Identity Provider (IdP) Integration

Identity Provider (IdP) integration can be key to meeting security requirements from your InfoSec team, and ease-of-use requirements for your customers. IdP solutions allow your customer to have only one set of credentials, and to use them anywhere.

FileWave Identity Provider (IdP) Integration Overview

What

Identity Provider (IdP) integration can be key to meeting security requirements from your InfoSec team, and ease-of-use requirements for your customers. IdP solutions allow your customer to have only one set of credentials, and to use them anywhere.

FileWave currently supports 4 IdP providers with version 15.5.x.

> Only one of each IdP may be configured.

When/Why

If you currently utilize an IDP provider, you'll want to start here to understand the supported platforms and the instructions for setting up access.

How

See below for links to articles on setup and requirements:

- IdP Setup: Microsoft Entra AD
- IdP Setup: Okta
- IdP Setup: Google
- IdP Setup: Keycloak
- Adding IdP Groups for FileWave Authentication
- Configuring DEP Profiles for IDP Authentication
- Admin Login in Using an IdP Provider
- IdP for Deployments and Smart Groups
- LDAP Admin Integration

Known Issue

At this time, FileWave IDP integration is limited to only FileWave Admin authentication and Apple device enrollment. Directory data synchronization (and custom fields) between the IDP source and FileWave is not supported at this time, but will be added in a future release. In the meantime, current LDAP(S) synchronization can be used as a stop-gap to achieve the same result.

IdP Setup: Microsoft Entra ID (Azure)

What

Before we can use AzureAD for authentication from FileWave, we must create a new application in the Azure Portal and give FileWave access to it. The whole purpose of this configuration is to give FileWave permissions to talk to your Microsoft Entra ID environment.

When/Why

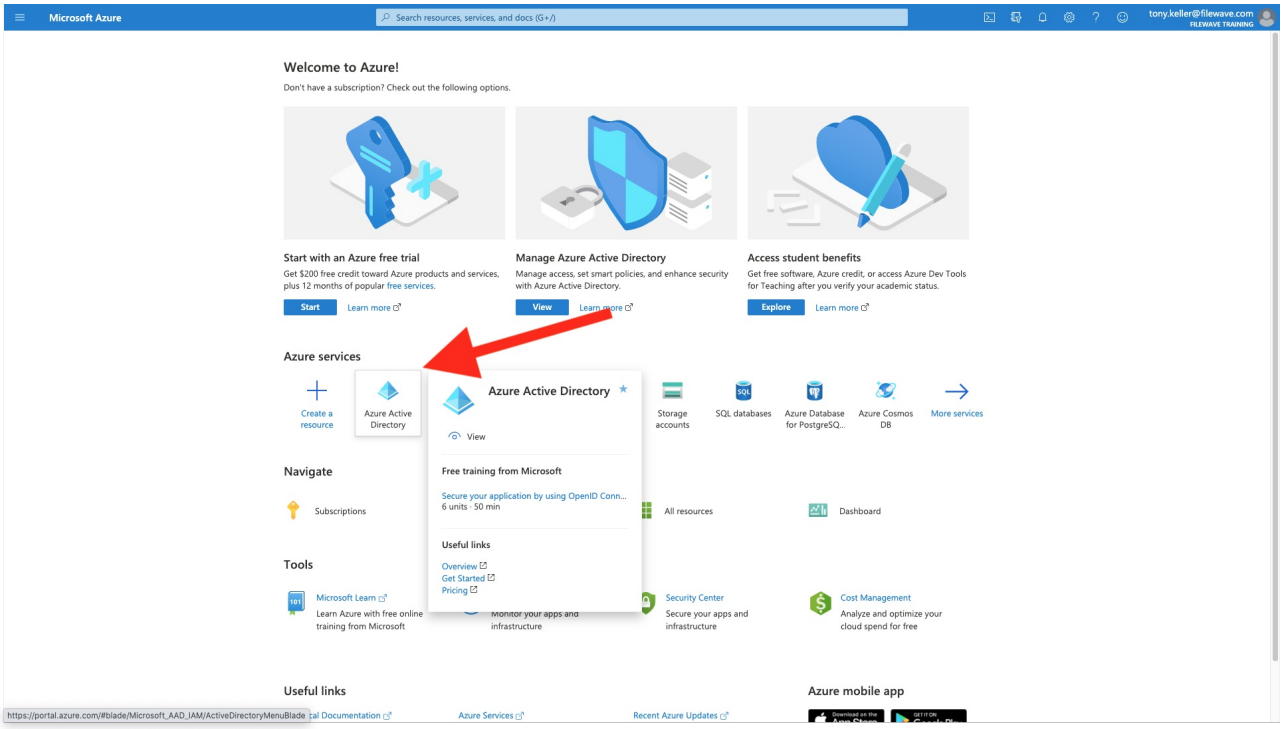
This configuration is required if you want to use AzureAD for authentication during device enrollment or during login to the FileWave Web and Native administrator consoles.

How

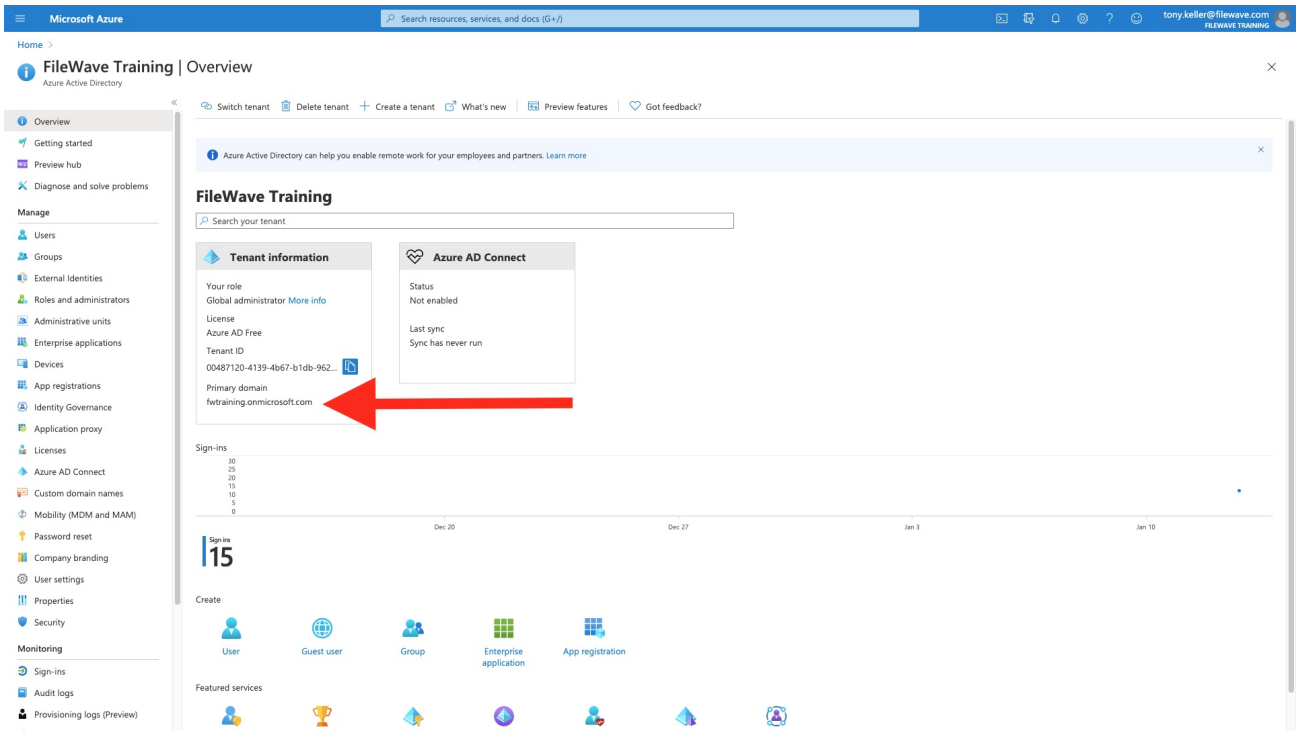
The configuration for access is all driven through an Microsoft Entra ID application, so we need to start with:

Part 1: Login to Microsoft Entra ID Portal

First, we'll login to Microsoft Entra ID at portal.azure.com with an administrator's account and click on Microsoft Entra ID as shown:



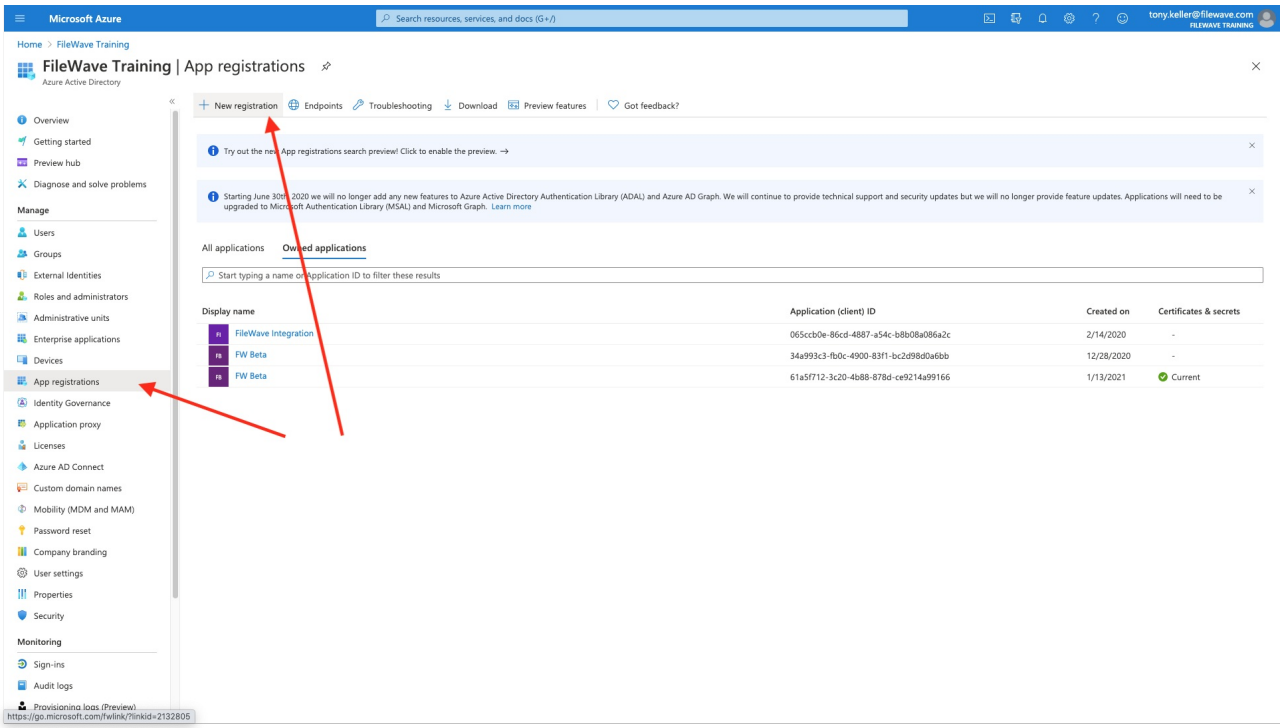
And make note of the domain info shown below:



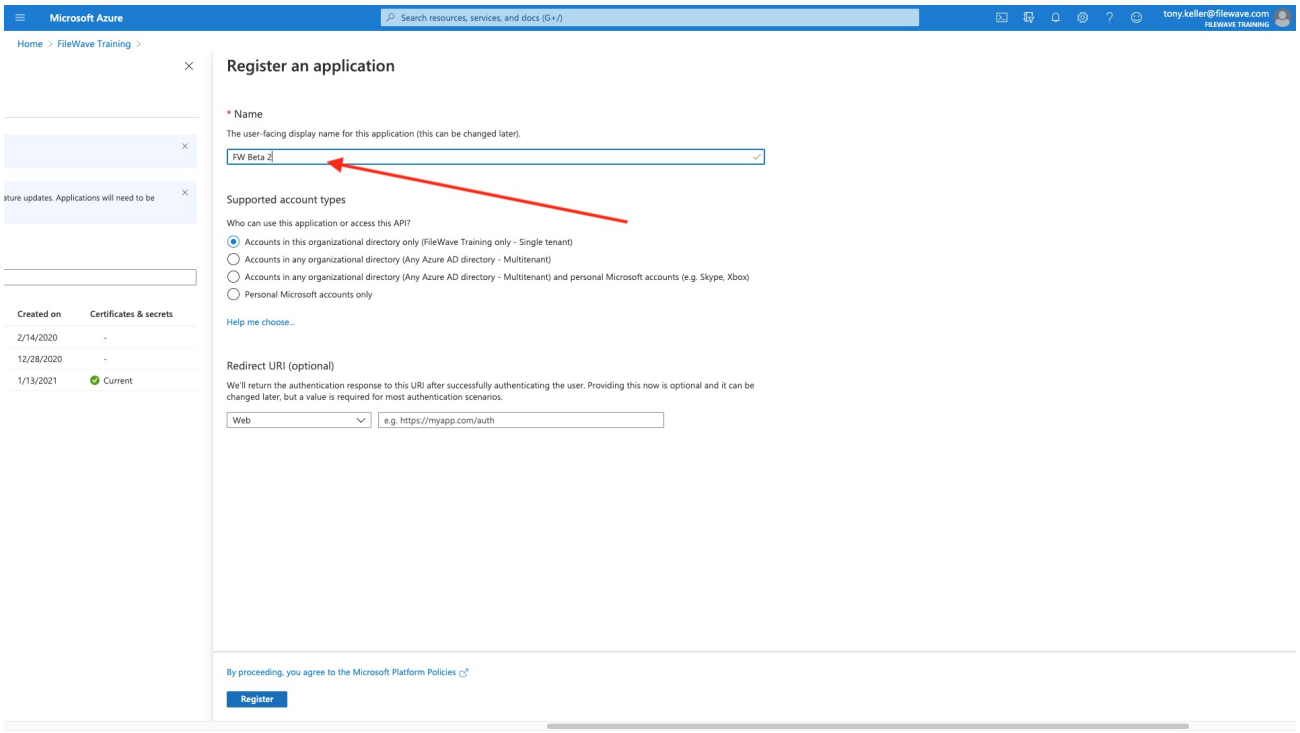
It is a good idea to take all of these elements and label/paste them into a document you store securely. Although we'll use them to configure FileWave, you can't access many of them from FileWave once they are stored.

Part 2: Create an App

Now we have to create an app for FileWave to talk to, and assign some right to it. First go to the app registrations menu, then click "new registration":

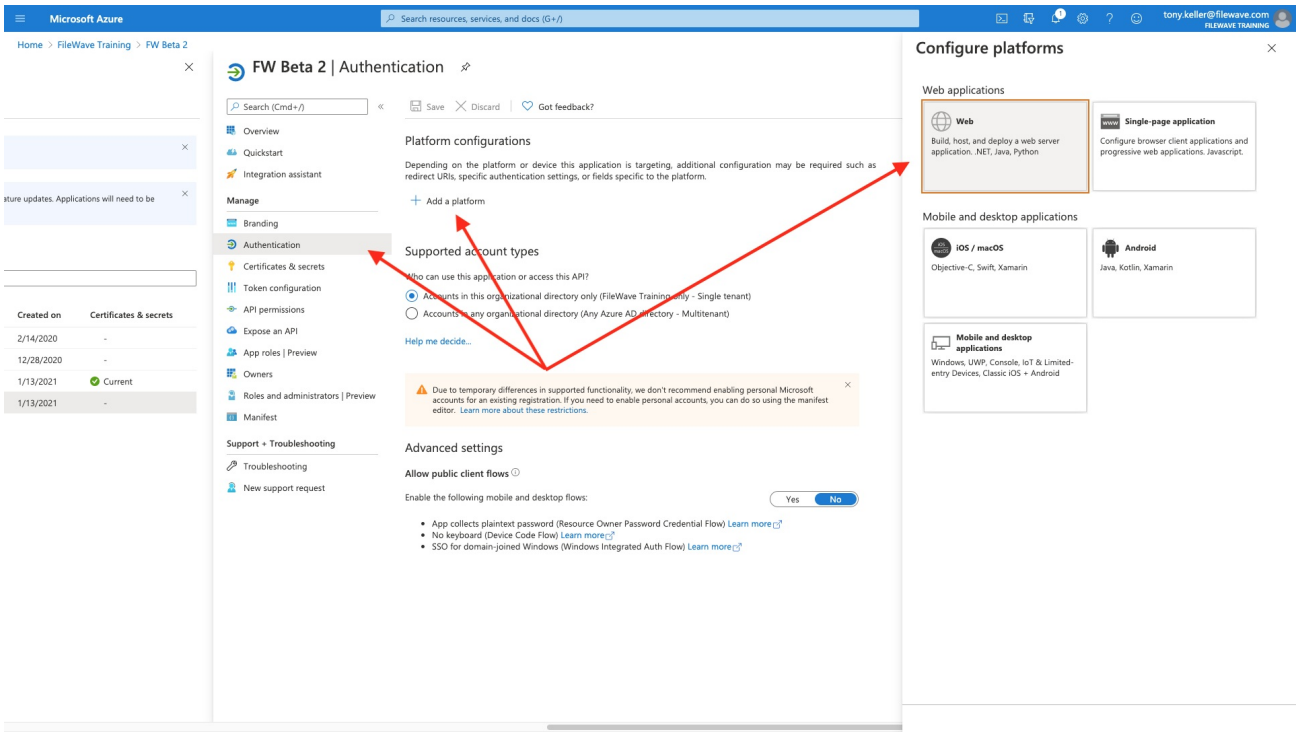


Specify a name for your app that is meaningful to you, and Register the app (we'll set the login URIs later).

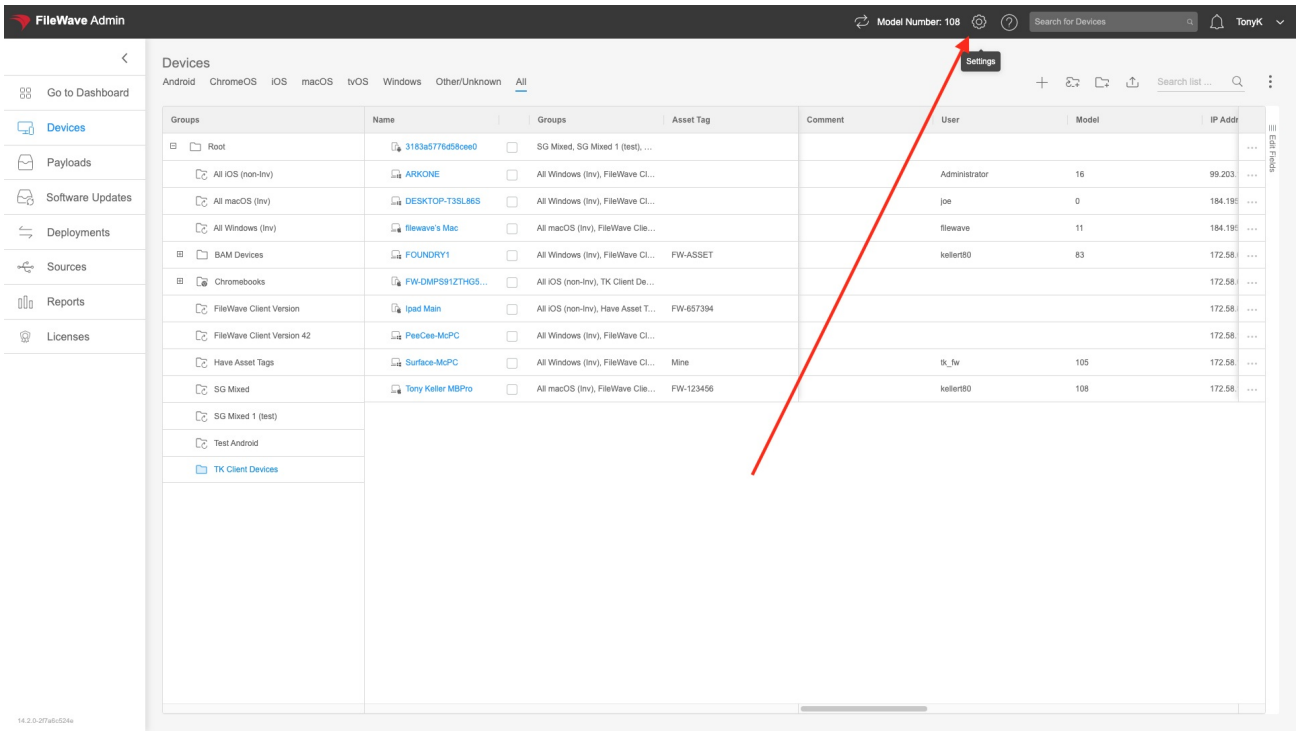


Part 3: Add a Platform and URI Addresses

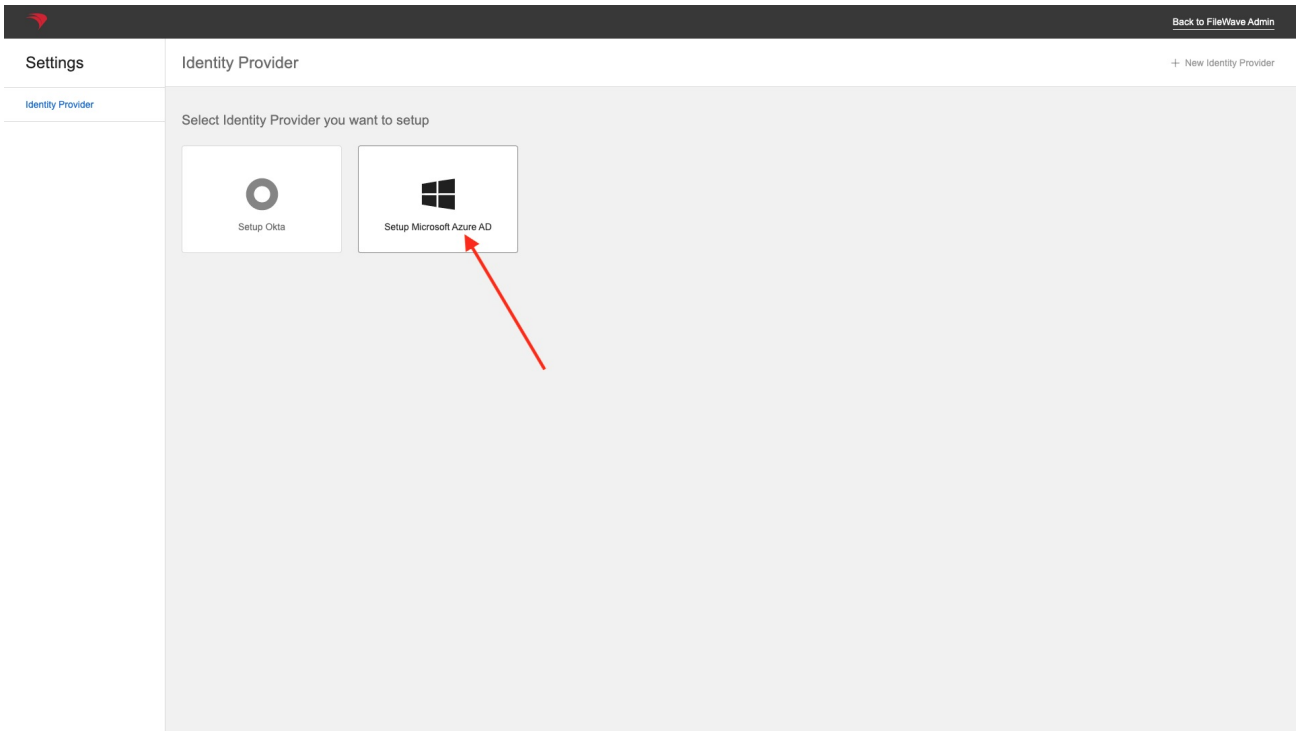
Within the app configuration, we'll choose Authentication, then Add a Platform, of type Web:



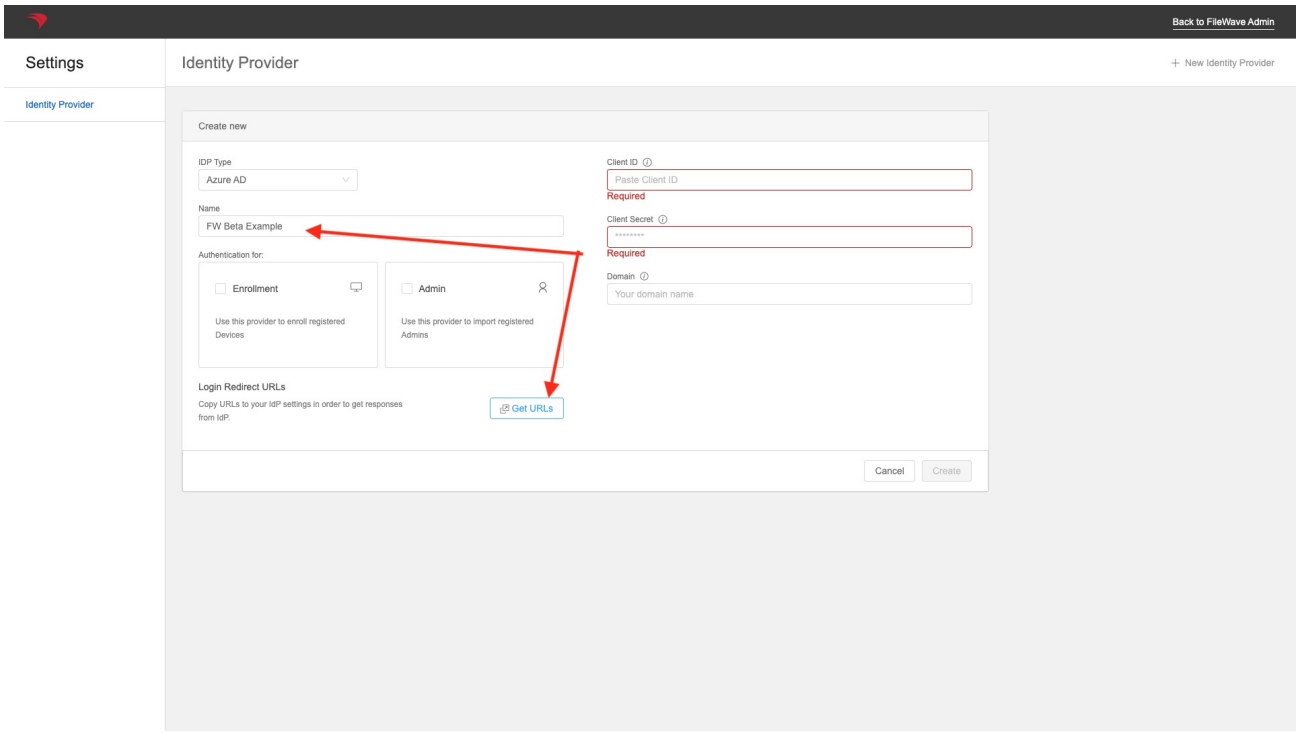
And for the web configuration, we'll need to copy some address from your FileWave server. You'll get them from the WebAdmin, Settings:, New AzureAD IDP, and then Get URLs as shown

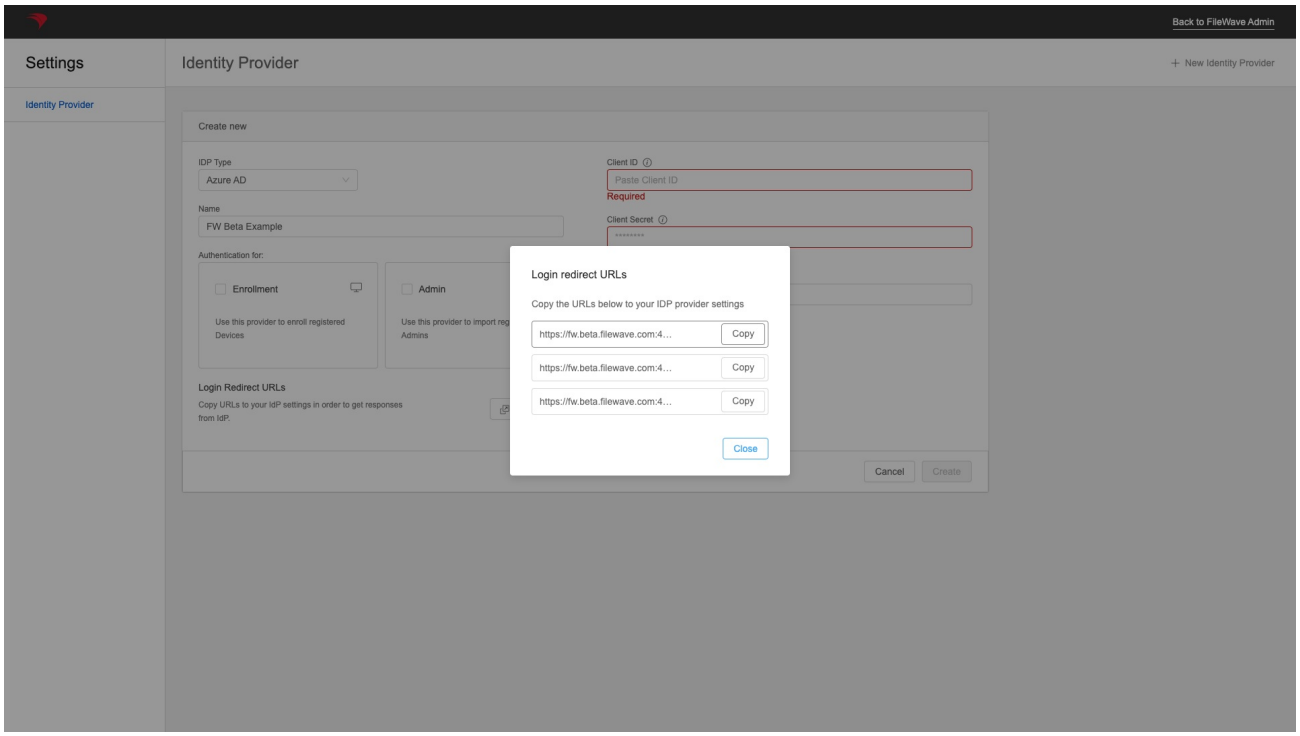


Then choose an Microsoft Entra ID IDP Provider

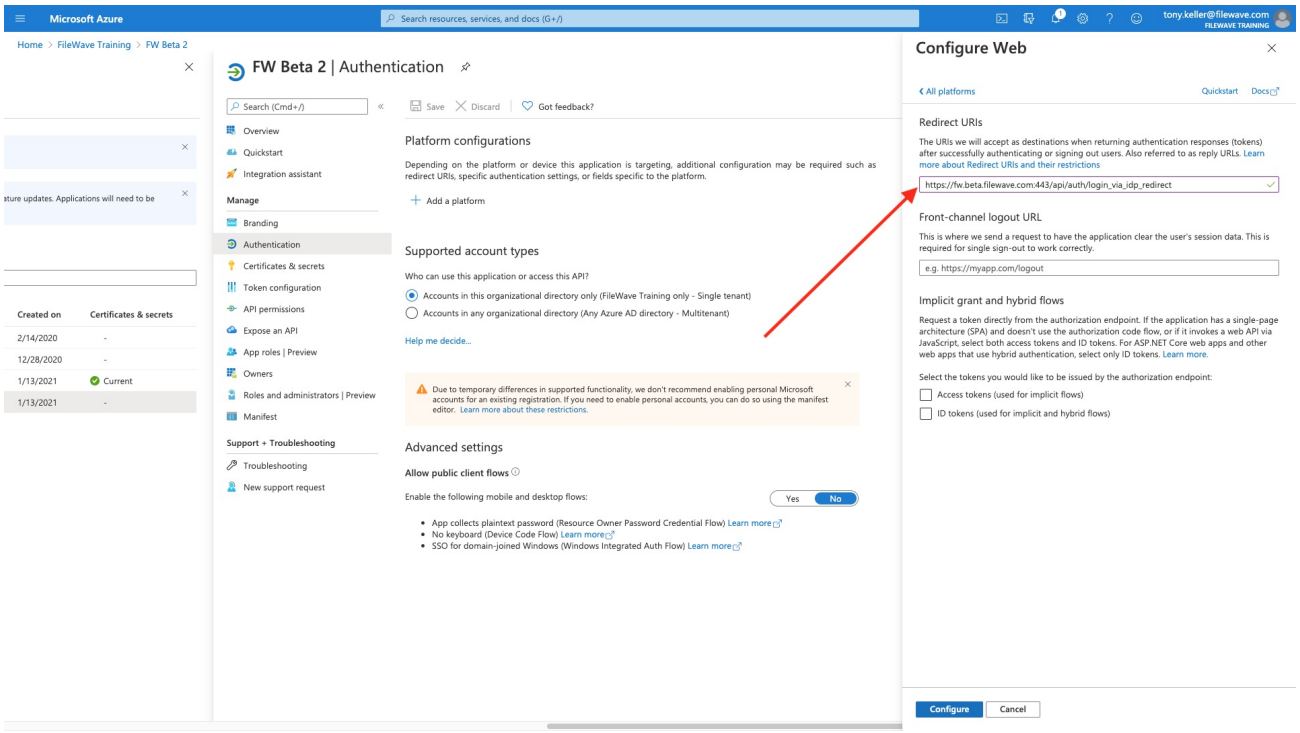


You can add a name now (or later), but you'll get the URLs from the "Get URLs" button:

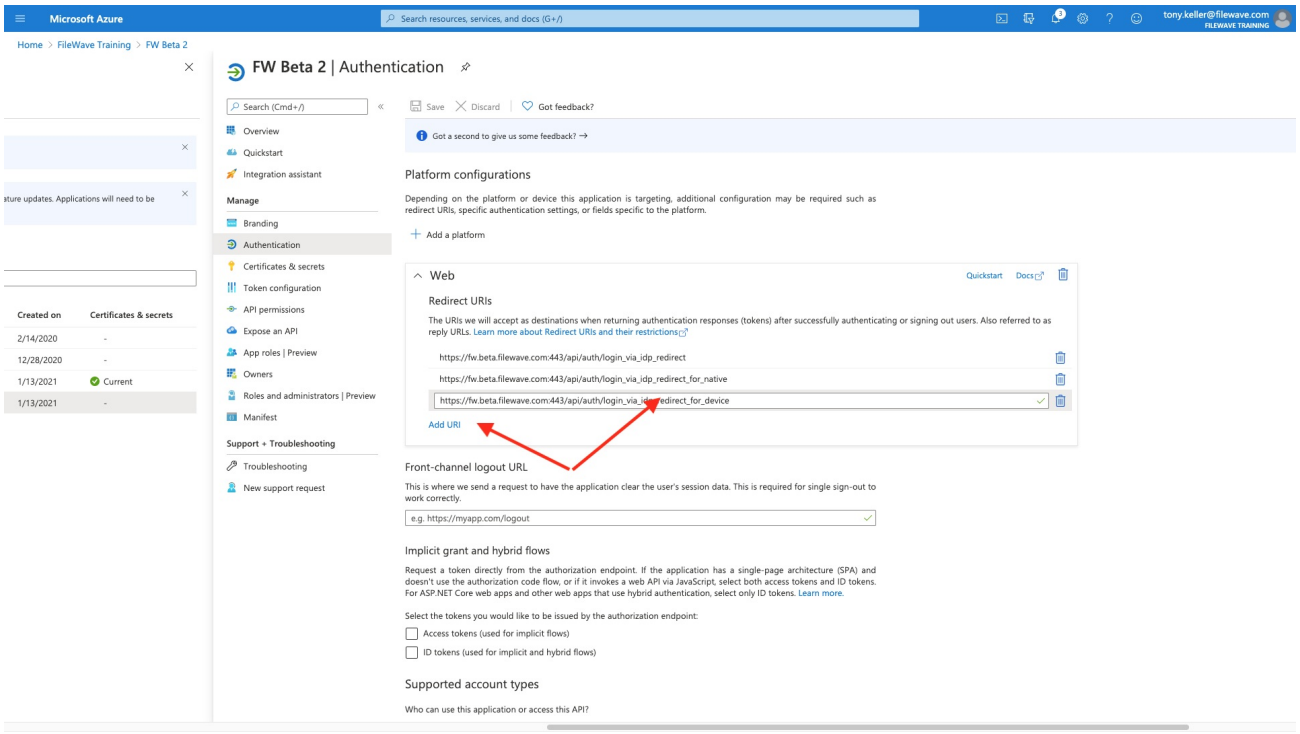




So now we'll enter one of the redirects, and click configure:



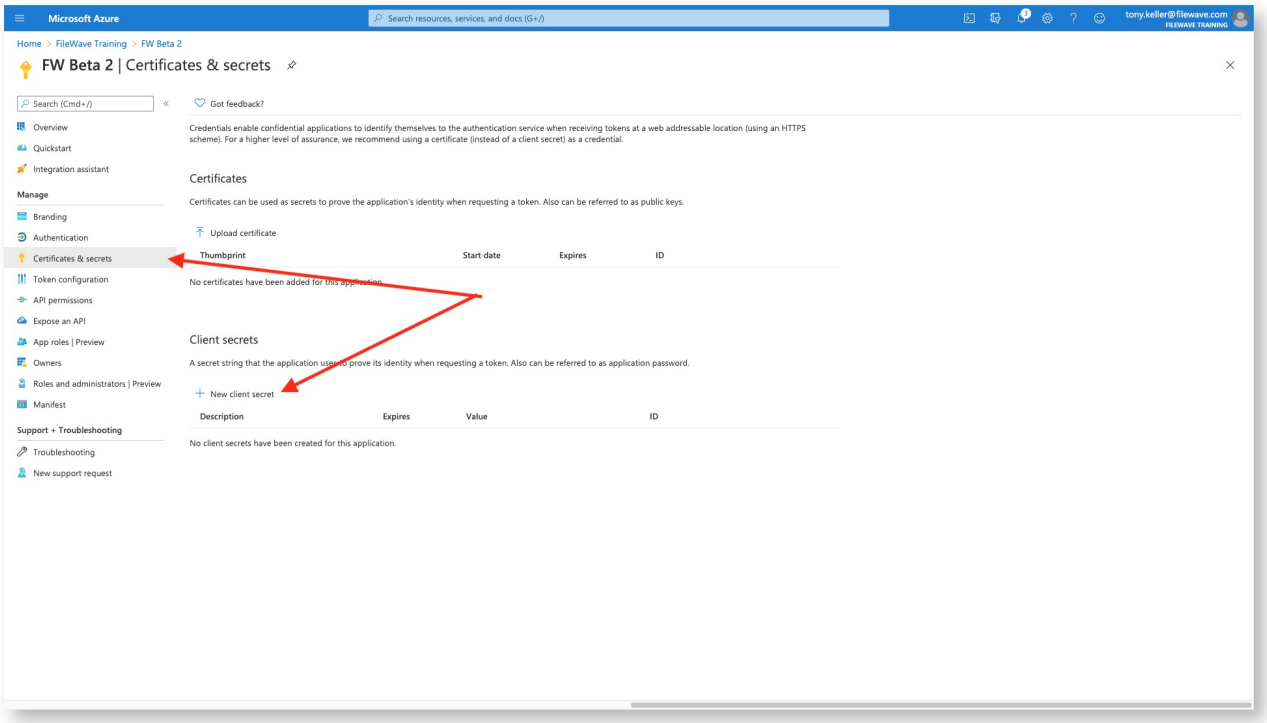
And then add the other two from here:



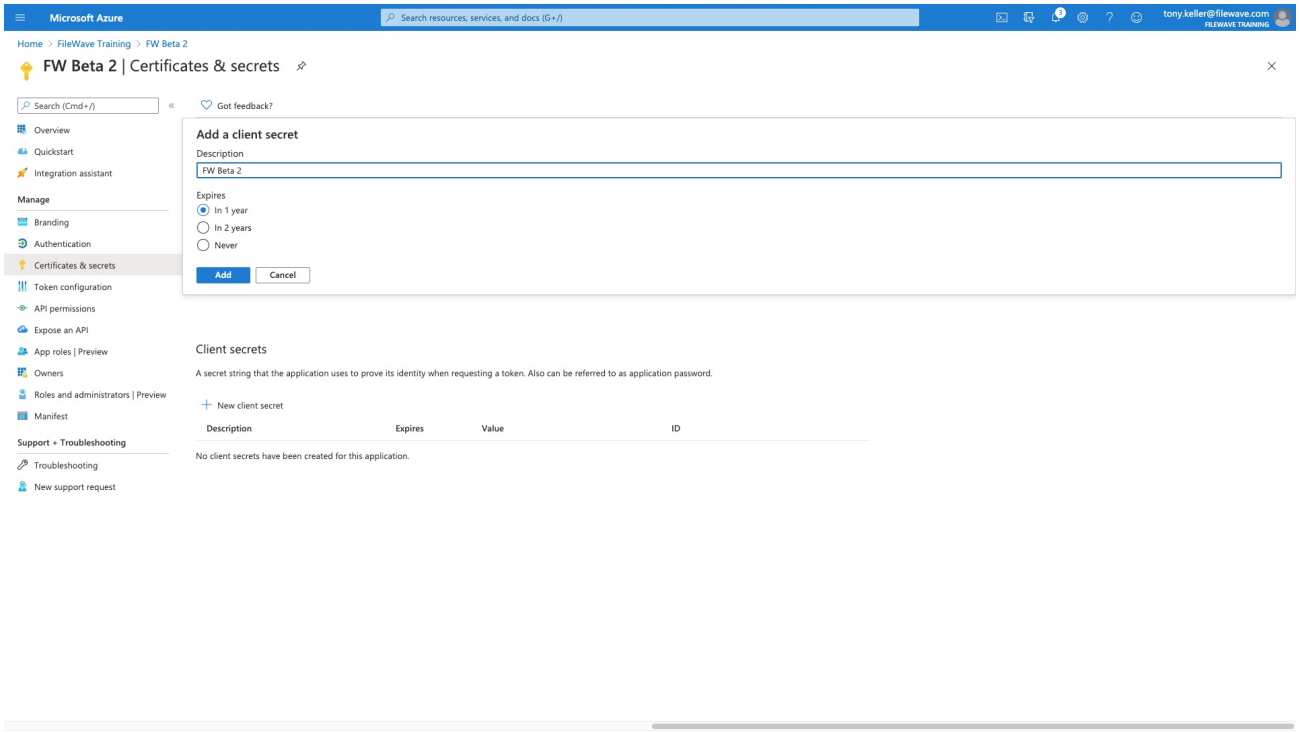
Make sure to hit Save at the top after you have entered all three.

Part 4: Cert & Secrets

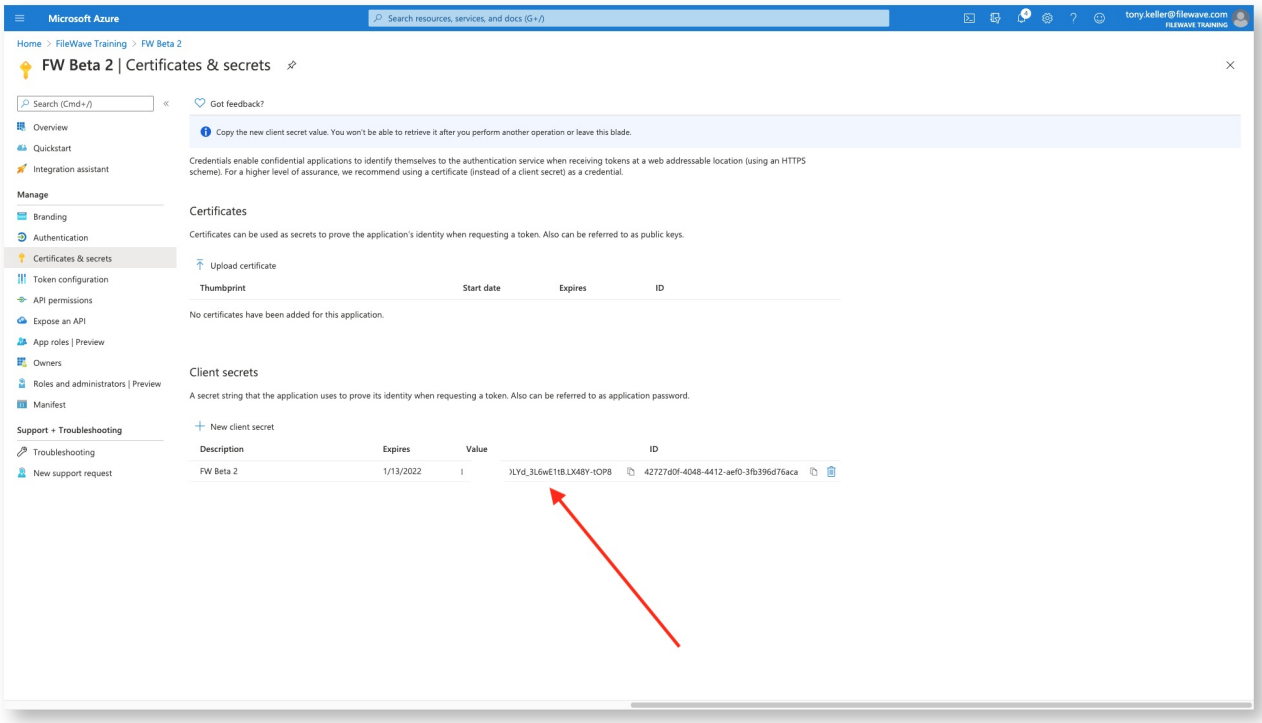
Now we are going to go to Certificates & Secrets to provide a way for FileWave to authentication to our new application. Click on New client secret



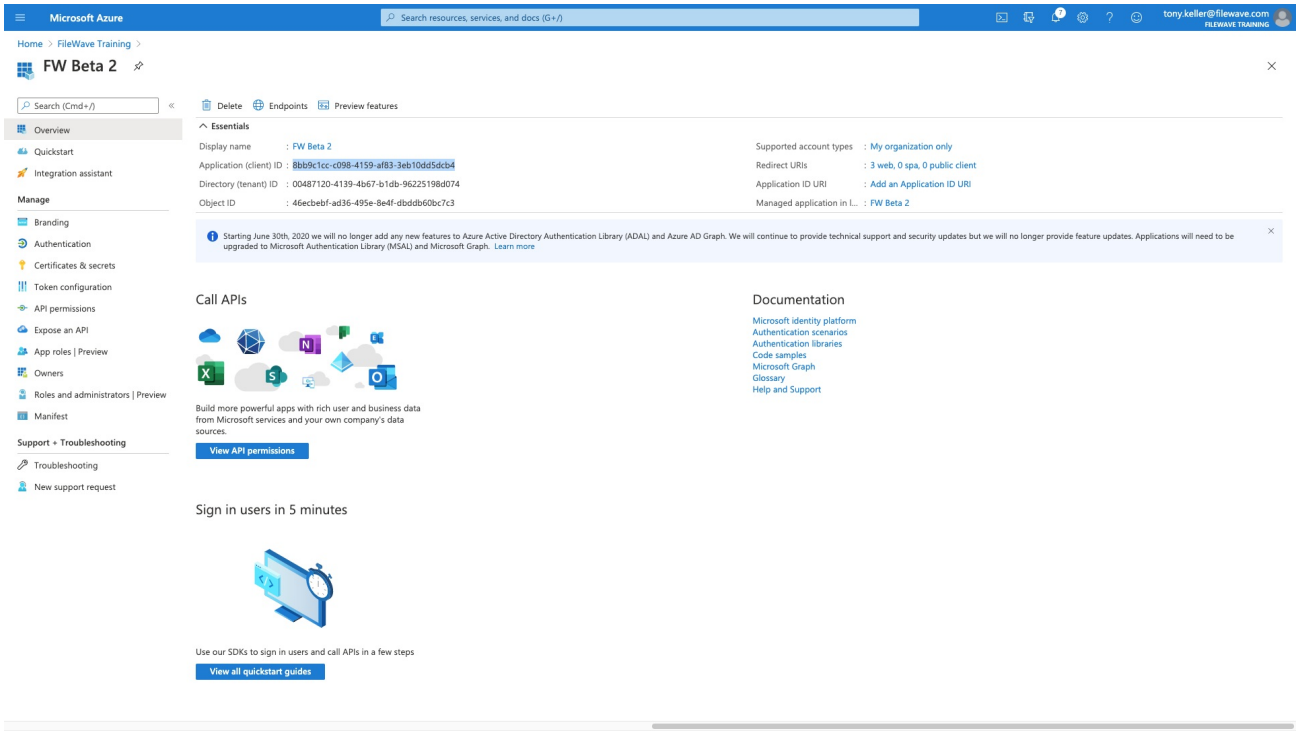
Then we give it a descriptive name:



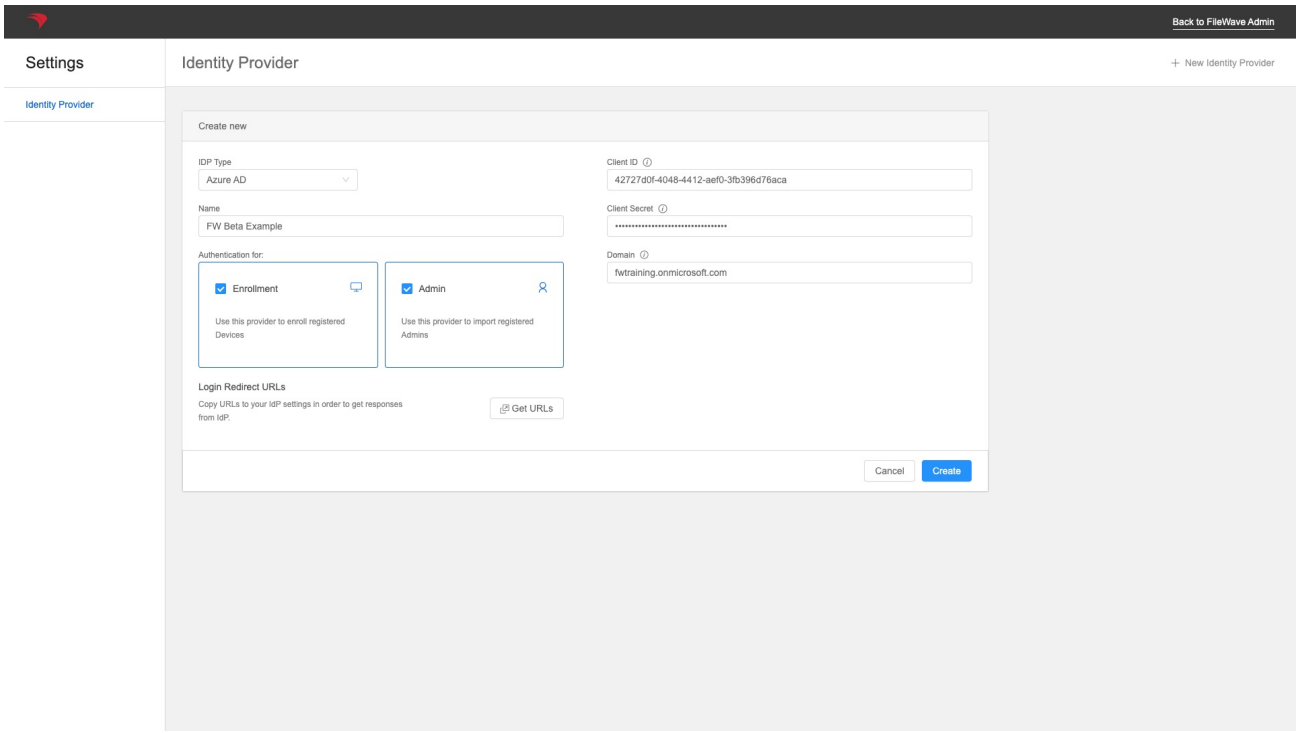
And then we'll want to get a copy of the Client Secret, and this is the ONLY time you can copy it. The one we need is under the 'Value' column.



Lastly, we get the The Client ID, you get from the overview page:



Each of the relevant values then gets copied into the FileWave config below:

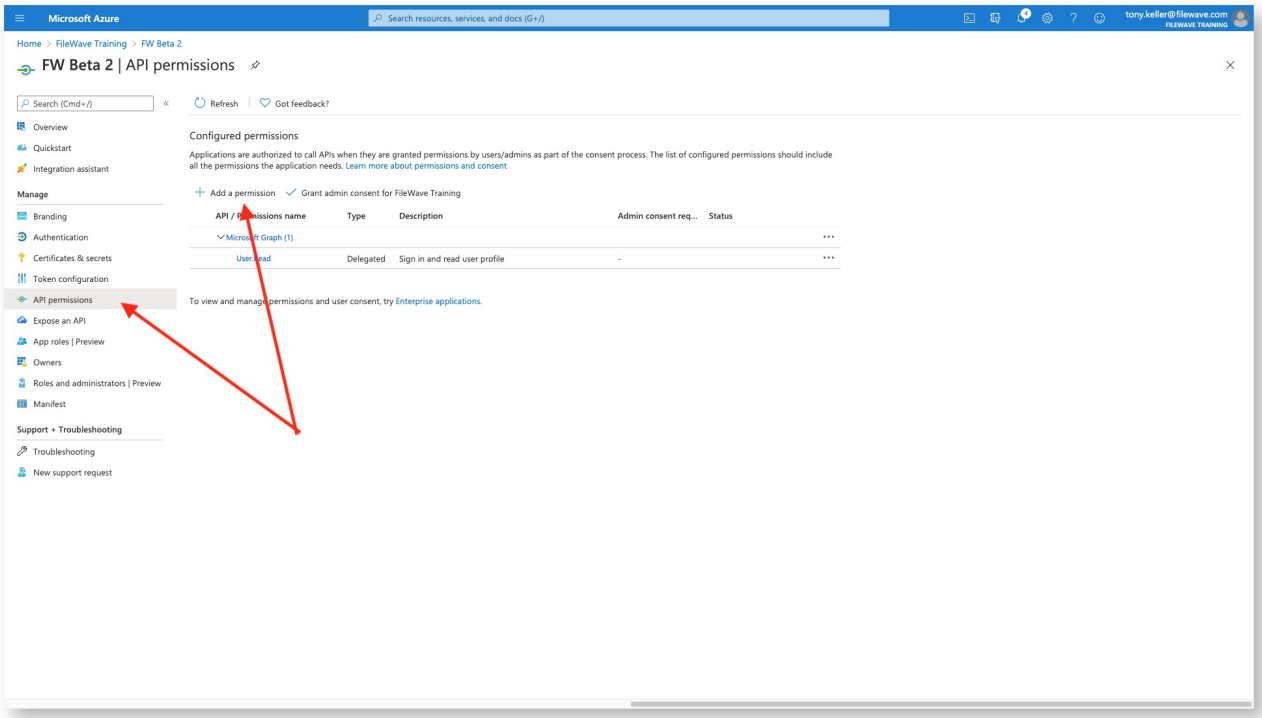


You'll check the checkbox for "Admin" if you want to be able to use AzureAD for login to the FileWave admin with AzureAD, and "Enrollment" if you want to use it for Apple device enrollment authentication. Note that multiple IDPs can be used for admin login, but only one for device enrollment.

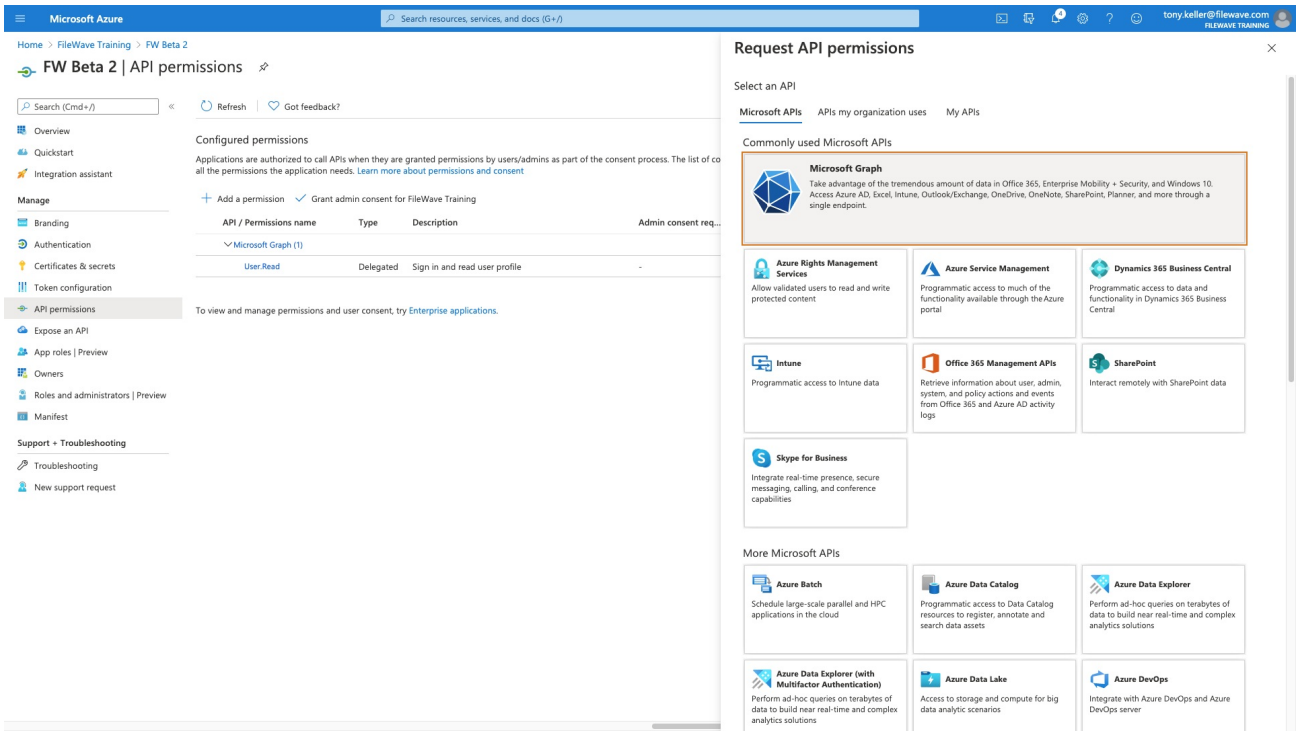
Part 5: App Permissions

Now we have to give our app permissions to read the directory so that it can pull group information into FileWave for browsing and rights assignment.

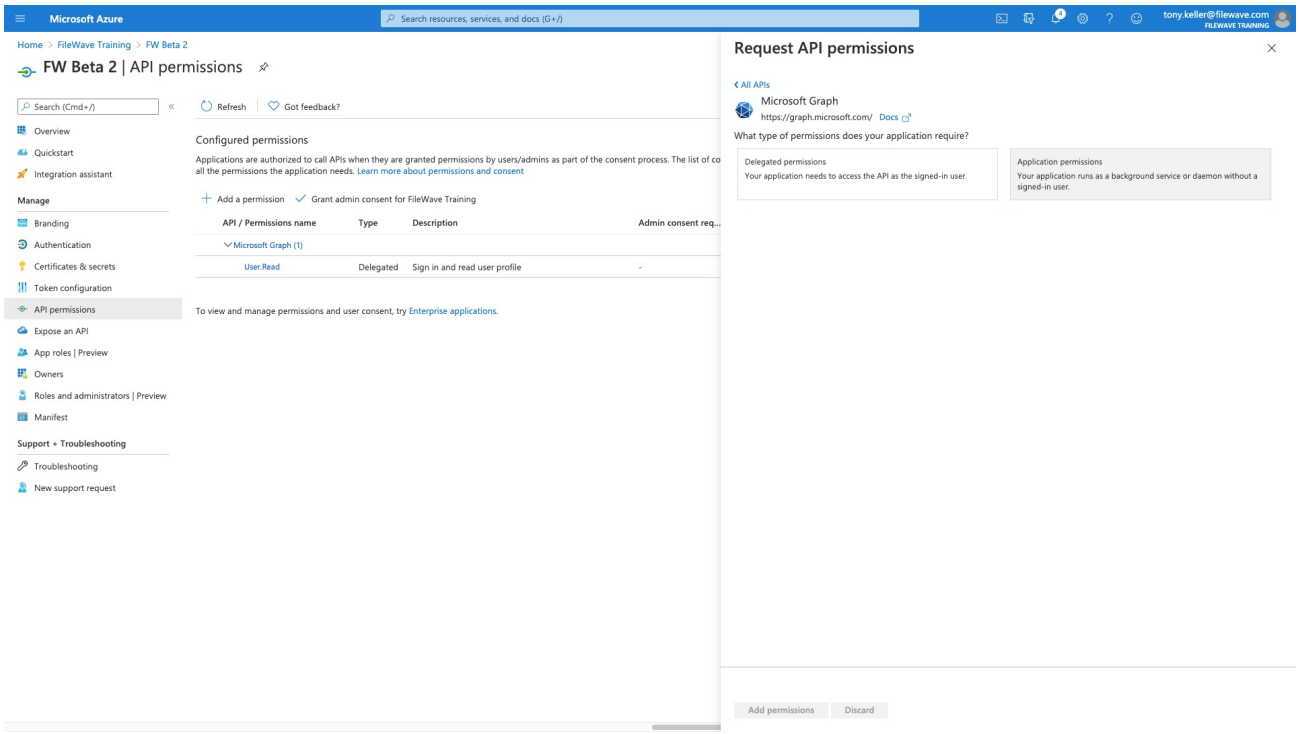
So, we'll go to the App Permissions section and start Adding Permissions



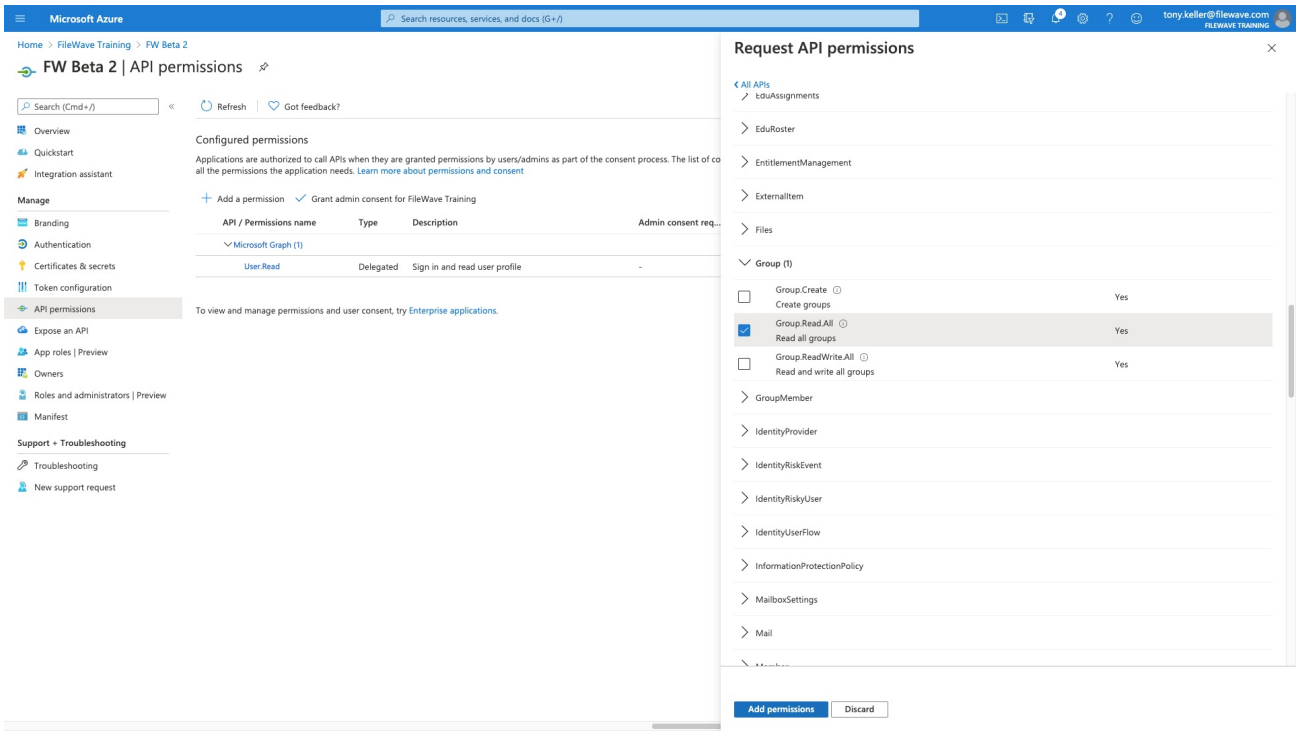
Our permissions are going to be for Microsoft Graph



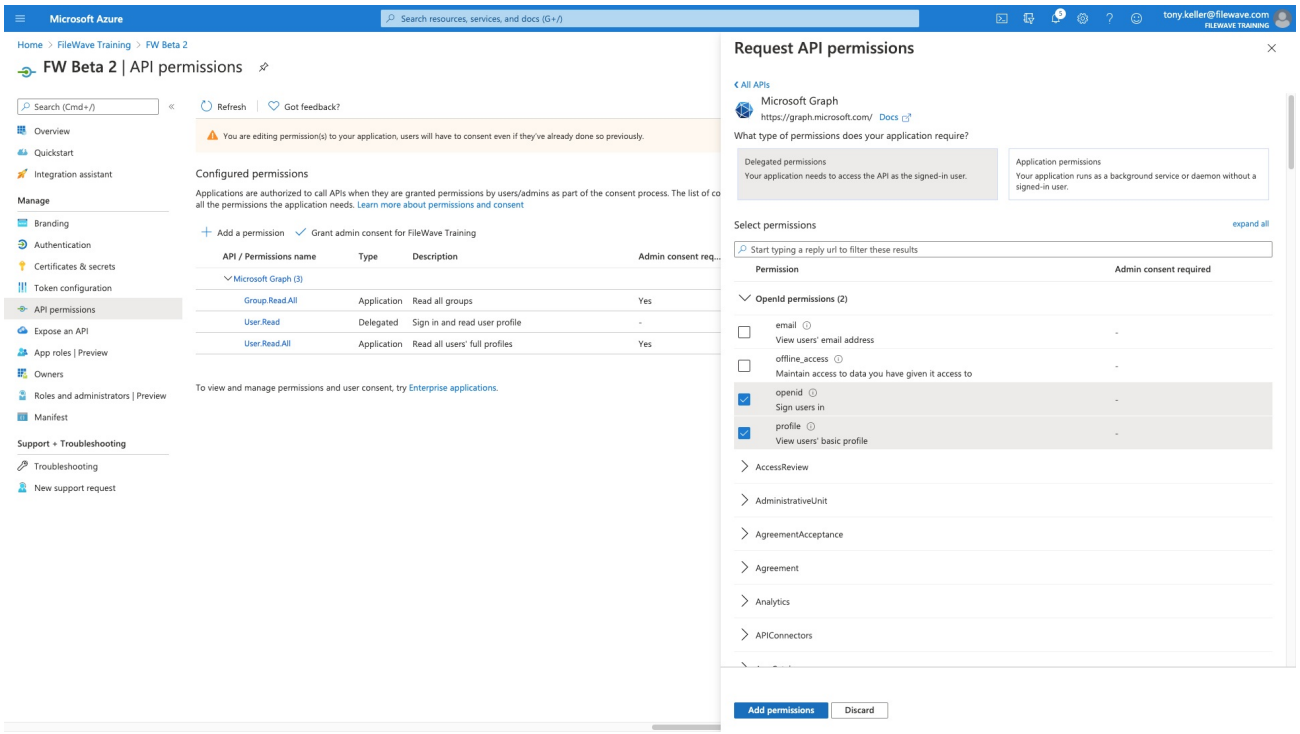
We'll start with an application permission:



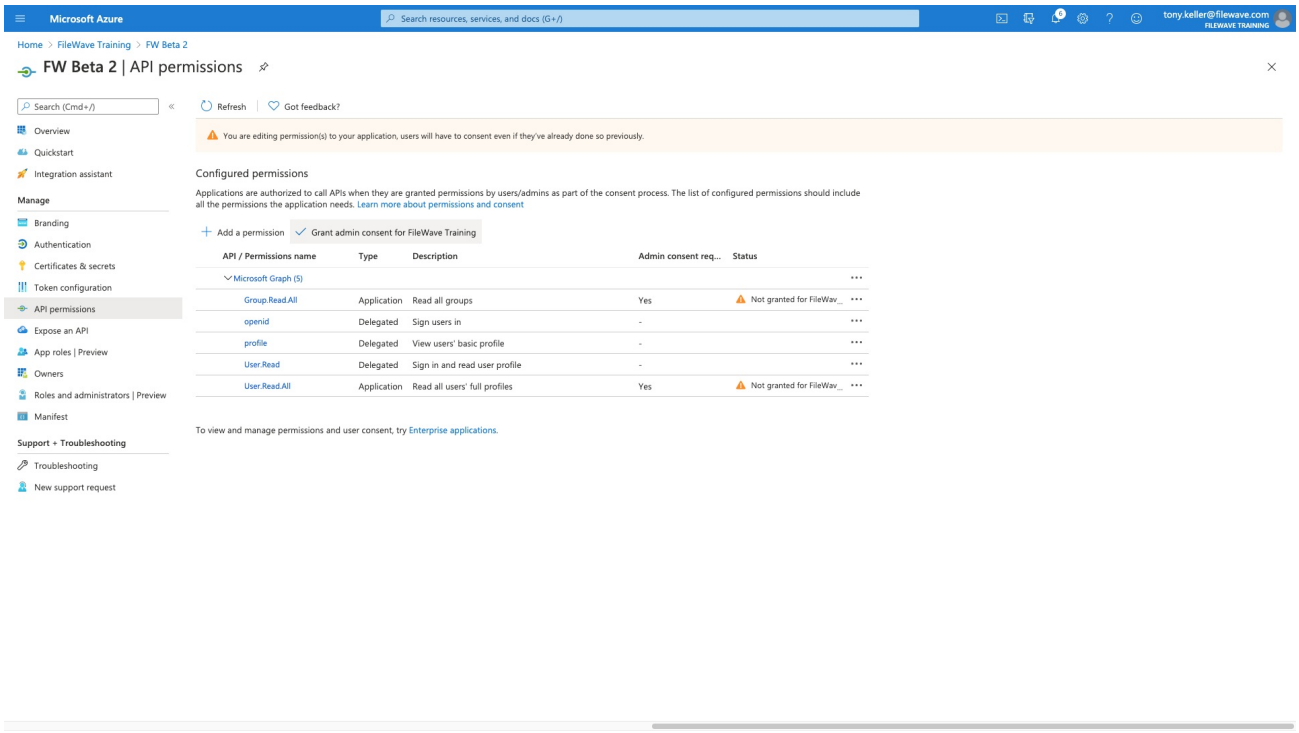
For Group Read All AND User Read All (not shown, but you can pick two at once):



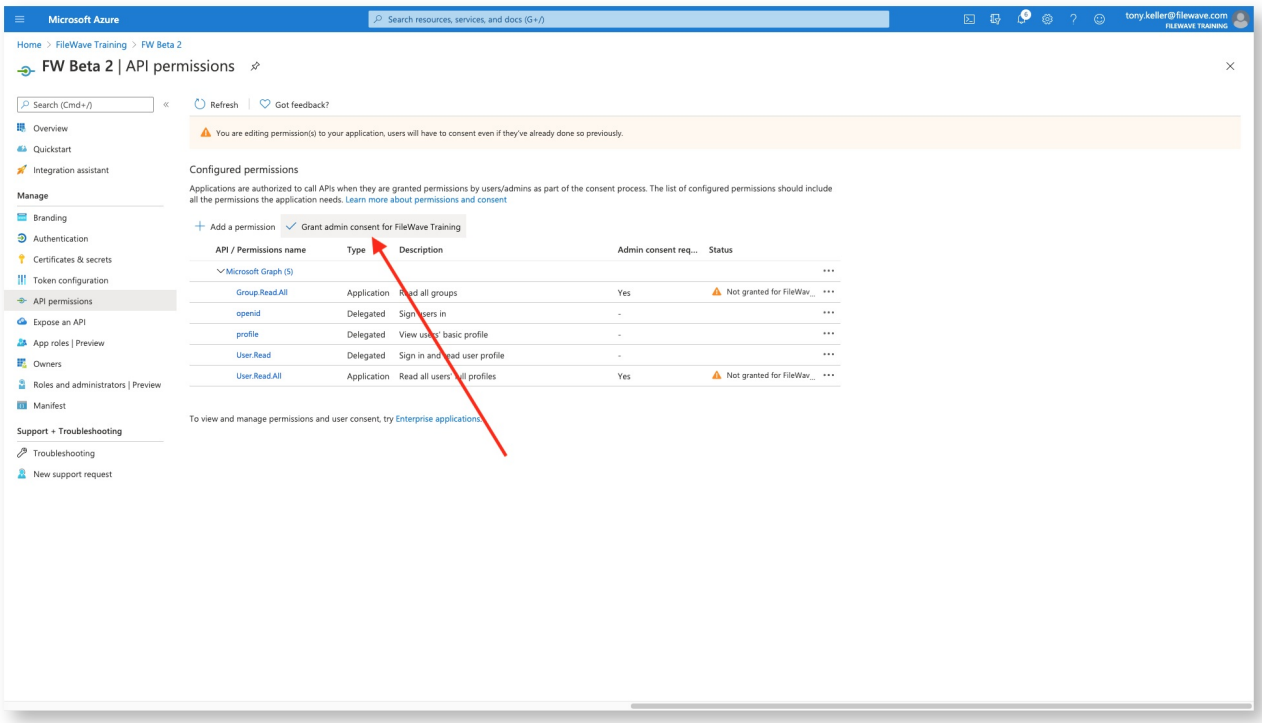
Then we'll add more permissions, but "delegated permissions" for open id and profile as shown:



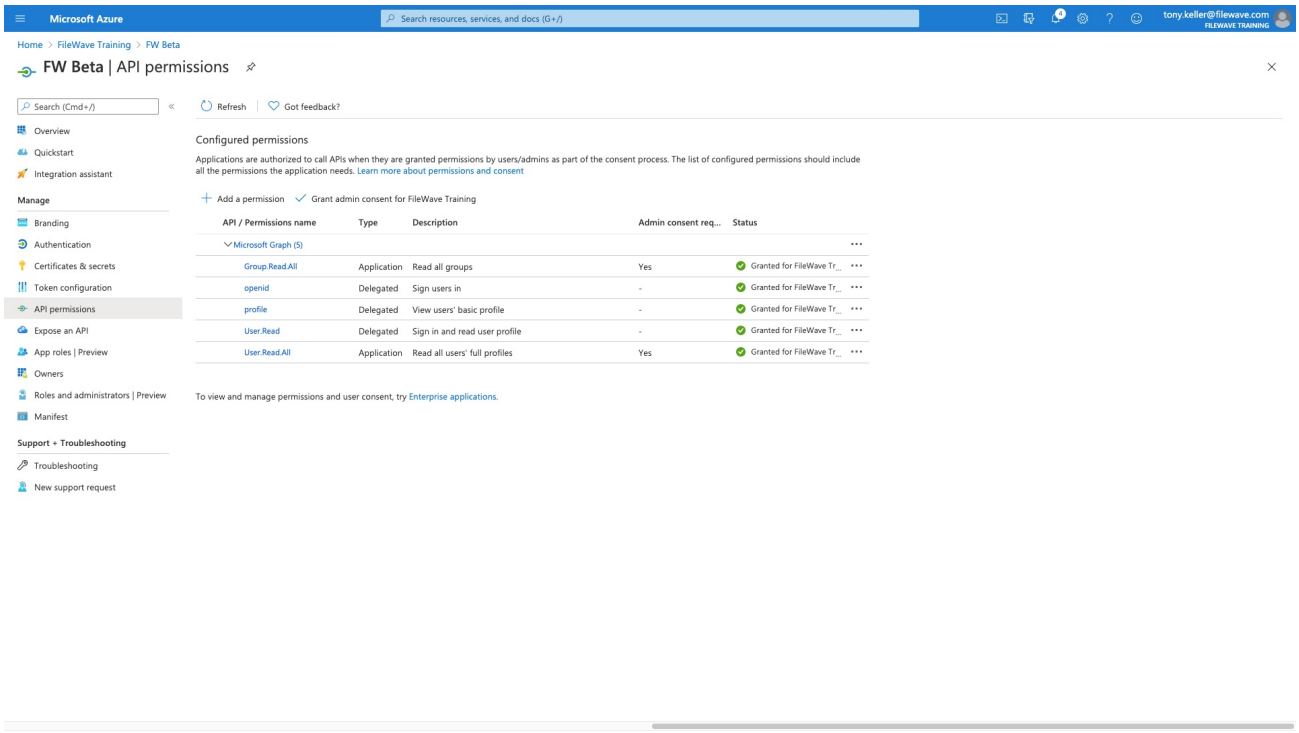
Our permissions then should look like this when we have them all



And then we just need to click Grant Consent to finish with the permissions



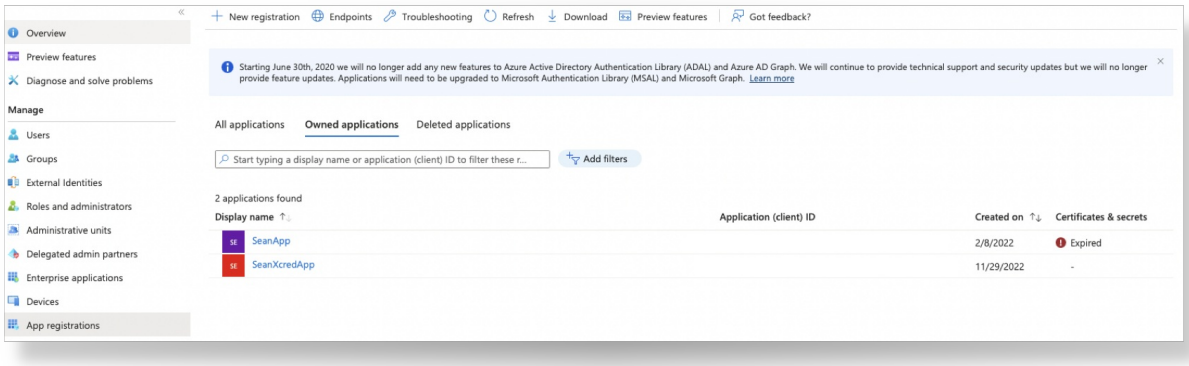
When they show as green, we are all done!



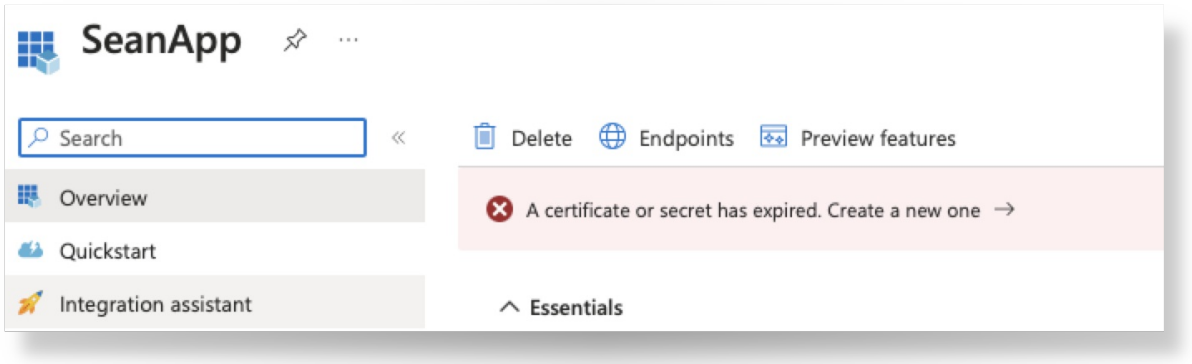
Part 6: App Registration Renewal

At some point the Certificate of the App will expire and a new certificate should be generated. The maximum you can set before expiry is 2 years.

From the App Registration view, expired certificates may be observed



For renewal, click on the Display Name of the App, followed by 'Create a new one ->'



Then generate a 'New client secret' similar to part 4 of this KB.

- Add a description
- Copy the secret from the 'Value' column, not the 'Secret ID'. Be sure to copy it just after creating your new secret, otherwise it will appear obfuscated the next time you attempt to view it.

This time though, you will only need to ddit the current IdP in FileWave Anywhere:

- Open Settings in the FileWave Admin
- Choose Edit from the selected IdP
- Paste in the new secret value and 'Save'

> The old, expired certificate may be deleted from within the Azure portal.

Related Content

- Adding IdP Groups for FileWave Authentication
- Configuring DEP Profiles for IDP Authentication
- Admin Login in Using an IdP Provider

IdP Setup: Okta

What

Starting with FileWave Version 14.2.0, we can use Okta for authentication from FileWave. We must create a new application in the Okta Portal and give FileWave access to it.

When/Why

This configuration is required if you want to use Okta for authentication during device enrollment or during login to the FileWave Web and Native administrator consoles.

How

> ⚠ Okta Admin UI
> The UI may look different depending on if you are using a Trial Okta organization or the regular, non-Trial version of the Okta.

Part 1: Login to the Okta Admin Portal

Okta Admin Portal

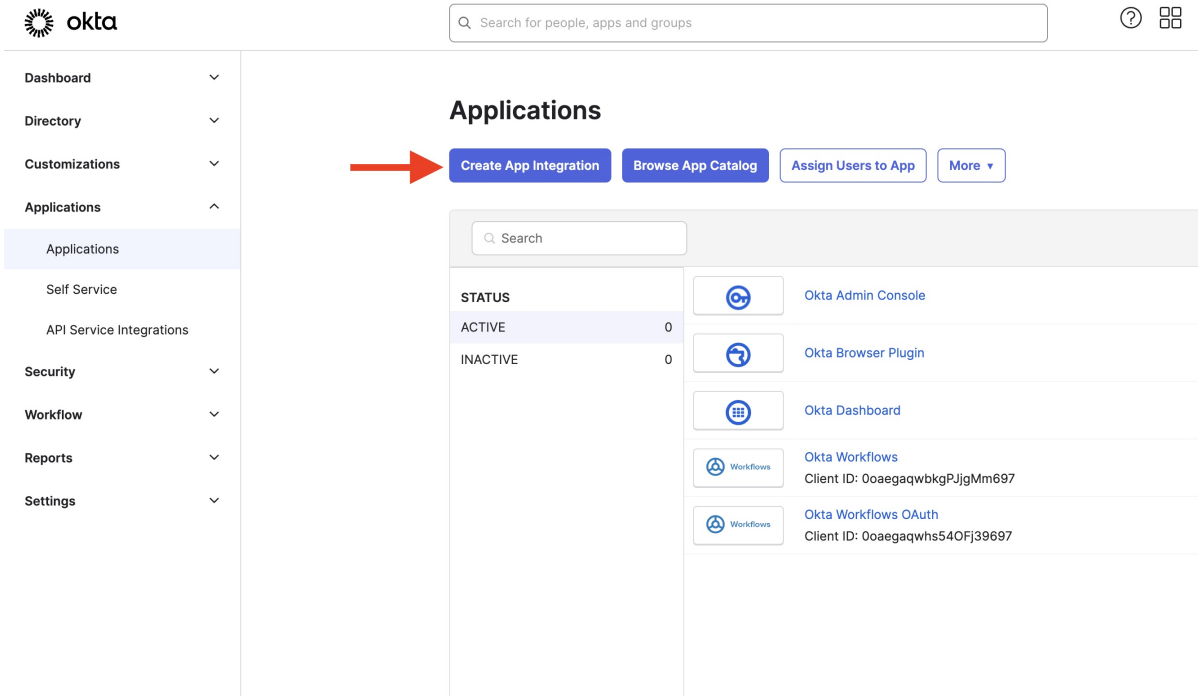
Begin by logging in to the Okta Admin Portal with an administrator's account. (https://example-admin.okta.com/admin)

Part 2: Create an Okta Application in the Okta Admin Portal

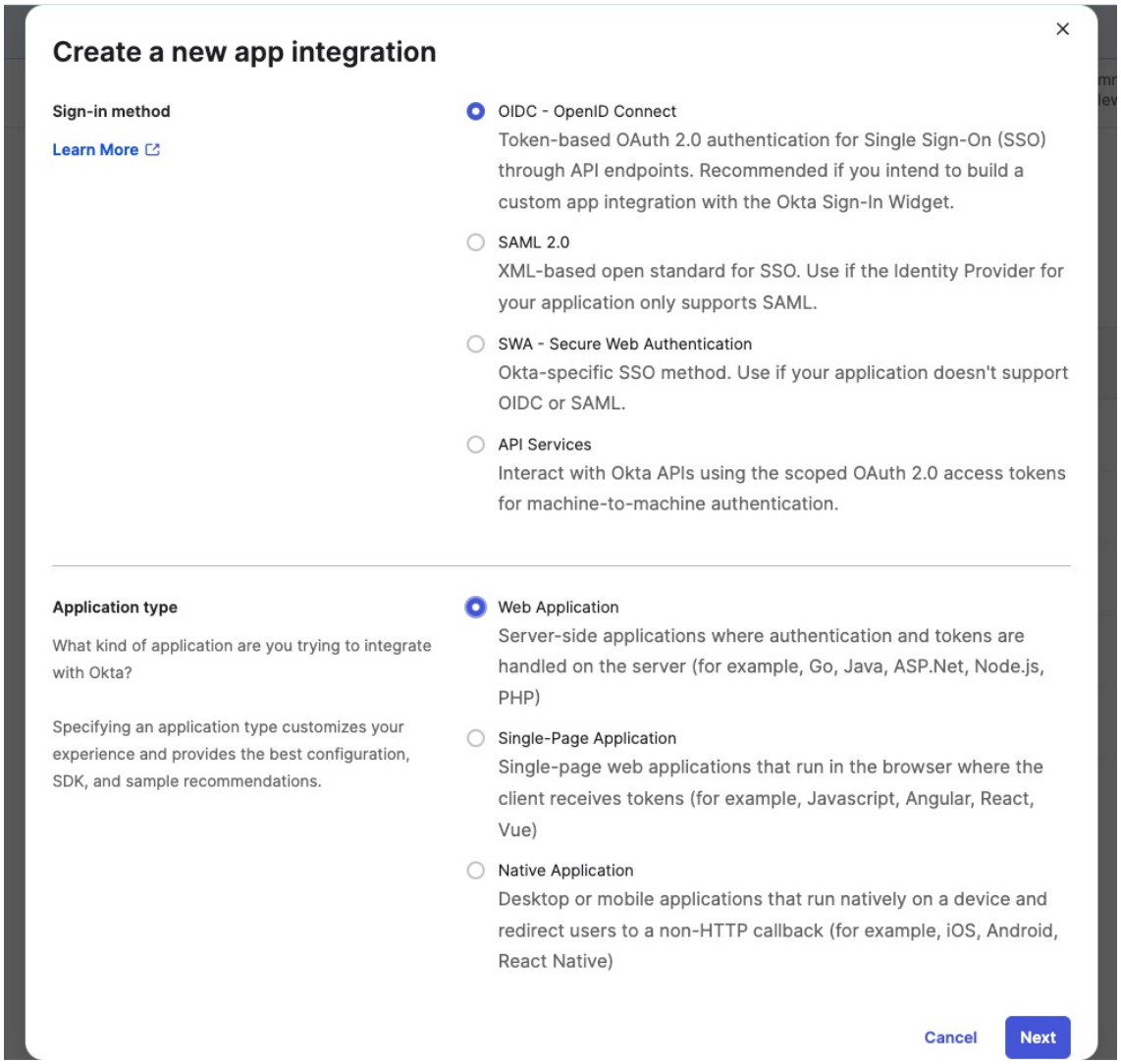
Create an Okta Application Integration in Okta Admin Portal

Now we are going to create an Okta application for FileWave to talk to and assign some rights to it.

1. First, open the Okta Admin > Menu > Applications > Applications menu and click the Create App Integration button.



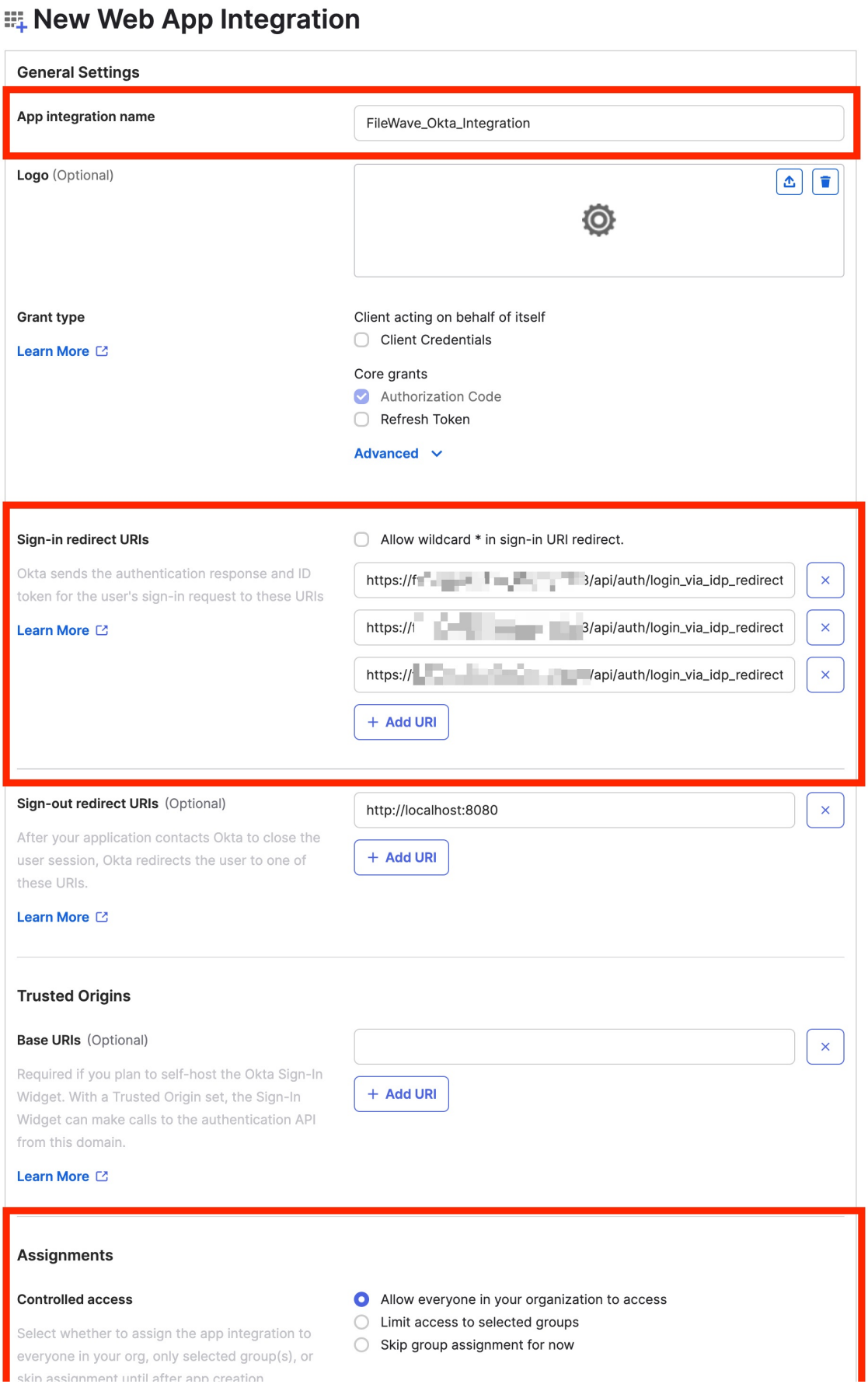
2. Next, select OIDC - OpenID Connect for the Sign-in method.
   1. Select Web Application for the Application Type.
   2. Click the Next button.



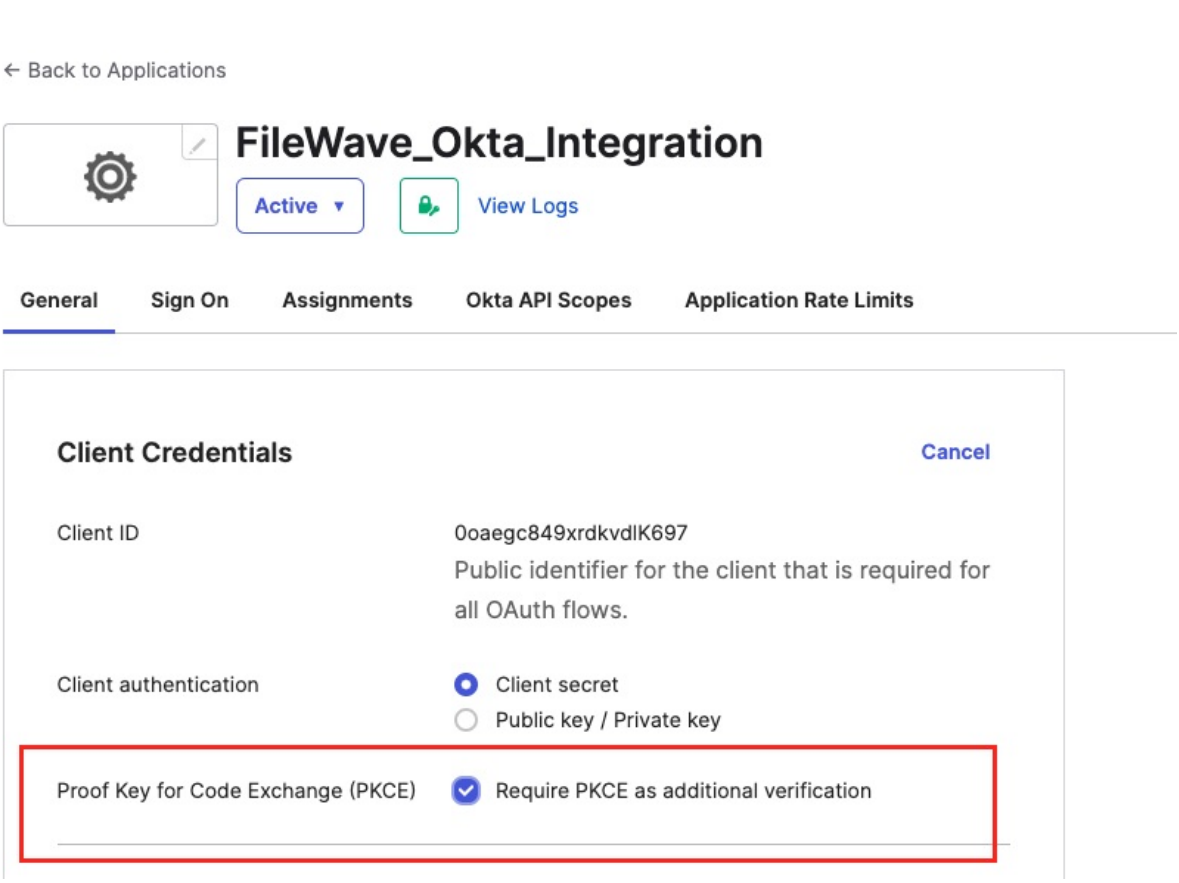
3. Next, configure your Application on the New Web App Integration page you've been redirected to.
    1. Input a meaningful name in the App integration name field.
    2. Click the Add URI button for the Sign-in redirect URIs setting.
        1. Input all of your FileWave Server's redirect URIs in the Sign-in redirect URIs setting.

> Login Redirect URIs for FileWave are displayed in the FileWave Web Admin Settings. (Login to Web Admin > Select "⚙' [Gear/Settings Icon] in top right > Identity Provider > Setup Okta > Get URLs)
>
> Login Redirect URIs are unique to your server, but will look something like the following:
>
> https://fwxserver.example.com:443/api/auth/login_via_idp_redirect
> https://fwxserver.example.com:443/api/auth/login_via_idp_redirect_for_native
> https://fwxserver.example.com:20443/api/auth/login_via_idp_redirect_for_device

    3. Under Assignments, choose whether you want to limit access to specific groups or integrate all users in the organization.
4. Click the Save button to create the Okta App integration.



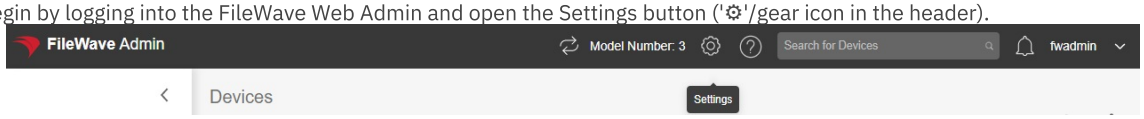
5. After Saving, you'll be Redirected to the application General Settings page. Next to Client Credentials, select Edit and check the box next to Proof Key for Code Exchange (PKCE) and Save.

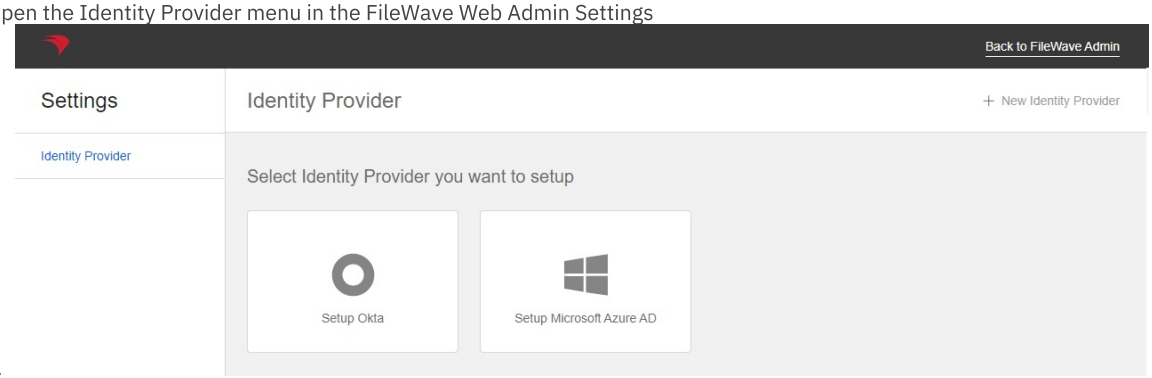


Part 3: Configure the Okta App in FileWave

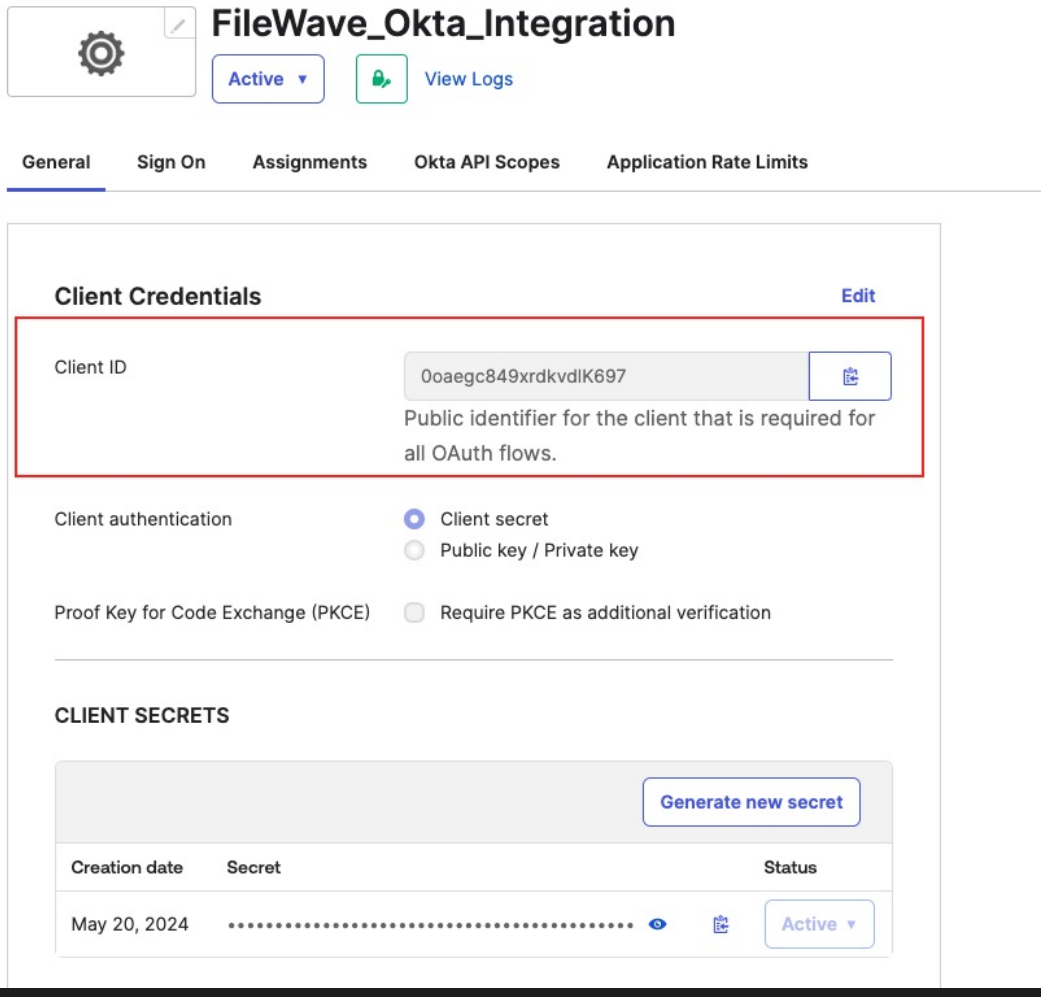
Configure an Okta App in the FileWave Web Admin Console

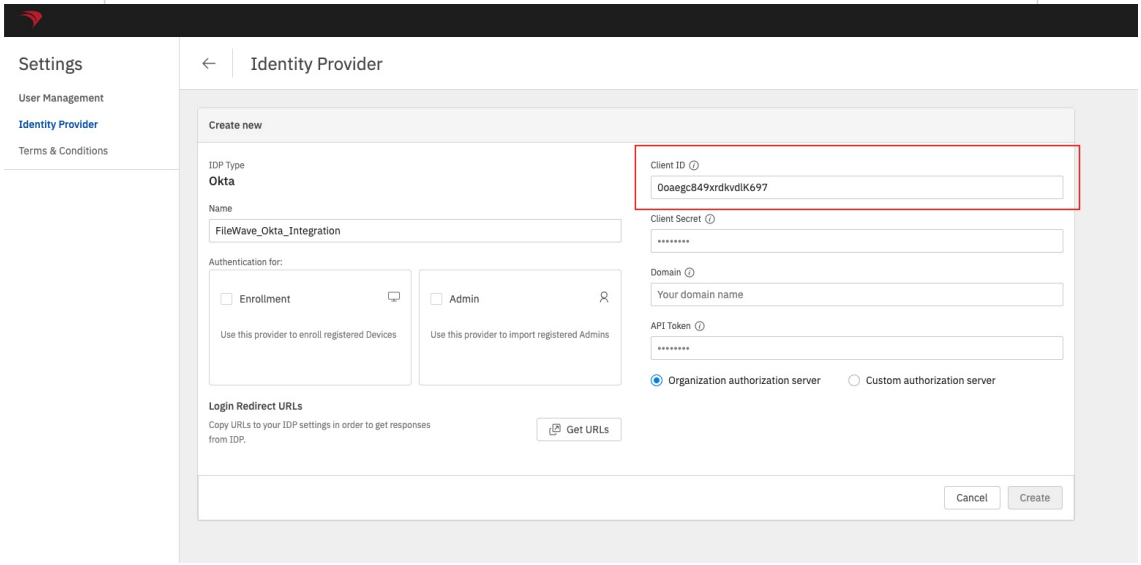
In order for FileWave to communicate with Okta for authentication the Okta App will need to be configured with FileWave.

1. Begin by logging into the FileWave Web Admin and open the Settings button ('⚙'/gear icon in the header).
    1. 

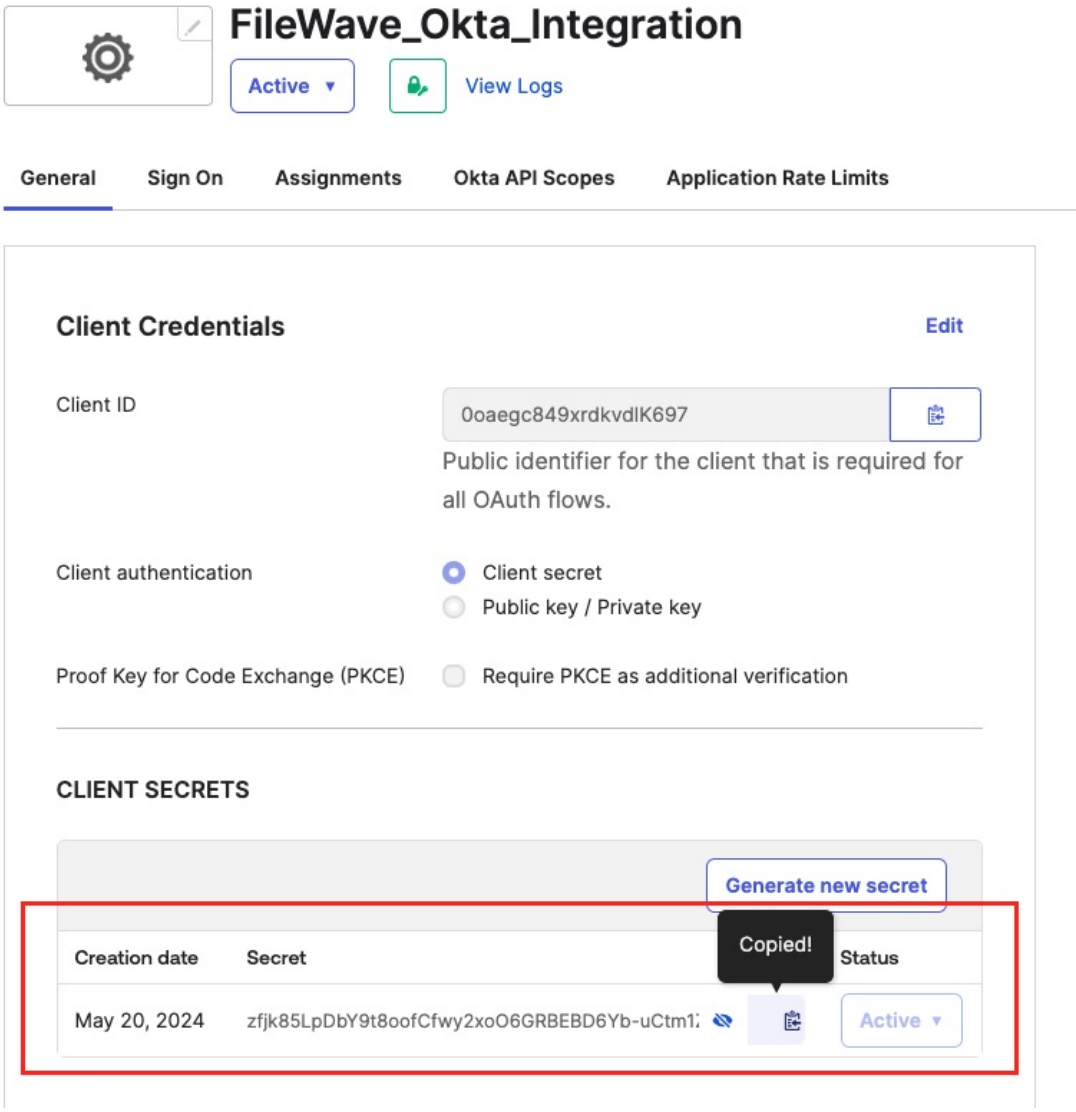
2. Open the Identity Provider menu in the FileWave Web Admin Settings
    1. 

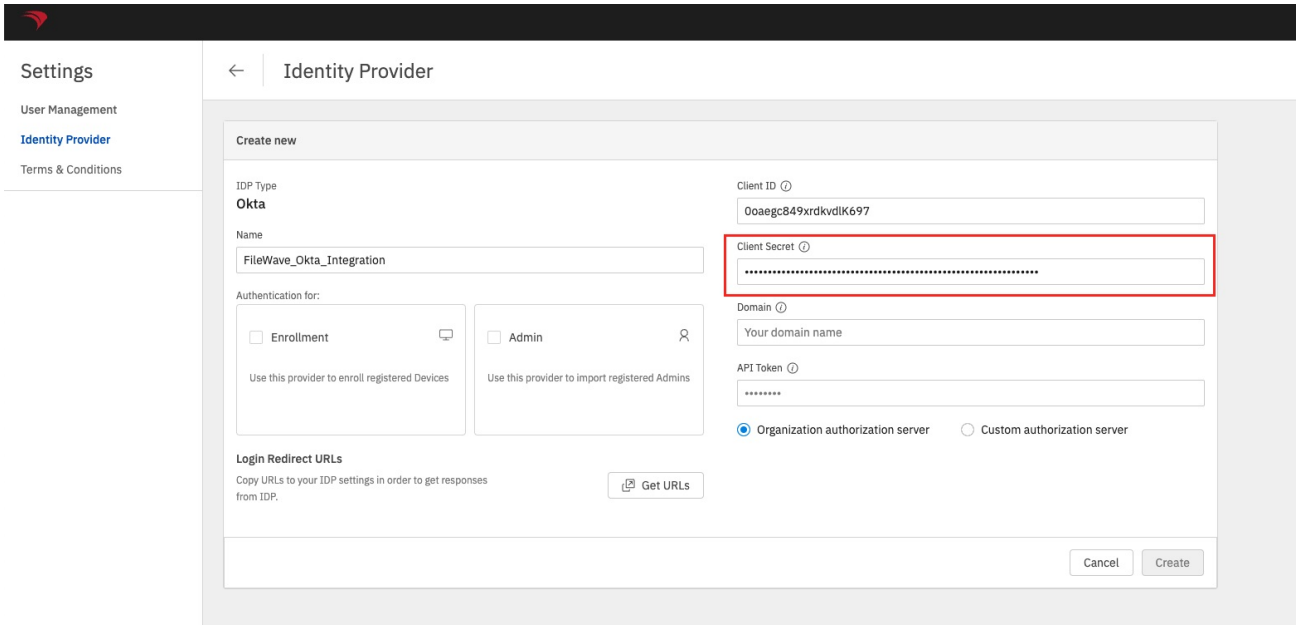
3. On the Identity Provider menu, click the Setup Okta button or New Identity Provider button in the top right if one has already been configured.
    1. Input a meaningful name in the Name field.
    2. Copy the Okta Client ID value found in the Okta page you were redirected to and paste in the Client ID field.





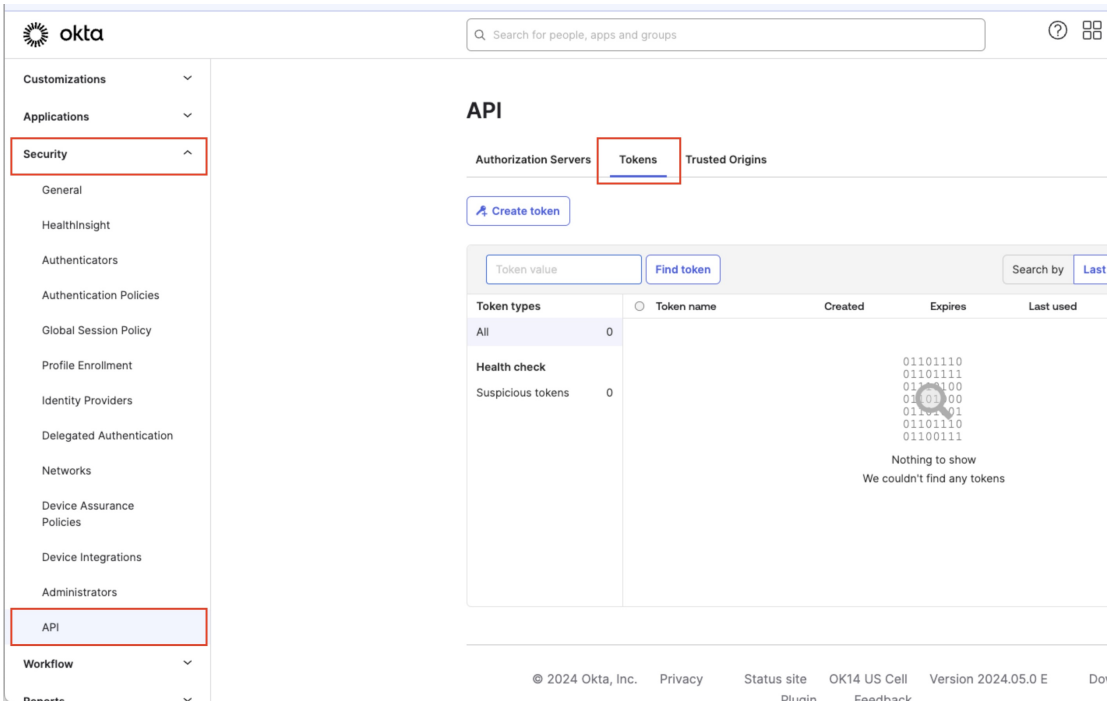
3. Input the Okta Client Secret value in the Client Secret field.



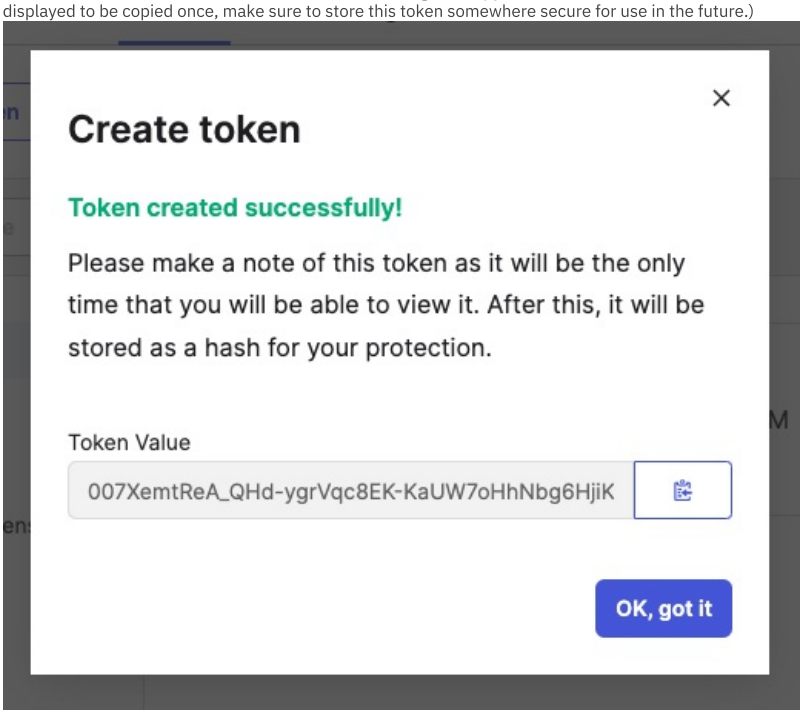


API Token

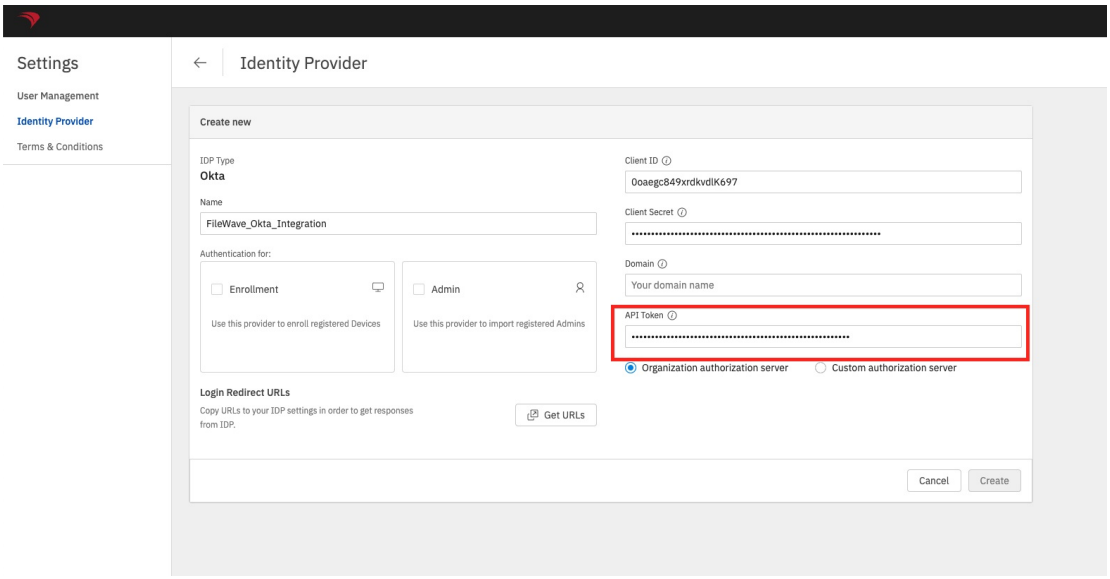
1. In Okta, open the Security > API menu and open the Tokens tab.



2. Click the Create Token button in the Tokens tab.
3. Input a meaningful name in the API token's Name field.
4. Click the Create Token button in the Create Token dialog and copy the API token and store it in a secure location. (Okta API tokens are only displayed to be copied once, make sure to store this token somewhere secure for use in the future.)



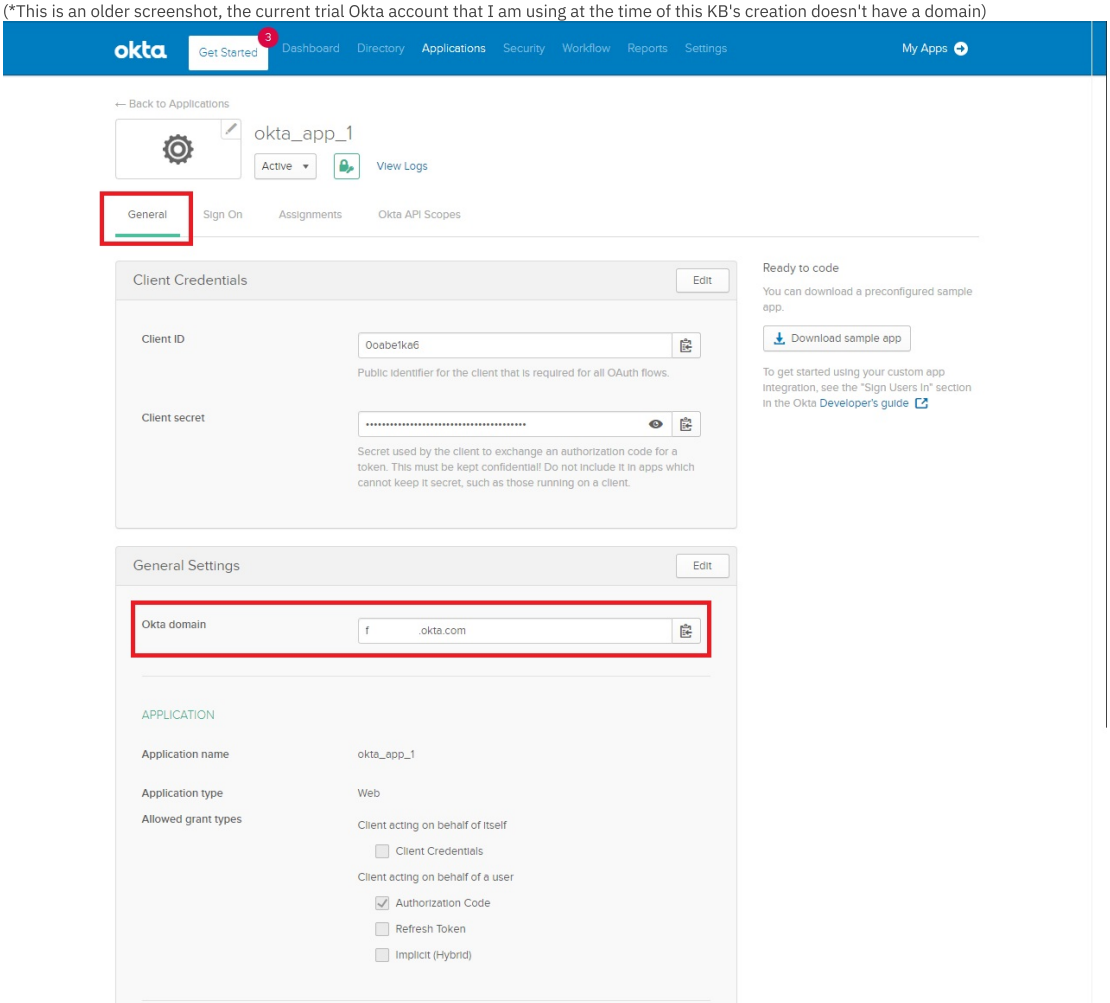
5. Copy and Paste the Token Value into the API Token field in the FileWave Admin Settings.



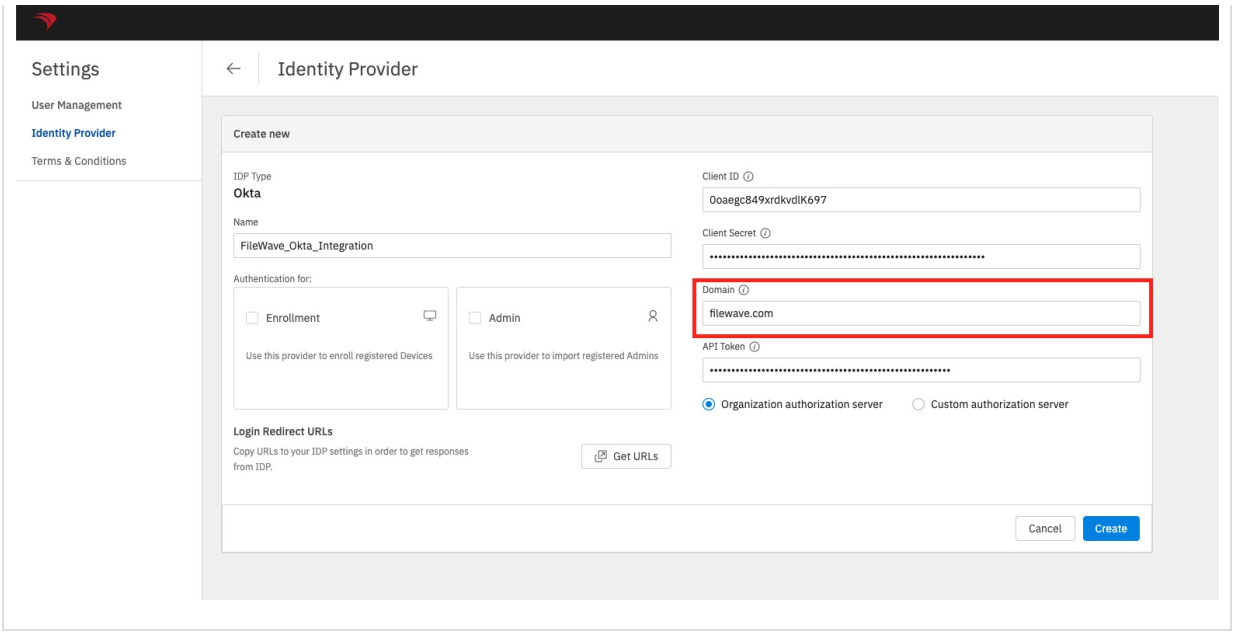
Okta Domain

1. Open the Okta Admin > Menu > Applications > Okta App > General tab and copy the Domain value to a secure location.

   (*This is an older screenshot, the current trial Okta account that I am using at the time of this KB's creation doesn't have a domain)



2. Input the Okta Domain in the Domain field. The value in FileWave should not be saved with the "https://" portion.



Part 4: Configuring and Authenticating with Okta Users

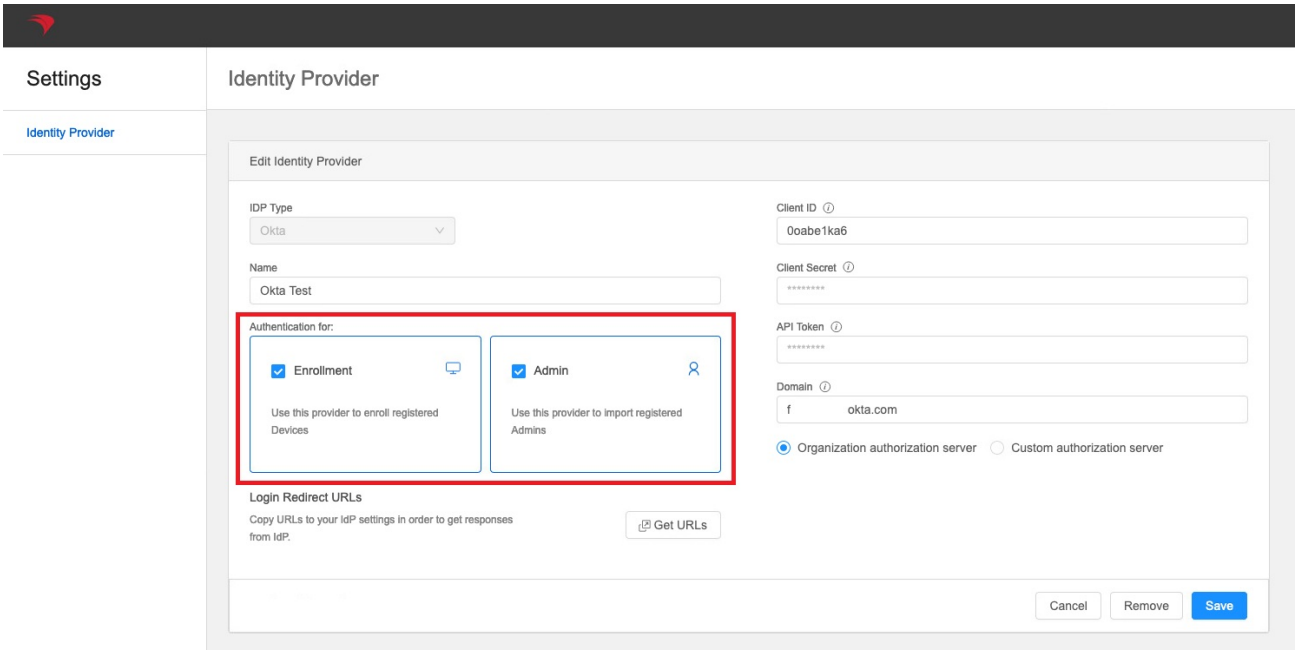
Configure an Okta Identity Provider for Authentication

An Okta App will need to be configured in the FileWave Identity Provider settings for use with FileWave Device enrollment and/or FileWave Admin authentication.

1. Begin by logging into the FileWave Web Admin and open the Settings button (gear icon in the header).
2. Click the Edit button on the Okta App card that will be used for authentication.
3. Check the Enrollment checkbox if you want to use this Okta App authentication for FileWave Device enrollment.
4. Check the Admin checkbox if you want to use this Okta App for FileWave Central and FileWave Anywhere console authentication.

ℹ Only one Identity Provider App instance (Okta, Azure AD, etc.) can be configured with the Admin authentication for each type of Identity Provider.

ℹ Only one Identity Provider can be configured for FileWave Device Enrollment authentication.



5. Click the Save button on the Okta App to confirm any authentication changes.

Configure FileWave Admin IdP Groups

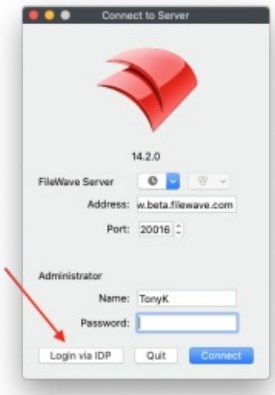
- FileWave Admin IDP Groups will need to be created in order to use the Okta App for authentication with the FileWave Native or Web Admin console.
- See: Adding IdP Groups for FileWave Authentication

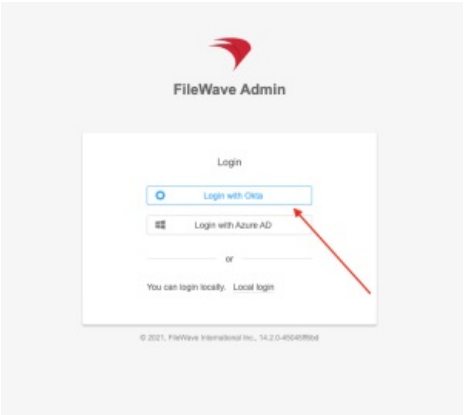
Authenticate with Okta during FileWave Device Enrollment

- Once the Enrollment checkbox is set for an IDP configuration then the Okta App can be used for authentication during FileWave Device enrollment.
- See: Configuring DEP Profiles for IDP Authentication

Login with Okta for FileWave Native or Web Admin Console

- Once FileWave Admin IDP Groups are created for an Okta App the Login with Okta option can be used with the FileWave Native or Web Admin console for authentication.
- See: Admin Login in Using an IdP Provider





Related Content

- IdP Setup: Azure AD
- Adding IdP Groups for FileWave Authentication
- Adding IdP Groups for FileWave Authentication
- Admin Login in Using an IdP Provider

IdP Setup: Google

What

Before we can use Google for authentication from FileWave, we must configure Google Workspace and give FileWave access to it. The whole purpose of this configuration is to give FileWave permissions to talk to your Google environment.

When/Why

This configuration is required if you want to use Google for authentication during device enrollment or during login to the FileWave Web and Native administrator consoles.

How

The configuration for access is all driven through Google Workspace.

Introduction

Setting up Google as IdP in Filewave means that we want to support users to log in with their Google account. We also want to allow Filewave services to query Google Workspace account users and groups.

In order to use Google as IdP and configure it inside Filewave, one has to obtain the following credentials from Google.

- Client ID
- Client secret
- Service key (JSON file)
- Service account

The process on how to obtain these is described below.

> To complete the steps below, one has to be logged in to a Google account and be a super administrator of the Google Workspace domain (more info)

Required Items

- Google Domain
  - Admin rights within the Google Domain
  - Pre-existing Google Organizational Unit structure (RECOMMENDED)
- Running FileWave Server
  - GCM Setup - Google Cloud Messaging (GCM/Firebase) Setup
  - FileWave HTTPS Root Trusted Certificate setup.

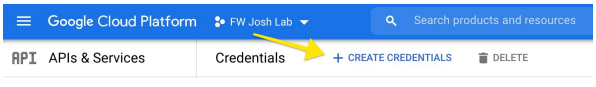
> NOTE: CANNOT be IP Address or self-signed cert. Must be FQDN - Instructions Linked Here

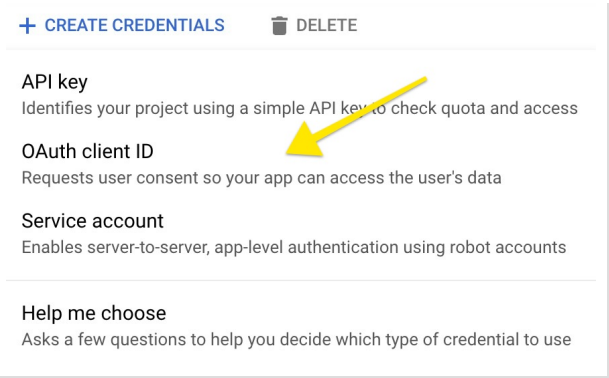
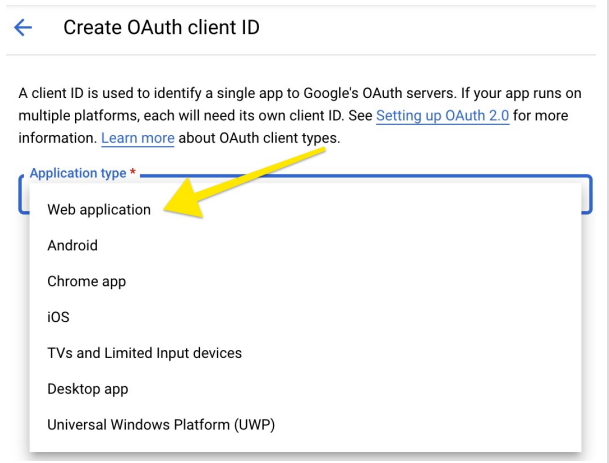
Domain verification

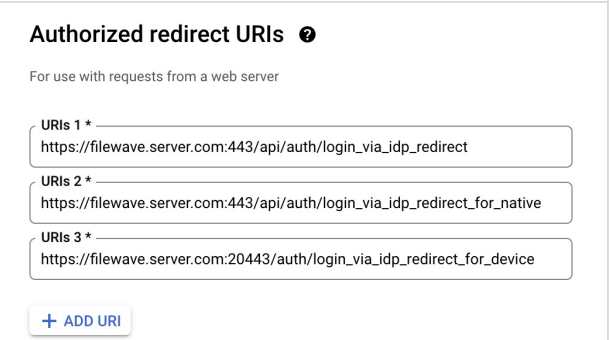
Google's API access to user's data may need to be reviewed and verified once setup is complete. For information please review, Google's OAuth API verification documentation.

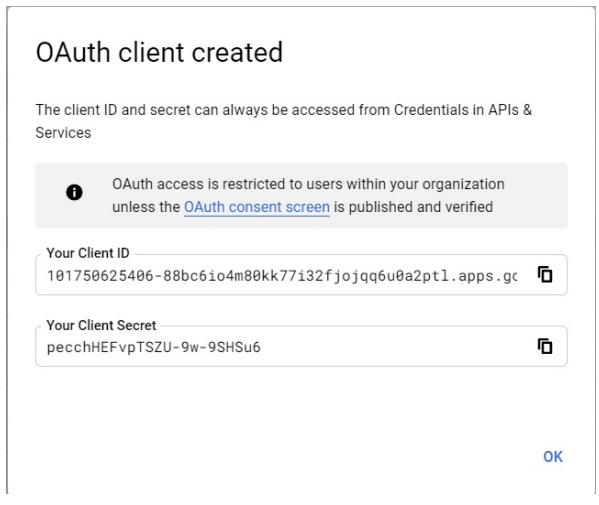
Client ID and client secret (Google)

Below is an excerpt on how to obtain a Client ID and client secret. For a more detailed tutorial and additional information, check the documentation.

Step	Example screenshot
(Step 1) - Navigate to https://console.cloud.google.com/apis/credentials	/
(Step 2) - Click on "Create credentials"	
(Step 3) - Choose "OAuth client ID"	

	
(Step 4) - In the next screen, choose "Web application"	

(Step 5) - In the configuration screen we need to name our OAuth client name and input correct Authorized redirect URIs.
NOTE
Please replace "filewave.server.com" with the correct URL of your server instance.
 	
`URL 1: https://filewave.server.com:443/api/auth/login_via_idp_redirect`
`URL 2: https://filewave.server.com:443/api/auth/login_via_idp_redirect_for_native`
`URL 3: https://filewave.server.com:20443/auth/login_via_idp_redirect_for_device`
	

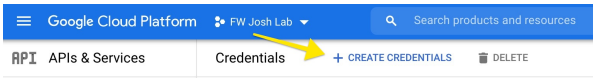
(Step 6) - Click CREATE, and your Client ID and Client secret will be generated. Please save them for later, as they are needed when configuring the FileWave server later on. Please note the message in grey about the OAuth access being restricted. You may also see a different message indicating that the consent screen needs to be verified. Click on the link in that grey text and ensure that the publishing status is In Production and that the User Type is External.	

Creating a service account (Google)

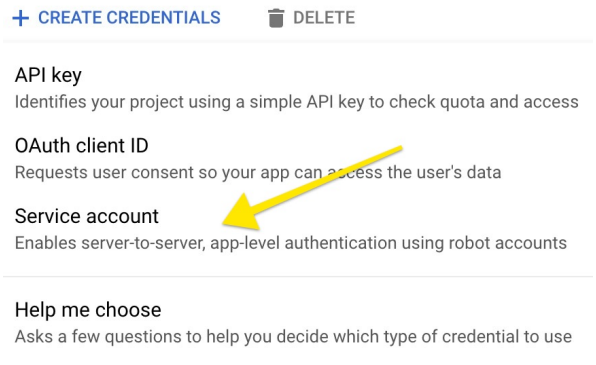
To support server-to-server interactions, first create a service account for your project in the API Console. - Google documentation

Step	Example screenshot
(Step 7) - Navigate to https://console.cloud.google.com/apis/credentials	/

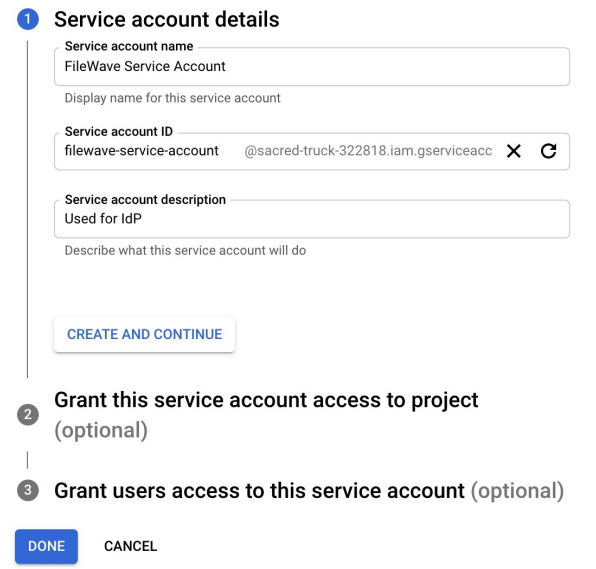
(Step 8) - Click on "Create credentials"



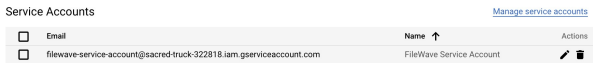
(Step 9) - Choose "Service account"



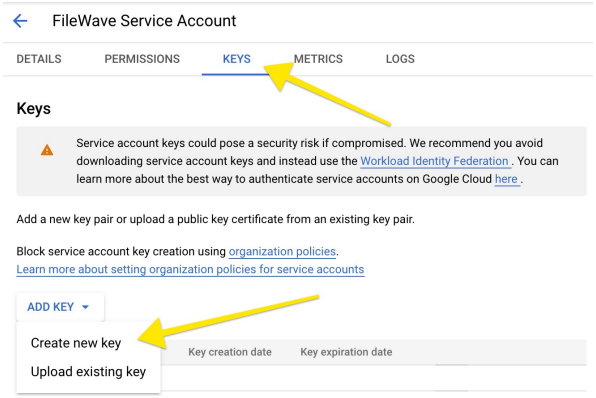
(Step 10) - Input required details and click "DONE".
NOTE
Skip optional steps 2 and 3, we will take care of it later.



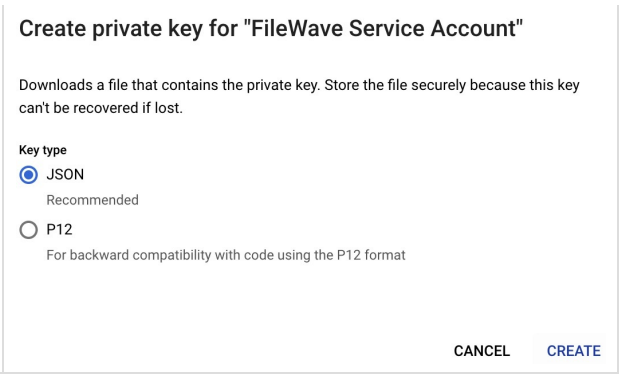
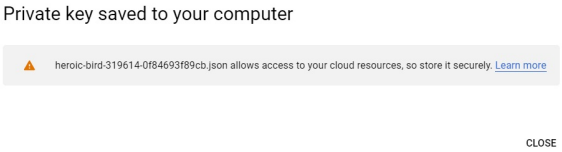
(Step 11) - Newly created service account should now be visible in the list of service accounts. (it might take few minutes)



(Step 12) - To create a service key under a newly created service account, click on the service account name (step above), select the 'KEYS' tab, and click on "Add key".

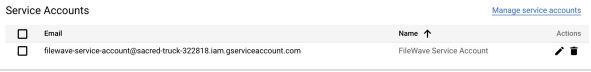
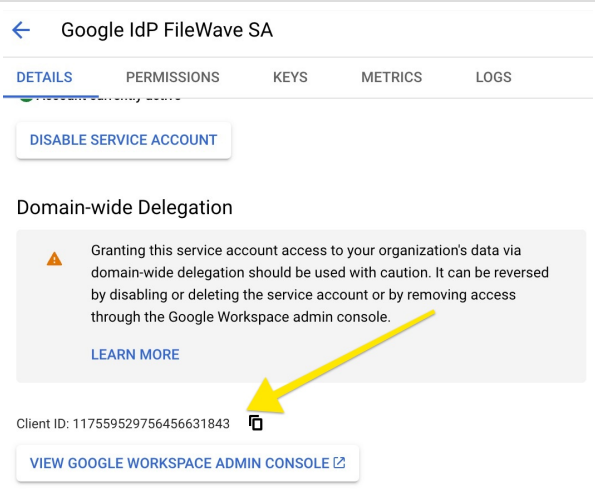
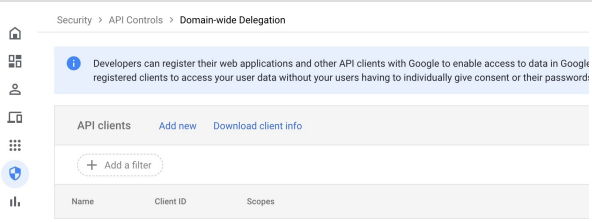


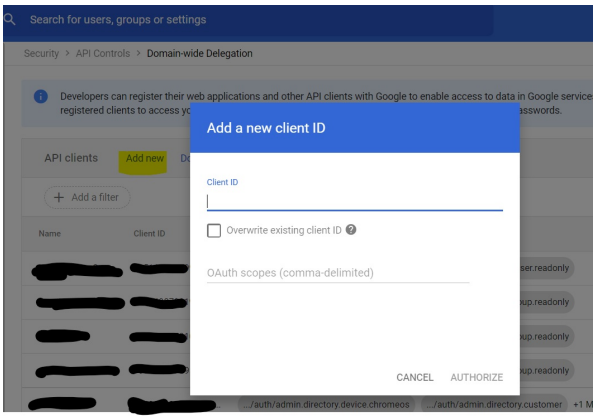
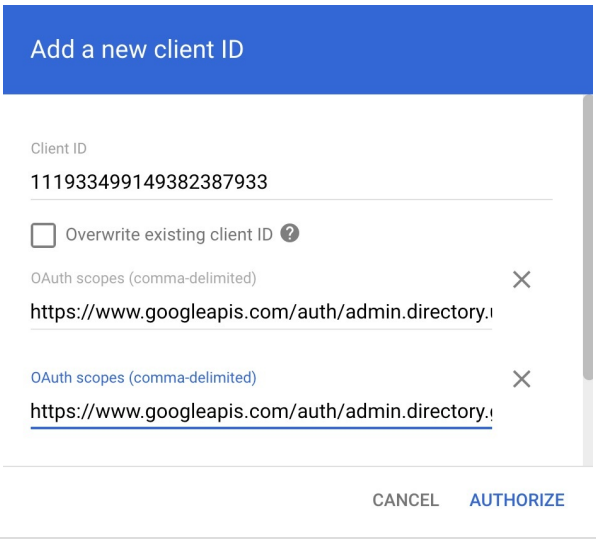
(Step 13) - Click on "Create new key", select JSON type and click "Create".

	
(Step 14) - Service key is now downloading to your computer. Save it, as it's needed in further configuration.	

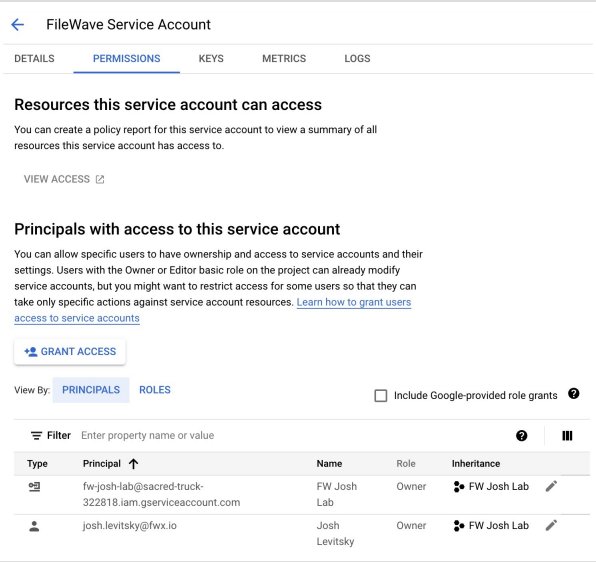
Configure Domain-Wide Delegation

If you want to access user data for users in your Google Workspace account, then delegate domain-wide access to the service account. - Google documentation

Step	Screenshot
(Step 15) - Navigate to https://console.cloud.google.com/apis/credentials	
(Step 16) - Open newly created service account details, by clicking on the service account name. Click SHOW ADVANCED SETTINGS. Save Client ID as it will be used later on..	
(Step 17) - Navigate to https://admin.google.com/ac/owl/domainwidedelegation	
(Step 18) - Click on "Add New" to create a new domain delegation. NOTE You will need super administrator permissions for this step.	

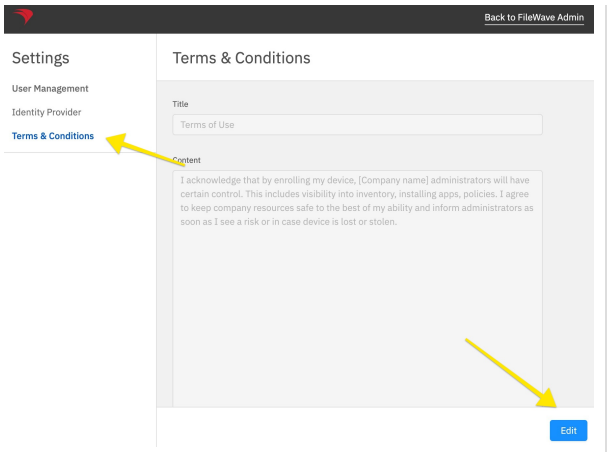
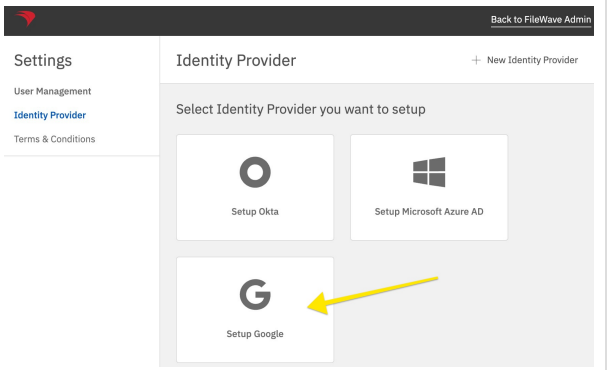
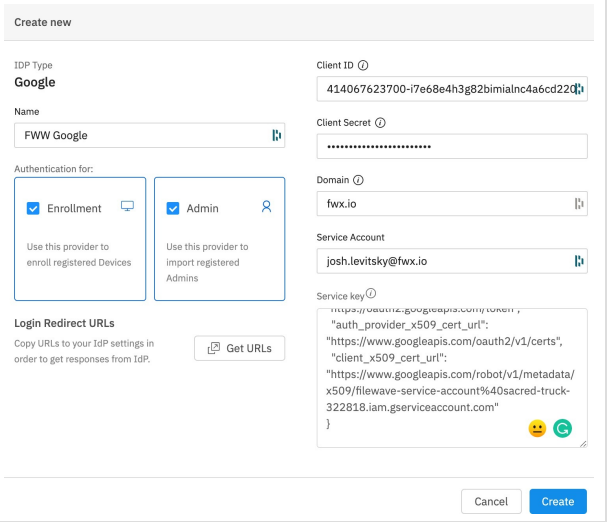
	
(Step 19) - In the Client ID, put in the Client ID from step 16. In the OAuth scopes, put in the following. https://www.googleapis.com/auth/admin.directory.user.readonly, https://www.googleapis.com/auth/admin.directory.group.readonly Click "Authorize".	

Service account and permissions

Step	Screenshot
(Step 20) - The next to last piece is setting up a service account. A service account is a user, that is going to be used in order to access resources. In order to add a user to a service account, navigate to https://console.cloud.google.com/apis/credentials and then click the service account you created, click on the Permissions tab, and add a user you'd like to use for accessing Google Workspace resources. NOTE Make sure the user has at least read access to the User and Group resource.	
The selected user's email becomes your service account token.	Example "josh.levitsky@fwx.io"

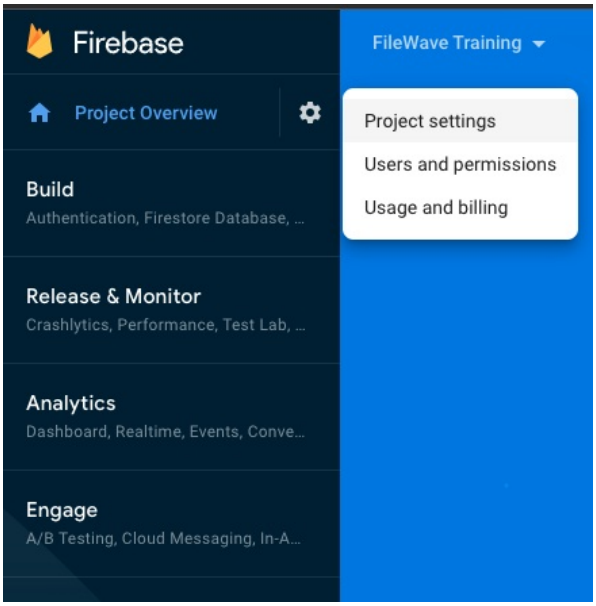
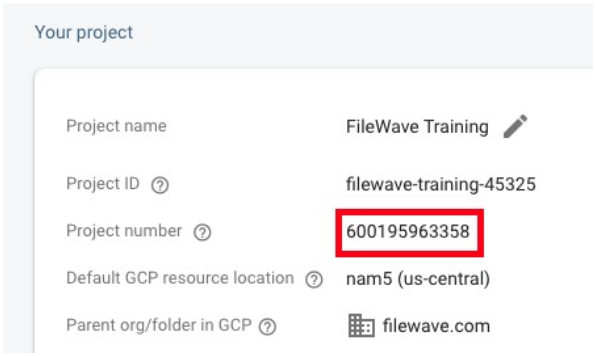
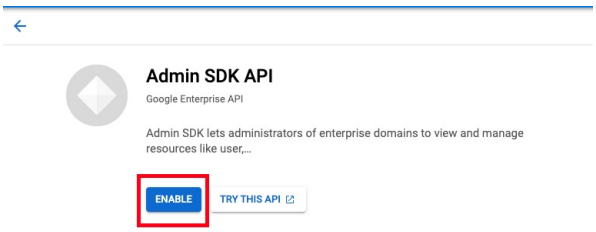
Configure Filewave server to use Google as IdP (Filewave)

Step	Screenshot
(Step 21) - The last piece of the puzzle is setting up Filewave to talk to Google. Navigate to https://filewave.server.com replacing the address with your FileWave server. Login as fwadmin to be sure you will have proper permissions to make the next changes. Click on the Settings gear icon at the top of the page.	
(Step 22) - Edit the Terms & Conditions to have appropriate text for your organization. This text is displayed when using an IdP to enroll devices.	

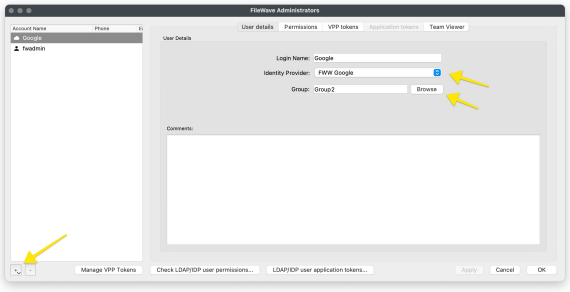
	
(Step 23) - Click Setup Google or if you already have another IdP setup then click New Identity Provider on the top right because this screen will look different.	
(Step 24) - This is where everything comes together. The Name is whatever you want to call this connection. Select if you want to use this for enrollment or for adding administrators or both. Enrollment here if selected will be to prompt a user on macOS or iOS/iPadOS to enter credentials so that you know who has the device. Admin here is to allow you to have technicians login to FileWave Central or Anywhere using the IdP. Insert the Client ID and Secret that you saved from step 6. (Not the Client ID from later on) The Domain is your domain. The Service Account was the user you granted access to the project in step 20. The Service Key is the contents of the JSON file you downloaded in step 14. Click Create once you have entered all of this information.	

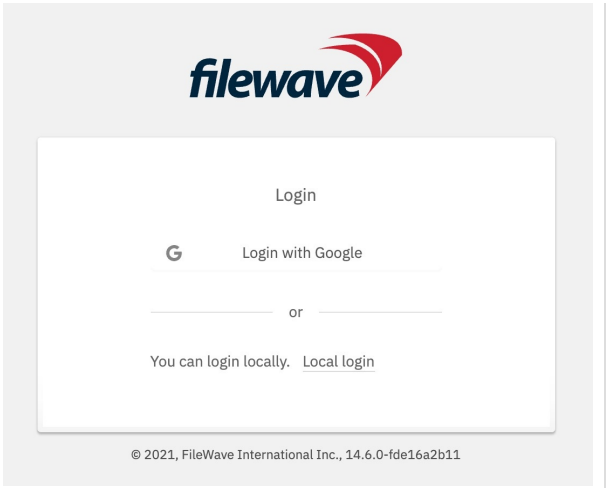
Enable Admin SDK API for your Firebase Project(Only needed if you haven't already setup Chromebooks in Filewave)

Step	Screenshot
(Step 25) - Now we need to enable the Admin SDK API for your project. Navigate to https://console.developers.google.com/apis/api/admin.googleapis.com/overview?project=<project-number> Fill in <project-number> is from Firebase/Project settings/General/Project number If you are unsure what this is you can find it via logging into http://console.firebase.google.com/ > click your Firebase Project > Click the gear icon at the top left to the right of "Project Overview" > Project Settings	

	
(Step 26) Copy the Project number and add that to the link. E.G https://console.developers.google.com/apis/api/admin.googleapis.com/overview?project=600195963358	
(Step 27) Click the Enable button	

Configure Filewave to allow Admins to use Google as IdP (Filewave)

Step	Screenshot
(Step 28) - Now that you have configured FileWave to talk to Google for Admin you need to go into the Native Admin to enable admins to actually log in and set their permissions. Launch the Native Admin and go to Assistants → Manage Administrators.	
(Step 29) - Click the + on the lower-left corner and pick IdP Group Account. On this screen, it is important to clarify that you are not defining a user here but a group of users. The Login Name is misleading here, and should be thought of as the name of the group of users so you might put something like Google - Desktop Techs and then for Identity Provider make sure your Google connection is selected that you set up in the prior steps. For Group click the Browse button and select the group that includes all of the users who will have access. If you will give all of your users the same level of permissions then you can use one group for all of your FileWave admins, but if you will use different levels of access then make an IdP Group Account on this window to define each of your groups of FileWave admins. In the image, you see a single entry for Google which might be appropriate if all of the FileWave admins are in a single group on the Google side.	
If everything was done correctly then your Web Admin login should look like the image shown. Click to Login with Google and try to log in. If you can not log in then the user may not be in a group that was given access in step 20 so go and check on the Google side to be sure. If the user can log in but can not perform tasks then ensure they are in the right group, and that you have configured the Permissions tab seen on step 20 to be sure they have the right permissions granted.	



Troubleshooting

If you try to login on via a browser, and get the error: "login-idp?Error=HTTPError" and "Error Authorization via IDP not carried out." or in the Django log you see `[ERROR] 2023-08-29 09:23:42,063 (views): Authentication through IDP failed. Exception: (HTTPError) 403 Client Error: Forbidden for url: https://www.googleapis.com/oauth2/v3/certs` then you may want to review FileWave Server should not have IPv6 enabled.

If you receive a generic error when attempting to iDP login, "iDP Authorization Failed", you may need to enable the Admin SDK API(steps 25-27 of guide) for the project by visiting the following sample URL (replace <project_ID> with your project ID) and clicking "Enable":

https://console.developers.google.com/apis/api/admin.googleapis.com/overview?project=<project_ID>

If you have access to the Django log for the server, it will give you the full details and direct link, so you can copy/paste/enable:

```
cat /usr/local/filewave/log/filewave_django.log
```

Sample Error:

"googleapiclient.errors.HttpError: <HttpError 403 when requesting https://admin.googleapis.com/admin/directory/v1/groups?domain=<domain>&alt=json returned "Admin SDK API has not been used in project <project_ID> before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/admin.googleapis.com/overview?project=<project_ID> then retry. If you enabled this API recently, wait a few minutes for the action to propagate to our systems and retry.". Details: "[{'message': 'Admin SDK API has not been used in project <project_ID> before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/admin.googleapis.com/overview?project=<project_ID> then retry. If you enabled this API recently, wait a few minutes for the action to propagate to our systems and retry.', 'domain': 'usageLimits', 'reason': 'accessNotConfigured', 'extendedHelp': 'https://console.developers.google.com'}]">"

Related Content

- Adding IdP Groups for FileWave Authentication
- Configuring DEP Profiles for IDP Authentication
- Admin Login in Using an IdP Provider

IdP Setup: Keycloak

What

Before we can use Keycloak for authentication from FileWave, we must configure Keycloak and give FileWave access to it. The whole purpose of this configuration is to give FileWave permissions to talk to your Keycloak environment.

When/Why

This configuration is required if you want to use Keycloak for authentication during device enrollment or during login to the FileWave Anywhere and Central administrator consoles.

How

Setting up Keycloak as IdP in Filewave means that we want to support users to log in with their Keycloak account. We also want to allow Filewave services to query Keycloak account users and groups.

In order to use Keycloak as IdP and configure it inside Filewave, one has to obtain the following credentials from Keycloak.

- Client ID
- Client Secret
- Realm URL
- Realm admin API URL

The process on how to obtain these is described below.

> To complete the steps below, one has to be logged in to a Keycloak instance and be an administrator of the instance to complete all aspects of setting up Keycloak.

Required Items

- Keycloak instance
  - Admin rights within the instance
  - Users and Groups which you will want to use to grant access to FileWave Central or Anywhere
- Running FileWave v15.5+ Server
  - FileWave HTTPS Root Trusted Certificate setup.

> NOTE: The FileWave Server CANNOT use only the IP Address or self-signed cert. Must use a FQDN - Instructions Linked Here

Configuring Keycloak

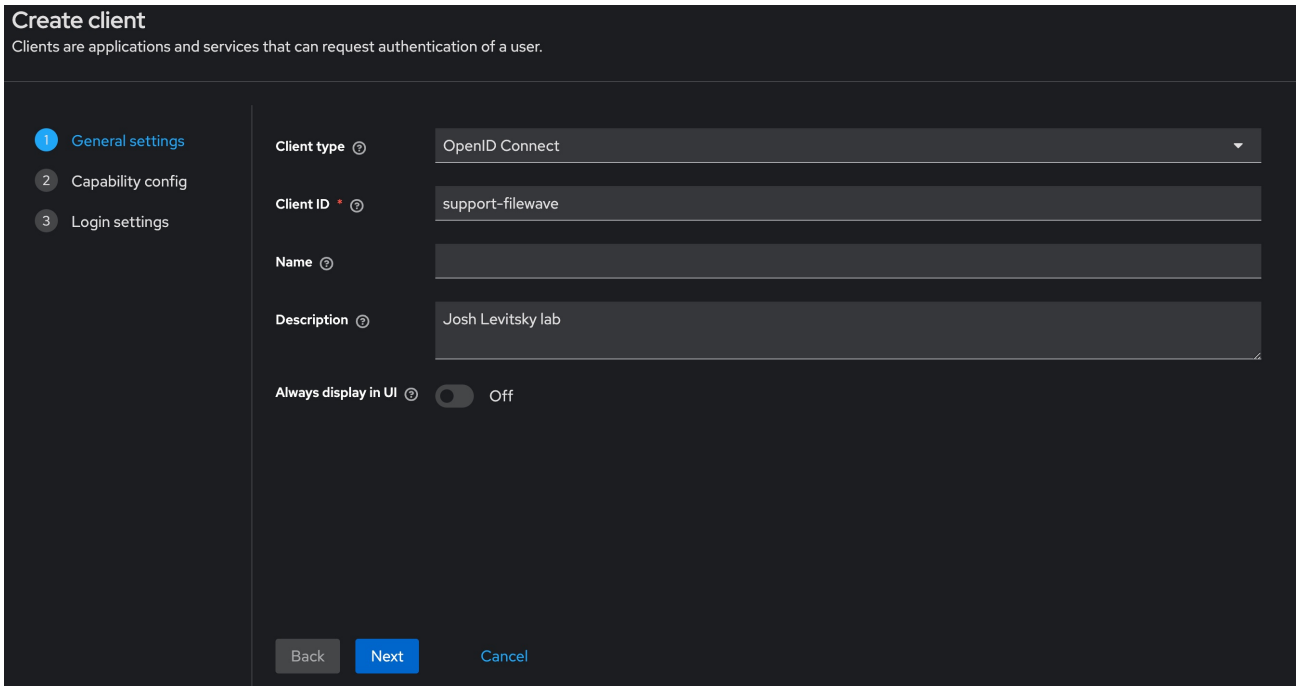
To begin you must have a Keycloak instance setup and have a Realm that you will be using with FileWave. If you already use Keycloak then this will be the case. A Realm is a container that will store all of your Keycloak things for an organization like Users, Groups and SSO Clients.

> The steps to create a Realm, Users, and Groups is more of a Keycloak function than a FileWave one. The steps outlined here will work as long as you are already using Keycloak.

Creating a Client App in Keycloak

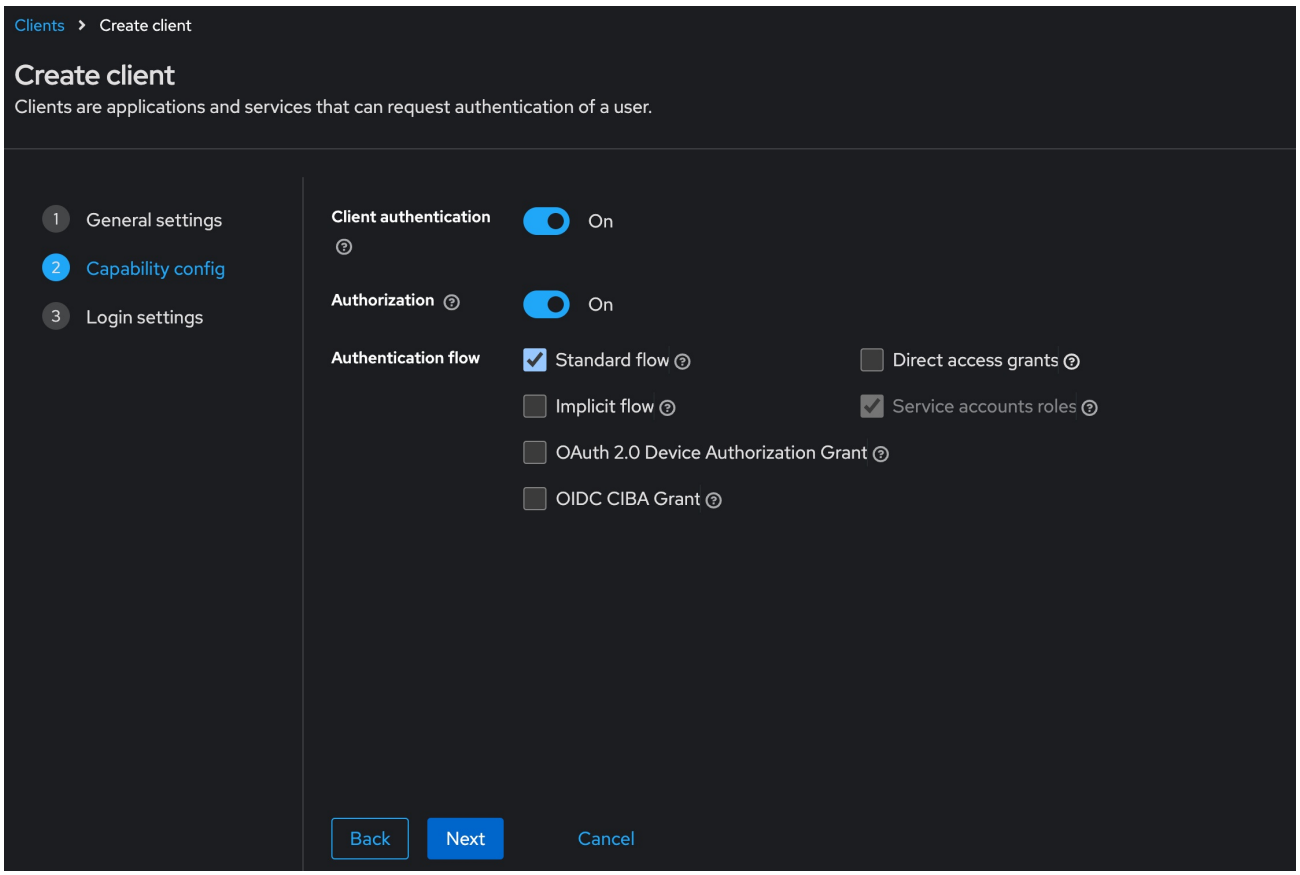
Select “Clients” in left menu bar and select “Create client” button

- Client type should be "OpenID Connect"
- Input Client ID in the “Client ID” label like "filewave" for example
- Name and Description can be blank or it is recommended to put something so you will remember why you created this like "FileWave Server" and some information about the server.
- Click "Next" to continue

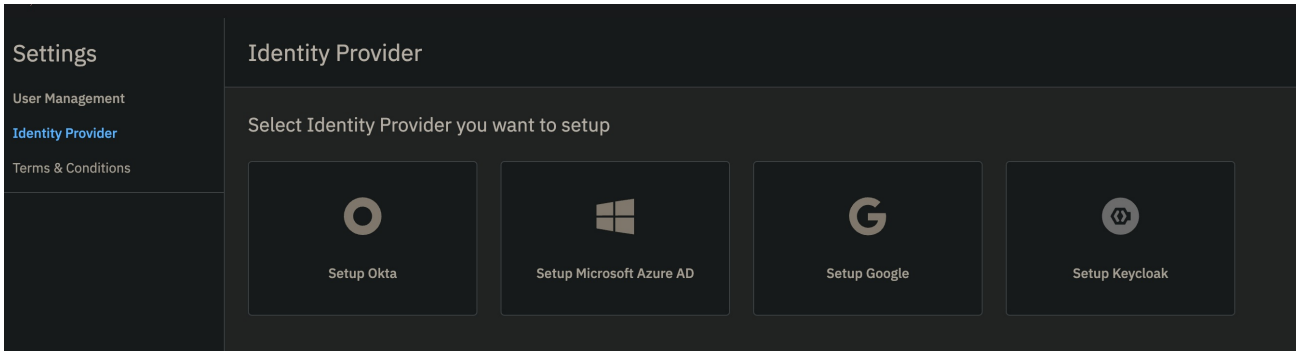


On the Capability config page:

- Turn on “Client authentication” and "Authorization"
- For Authentication flow check “Standard flow and Service accounts roles”



In this next step you are going to login to FileWave Anywhere and get the URLs needed for this page. Open a new browser tab and go to https://filewave.your_filewave_server.com replacing the host in the URL with your FileWave Server. This step is fairly quick and easy. Click the gear icon on the top right of Anywhere and then click "Setup Keycloak"



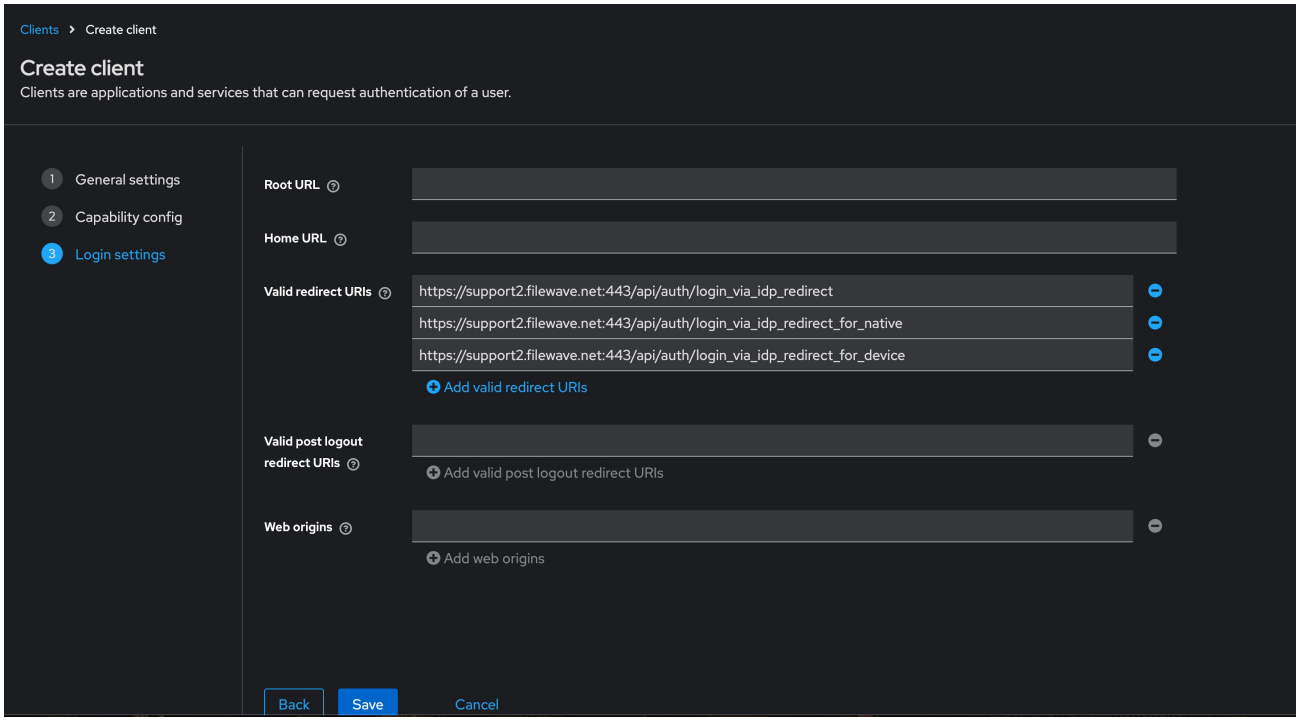
On the next page click "Get URLs" and get the 3 URLs which will look like the following but be for your FileWave instance:

```
https://support2.filewave.net:443/api/auth/login_via_idp_redirect
https://support2.filewave.net:443/api/auth/login_via_idp_redirect_for_native
https://support2.filewave.net:20443/api/auth/login_via_idp_redirect_for_device
```

Now return to your Keycloak tab of your browser and continue:

On the Login settings page:

- Add Valid redirect URLs in “Valid redirect URLs” one at a time clicking the + button to add the next one and pasting in each of the 3 URLs you obtained from FileWave Anywhere.
- Click the “Save” button

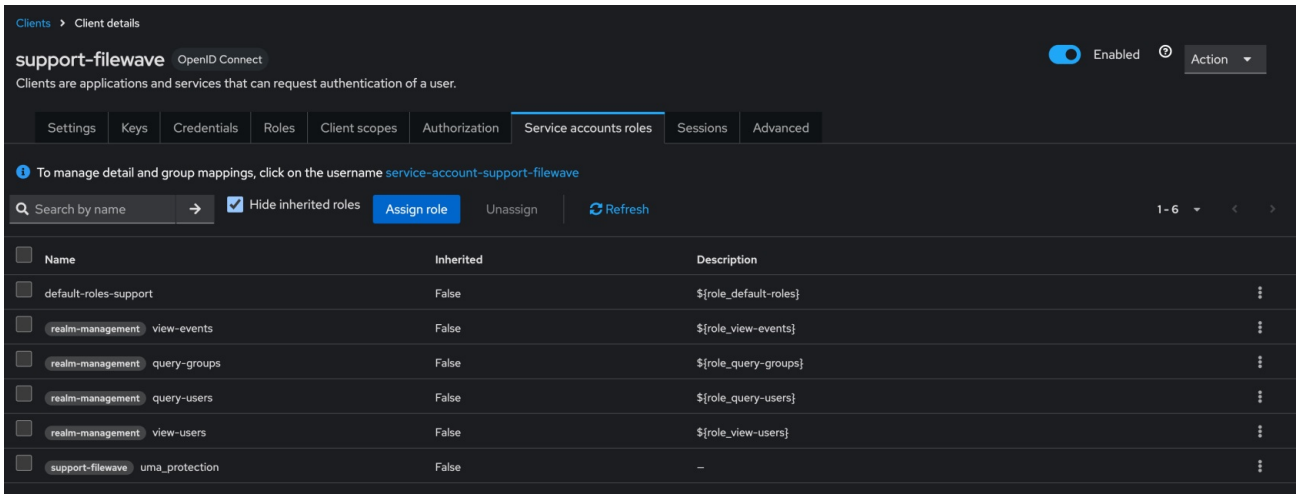


At this stage you should be looking at the details for the Client you just created in Keycloak but if it isn't you can:

- Select “Clients” in left menu bar
- Select the client you created.

Now on the details for the Client you created click “Service account roles” tab on the top of the details page.

- Use the "Assign Role" button to assign a few needed Roles. Assign these roles to the client using the search box to find them:
  - query-groups
  - query-users
  - view-users
  - view-events



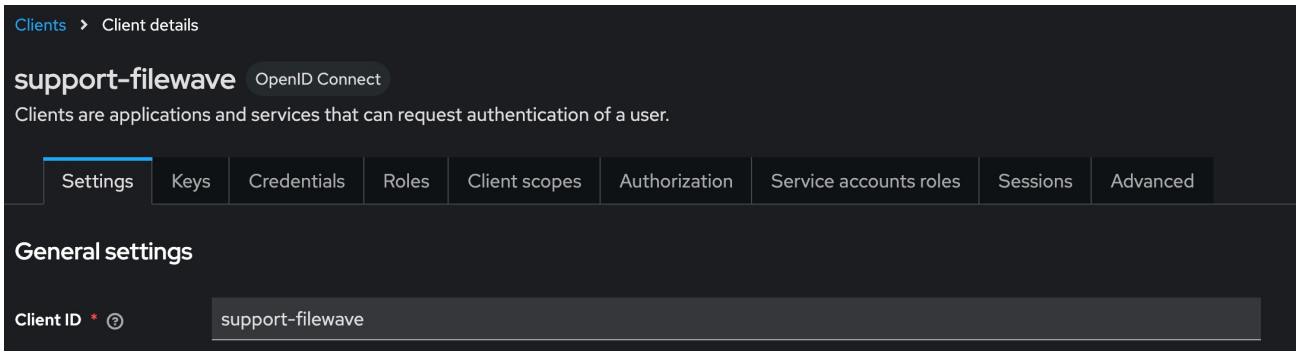
Obtaining the client ID and client secret

At this stage you should be looking at the details for the Client you just created in Keycloak but if it isn't you can:

- Select “Clients” in left menu bar
- Select the client you created.

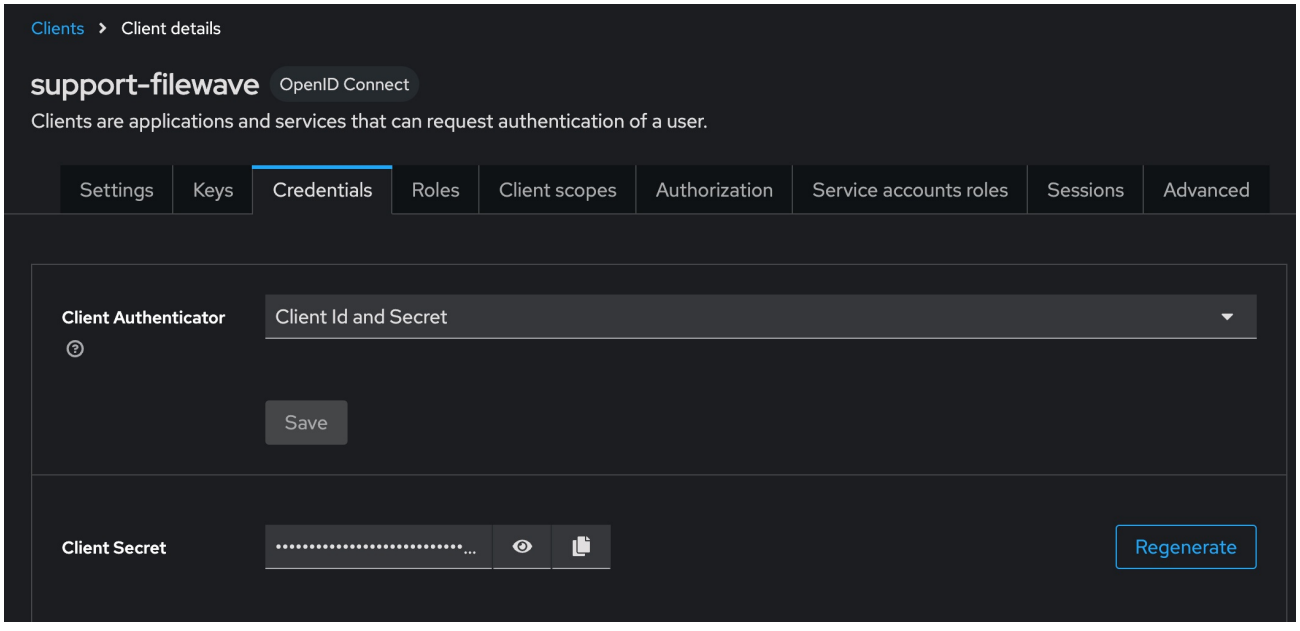
Now on the details for the Client you created click “Settings” tab on the top of the details page.

- Note the “Client ID”



Now on the details for the Client you created click “Credentials” tab on the top of the details page.

- Note the “Client Secret”

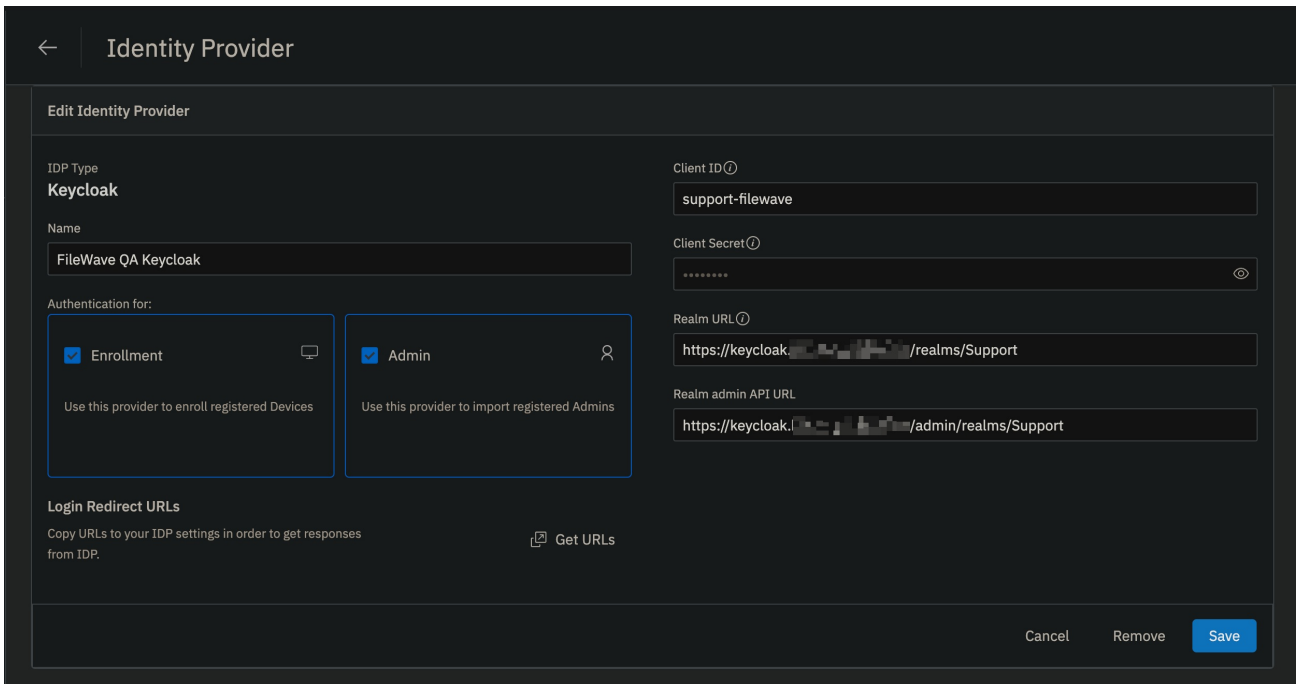


In this next step you are going to login to FileWave Anywhere again. Go back to the tab where you went to https://filewave.your_filewave_server.com replacing the host in the URL with your FileWave Server. If your prior session timed out then once logged in just click the gear icon on the top right of Anywhere and then click "Setup Keycloak" Otherwise you will be back on the setup page where you were before.

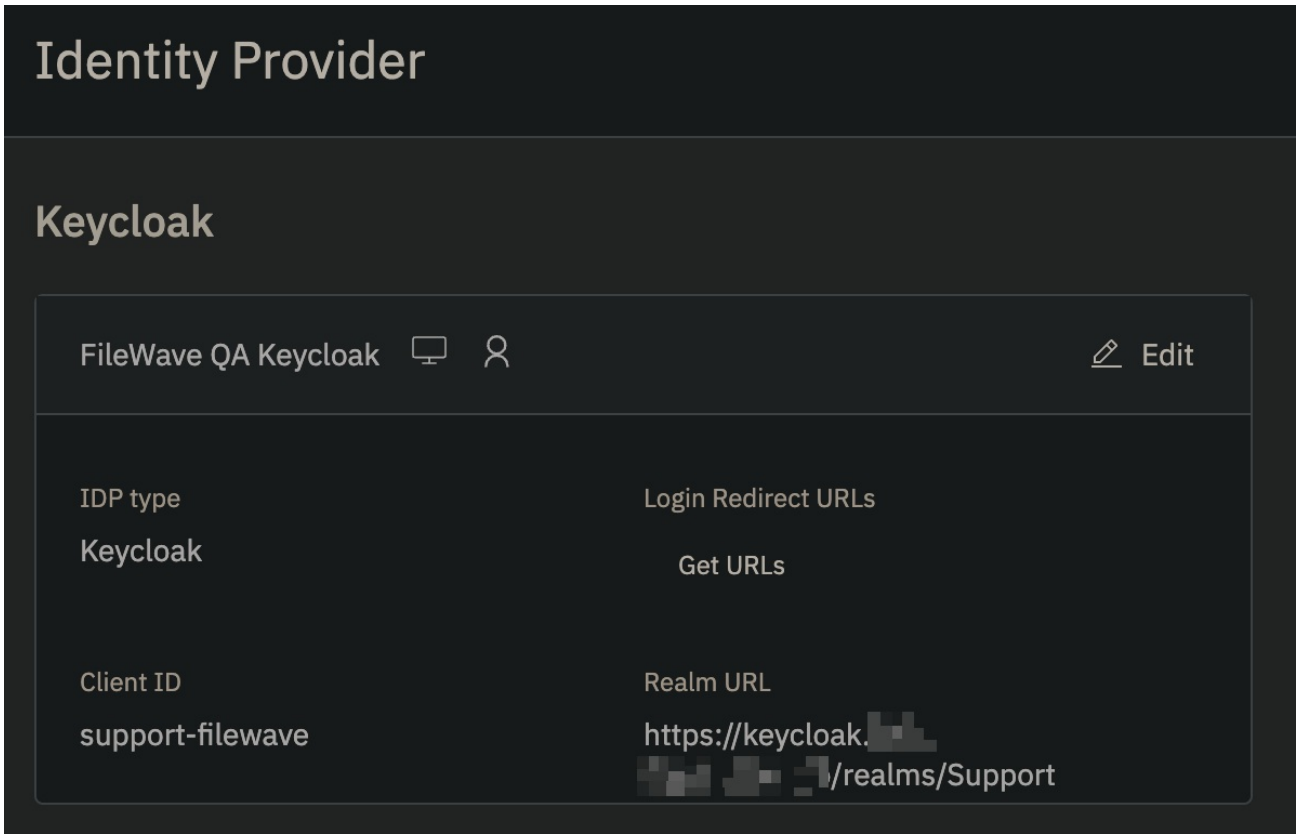
Here you will enter the "Client ID" and "Client Secret" that you copied from Keycloak. You'll want to put something in the "Name" field like which Keycloak you are pointing at if you have multiple in your organzation. You'll want to select "Enrollment" and or "Admin" for how you want to use the IdP.

> Enrollment here if selected will be to prompt a user on macOS or iOS/iPadOS to enter credentials so that you know who has the device.
>
> Admin here is to allow you to have technicians login to FileWave Central or Anywhere using the IdP.

For the "Realm URL" and "Realm admin API URL" these will be for your Keycloak instance for your Realm you are using. In the image you'll see Realm URL = https://keycloak.mycompany.com/realms/Support and Realm admin API URL = https://keycloak.mycompany.com/admin/realms/Support where the Realm name was Support.



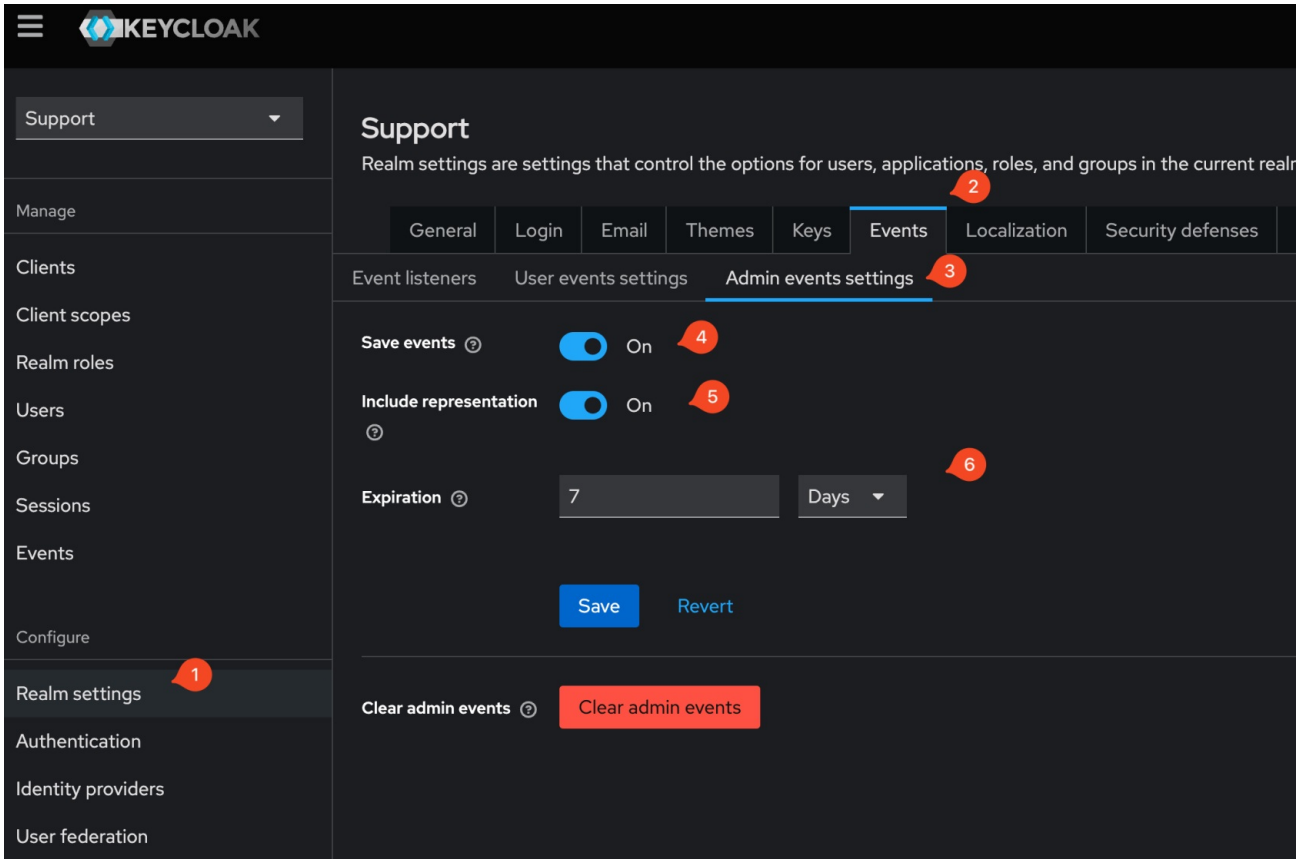
After clicking Create you should see the following if it was able to successfully reach Keycloak.



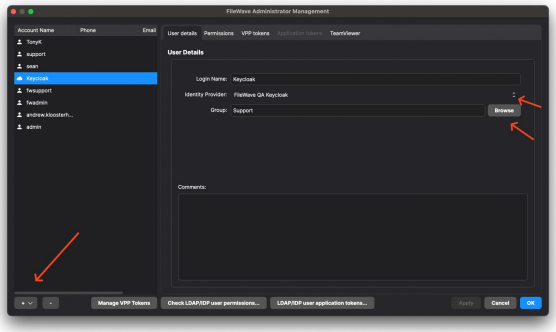
Configure Keycloak Realm Settings

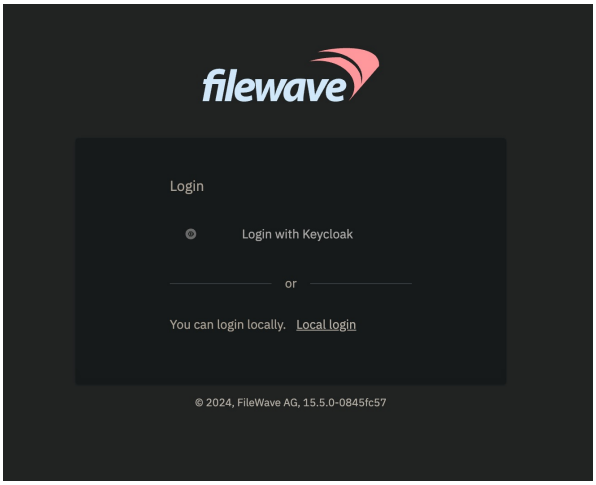
In Keycloak go to Realm settings for the Realm you are configuring and configure the Events -> Admin events settings as follows;

- Save events: ON
- Include representation: ON
- Expiration: 7 days



Configure Filewave to allow Admins to use Keycloak as IdP (Filewave)

Step	Screenshot
Now that you have configured FileWave to talk to Keycloak for Admin you need to go into the Native Admin to enable admins to actually log in and set their permissions. Launch the Native Admin and go to Assistants → Manage Administrators.	
(Step 29) - Click the + on the lower-left corner and pick IdP Group Account. On this screen, it is important to clarify that you are not defining a user here but a group of users. The Login Name is misleading here, and should be thought of as the name of the group of users so you might put something like Keycloak - Desktop Techs and then for Identity Provider make sure your Keycloak connection is selected that you set up in the prior steps. For Group click the Browse button and select the group that includes all of the users who will have access. If you will give all of your users the same level of permissions then you can use one group for all of your FileWave admins, but if you will use different levels of access then make an IdP Group Account on this window to define each of your groups of FileWave admins. In the image, you see a single entry for Keycloak which might be appropriate if all of the FileWave admins are in a single group on the Keycloak side.	
If everything was done correctly then your Web Admin login should look like the image shown. Click to Login with Keycloak and try to log in. If you can not log in then the user may not be in a group that was given access to the Keycloak Client in Keycloak so go and check on the Keycloak side to be sure. If the user can log in but can not perform tasks then ensure they are in the right group, and that you have configured the Permissions tab in FileWave Central to be sure they have the right permissions granted.	



Troubleshooting

If you try to login on via a browser, and gets the error: "login-idp?Error=HTTPError" and "Error Authorization via IDP not carried out." or in the Django log you see `[ERROR] 2023-08-29 09:23:42,063 (views): Authentication through IDP failed. Exception: (HTTPError) 403 Client Error: Forbidden for url:` then you may want to review FileWave Server should not have IPv6 enabled.

Related Content

- Adding IdP Groups for FileWave Authentication
- Configuring DEP Profiles for IDP Authentication
- Admin Login in Using an IdP Provider

Adding IdP Groups for FileWave Authentication

What

Once your IdP is configured as an authentication source, we can use it to allow directory groups to authenticate into FileWave.

When/Why

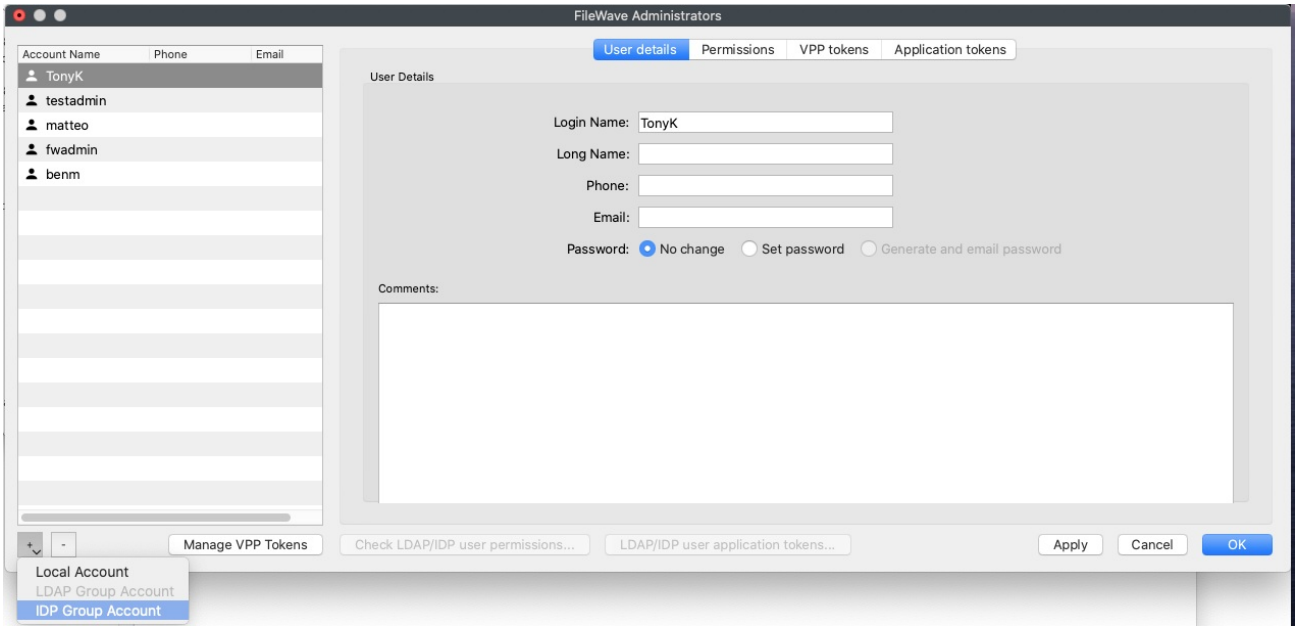
We'll use this as the configuration for admins to login, and to assign permissions. This method is especially helpful if you require 2 Factor Authentication through your IdP.

How

Setting up the group is in a few steps in the Native admin:

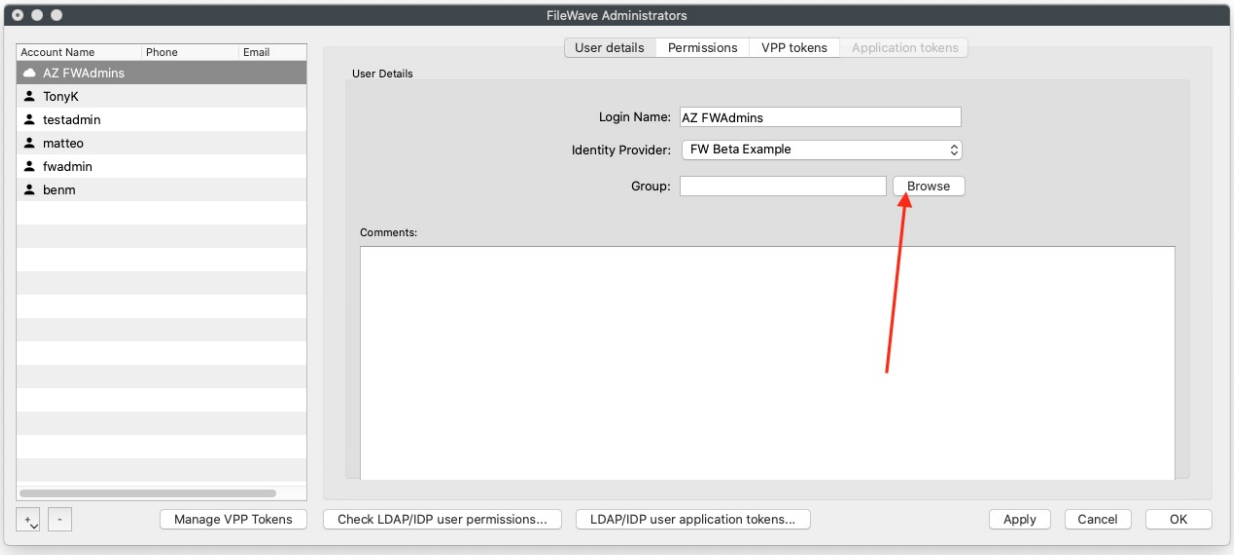
Assistants→ Manage Administrators

Add and IDP Group Account, (lower left, and you may notice it is similar to an LDAP group, but easier)

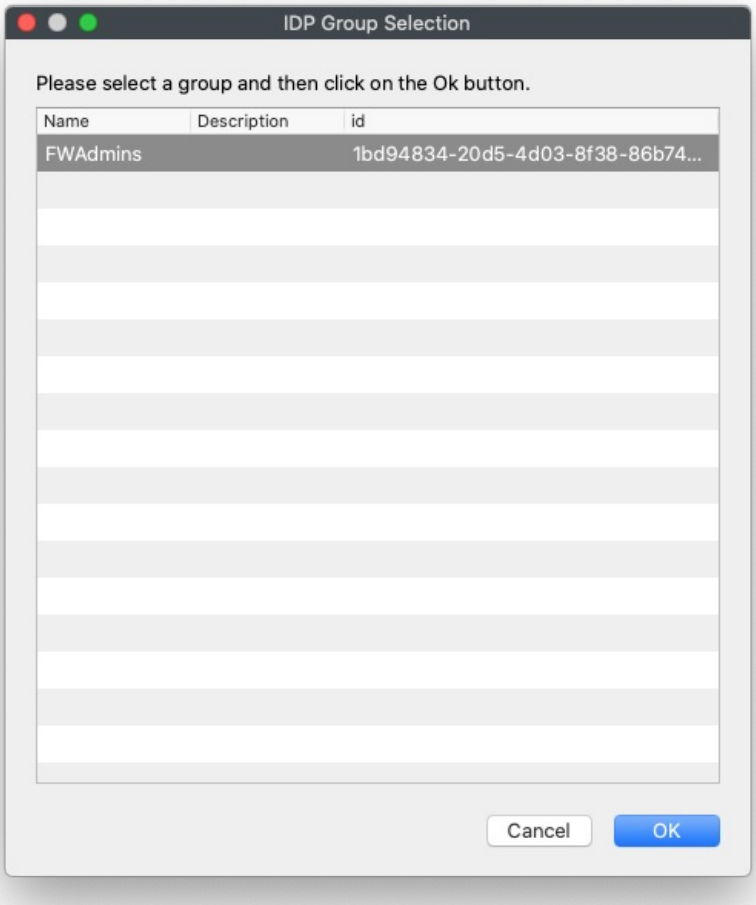


Give the group a name, and assign permissions as you would any normal local or LDAP based account.

Then, specify your IdP provider and find your IdP group by clicking the Browse button



There is only have one group in this test environment, but all of your security groups would show here:



Click OK, and Apply, and anyone in that group can now login to either the native or WebAdmin using their IdP credentials. Remember to also assign VPP Token rights if needed!

Related Content

- IdP Setup: Google
- IdP Setup: Azure AD
- IdP Setup: Okta
- Configuring DEP Profiles for IDP Authentication
- Admin Login in Using an IdP Provider

Configuring DEP Profiles for IDP Authentication

What

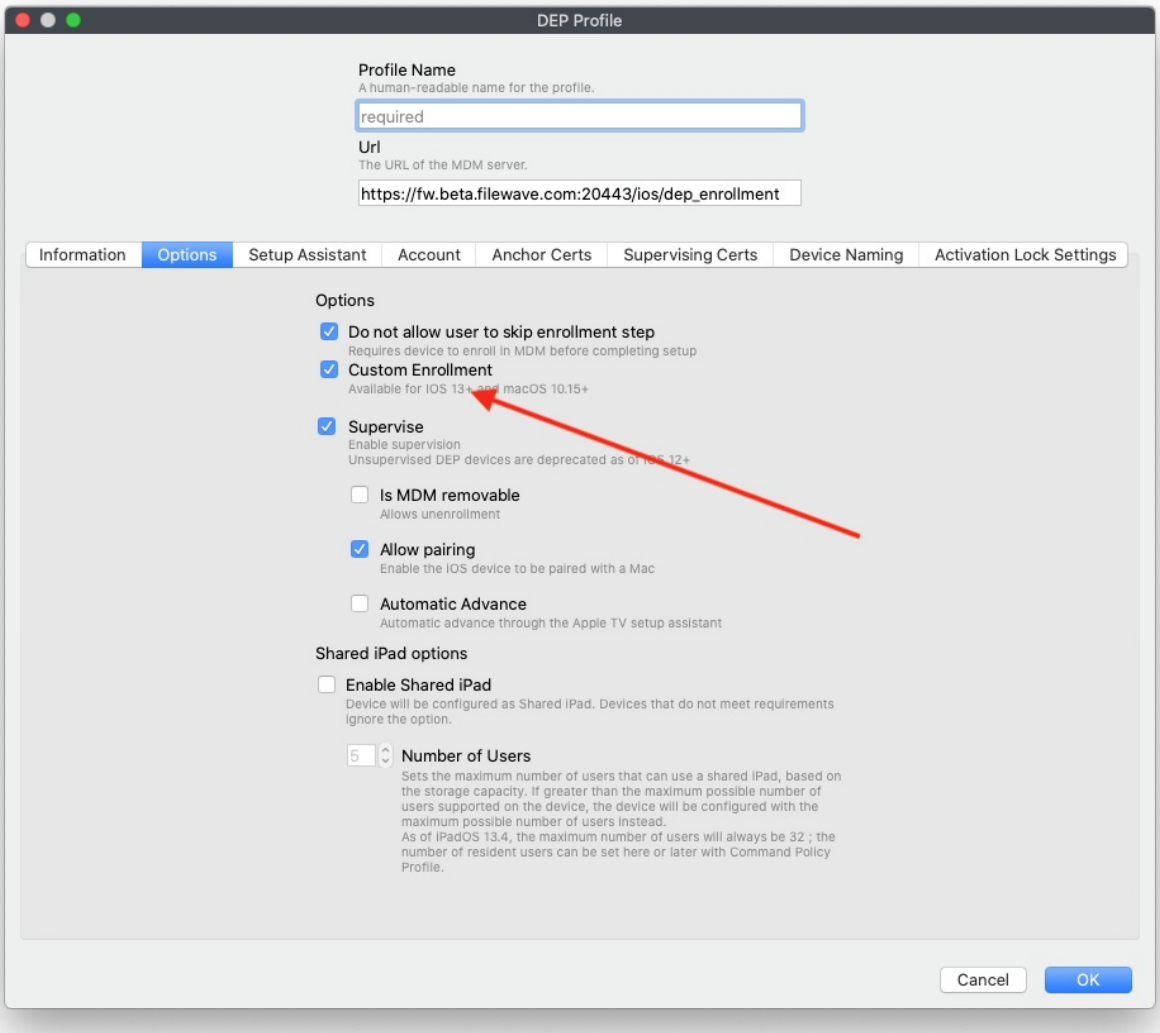
Configuring Apple Devices DEP Profiles to use IDP authentication.

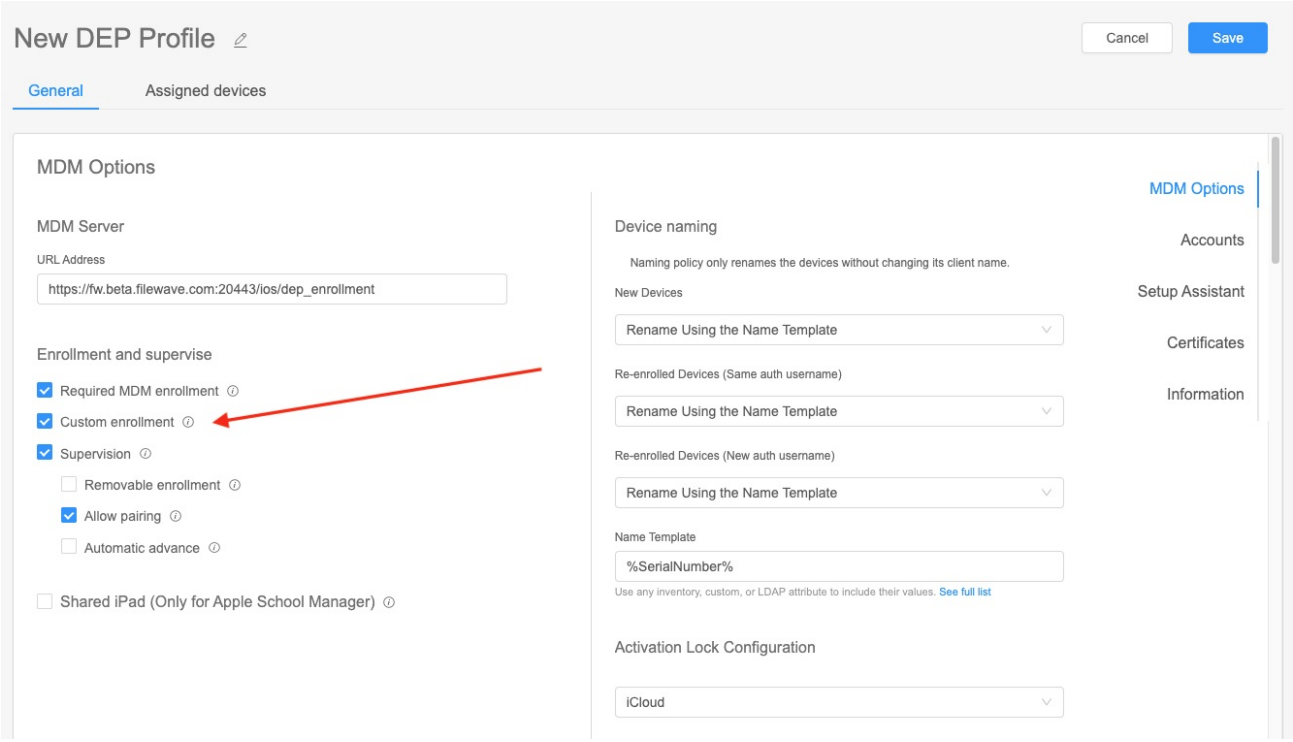
When/Why

We'll need to configure each DEP profile with which we would like to use IDP authentication (but it is simple to do)

How

You'll simply notice there is a new checkbox in the DEP profile for "Custom Enrollment". If that checkbox is checked in a profile, IDP enrollment will be used (if configured of course):

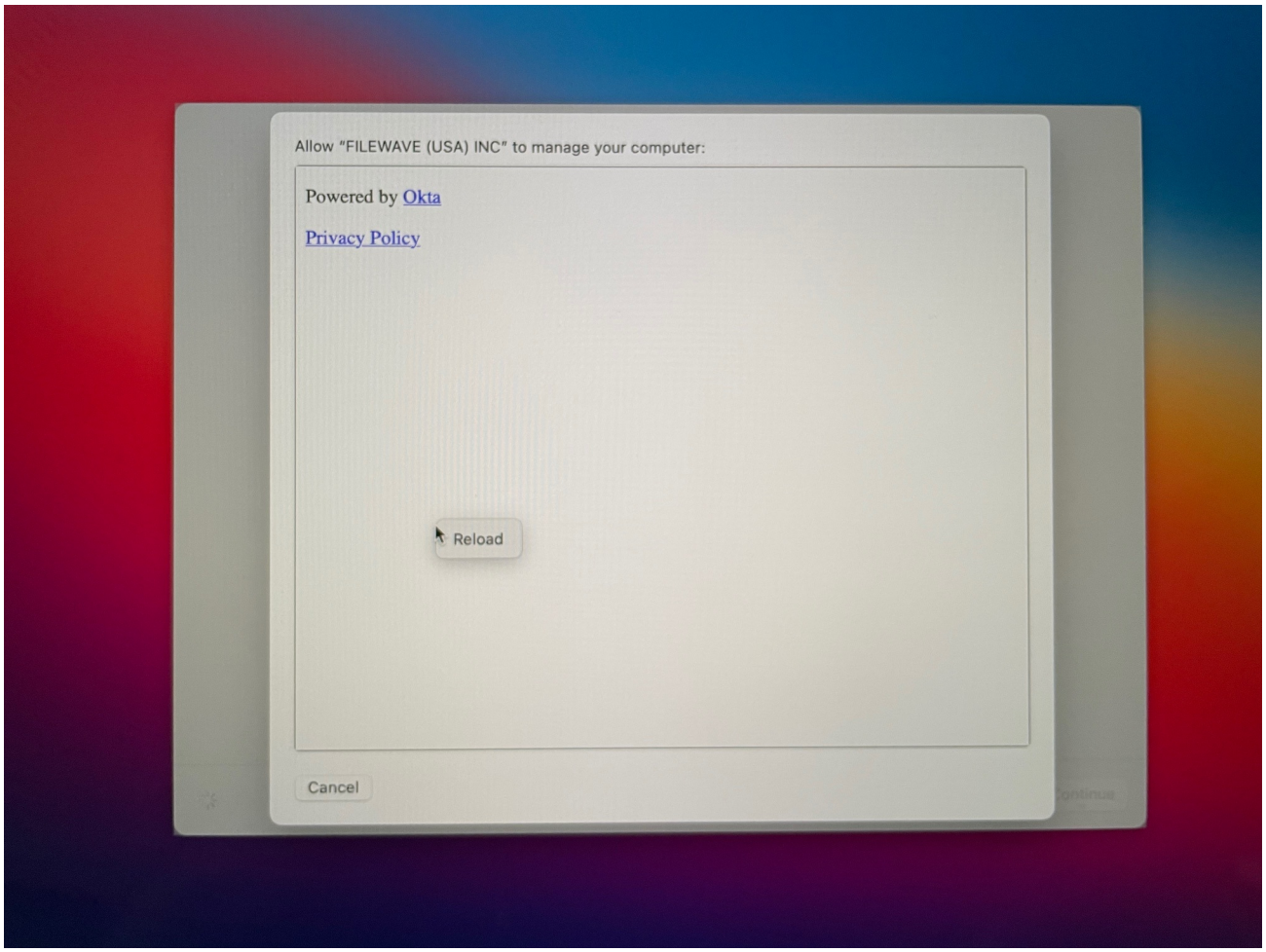


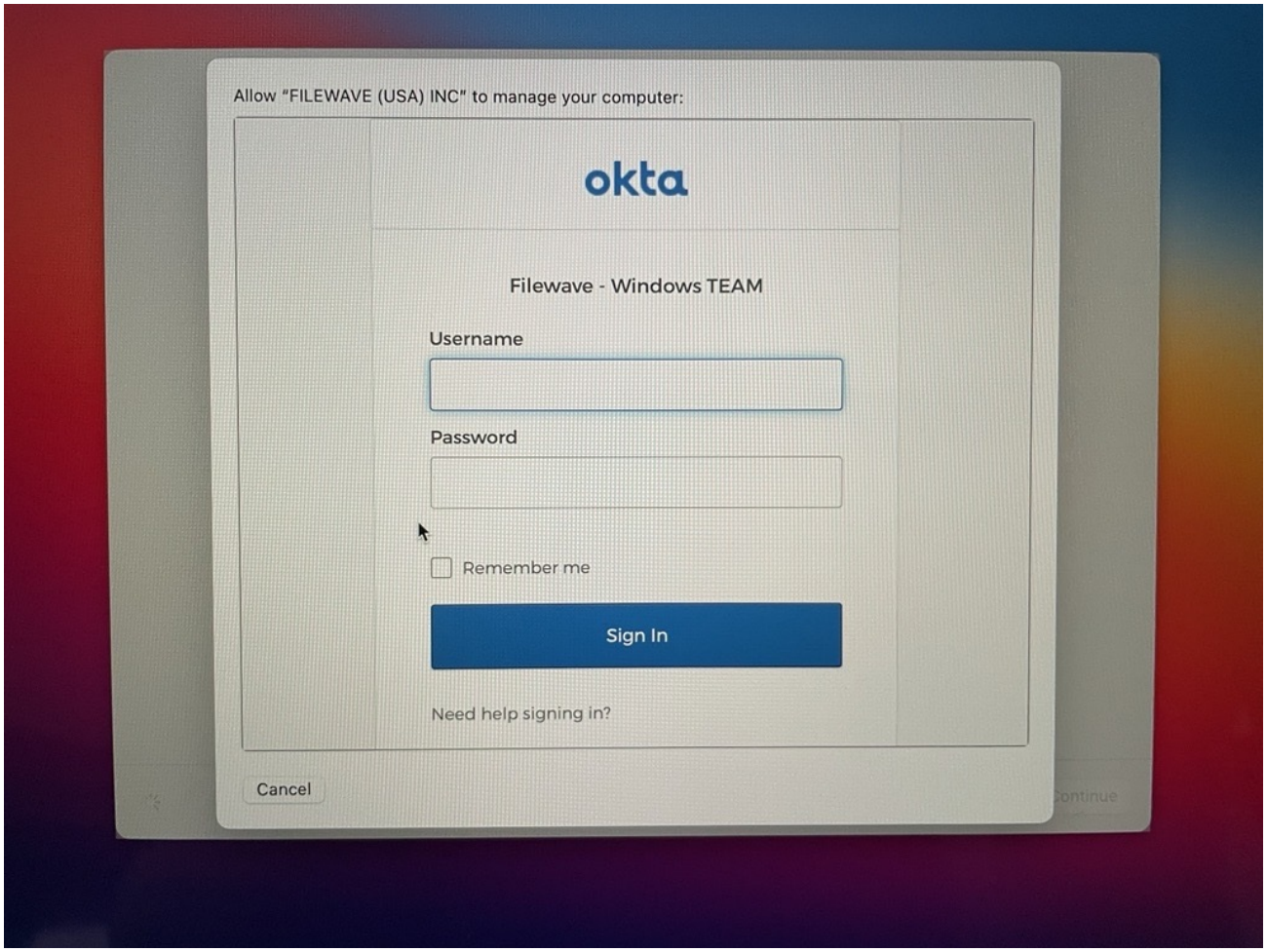


Once configured, you'll notice your devices will begin prompting for IDP authentication at enrollment time.

Known Issue

With Okta integration for macOS DEP enrollment there is a known issue with the initial load of the login window. You will see that window appear with what looks like a bad page load, which is basically correct. If you right-click, reload this page, it will load correctly. (See below). Note that this issue will be resolved in an upcoming revision.





Related Content

- IdP Setup: Google
- IdP Setup: Azure AD
- IdP Setup: Okta
- Admin Login in Using an IdP Provider

Admin Login in Using an IdP Provider

What

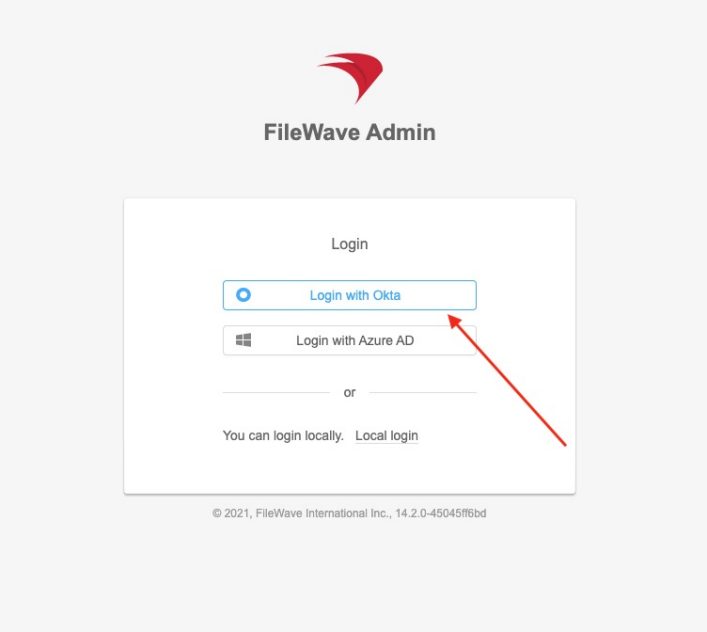
You'll notice some new options now for login once an IdP provider is specified.

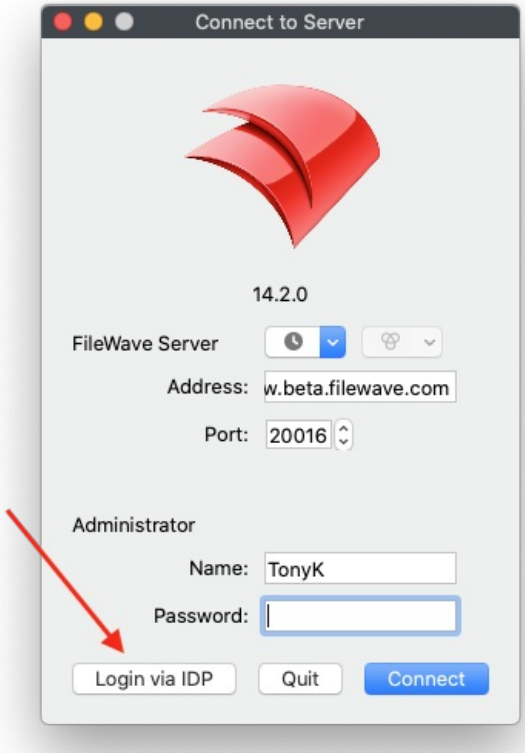
When/Why

We'll want to use these new options whenever we want to login using IdP credentials.

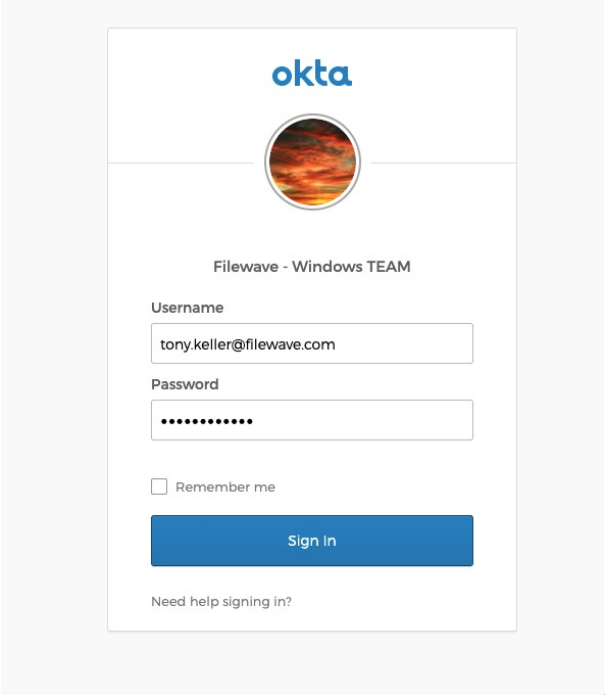
How

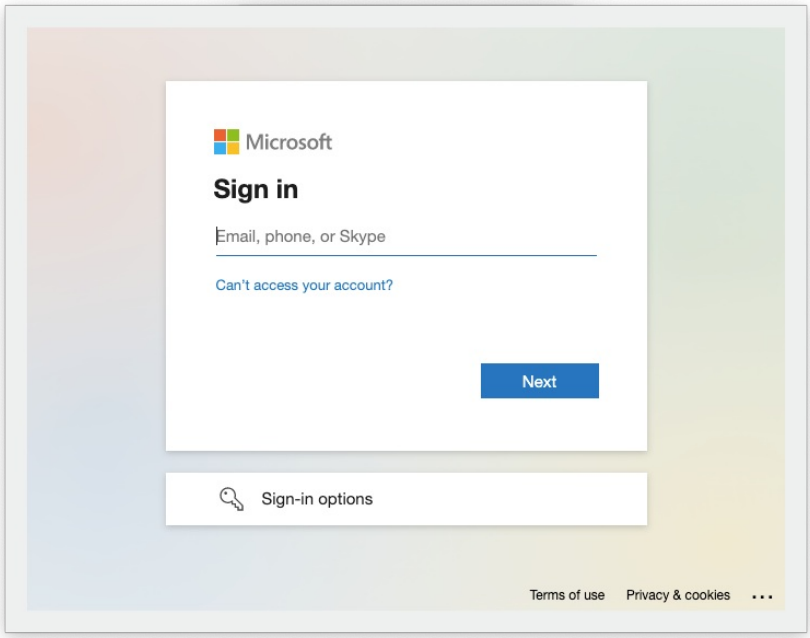
In both the Anywhere and Central admins, you just have to click a button to login in the alternate manner:





And, in both cases, you'll be prompted for the IDP's login information





Logging in and out with an IdP isn't the same in the web admin as a "local" account. If you have other sessions open with your IDP credentials, you'll find that you authenticate straight through. And, "logout" of the FileWave Admin does not log you out of other IdP related web sessions.

Related Content

- IdP Setup: Google
- IdP Setup: Azure AD
- IdP Setup: Okta
- Configuring DEP Profiles for IDP Authentication
- Adding IdP Groups for FileWave Authentication

IdP for Deployments and Smart Groups

What

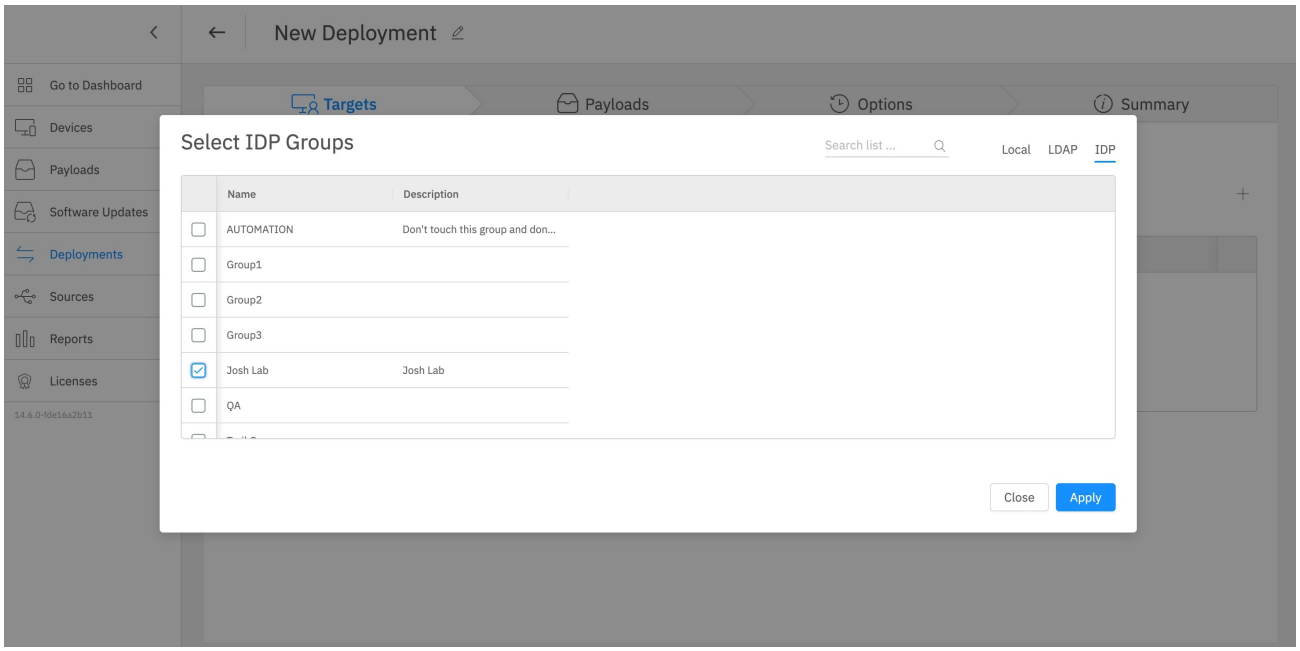
As a FileWave administrator using IdP enrollment of devices, I need to report on what groups devices are a part of in order to report on them and target software.

When/Why

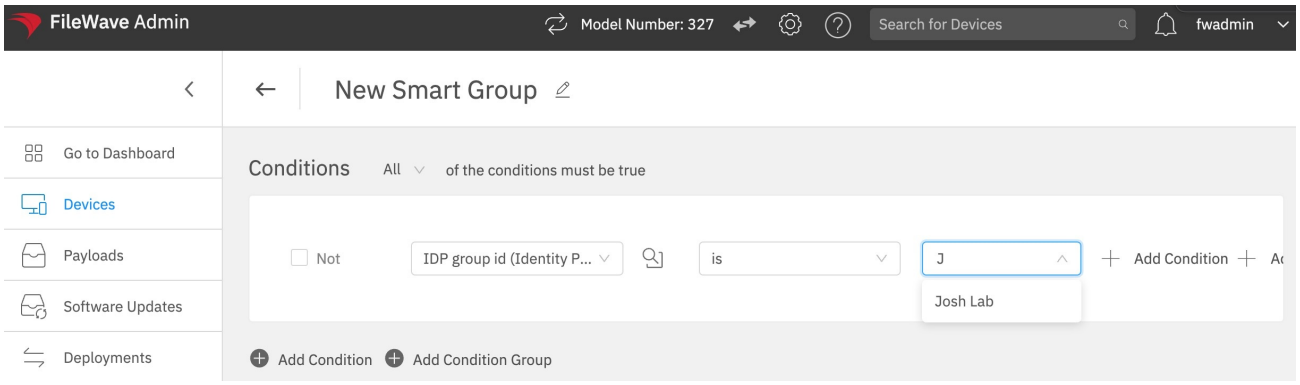
There is a new field that is populated which you can use for targeting deployments in the Web Admin, and for reporting queries both in Web Admin and the Native Admin.

How

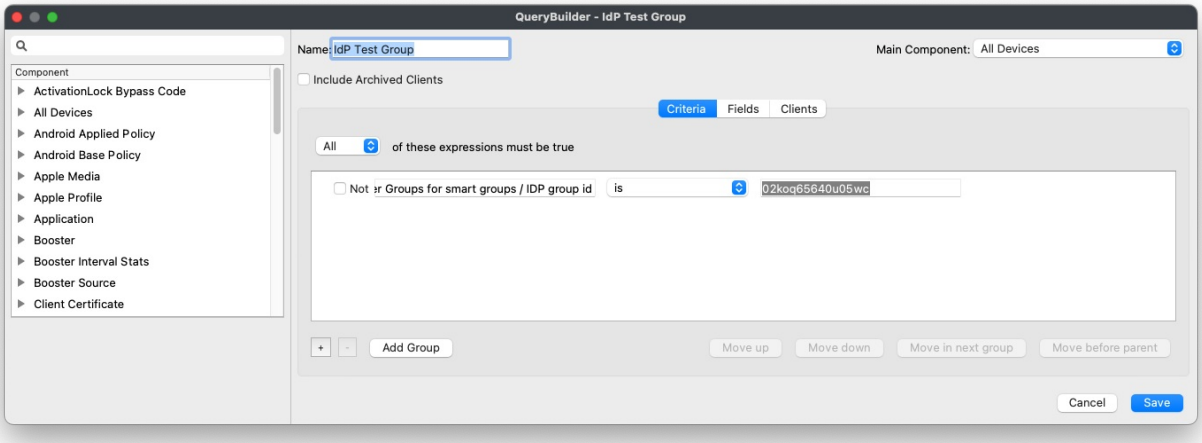
When making deployments in the Web Admin note the IDP selection on the top right. You can then see the groups that come in from the IdP connection.



And here is what can be used in Queries both in Native and Web Admin where the IDP group id would be the most likely used field. As you can see below you can start to type a group name and if it exists then the group name will appear below the text field. In this case, Josh Lab is a group in Google.



And if you choose to edit a smart group like this in the native admin, you'll see that what is actually saved by this is the group id:


QueryBuilder - IdP Test Group
Component
ActivationLock Bypass Code
All Devices
Android Applied Policy
Android Base Policy
Apple Media
Apple Profile
Application
Booster
Booster Interval Stats
Booster Source
Client Certificate
Name IdP Test Group
Main Component: All Devices
Include Archived Clients
Criteria
Fields
Clients
All
of these expressions must be true
Not
r Groups for smart groups / IDP group id
is
02koq65640u05wc
Add Group
Move up
Move down
Move in next group
Move before parent
Cancel
Save

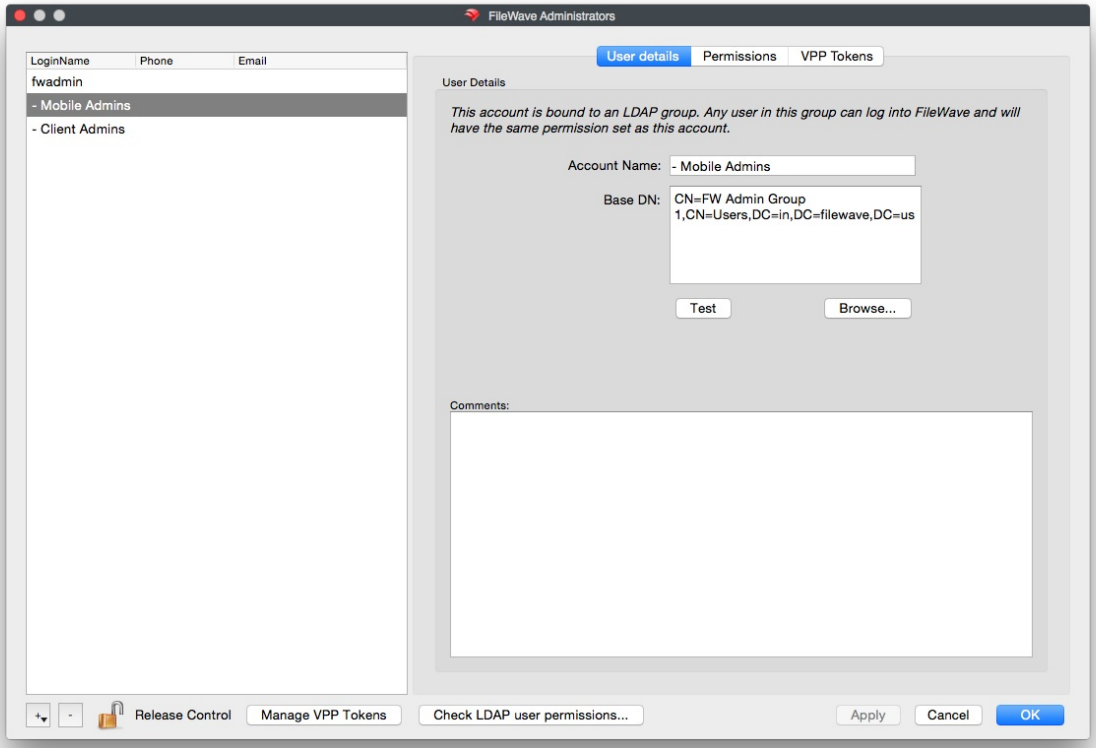
LDAP Admin Integration

This document will walk you through the process of integrating your LDAP admin accounts into the FileWave Admin. This will allow you to log into the FileWave Admin Console as an admin account located in your AD, OD, or eDir environment. Keep in mind only Active Directory is able to detect recursive membership. FileWave will not be able to detect nested groups in an Open Directory or eDirectory LDAP directory.

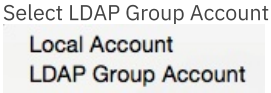
Please note: This guide is not a replacement for the manual, and assumes you have already setup your FileWave Management Server. This document also assumes that your FileWave server has the LDAP section in the preferences filled out and connecting properly.

Steps for setup:

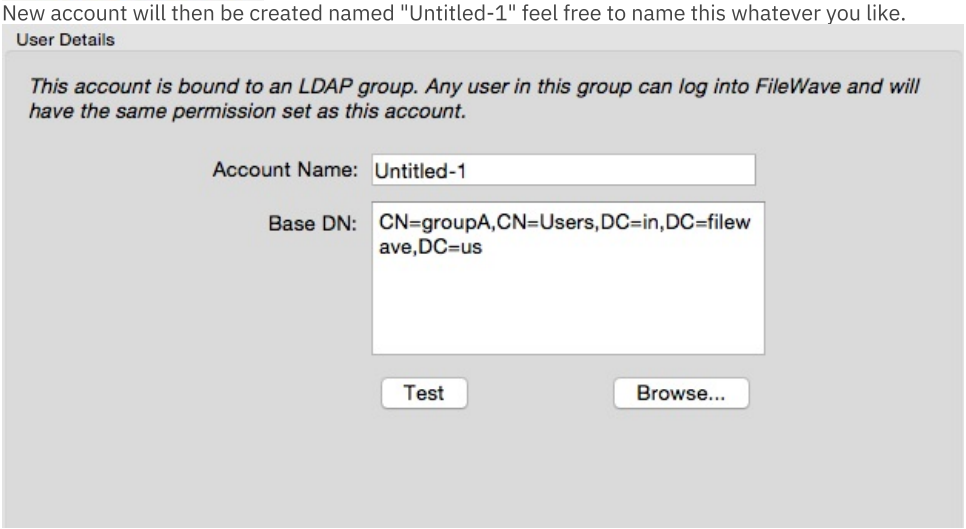
1. Open the FileWave Administrators window by navigating to the Assistants menu, and then selecting Manage Administrators. Once in the FileWave Administrators window, hit the "+" button at the button left of the window.



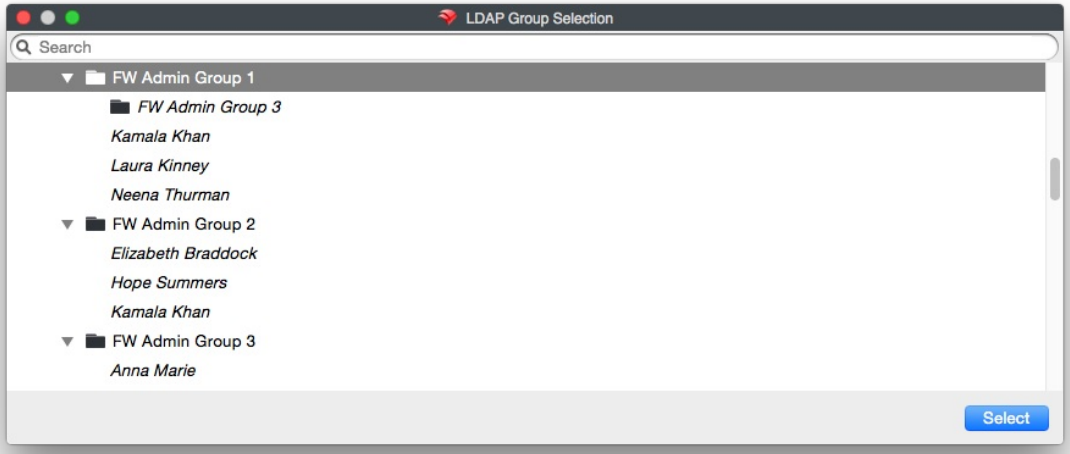
2. Select LDAP Group Account



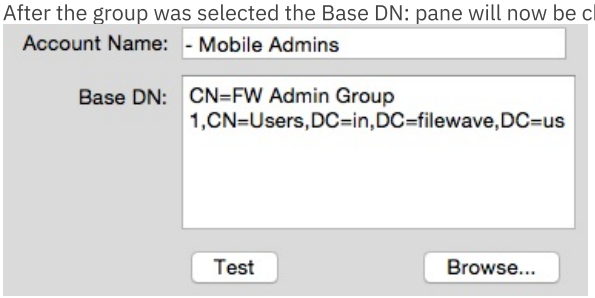
3. New account will then be created named "Untitled-1" feel free to name this whatever you like.



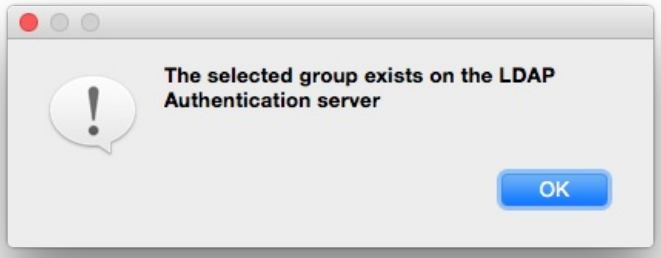
4. Once you have named your account, locate and click the Browse... button at the bottom right of the Base DN: pane
5. You will now be prompted with the LDAP browser where you can now find and hit Select for the group you want to associate. This will associate all the users in your specified group. As an added feature, most Active Directory environments also allows other groups, which are a members of the group you selected to, be included. This allows users in those "sub-groups" to be associated as well.



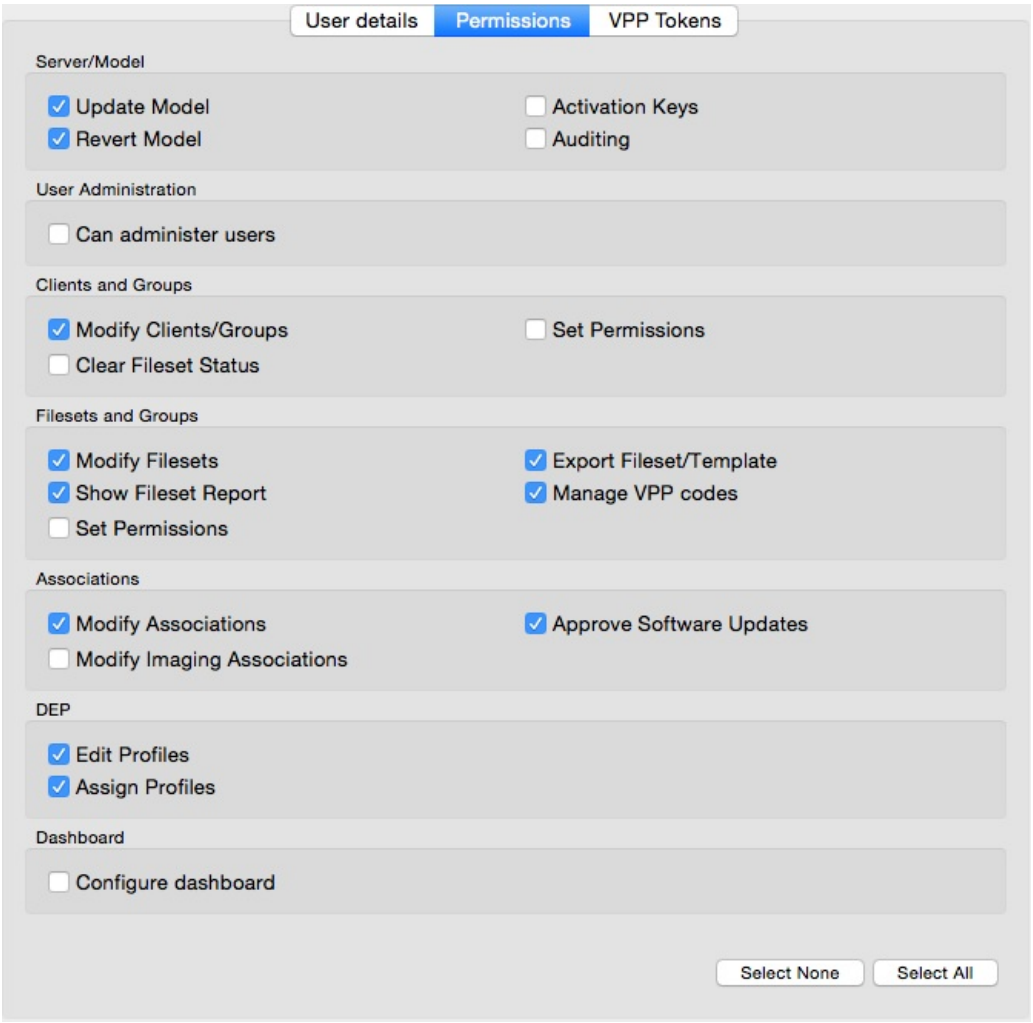
6. After the group was selected the Base DN: pane will now be changed to the DN of the group



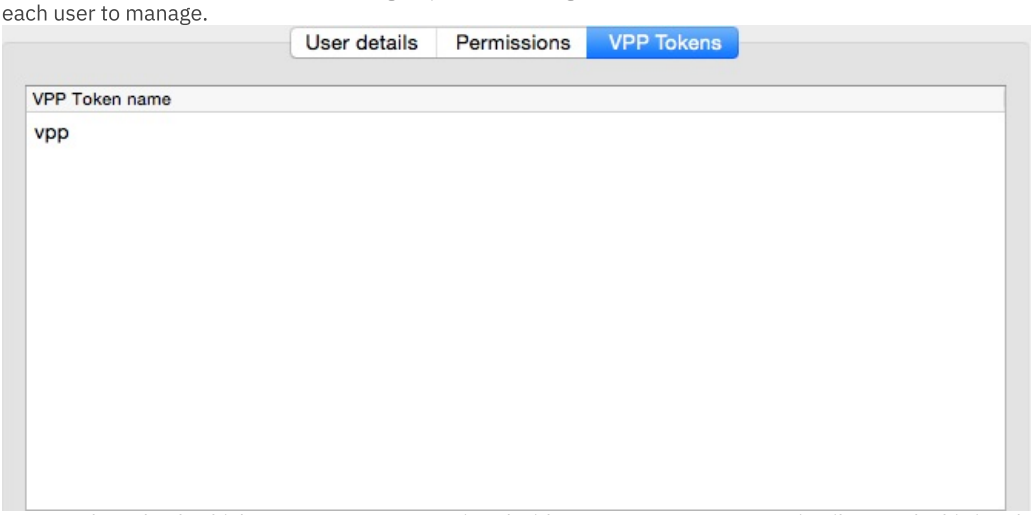
7. Hitting the Test button at this point will tell you if the selected group exists or not on the LDAP server.



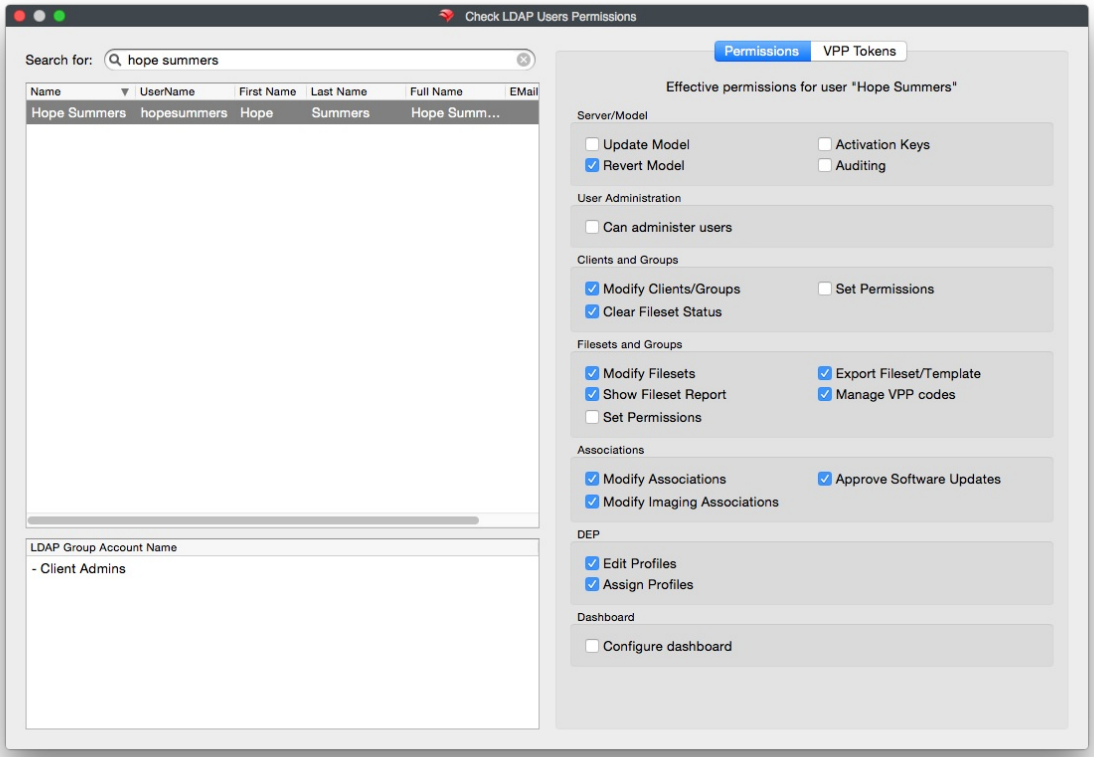
8. The next step is to create the permissions you would like every user in the group you added from LDAP to have in FileWave.



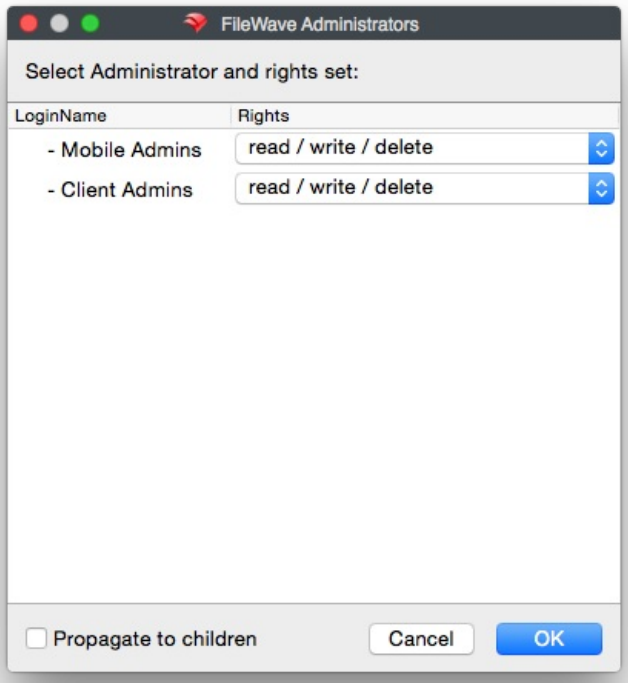
9. The final tab is called VPP Tokens. These will be the VPP Tokens that this group of users can manage in FileWave. To add or remove VPP token access for users and groups, click Manage VPP Tokens, and hit the check box for each token you want each user to manage.



10. You can then check which LDAP users are associated with an LDAP Group Account in FileWave by hitting the "Check LDAP Permissions..." button at the bottom of the window.
11. In the "Check LDAP User Permissions..." window, simply type the account you would like to find into the search bar in the top left of the window. Once you hit enter, locate the account you want, and select it. You will see the LDAP Group Account name in the bottom left hand pane, and the permissions the account has in FileWave on the right.
Please Note: If you have one account in multiple groups and it gets into more than one LDAP Group account in FileWave, they will receive the cumulative permissions of those groups.



12. Now that you have completed the setup of these groups and accounts, you can now assign permissions throughout FileWave for what the accounts can manage regarding Filesets and Client, group and objects. Simply find your object or group (both standard or smart groups), right click then select Select Permissions.



Congratulations! You have now integrated your LDAP Admins into FileWave!

Troubleshooting

Directory data syncronization between IdP and FW is not supported

At this time, FileWave IDP integration is limited to only FileWave Admin authentication and Apple device enrollment. Directory data synchronization (and custom fields) between the IdP source and FileWave is not supported at this time, but will be added in a future release. In the meantime, current LDAP(S) synchronization can be used as a stop-gap to achieve the same result.

IdP Redirection URL change (15.5.1+)

What

In FileWave 15.5.1 there was a change to the redirection URLs used for an IdP setup in FileWave so that the 3rd URL would use port 20443 instead of the usual 443 for HTTPS.

When/Why

In FileWave 15.5.1 we wanted to account for servers where port 443 was not exposed to the Internet but where clients would enroll via an IdP so a change in port had to be made. All of the setup documentation was updated, but if you setup your server in the past then you may need to update the URLs within your IdP.

How

Review the IdP setup article for the platform you use (links below in Related Content) and ensure that you check that the 3rd redirect URL is using 20443 instead of 443 or it may have no port listed at all prior to FileWave 15.5.1.

FileWave 15.5.1 and newer looks like this for the URL in question;

https://FWXSERVER:20443/auth/login_via_idp_redirect_for_device

FileWave earlier than 15.5.1 would have had the same URL but it would not have had the port or it would have listed 443;

https://FWXSERVER:443/auth/login_via_idp_redirect_for_device

You will find the proper URL for your setup if you review the IdP setup and repeat the step where you copy URLs from your FileWave Server. The other 2 URLs are on port 443. For best results always copy the URLs from FileWave Anywhere as the instructions show so that you get the URL as it should be for your actual server.

Related Content

- IdP Setup: Google
- IdP Setup: Keycloak
- IdP Setup: Okta
- IdP Setup: Microsoft Entra ID (Azure)

Enrolling Apple devices why am I prompted for IdP login?

What

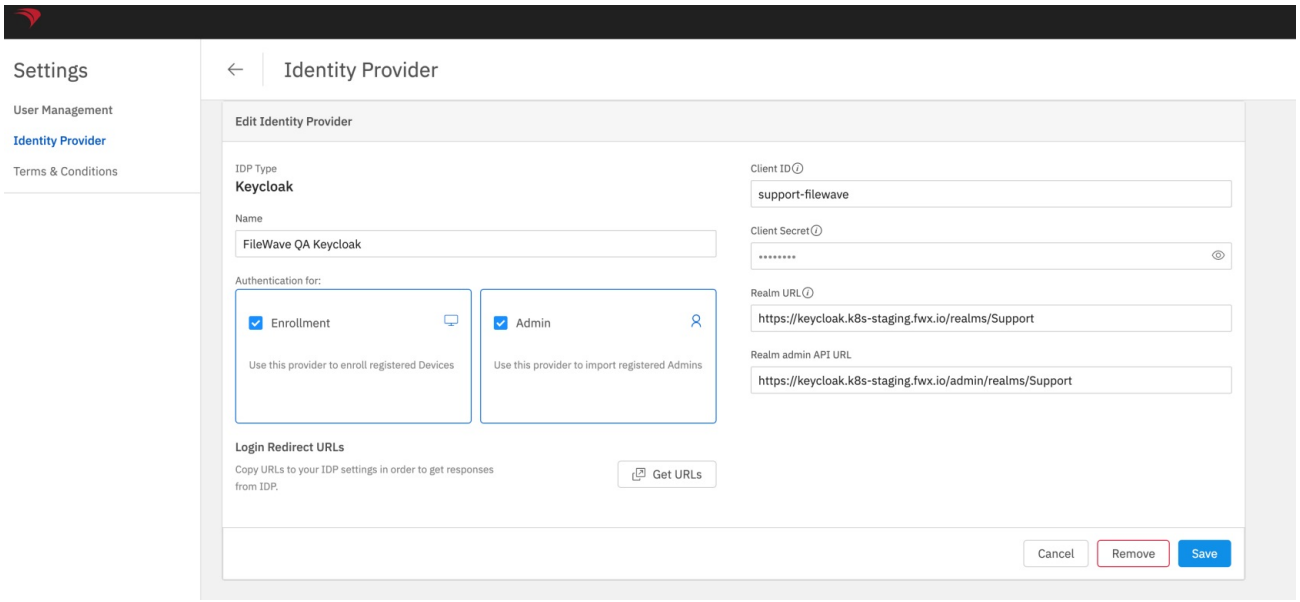
When I enroll a macOS, iOS or iPadOS device a pop-up shows asking me to login to Google, Keycloak, Okta or Microsoft Entra ID (Azure) and I'm not sure why.

When/Why

This can happen if you setup an IdP in FileWave and enabled the "Enrollment" checkbox.

How

Login to FileWave Anywhere and go to Settings and edit your IdP configuration as seen in the image below. Uncheck Enrollment if you do not want this behavior. Conversely if you want to enable this behavior then go back and check the box.



Related Content

- IdP Setup: Google
- IdP Setup: Keycloak
- IdP Setup: Okta
- IdP Setup: Microsoft Entra ID (Azure)

Renaming Azure Active Directory (Azure AD) to Microsoft Entra ID

What

Microsoft has announced the renaming of Azure Active Directory (Azure AD) to Microsoft Entra ID. This name change aims to unify the Microsoft Entra product family, reflect the progression to modern multicloud identity security, and simplify secure access experiences.

When/Why

The name change is part of Microsoft's effort to streamline its identity and access management offerings. By renaming Azure AD to Microsoft Entra ID, Microsoft intends to provide a consistent identity security experience across its product lineup. This change aligns with the company's strategy to enhance secure access for education organizations, corporations, state and local government, and other customers.

How

No action is required from users who are currently using Azure AD or deploying it in their organizations. The service will continue to function without interruption, and all existing deployments, configurations, and integrations will remain unaffected.

Users can still access the familiar capabilities of Azure AD through the Azure portal, Microsoft 365 admin center, and the Microsoft Entra admin center. All features, capabilities, licensing, terms, service-level agreements, product certifications, support, and pricing will remain the same.

The new name for standalone offers will be Microsoft Entra ID Free, Microsoft Entra ID P1, and Microsoft Entra ID P2. However, the capabilities included in the current Azure AD plans will not change. Microsoft Entra ID will continue to be included in Microsoft 365 licensing plans, such as Microsoft 365 E3 and Microsoft 365 E5. More details on pricing and inclusions can be found on the pricing and free trials page.

The renaming does not impact the following:

- Microsoft Authentication Library (MSAL)
- Microsoft Graph
- Microsoft Graph PowerShell
- Windows Server Active Directory
- Active Directory Federation Services (AD FS) and Active Directory Domain Services (AD DS)
- Azure Active Directory B2C
- Any deprecated or retired functionality, feature, or service of Azure AD

Related Content

- Source: Microsoft Learn - Renaming Azure Active Directory (Azure AD) to Microsoft Entra ID