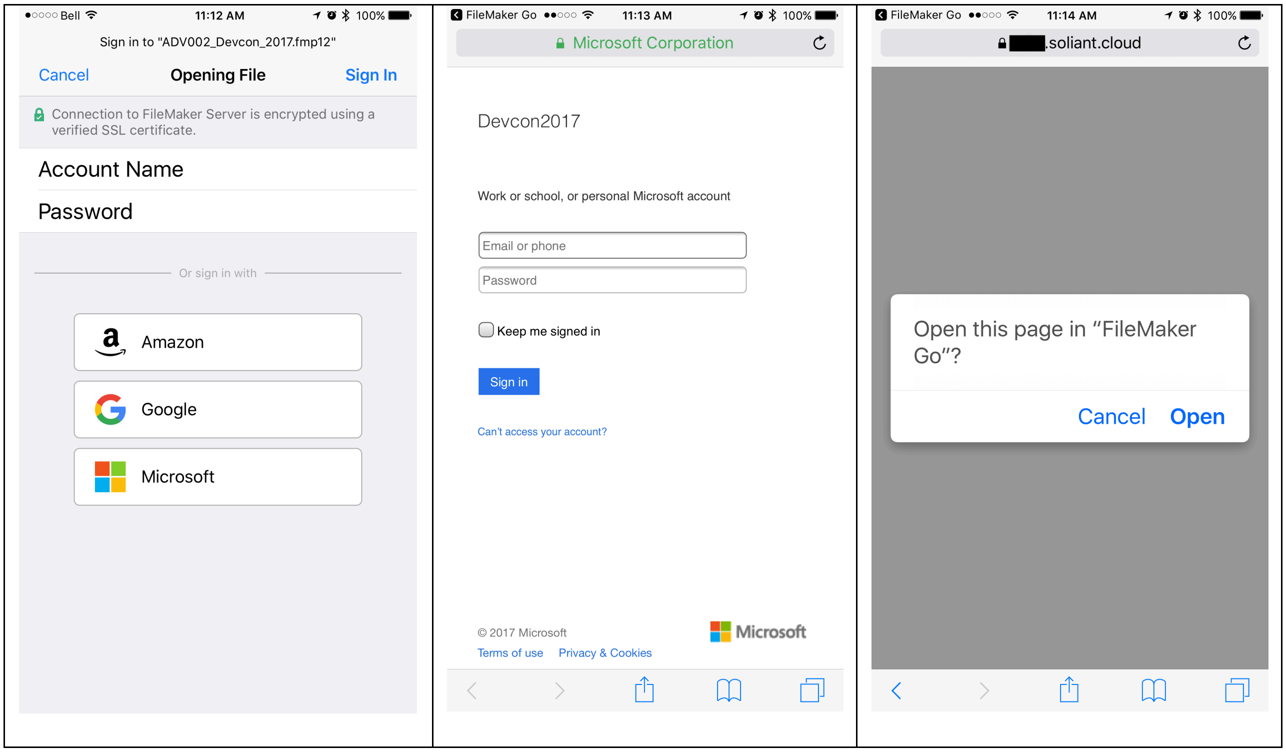
wim@wimdecorte.com

One Google Account for everything Google

Sign in to open
"ADV002_Devco

In all supported browsers, a new browser window will open to handle the login and that extra window will close itself if the login is successful.

In FileMaker Go it behaves very much the same, with Safari popping up a new login window and then closing that. There is an extra dialog when the browser hands control back to FileMaker.


Sign in to "ADV002_Devcon_2017.fmp12"

Connection to FileMaker Server is encrypted using a verified SSL certificate.

Account Name

Password

Microsoft Corporation

Devcon2017

Work or school, or personal Microsoft account

☐ Keep me signed in

Can't access your account?

© 2017 Microsoft

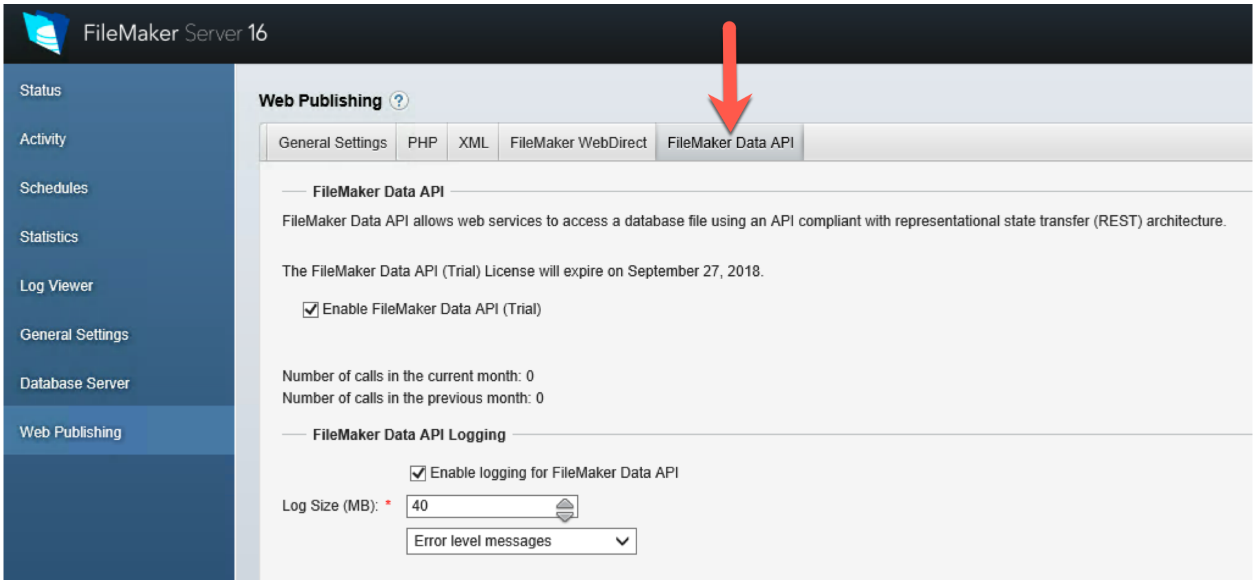
[redacted].soliant.cloud

Open this page in “FileMaker Go”?

If the browser has cached credentials for the provider the login will just briefly flash the new window and the user will be logged into FileMaker without needing to enter his credentials.

External Authentication and the new Data API

FileMaker Server 16 introduces a brand new Data API that turns FileMaker Server into a RESTful web service. This first version is released as a trial that expires in September of 2018. By then the next version of the FileMaker platform will have been released and we expect this Data API to be officially released then.



FileMaker Data API

FileMaker Data API allows web services to access a database file using an API compliant with representational state transfer (REST) architecture.

The FileMaker Data API (Trial) License will expire on September 27, 2018.

☑ Enable FileMaker Data API (Trial)

Number of calls in the current month: 0
Number of calls in the previous month: 0

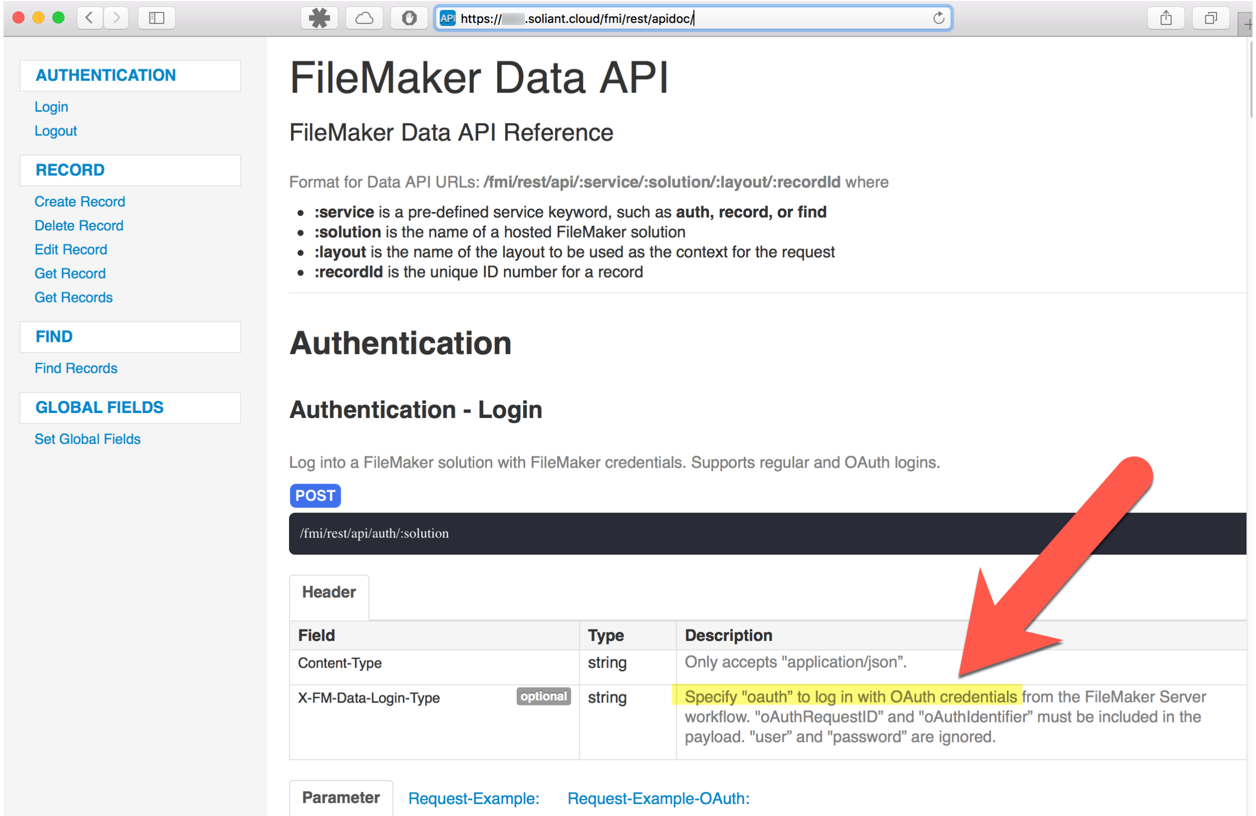
FileMaker Data API Logging

☑ Enable logging for FileMaker Data API

Log Size (MB): * 40

Error level messages

The Data API comes with excellent documentation that is available on your FileMaker Server. Point your browser to ‘https://<your server>/fmi/rest/apidoc’ to access it. Under ‘Authentication’ you will find information on how to set up authentication through Azure AD, Amazon or Google.



https://[redacted].soliant.cloud/fmi/rest/apidoc/

AUTHENTICATION
- Login
- Logout

RECORD
- Create Record
- Delete Record
- Edit Record
- Get Record
- Get Records

FIND
- Find Records

GLOBAL FIELDS
- Set Global Fields

FileMaker Data API

FileMaker Data API Reference

Format for Data API URLs: **/fmi/rest/api/:service/:solution/:layout/:recordId** where

- **:service** is a pre-defined service keyword, such as **auth, record, or find**
- **:solution** is the name of a hosted FileMaker solution
- **:layout** is the name of the layout to be used as the context for the request
- **:recordId** is the unique ID number for a record

Authentication

Authentication - Login

Log into a FileMaker solution with FileMaker credentials. Supports regular and OAuth logins.

POST

`/fmi/rest/api/auth/:solution`

Header

Field	Type	Description
Content-Type	string	Only accepts "application/json".
X-FM-Data-Login-Type optional	string	Specify "oauth" to log in with OAuth credentials from the FileMaker Server workflow. "oAuthRequestID" and "oAuthIdentifier" must be included in the payload. "user" and "password" are ignored.

Parameter Request-Example: Request-Example-OAuth:

/fmi/rest/login → what is there?

/fmi/rest/login?database=x&layout=y&callback=z

in todd's example the callback is this same page (location.href)

Need more

Point to Todd Geist's website

Create ASP.net or PHP version of this

What about FileMaker Cloud?

FileMaker Cloud is the youngest member of the FileMaker product line. It is an Amazon AWS 'appliance' that is easy to deploy and easy to maintain since you do not have to worry about patching or upgrading the underlying operating system (CentOS Linux) and installing FileMaker Server updates is extremely easy.

FileMaker Cloud is on its own release cycle independent from the other products. At the time of this writing (April 2017) it is still based on the core of FileMaker Server 15 and does not currently support any form of External Authentication. Not the three traditional providers nor the three new ones.

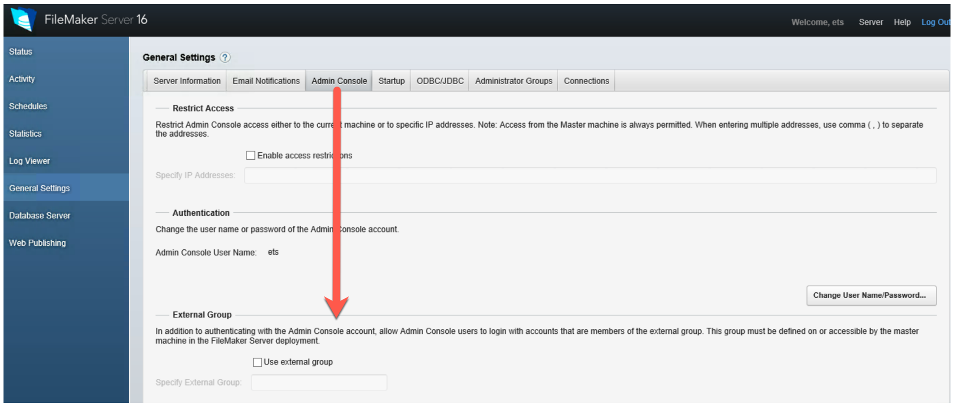
We do expect that FileMaker Cloud will release updates that are based on the FileMaker Server 16 code-base and that will support Azure AD, Google and Amazon.

You can of course install the full version of FileMaker Server 16 'in the cloud' on a Windows AWS instance, or a Microsoft Azure virtual machine or a Google Cloud machine, and take full advantage of all its features, including these three new authentication providers. At Soliant we work closely with Amazon AWS for our soliant.cloud hosting offering.

Gotchas

This last section outlines some things to consider about using the OAuth providers.

- This will be obvious but it bears repeating. Both the FileMaker Server and the FileMaker client need to have access to the internet. There may be some restrictions in this area that would need to be resolved before this feature can be used.
- The Azure AD secret key has an exipiry date. This key needs to be refreshed before it expires to prevent a service interruption. That is something to put on the calendar and plan ahead of time.
- The app name for Google, Azure and Amazon (profile or app approach) covers all solutions hosted on FileMaker Server, not just one FileMaker solution. As mentioned earlier, since that app name is visible on some of the provider's login pages, it is important to pick a name that will not cause confusion for any user of any solution hosted on the FileMaker Server that is configured for the provider's app.
- The new Oauth providers can not be used for external authentication to the FileMaker Server admin console.



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: ets

External Group

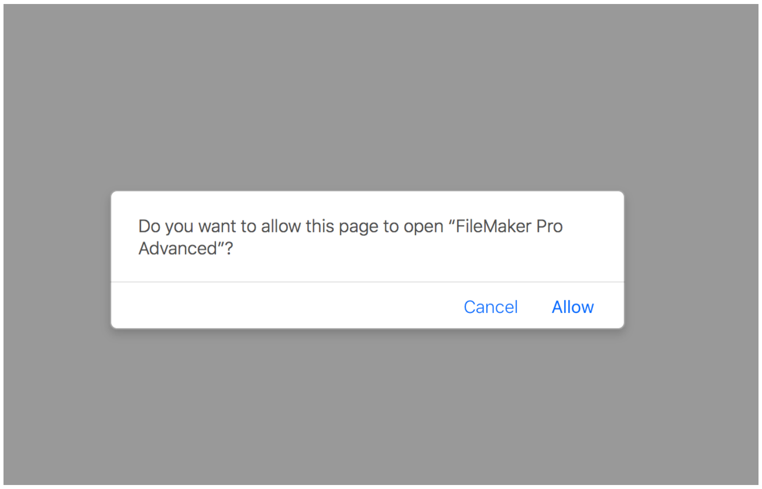
In addition to authenticating with the Admin Console account, allow Admin Console users to login with accounts that are members of the external group. This group must be defined on or accessible by the master machine in the FileMaker Server deployment.

☐ Use external group

Specify External Group:

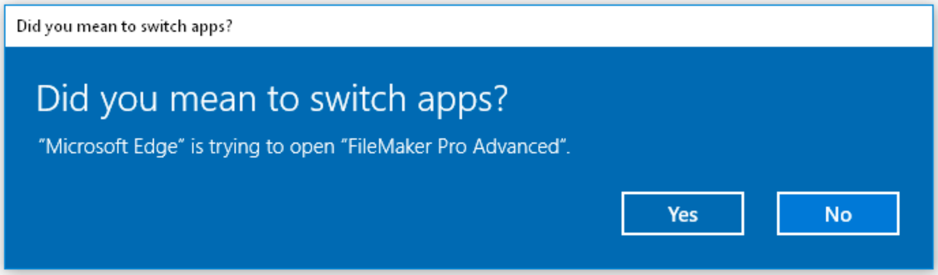
Traditional external authentication through AD / OD and Local Groups does still work though.

- The actual login is done in the browser and there is some specific browser behavior to be aware of.
  - The default browser is used as soon as you click one of the provider buttons on the FileMaker login dialog. There is no setting in FileMaker to specify what browser to use, it uses the default as set up in the operating system.
  - When the authentication on the providers web site was successful, a blank tab is left open if the browser was already running.
  - If the browser was not open (launched) then it will launch for the login and quit when done.
  - Some browsers will ask for a confirmation before handing control back to FileMaker, the screenshot below for instance is Safari's behavior.



Do you want to allow this page to open "FileMaker Pro Advanced"?

or in Microsoft Edge:



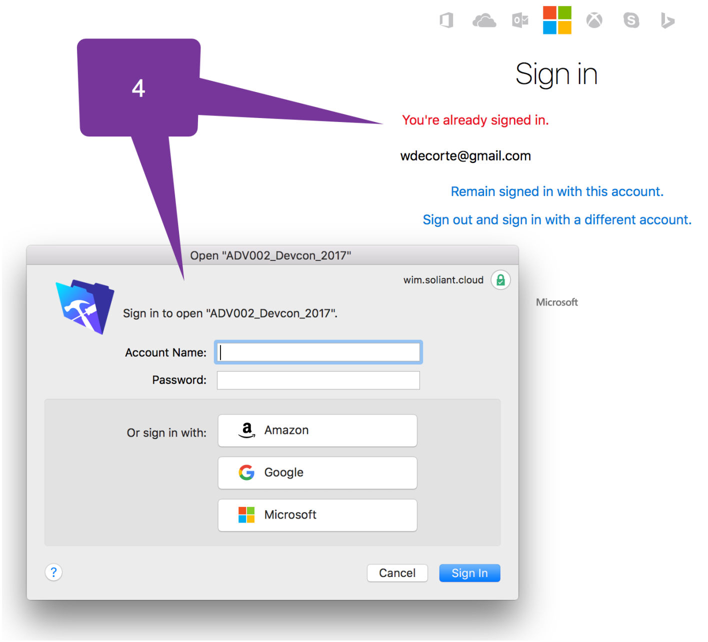
Did you mean to switch apps?

Did you mean to switch apps?

"Microsoft Edge" is trying to open "FileMaker Pro Advanced".

Also keep in mind that the browser may have cached credentials. If a user logs into the FileMaker solution with x@y.com through Azure then the browser will remember that. And to be completed

Logged a bug report on this; if the user is already logged in but with no browser windows or tabs open, then this is the end result: Azure recognizes that the user is already logged on, but does not communicate properly with FM to let the user in:



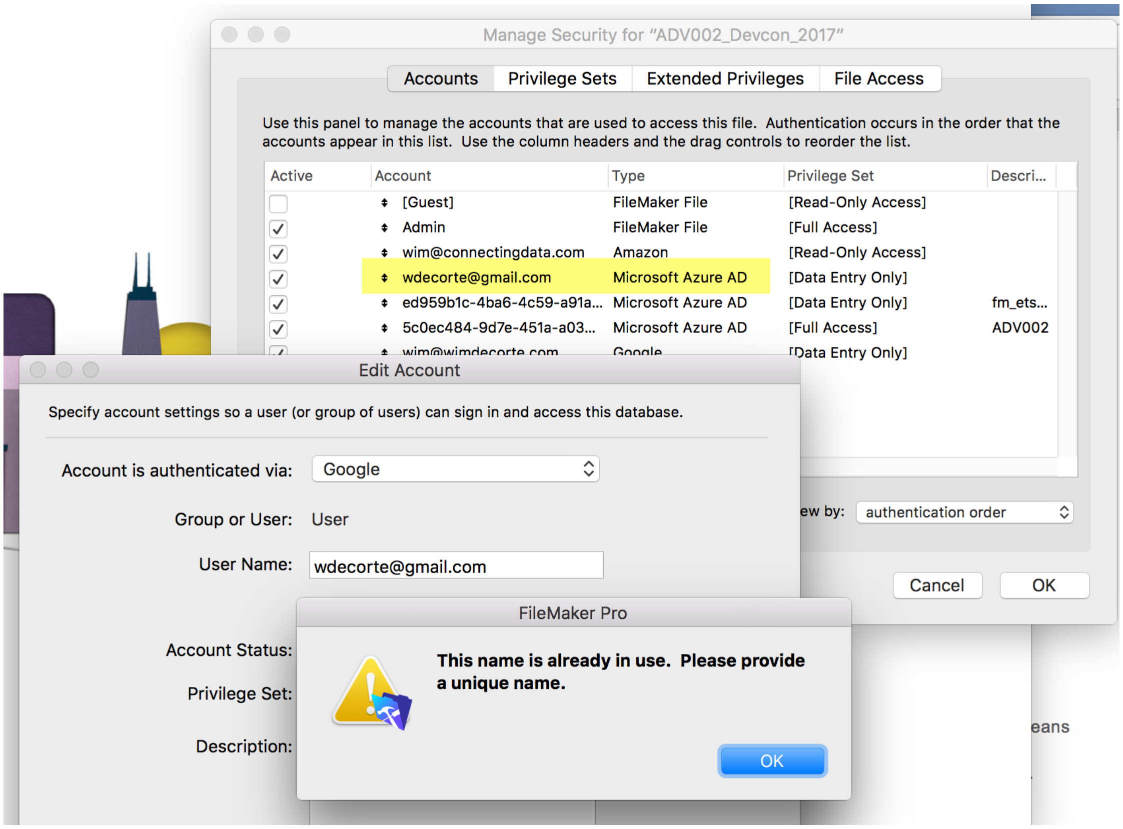
You're already signed in.

wdecorte@gmail.com

Sign in to open "ADV002_Devcon_2017".

→ in retesting it works fine – waiting on feedback from ETS

- Can you use the same email address / account for multiple providers? FileMaker requires each account to be unqiue. That means that you can not use the same email address across multiple OAuth providers. The account we used in our Azure examples (wdecorte@gmail.com) is obviously a Google account but we used it for our Microsoft account (we simply used it to create a Microsoft account). We have it in our FileMaker solution as an Azure AD account. If we try to add that email address again to the FileMaker solution but this time as a Google account, we get an error saying that the account name has to be unique.



Manage Security for "ADV002_Devcon_2017"

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 list. Use the column headers and the drag controls to reorder the list.

Active	Account	Type	Privilege Set	Descri...
☐	[Guest]	FileMaker File	[Read-Only Access]	
☑	Admin	FileMaker File	[Full Access]	
☑	wim@connectingdata.com	Amazon	[Read-Only Access]	
☑	wdecorte@gmail.com	Microsoft Azure AD	[Data Entry Only]	
☑	ed959b1c-4ba6-4c59-a91a...	Microsoft Azure AD	[Data Entry Only]	fm_ets...
☑	5c0ec484-9d7e-451a-a03...	Microsoft Azure AD	[Full Access]	ADV002
☑	wim@wimdecorte.com	Google	[Data Entry Only]	

ew by: authentication order

Edit Account

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

Account is authenticated via: Google

Group or User: User

User Name: wdecorte@gmail.com

Account Status:

Privilege Set:

Description:

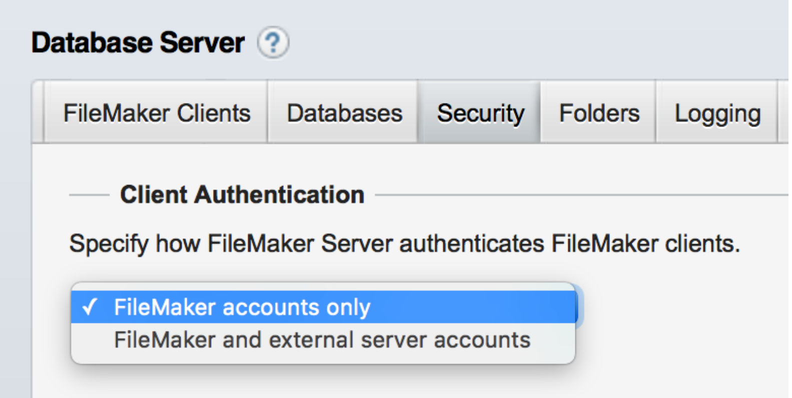
FileMaker Pro

This name is already in use. Please provide a unique name.

mention Amazon AWS IAM?

- More than you bargained for?

  In the FileMaker Server admin console when you enable 'FileMaker and External Accounts' to activate the toggles for the Amazon / Azure / Google providers:



Database Server

Client Authentication

Specify how FileMaker Server authenticates FileMaker clients.

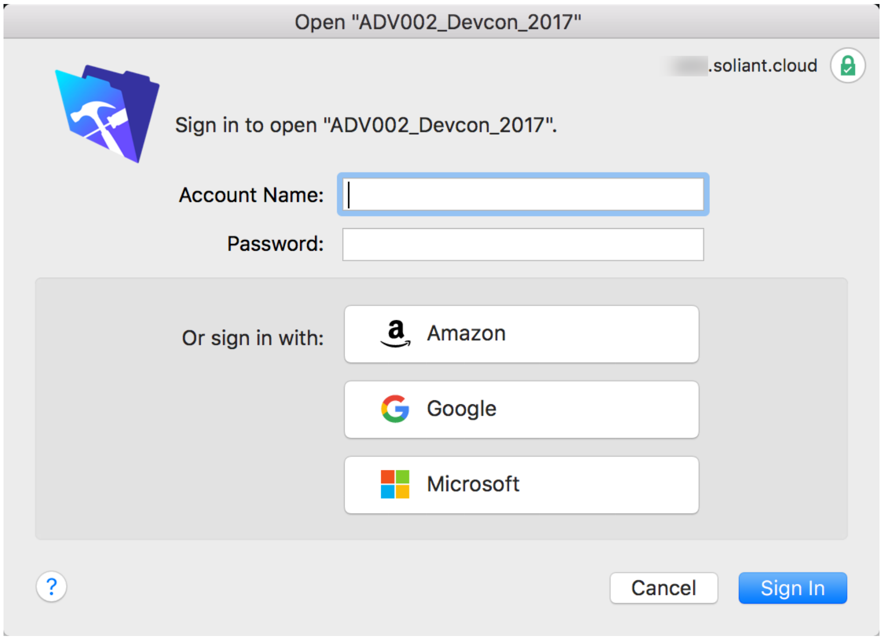
✓ FileMaker accounts only
FileMaker and external server accounts

You also automatically enable the three traditional external authentication providers (AD, OD and Local Accounts/Groups). That may not be plainly obvious. Those require no further configuration but are immediately enabled.

If you have no accounts in the FileMaker solution that are set to ‘Authenticate via External Server’ then there will be no interference. If you do have traditional EA accounts in your FileMaker solution then be careful with the names used for Azure AD groups vs. those for normal AD groups and pay special attention to the authentication order in the list of FileMaker accounts.

- The FileMaker login dialog

  The login dialog will display all the OAuth providers that have been configured for the server, **EVEN** if there are no Azure, Google or Amazon accounts in the file you are trying to access. That can be a bit misleading and may cause users to try to log in with one of those accounts when the file does not allow it.



Open "ADV002_Devcon_2017"

[redacted].soliant.cloud

Sign in to open "ADV002_Devcon_2017".

- Make sure to keep your deployment procedures up-to-date. The Azure / Amazon / Google web sites tend to change fairly frequently so whatever screenshots and write-ups you have will likely go stale over time. By checking those regularly you can avoid a lot of confustion when you need to recreate the whole deployment when it counts the most, in a disaster recovery situation.
- Cached Credentials. Browsers can remember the session when you last logged into one of the three providers. On machines where many people need to use the FileMaker solution from the same machine this can lead to people being logged in with someone else’s credentials and the associated level of rights that are not their own.

The Identity Provider Landscape

It is not a coincidence that FileMaker Inc. decided to add support for Microsoft, Amazon and Google accounts at this time. Federated Identity Management is a hot topic these days as a byproduct of the industry's drive to have more systems and resources in the 'Cloud'. If you have a particular system hosted in the cloud and you have another system on-premise that takes care of your identity management, can you join those two in a federation so that they cooperate? Or can you deletegate the whole of the identity management to a dedicated 3rd-party Identity Provider and connect all the systems to it?

These are questions that occupy the IT Manager's mind these days. And you can expect questions along these lines when the integration of FileMaker products into this landscape is brought up. We think it is important to keep informed about what is happening in this realm.

There are 'big iron' identity providers like Ping[7], Okta[8], CA (the old 'SiteMinder')[9], Amazon AWS IAM[10] and many others. There are standards such as SAML[11] for data exchange between identity providers and identity consumers. FileMaker does not currently integrate natively with these, and while it can be made to work it does take careful consideration to not compromise security in an effort to make identity management easier.

For a more in-depth discussion about FileMaker and FIM, see the white paper by Steven H. Blackwell: "xxxx"

---

[7] https://www.pingidentity.com/en.html

[8] https://www.okta.com/

[9] https://www.ca.com/us/products/identity-management.html?intcmp=headernav

[10] https://aws.amazon.com/iam/?hp=tile&so-exp=below

[11] https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language