

# 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:

< ← New Azure AD Account ✓

Go to Dashboard

Devices

Payloads

Software Updates

Deployments

Sources

Reports

Licenses

14.5.1-1469aad02a

**1. Add FileWave as MDM application**  
Login to Azure AD and add FileWave as On-premises MDM application in Mobility tab. [Login to Azure AD](#)

**2. Paste URLs into Azure AD**  
Paste Terms of Use URL and Discovery URL in Configure view.

Terms of Use URL  
<https://ehsanmbp.fwx.one:443/filewave/api/windows/> [Copy](#)

Discovery URL  
<https://ehsanmbp.fwx.one:443/filewave/api/windows/> [Copy](#)

**3. Enter information**  
Find needed info in Overview tab

Tenant ID\*

App ID\*

**4. Download FileWave Certificate**  
Download FileWave Certificate then proceed to the next step [Download certificate](#)

**5. Upload FileWave Certificate into Azure AD**  
Go to Azure AD portal and upload it in Certificate & secrets tab. [Check status](#)

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 WIP) 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\_.\_

Azure Active Directory admin center

Dashboard > FWX.io

**FWX.io | Mobility (MDM and MAM)**

Overview

Getting started

Preview features

Diagnose and solve problems

**Manage**

Users

Groups

External identities

Roles and administrators

Administrative units

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Licenses

Azure AD Connect

Custom domain names

**Mobility (MDM and MAM)**

Password reset

Company branding

User settings

Properties

Security

Monitoring

Columns

Name
AlernMDM
Alex Sosim MDM application
Alex_MDM_APP
Alexi_AzureMDM
AlexS_AzureMDM
AlmirM_AzureMDM
Avery_AzureMDM
BrandonY_AzureMDM
BranMDM
DarceyApp
EhsanMDM
EmirS_MDM
FW_1450_Test
FWBeta
HAMID MDM
HariS_AzureMDM
JerryCApp
JohnBApp
Jure's MDM
Kevin FW Instance
KonstantinL_AzureMDM
ManishaM_MDM
MariaM AzureMDM

## Configuring your MDM application

- 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:
  - MDM user scope: This is where you indicate which users can enroll their devices using this MDM application. you can either choose:
    - All: Force all users to use this MDM application. (Preferred)
    - 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.
  - MDM terms of use URL:  
Copy the value from the form you opened up in you FileWave AnyWhere (Web Admin) earlier.
  - 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:

**Documentation app**

Search (Cmd+/) Delete Endpoints Preview features

**Overview**

**Essentials**

Display name : Documentation app

Application (client) ID : 25912fa2-f003-4938-b4f6-6b74634e7cde

Object ID : 2c8c228e-737c-4cea-bb5f-21560f616a0d

Directory (tenant) ID : b92445c3-2c1d-4cbe-ae6c-80f9fd9dce9e

Supported account types : My organization only

Client credentials : Add a certificate or secret

Redirect URIs : Add a Redirect URI

Application ID URI : https://fwwio2.onmicrosoft.com/f18223e0-0794-4d30-bc94-3a2ab1...

Managed application in L... : Documentation app

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

**Get Started** Documentation

**Build your application with the Microsoft identity platform**

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

**Call APIs**

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources. [View API permissions](#)

**Sign in users in 5 minutes**

Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app. [View all quickstart guides](#)

**Configure for your organization**

Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications. [Go to Enterprise applications](#)

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.

**FW Support Server | Expose an API**

Search Got feedback?

Application ID URI : https://support.filewave.net

**Scopes defined by this API**

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use "App roles" and define app roles assignable to application type. [Go to App roles](#)

+ Add a scope

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
https://support.filewave.net/user_impersonation	Admins and users	Access FW Support Server	Access FW Support Server	Enabled

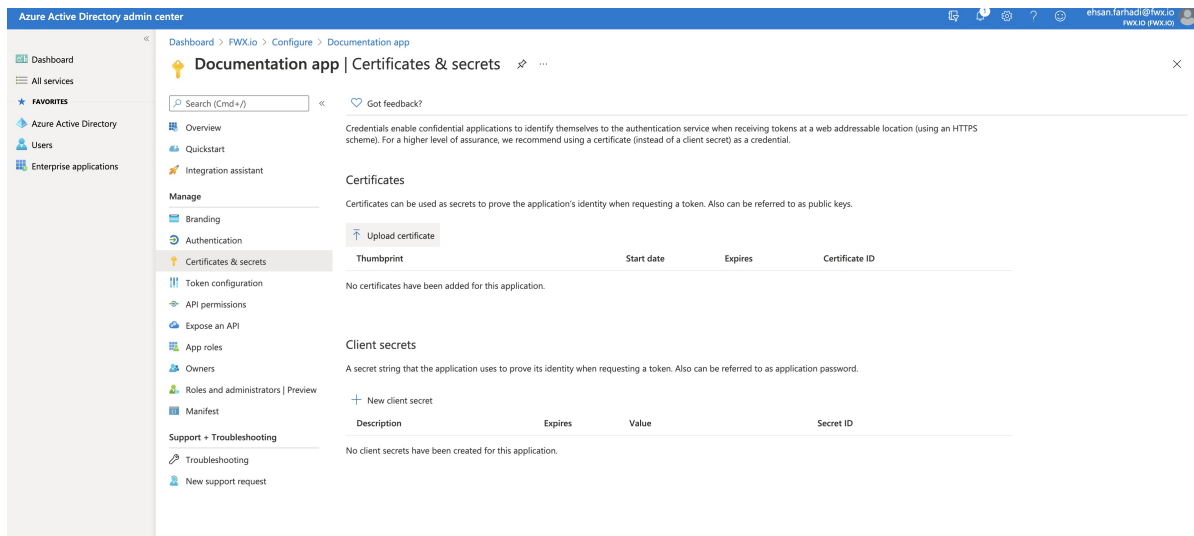
**Authorized client applications**

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

+ Add a client application

Client Id	Scopes
No client applications have been authorized	

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](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 #5

★Created 15 June 2023 15:13:46 by Andrew Kloosterhuis

✍Updated 20 May 2025 13:54:47 by Josh Levitsky