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

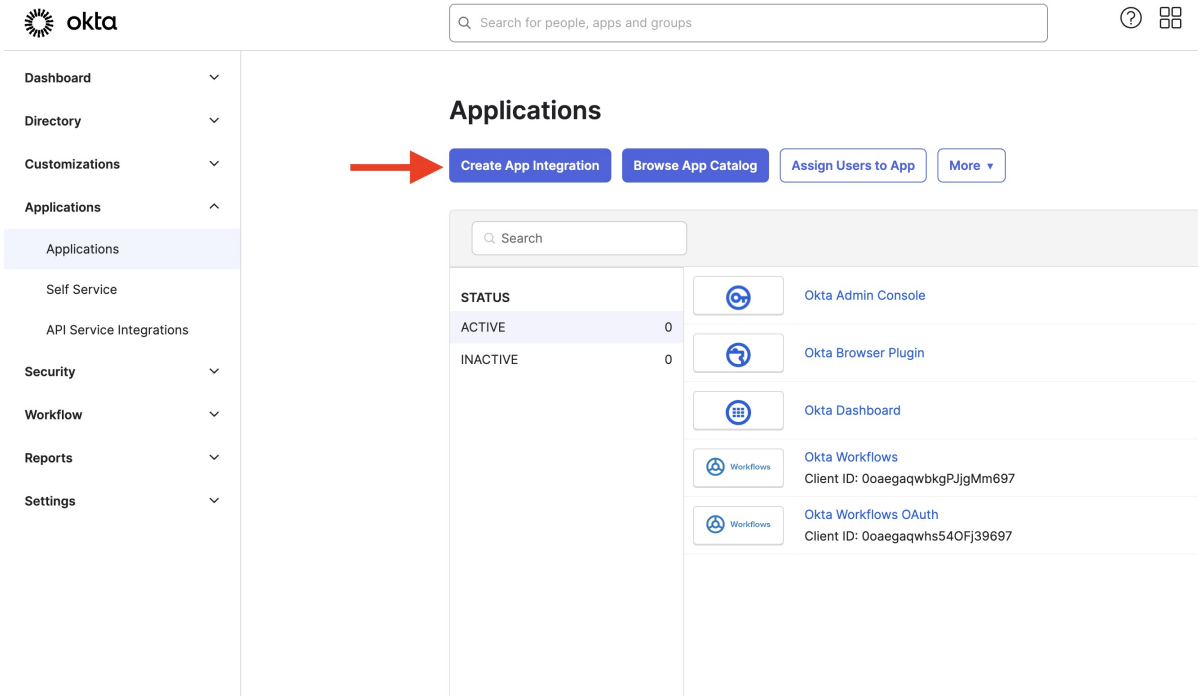
Begin by logging in to the Okta Admin Portal with an administrator's account. (https://example-admin.okta.com/admin)

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

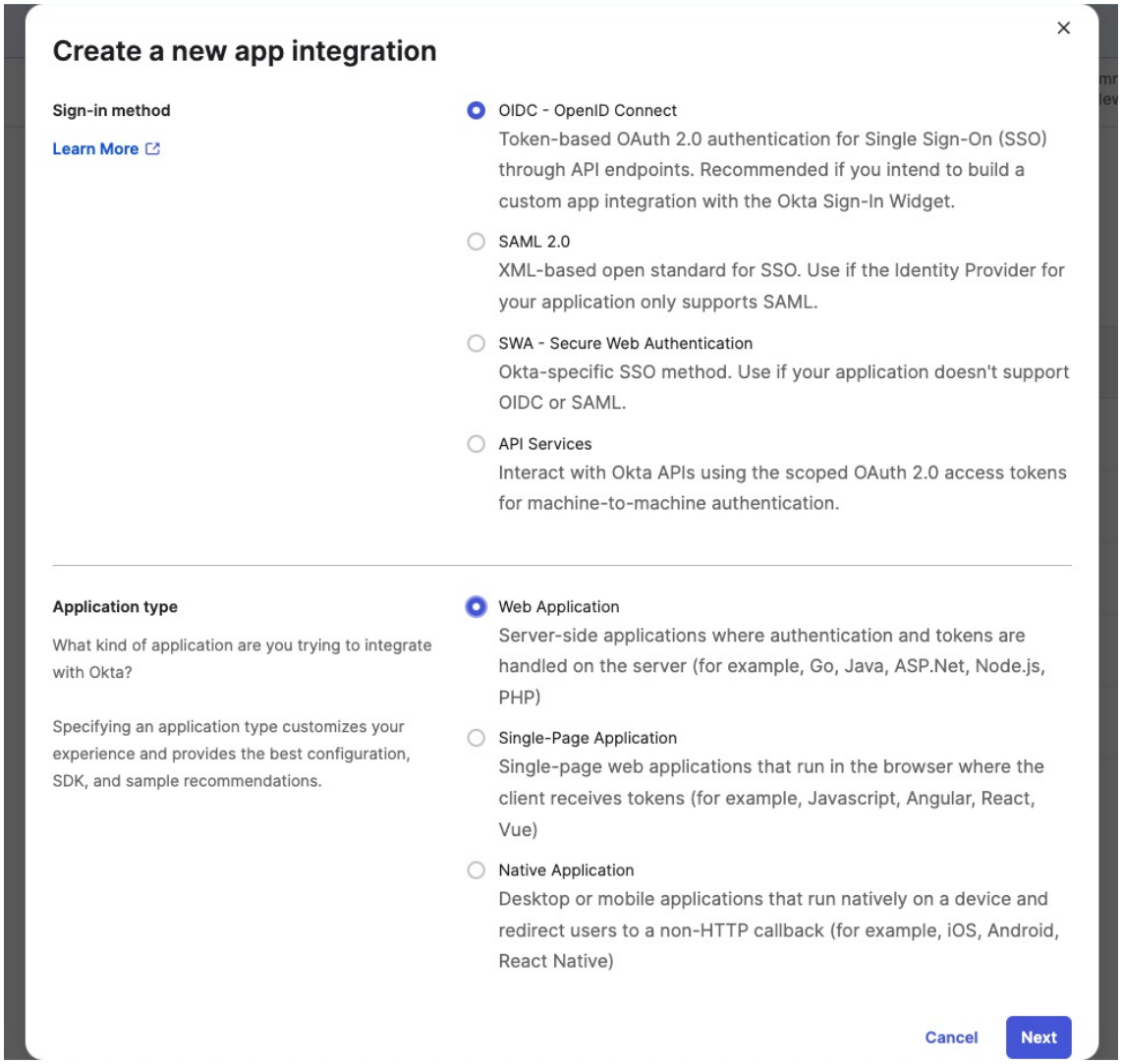
Create an Okta Application Integration in Okta Admin Portal

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.



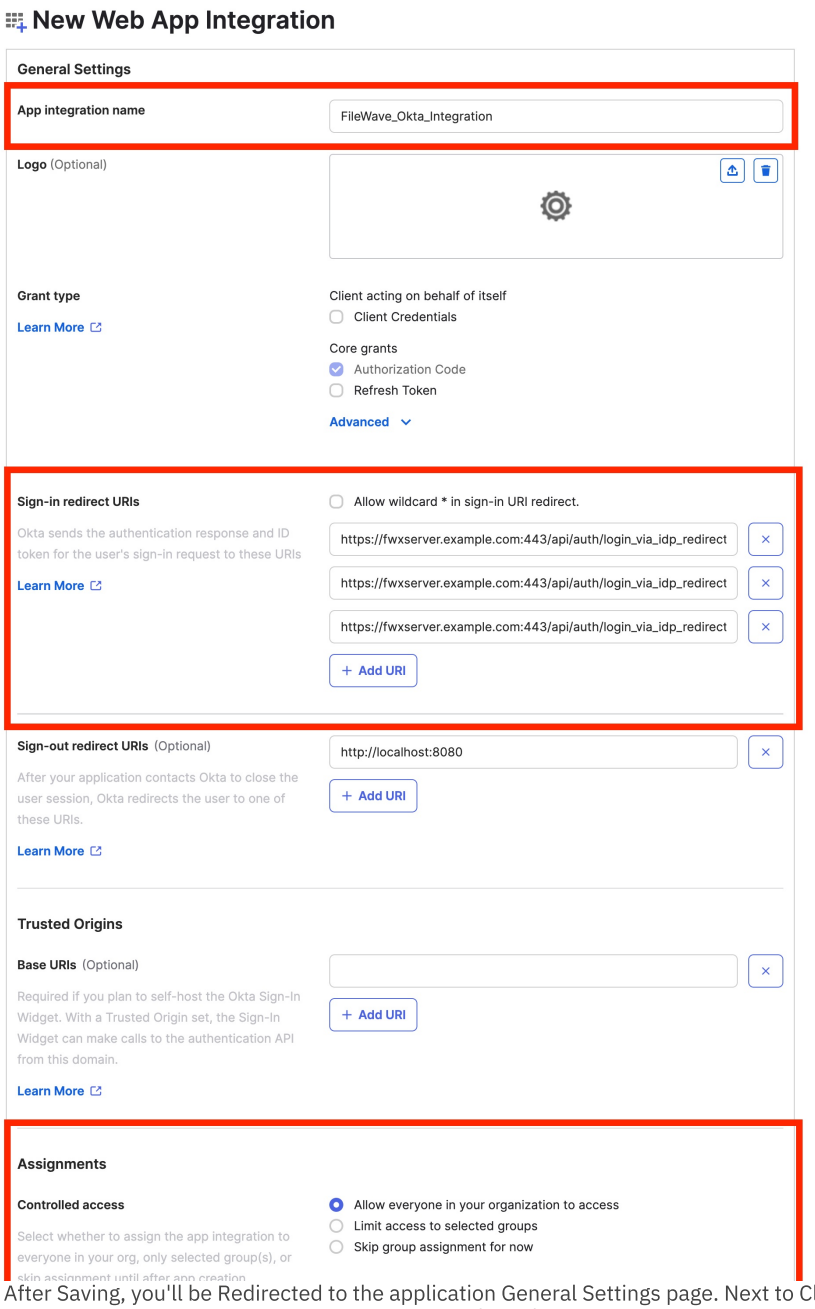
2. Next, select OIDC - OpenID Connect for the Sign-in method.
   1. Select Web Application for the Application Type.
   2. Click the Next button.



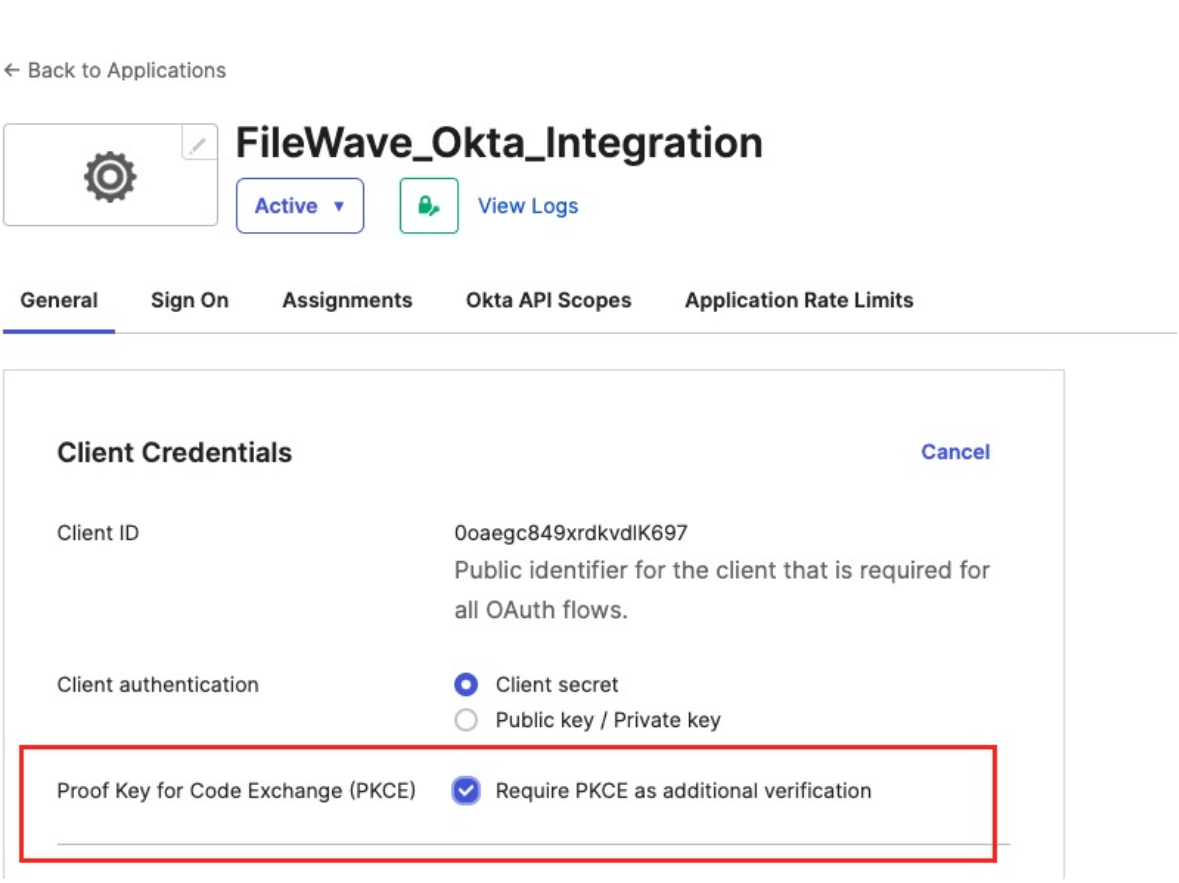
3. Next, configure your Application on the New Web App Integration page you've been redirected to.
    1. Input a meaningful name in the App integration name field.
    2. Click the Add URI button for the Sign-in redirect URIs setting.
        1. Input all of your FileWave Server's redirect URIs in the 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:443/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.



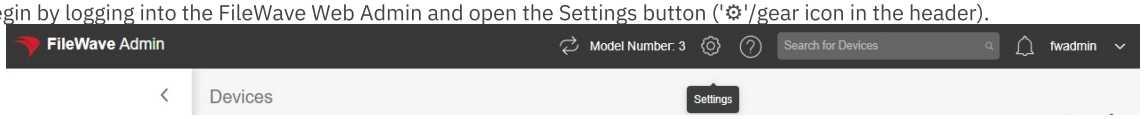
5. After Saving, you'll be Redirected to the application General Settings page. Next to Client Credentials, select Edit and check the box next to Proof Key for Code Exchange (PKCE) and Save.

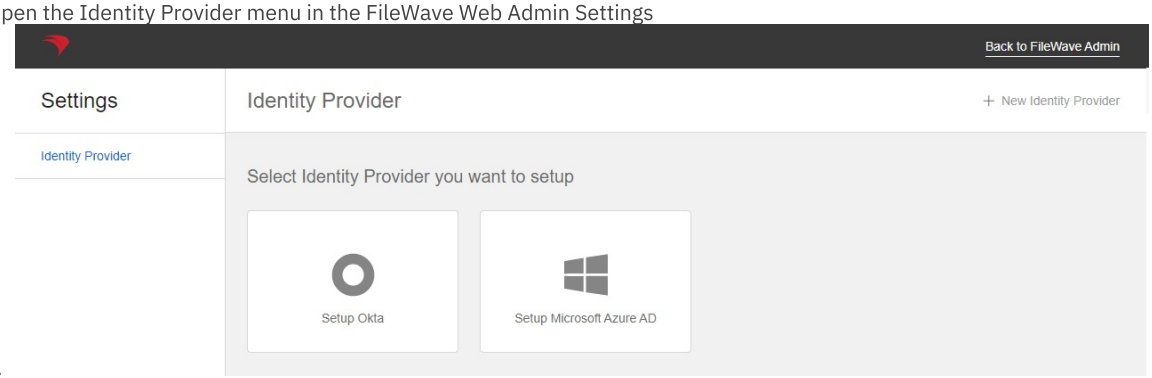


Part 3: Configure the Okta App in FileWave

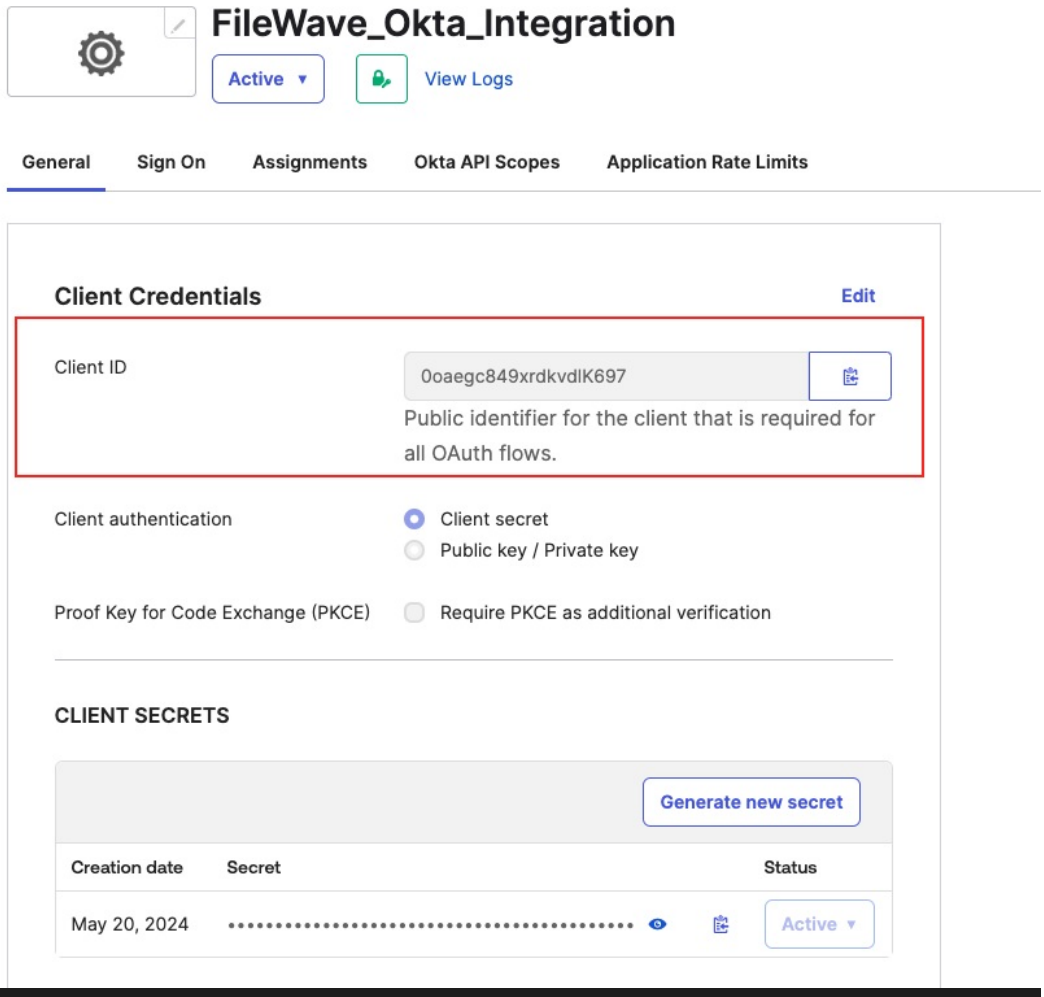
Configure an Okta App in the FileWave Web Admin Console

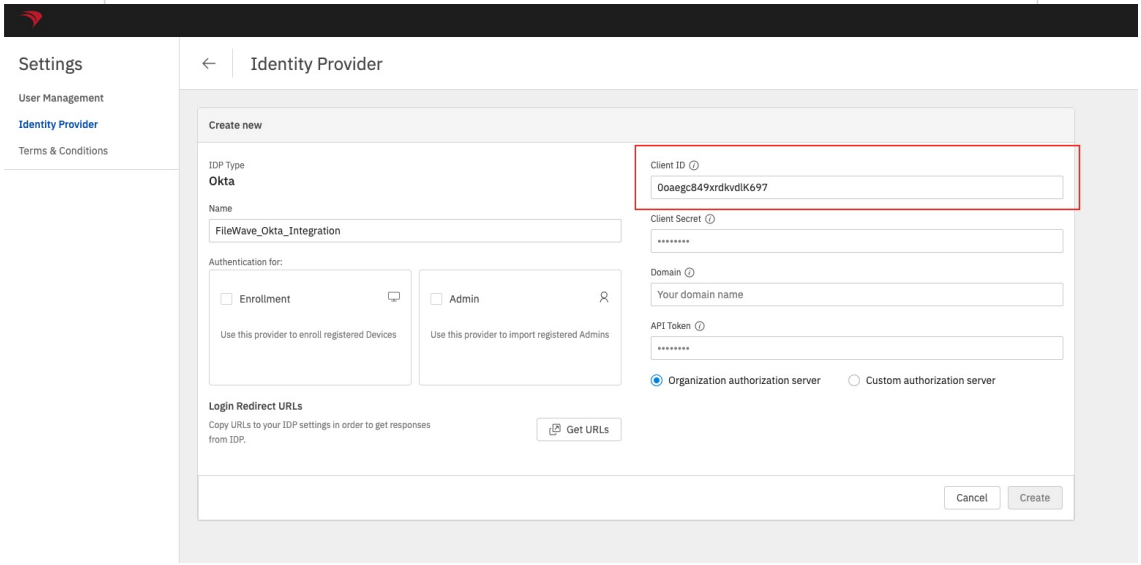
In order for FileWave to communicate with Okta for authentication the Okta App will need to be configured with FileWave.

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

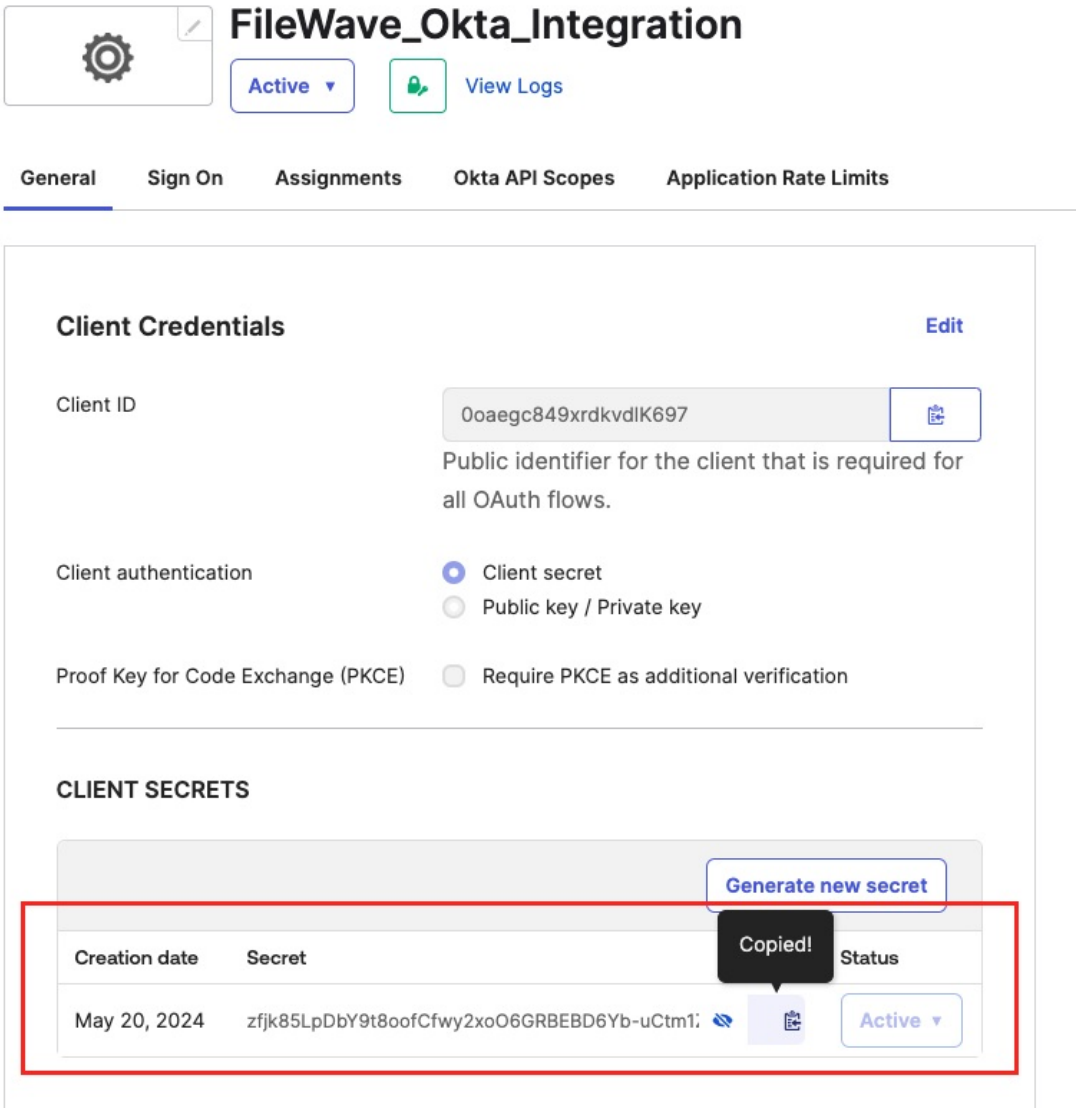
2. Open the Identity Provider menu in the FileWave Web Admin Settings
    1. 

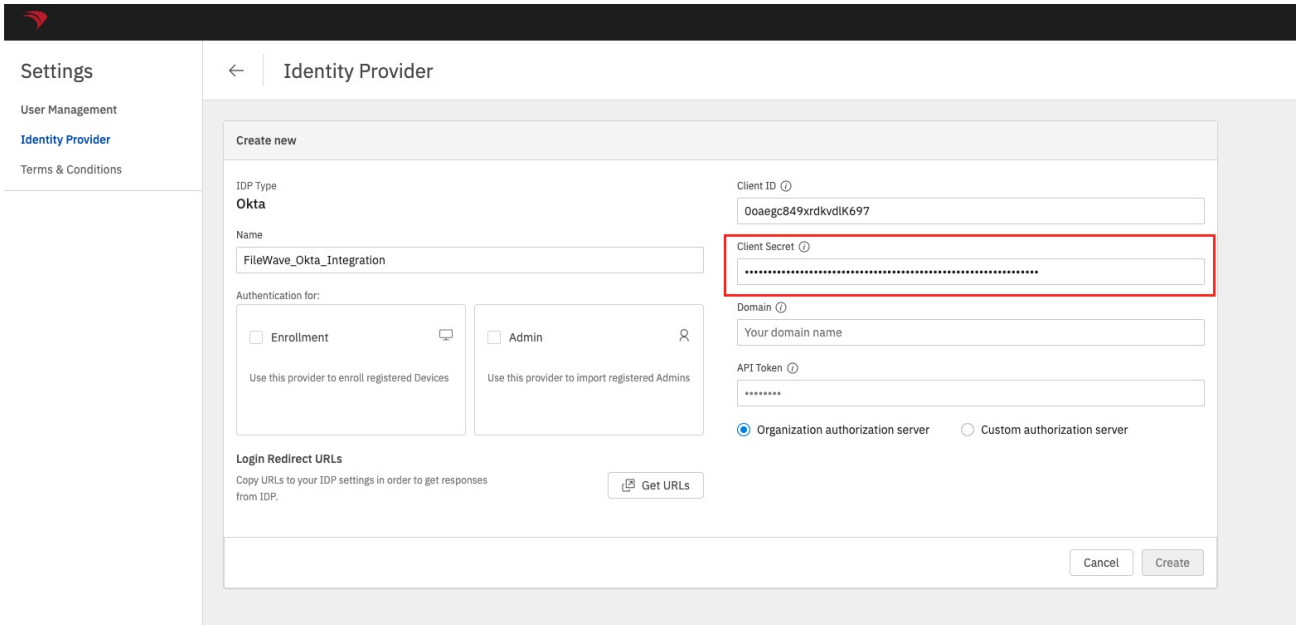
3. On the Identity Provider menu, click the Setup Okta button or New Identity Provider button in the top right if one has already been configured.
    1. Input a meaningful name in the Name field.
    2. Copy the Okta Client ID value found in the Okta page you were redirected to and paste in the Client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





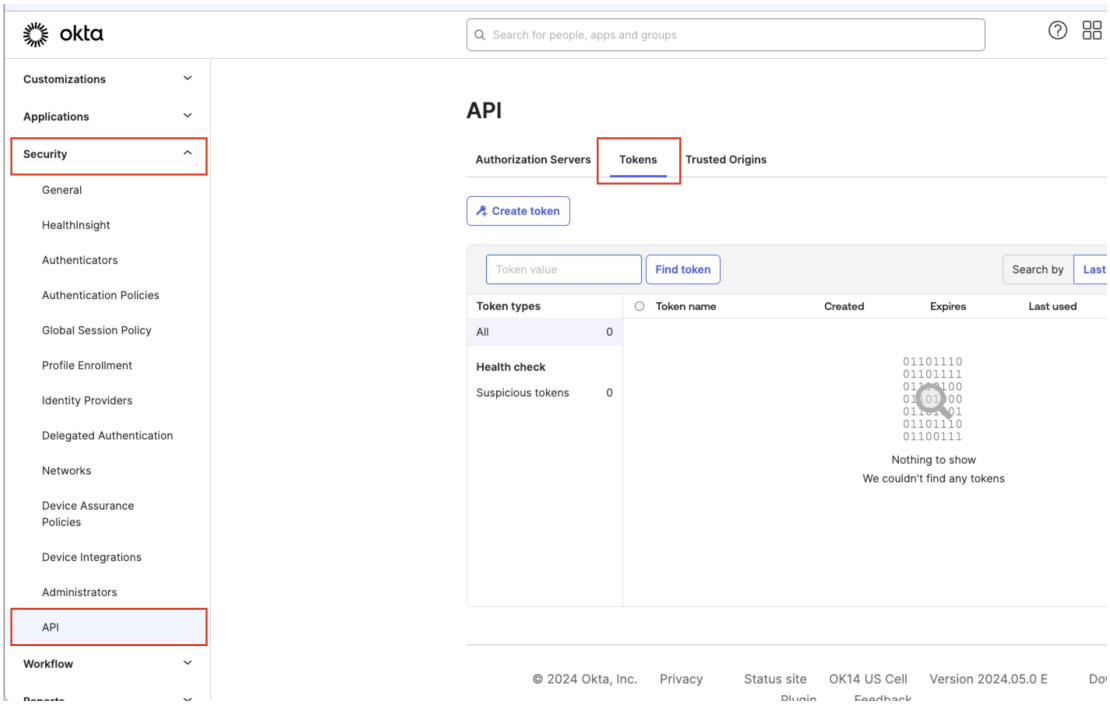
3. Input the Okta Client Secret value in the Client Secret field.



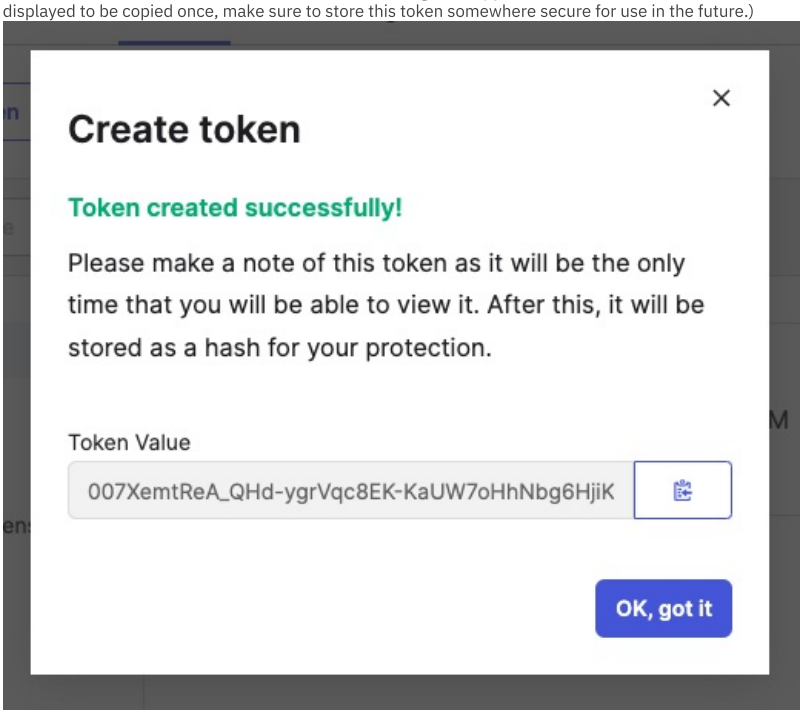


API Token

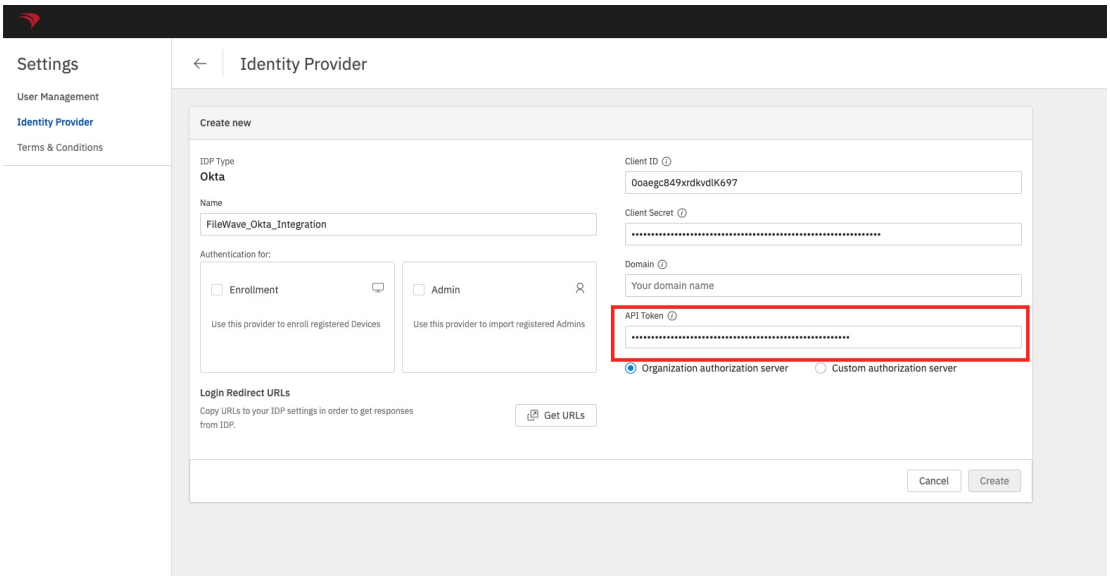
1. In Okta, open the Security > API menu and open the Tokens tab.



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.)



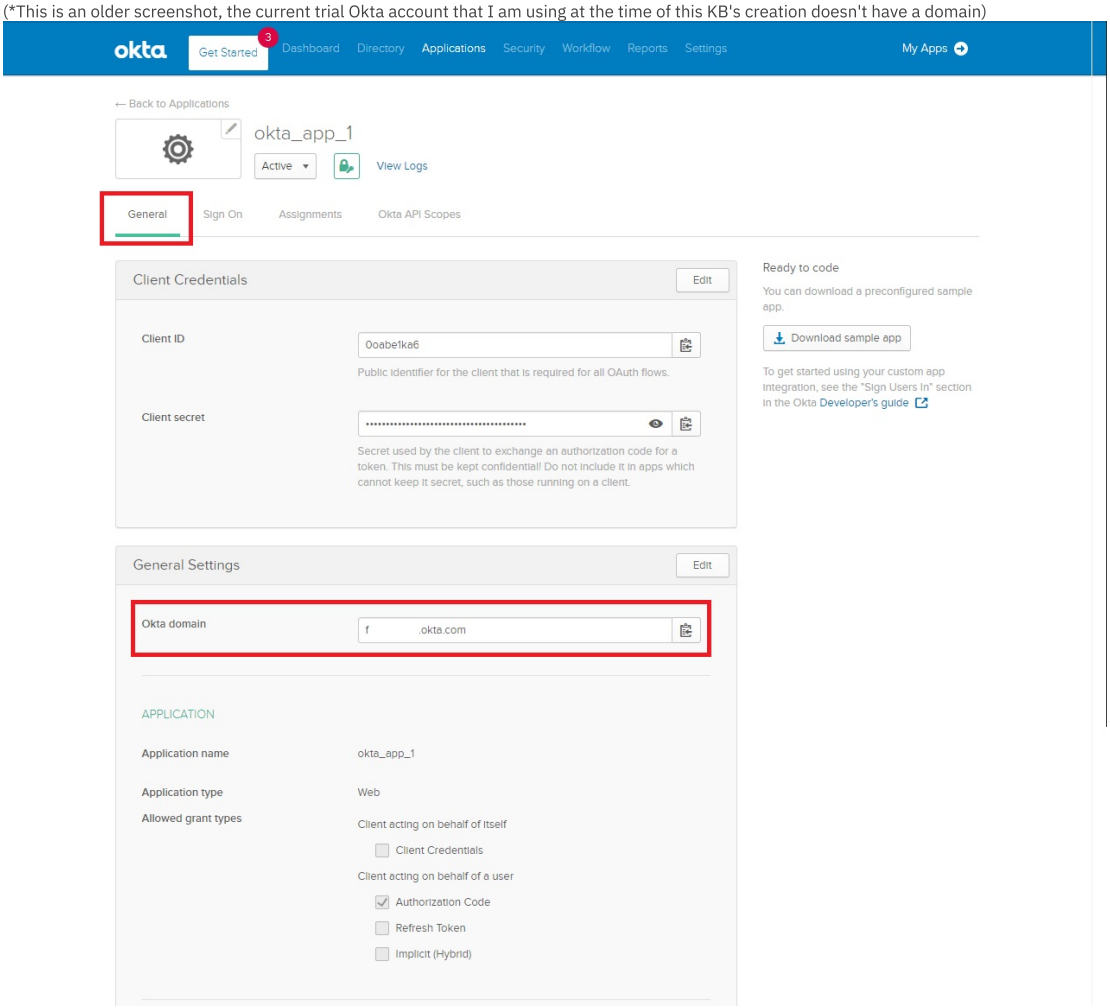
5. Copy and Paste the Token Value into the API Token field in the FileWave Admin Settings.



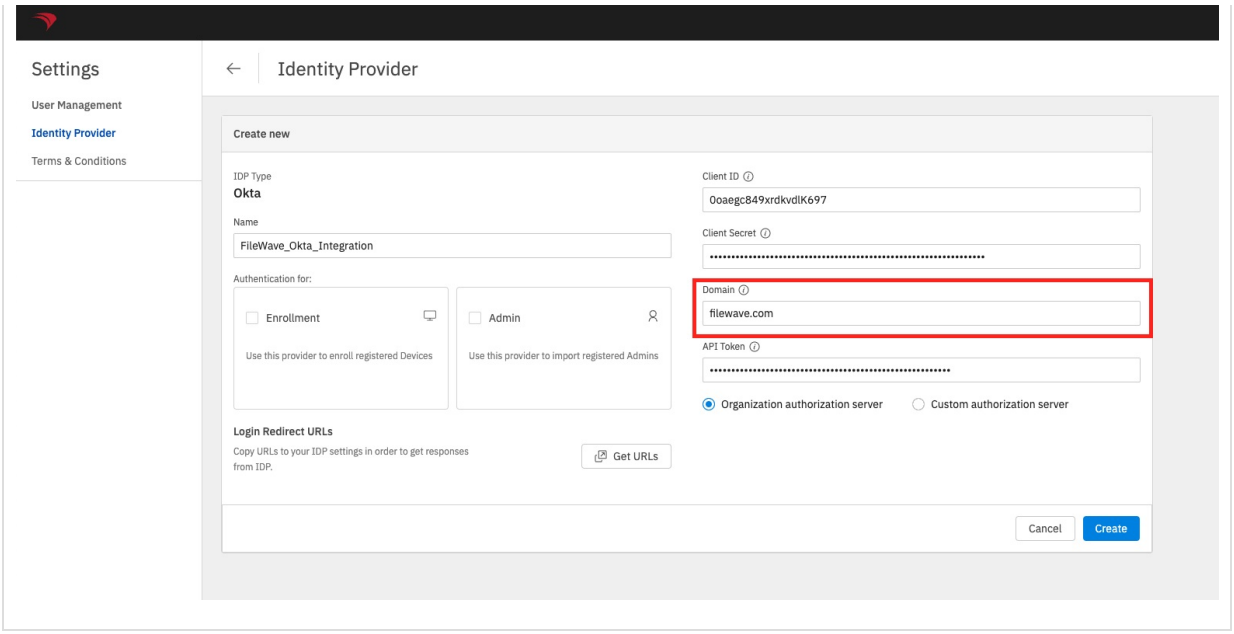
Okta Domain

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

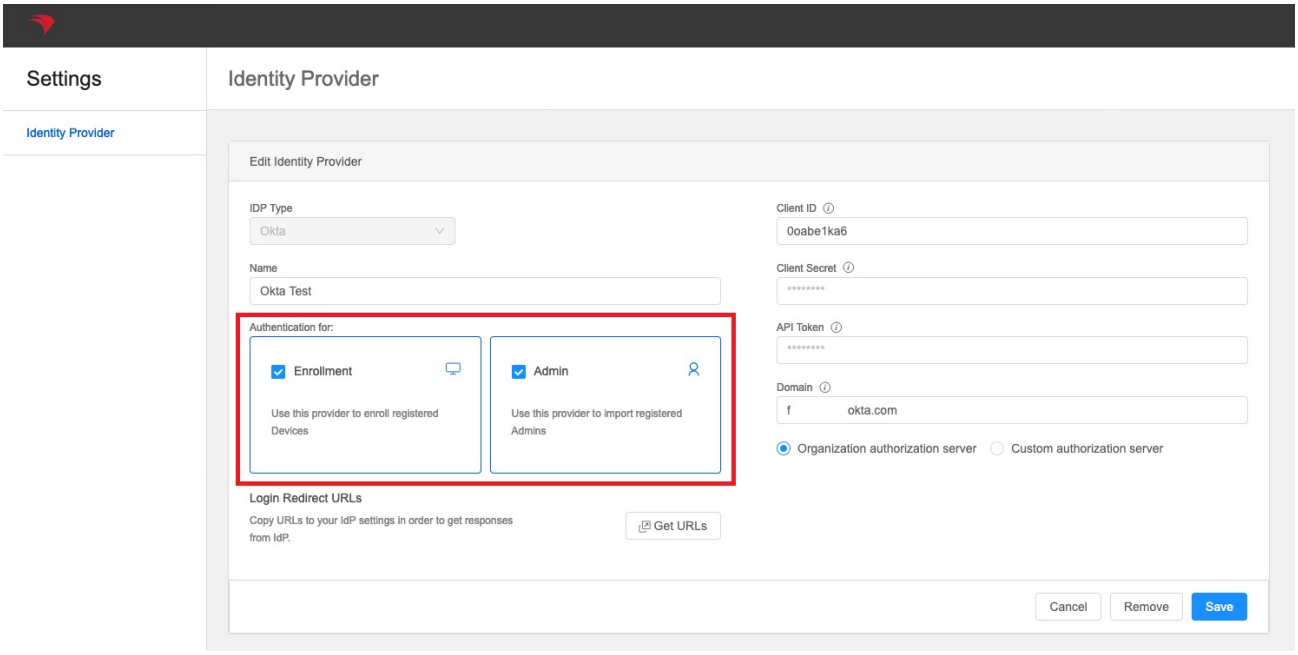
Configure an Okta Identity Provider for Authentication

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 Native and Web Admin 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

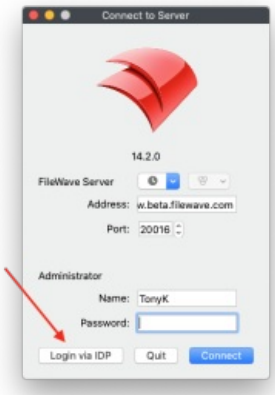
or Web Admin console.
- See: Adding IdP Groups for FileWave Authentication

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

Revision #5
★Created 21 June 2023 20:18:36 by Josh Levitsky
Updated 20 May 2024 16:49:02 by Emma Ainsworth