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

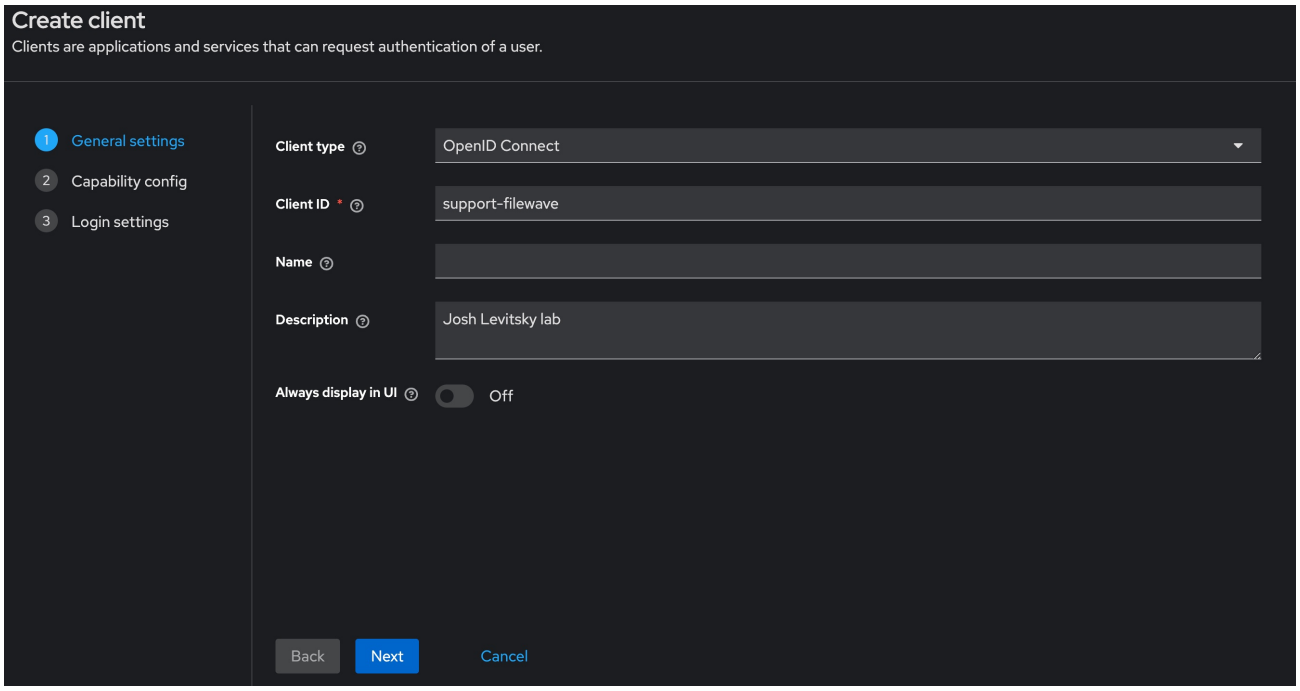
To begin you must have a Keycloak instance setup and have a Realm that you will be using with FileWave. If you already use Keycloak then this will be the case. A Realm is a container that will store all of your Keycloak things for an organization like Users, Groups and SSO Clients.

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

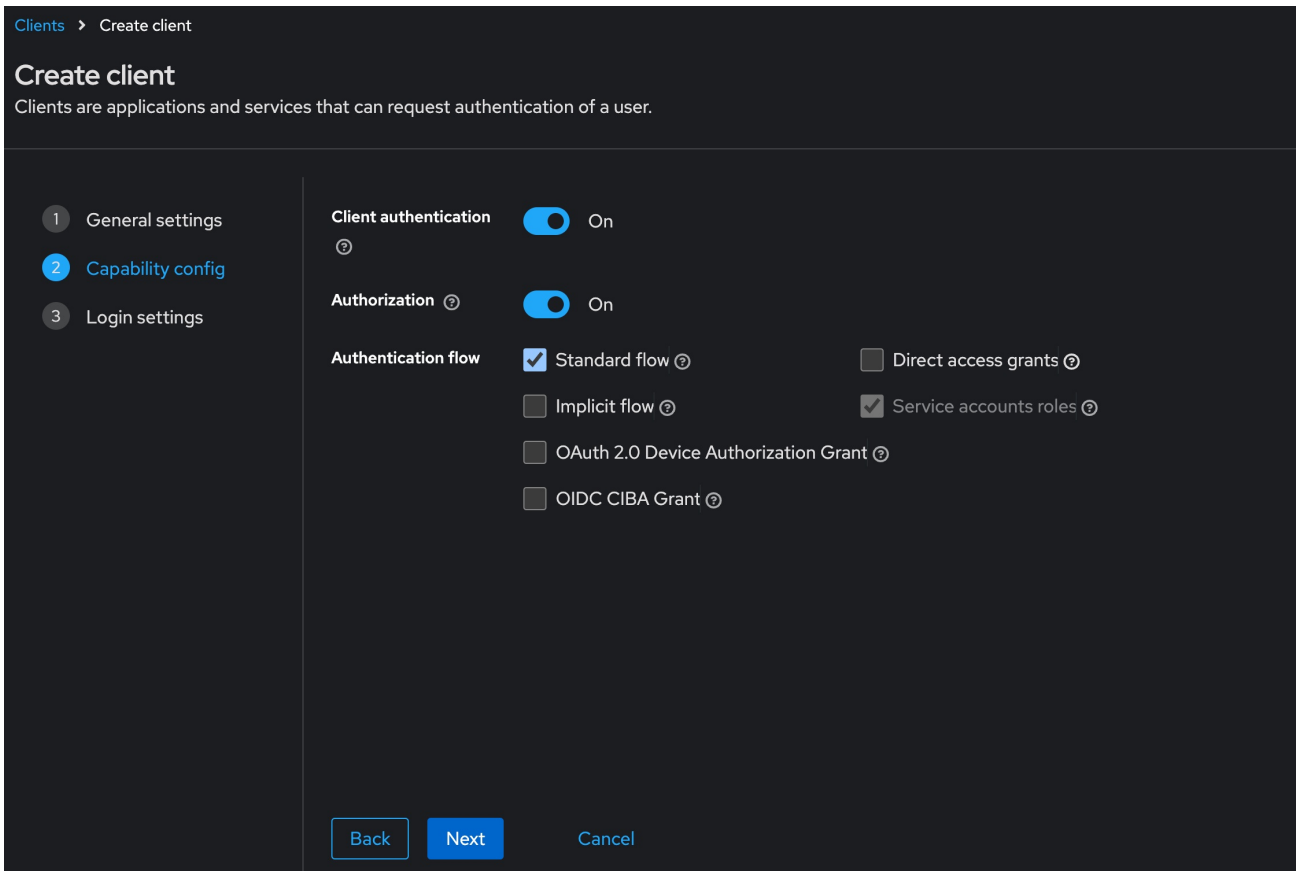
Select “Clients” in left menu bar and select “Create client” button

- 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

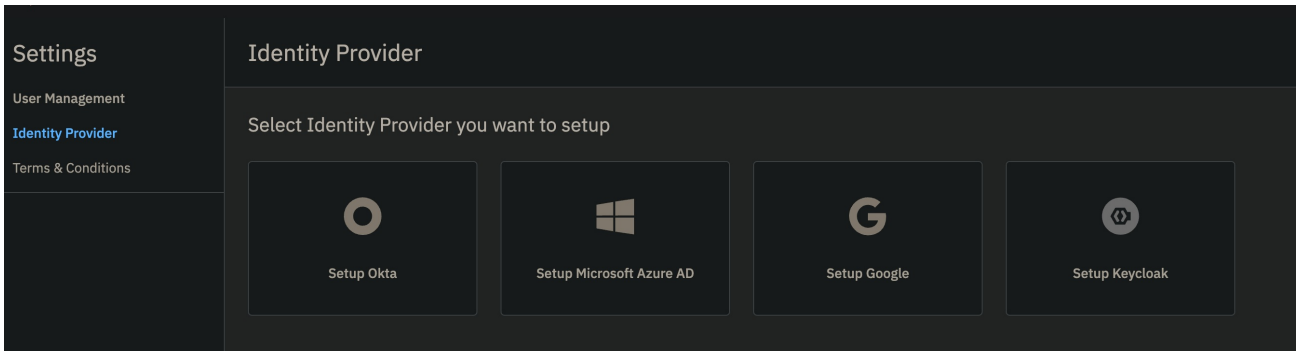


On the Capability config page:

- 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"



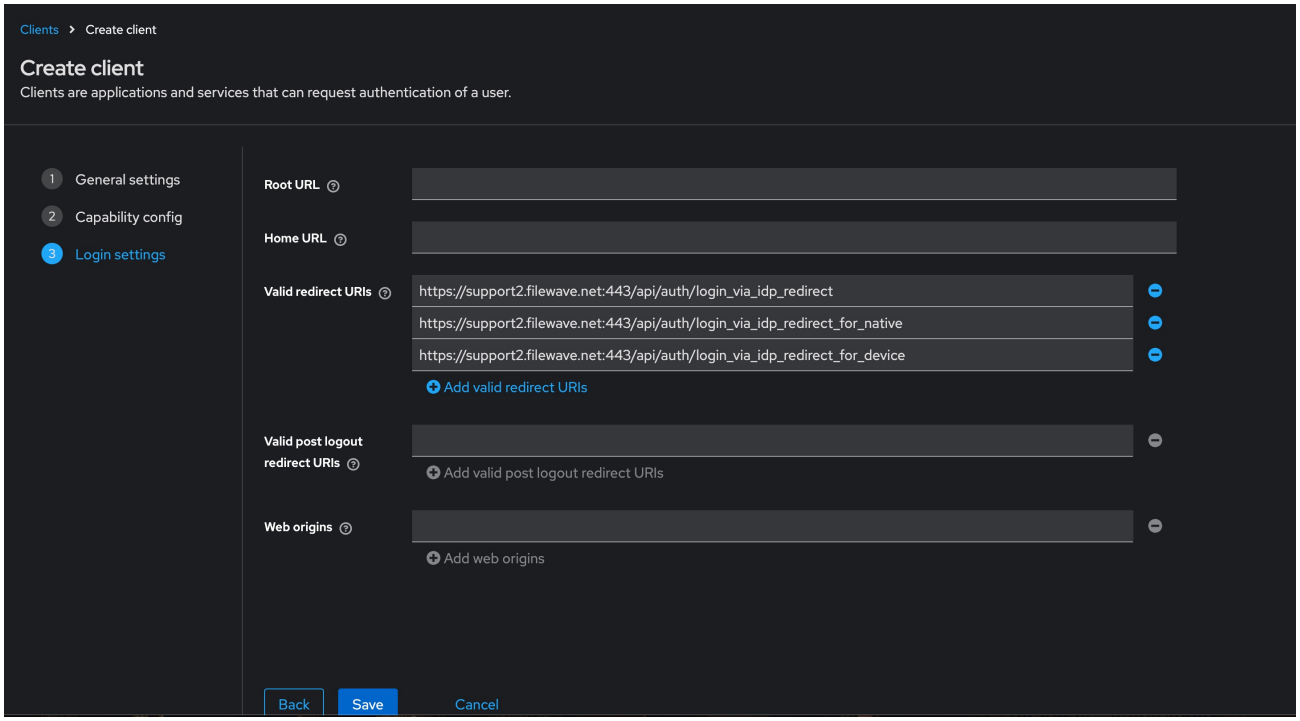
On the next page click "Get URLs" and get the 3 URLs which will look like the following but be for your FileWave instance:

```
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:443/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

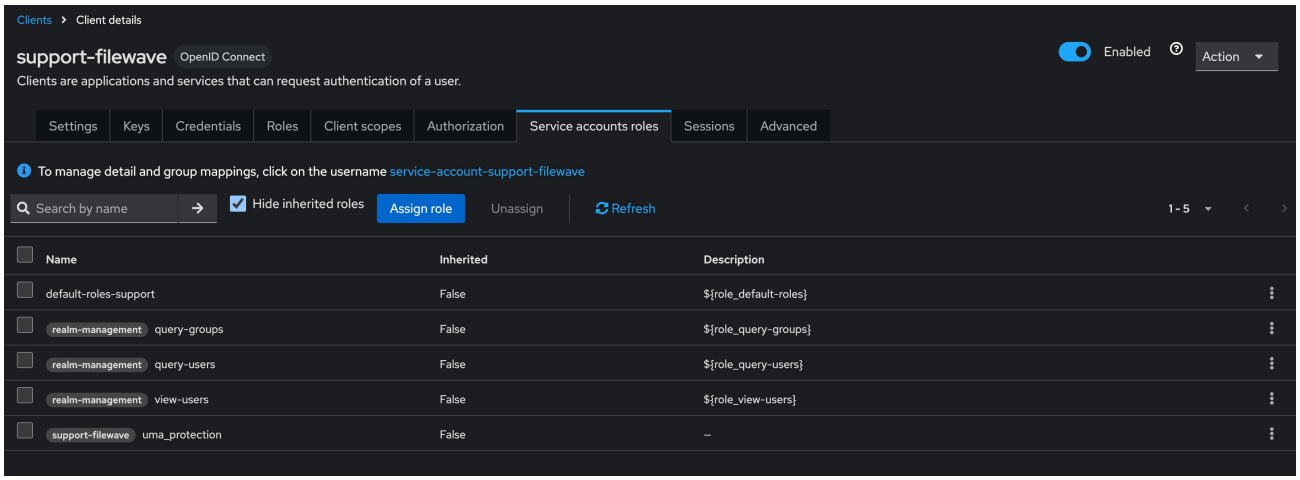


At this stage you should be looking at the details for the Client you just created in Keycloak but if it isn't you can:

- 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



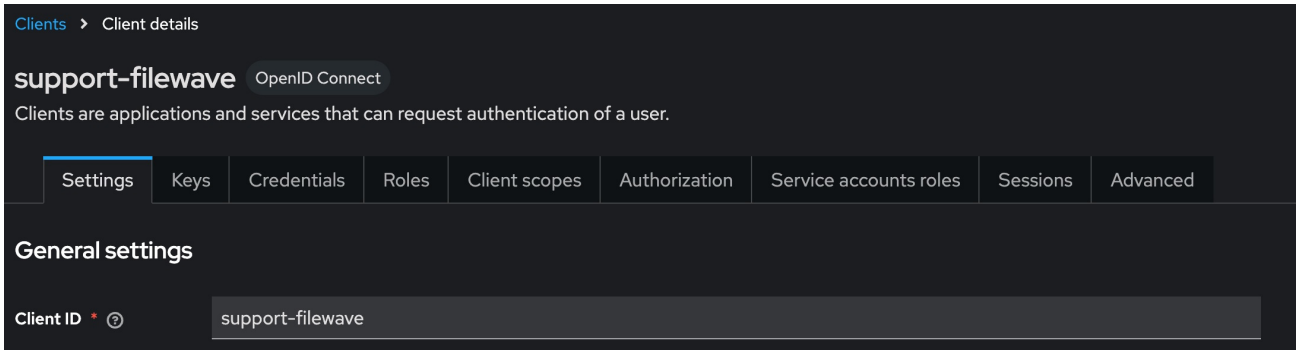
Obtaining the client ID and client secret

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.

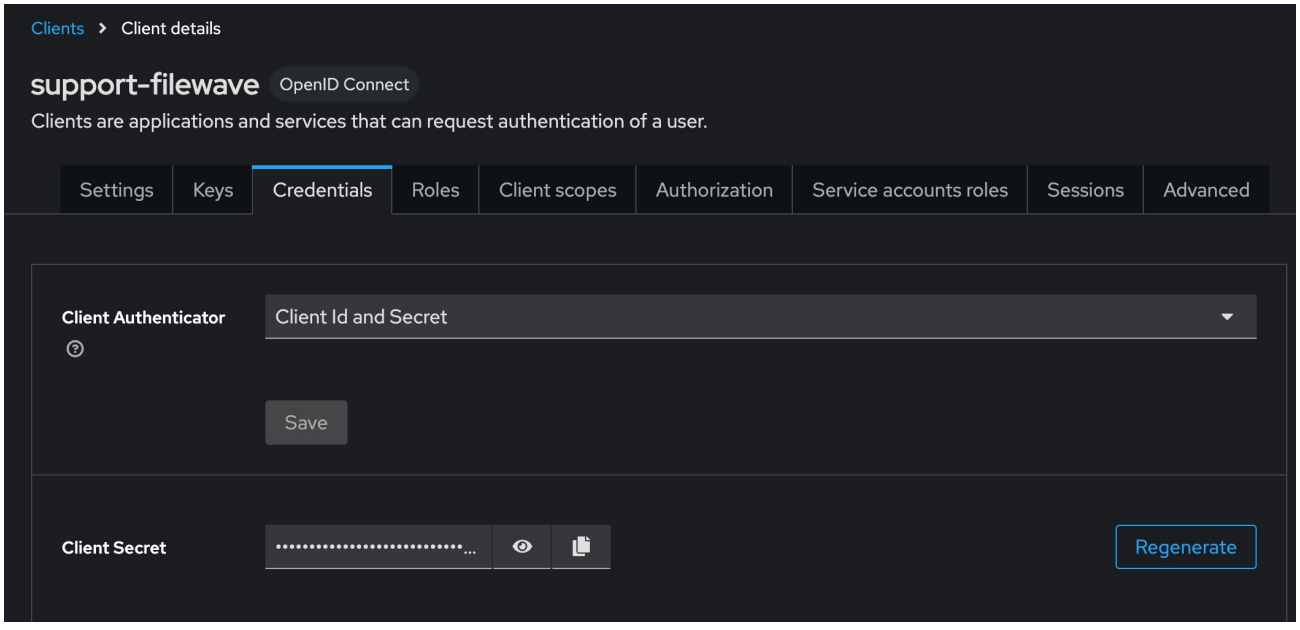
Now on the details for the Client you created click “Settings” tab on the top of the details page.

- Note the “Client ID”



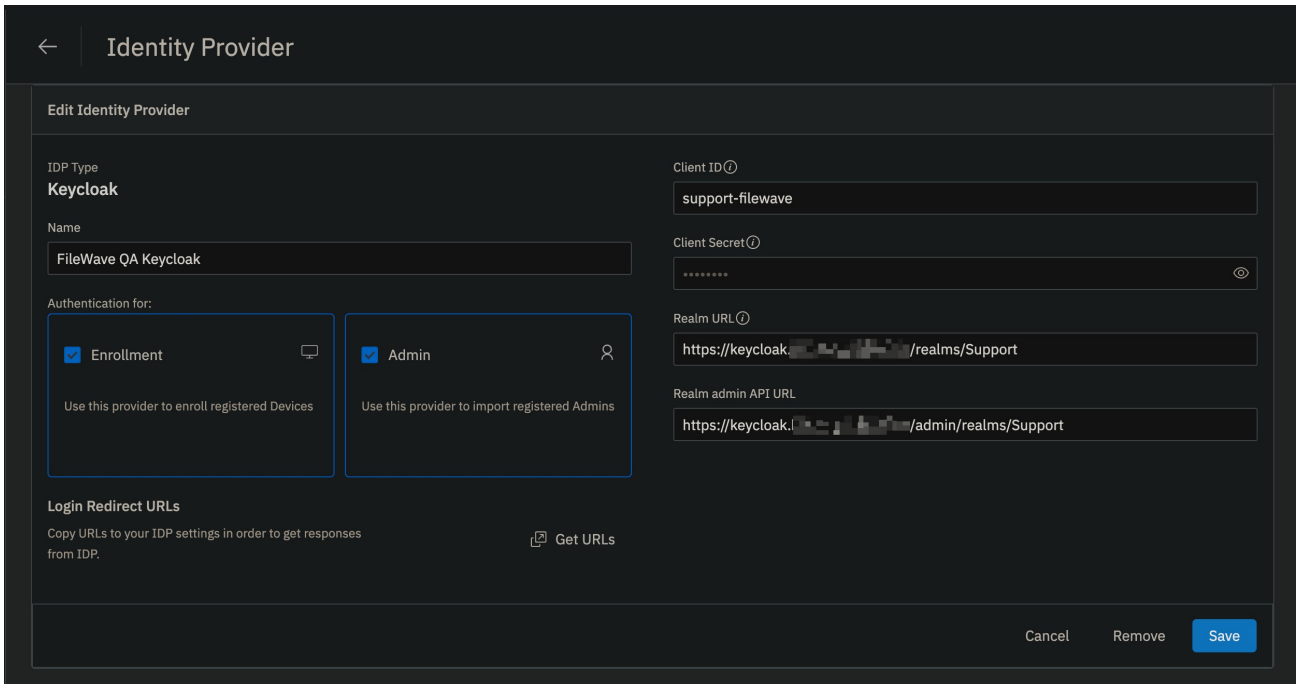
Now on the details for the Client you created click “Credentials” tab on the top of the details page.

- Note the “Client Secret”

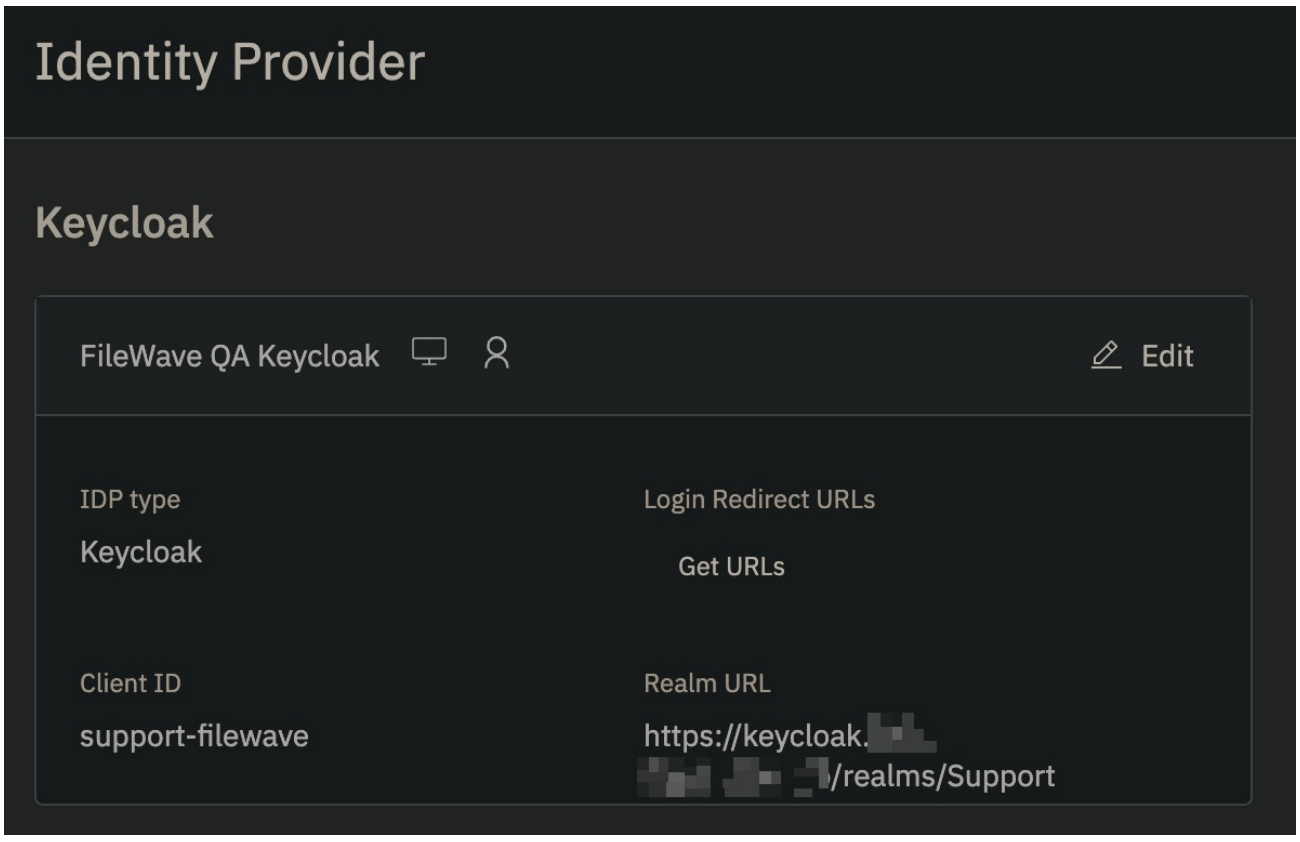


In this next step you are going to login to FileWave Anywhere again. Go back to the tab where you went to https://filewave.your_filewave_server.com replacing the host in the URL with your FileWave Server. If your prior session timed out then once logged in just click the gear icon on the top right of 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. Admin is for logins to FileWave Central and Anywhere. 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.

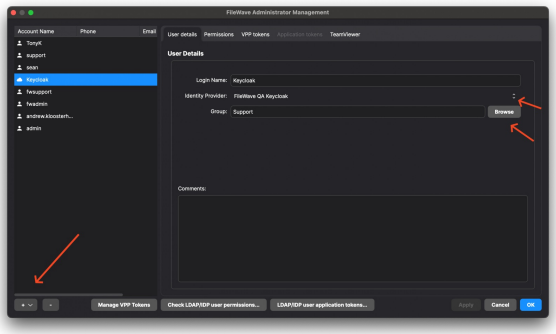
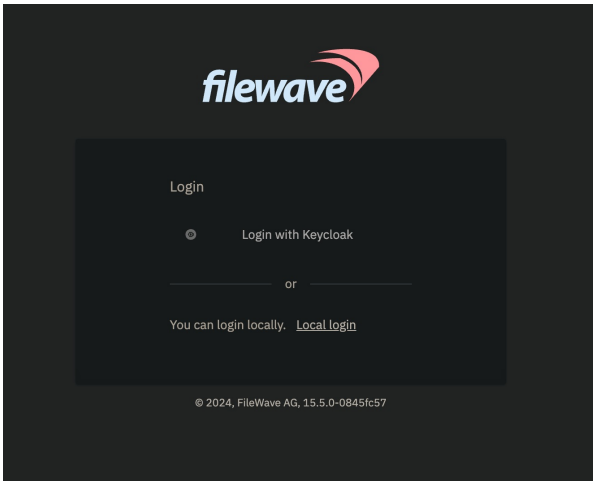


After clicking Create you should see the following if it was able to successfully reach Keycloak.



Configure 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

Revision #17
★Created 7 October 2024 13:31:29 by Josh Levitsky
Updated 4 November 2024 13:26:20 by Josh Levitsky