Part 3: Setting up the Portal App

What

The configuration of your Windows MDM integration will all be driven by an application you yourself create in the Microsoft Entra Portal.

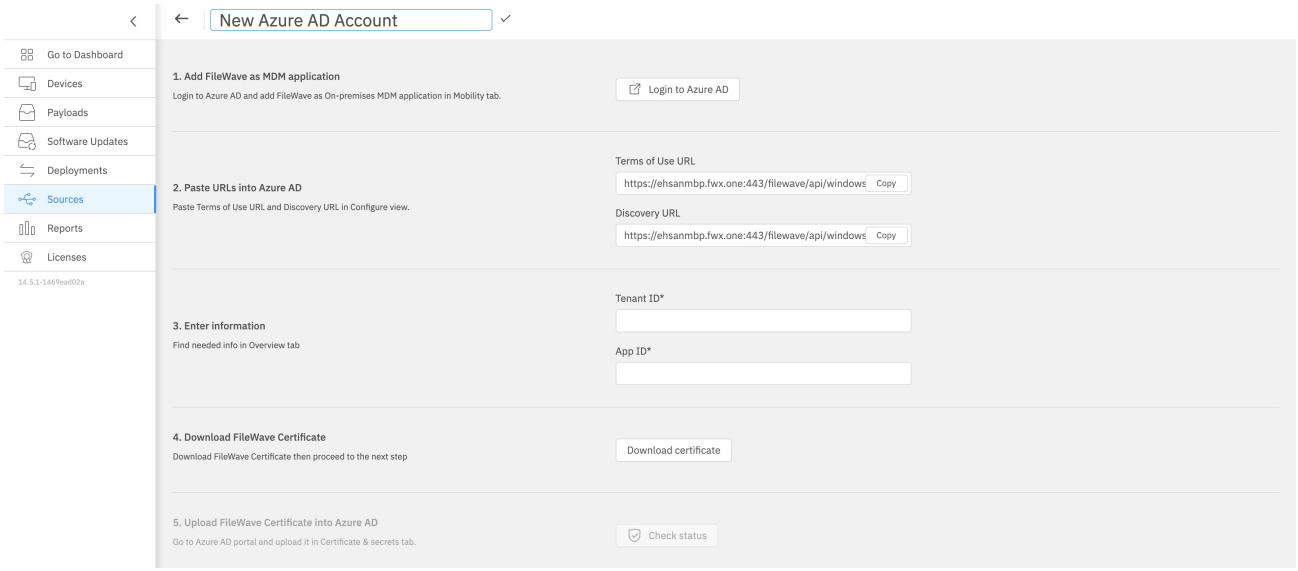
When/Why

This application is the linch pin that ties your devices (in AutoPilot), through your user accounts (the group associated with the app), into redirection to your FileWave MDM server. Detailed setup steps follow.

How

Add Microsoft Entra ID account in FileWave

1. Open your FileWave AnyWhere (Web Admin) page and navigate to sources.
2. Click the Microsoft tab.
3. Click on New account and you should see the following form:



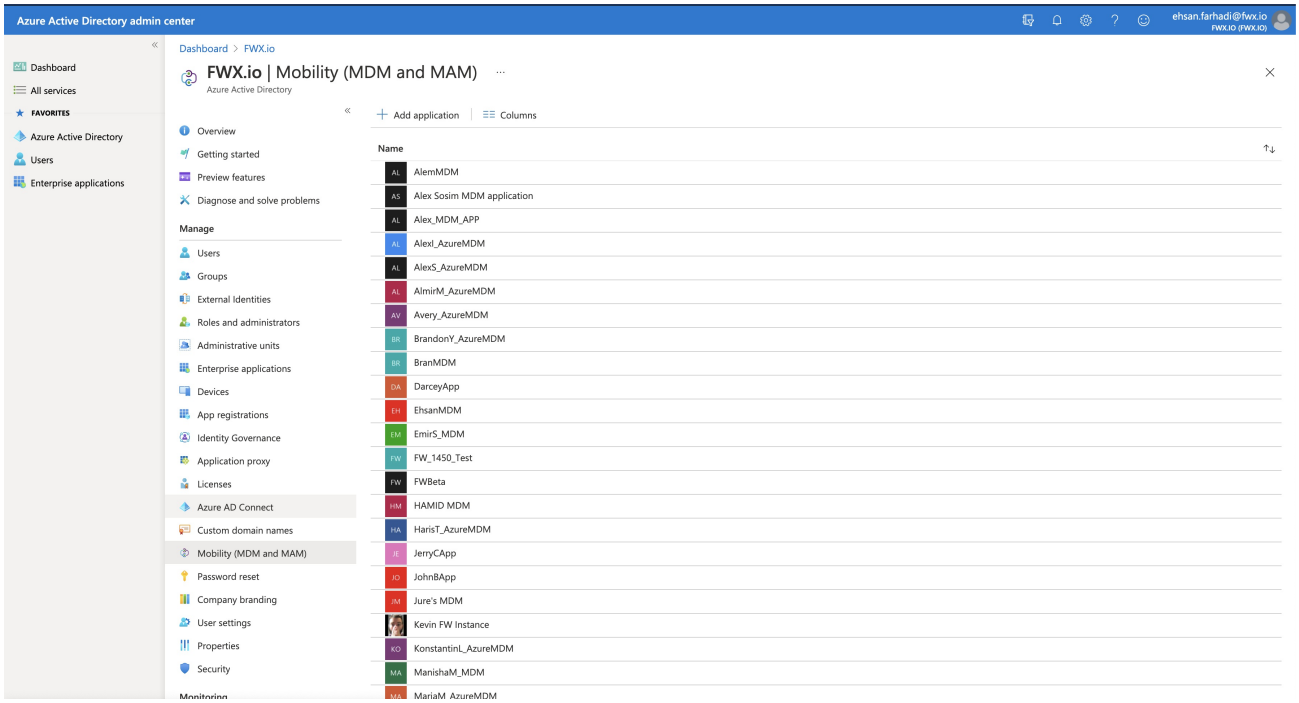
Keep this form open for completion in later steps.

Configuring Microsoft Entra ID

Creating MDM application

In order to enable MDM enrollment, first you need to configure your Microsoft Entra ID to recognizes your FileWave server as your MDM.

1. Go to your Microsoft Entra ID portal: https://aad.portal.azure.com
2. From dashboard navigate to Microsoft Entra Active Directory → Mobility (MDM and MAM) and then click Add application.
3. In new application form, select On-premises MDM application, give it a name and a log and click on add_._



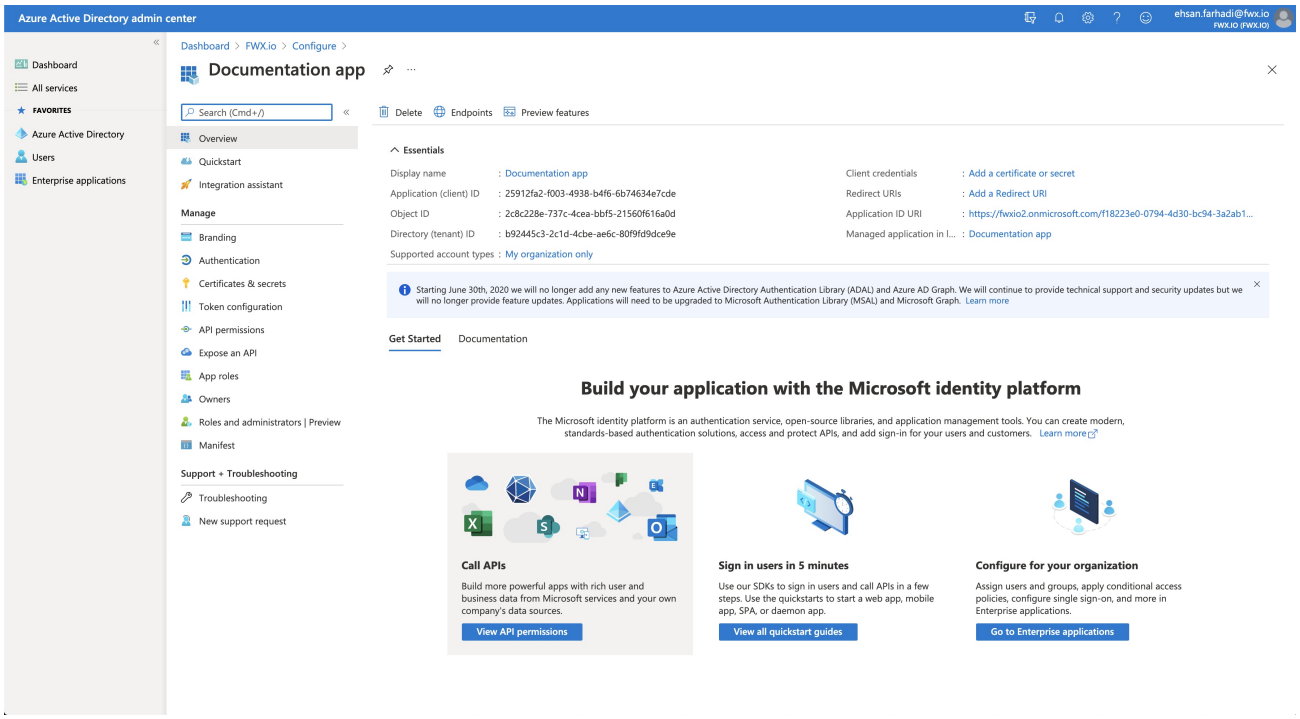
Configuring your MDM application

1. Go back to the list of MDM applications from step 2 above, and open the application you have just created. You should be able to see the following options:
    1. MDM user scope: This is where you indicate which users can enroll their devices using this MDM application. you can either choose:
        1. All: Force all users to use this MDM application. (Preferred)
        2. Some: You can select user groups which are allowed to use this MDM application to enroll their devices. If you do use this then you will need to make sure that you make a Group to restrict this, and add all of the users who will have their devices managed by MDM in that same group.
    2. MDM terms of use URL:
    Copy the value from the form you opened up in you FileWave AnyWhere (Web Admin) earlier.
    3. MDM discovery URL:
    Copy the value from the form you opened up in you FileWave AnyWhere (Web Admin) earlier.

It is very important that if you have another solution in place like InTune that you make sure that you do not have both InTune and FileWave enabled for the same users. You may get an error about not having permission to enroll devices. You can test this by disabling the Intune MDM (or another vendor) in Microsoft Entra by setting it to None and then wait 5 minutes and you would be able to enroll using FileWave. Think about which MDM solution you want to be for your different users in your environment. A single device can only really be in a single MDM. You can enroll to Intune for MDM and install the FileWave agent for instance, but then you could only push Windows Profiles from InTune. Everything else would work just fine in FileWave for those devices.

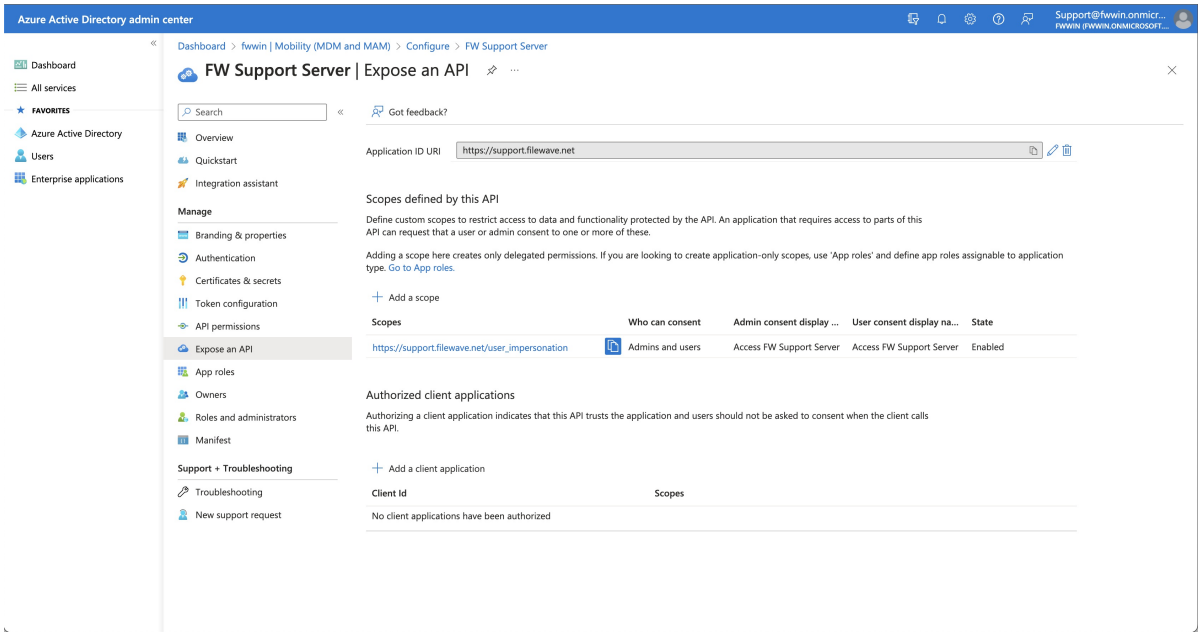
Integrating FileWave and Microsoft Entra

After configuring your MDM application, on the same page, you will see a small link that reads: On-premises MDM application settings. Click on it in order to open your on-premise application settings. You should see the following page:

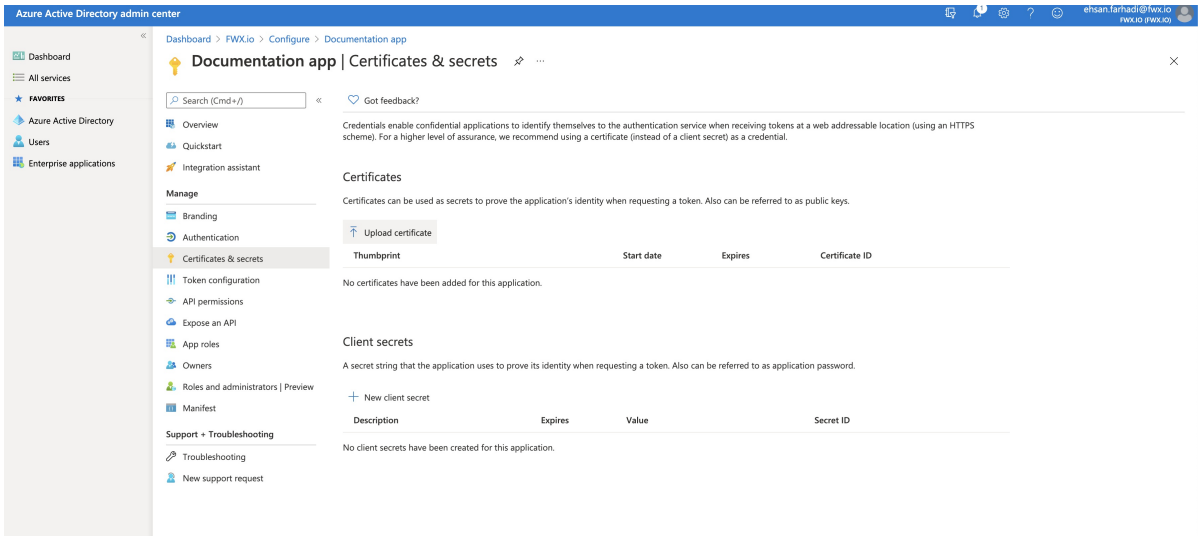


From here there are only few steps left!

1. Copy the Application ID and Tenant ID from this page and paste it in the Microsoft Entra Account form in FileWave AnyWhere (Web Admin) (which you kept open from earlier)
2. The Application ID URI value in your MDM app (in Microsoft Entra ID) must match your FileWave server URL, to fix that, go to "Expose an API" on the left side, and edit the URL there. The URL should be like https://example.filewave.net replacing that with your server's DNS name.



3. Go back to the Microsoft Entra account form in your FileWave AnyWhere (Web Admin), and download the FileWave certificate.
4. Once you have the certificate, go back to the Microsoft Entra ID portal, navigate to Certificates & secrets and upload your certificate to your Microsoft Entra MDM application there.



5. Once the Certificate is uploaded, wait couple of seconds, then go back to FileWave AnyWhere (Web Admin), in the already open Microsoft Entra account form and click on Check Status button.
6. As soon as you see the green light, go ahead and save your Microsoft Entra account.

You are now ready to enroll a device in to Windows MDM.

Application tenant or consent messages

You may see a message similar to below:

- AADSTS500011 – The resource principal named [URI] was not found in the tenant named [guid]. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You might have sent your authentication request to the wrong tenant.

If you're trying to log in from an application that doesn't support user consent flow or you're unable to use it otherwise, you can use the same special login URL crafting trick that I proposed in my article for resolving consent-related issues when getting error AADSTS650001, and create a URL like this:

- https://login.microsoftonline.com/[tenant_name_in_onmicrosoft.com-form]/oauth2/authorize?client_id=[appId]&response_type=code&redirect_uri=http://your-uri-here&nonce=1234&resource=https://graph.windows.net&prompt=consent.

If the application requires admin consent, you may replace "consent" with "admin_consent".

Revision #4
★Created 15 June 2023 15:13:46 by Andrew Kloosterhuis
✎Updated 13 July 2023 13:04:54 by Josh Levitsky