

# 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.

The screenshot shows the Okta Admin Portal interface. On the left is a sidebar with a navigation menu. The 'Applications' menu item is expanded, and 'Applications' is selected. The main content area is titled 'Applications' and features a search bar and three buttons: 'Create App Integration' (highlighted with a red arrow), 'Browse App Catalog', and 'Assign Users to App'. Below these buttons is a table listing existing applications.

STATUS	
ACTIVE	0
INACTIVE	0

Icon	Application Name	Client ID
	Okta Admin Console	
	Okta Browser Plugin	
	Okta Dashboard	
	Okta Workflows	Client ID: 00aegaqwbkgPJgMm697
	Okta Workflows OAuth	Client ID: 00aegaqwhs54OFj39697

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

Create a new app integration

×

Sign-in method

[Learn More](#)

☒ **OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

☐ **SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

☐ **SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

☐ **API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?  
  
Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

☒ **Web Application**  
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

☐ **Single-Page Application**  
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

☐ **Native Application**  
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

Cancel

Next

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)

[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_native)

[https://fwxserver.example.com:443/api/auth/login\\_via\\_idp\\_redirect\\_for\\_device](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.

## New Web App Integration

**General Settings**

**App integration name**

**Logo** (Optional)

**Grant type**  
[Learn More](#)

☐ Client acting on behalf of itself  
☐ Client Credentials

**Core grants**  
☒ Authorization Code  
☐ Refresh Token  
[Advanced](#)

**Sign-in redirect URIs** ☐ Allow wildcard \* in sign-in URI redirect.  
Okta sends the authentication response and ID token for the user's sign-in request to these URIs  
[Learn More](#)

[+ Add URI](#)

**Sign-out redirect URIs** (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.  
[Learn More](#)

[+ Add URI](#)

**Trusted Origins**

**Base URIs** (Optional)

Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.  
[Learn More](#)

[+ Add URI](#)

**Assignments**

**Controlled access**  
☒ Allow everyone in your organization to access  
☐ Limit access to selected groups  
☐ Skip group assignment for now  
Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation

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.



## FileWave\_Okta\_Integration

Active ▾



View Logs

General

Sign On

Assignments

Okta API Scopes

Application Rate Limits

### Client Credentials

Cancel

Client ID

00aegc849xrdkvdIK697

Public identifier for the client that is required for all OAuth flows.

Client authentication



Client secret



Public key / Private key

Proof Key for Code Exchange (PKCE)



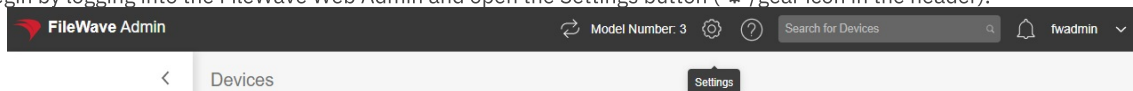
Require PKCE as additional verification

## Part 3: Configure the Okta App in FileWave

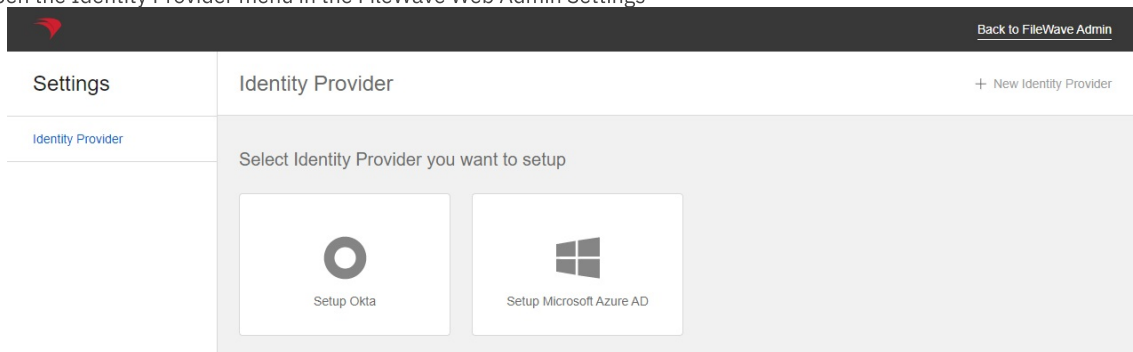
### Configure an Okta App in the FileWave Web Admin Console

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.



# FileWave\_Okta\_Integration

Active ▾

 View Logs

General

Sign On

Assignments

Okta API Scopes


Application Rate Limits

## Client Credentials

Edit

Client ID

Ooaegc849xrdkvdIK697



Public identifier for the client that is required for all OAuth flows.

Client authentication

☒ Client secret



☐ Public key / Private key


Proof Key for Code Exchange (PKCE)

☐ Require PKCE as additional verification

## CLIENT SECRETS

Generate new secret

Creation date	Secret	Status
May 20, 2024	..... <div></div>	<div> Active ▾</div>



Settings

User Management

Identity Provider

Terms & Conditions

←

Identity Provider

Create new

IDP Type

Okta

Name

FileWave\_Okta\_Integration

Authentication for:

☐ Enrollment


Use this provider to enroll registered Devices

☐ Admin

Use this provider to import registered Admins

Login Redirect URLs

Copy URLs to your IDP settings in order to get responses from IDP.

 Get URLs

Client ID ⓘ

Ooaegc849xrdkvdIK697

Client Secret ⓘ

.....

Domain ⓘ

Your domain name

API Token ⓘ

.....

☒ Organization authorization server

☐ Custom authorization server

Cancel

Create

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

## Client Credentials

[Edit](#)

Client ID

Ooaegc849xrdkvdIK697



Public identifier for the client that is required for all OAuth flows.

Client authentication

- ☒ Client secret
- ☐ Public key / Private key

Proof Key for Code Exchange (PKCE)

- ☐ Require PKCE as additional verification

## CLIENT SECRETS

[Generate new secret](#)

Creation date	Secret	Status
May 20, 2024	zfk85LpDbY9t8oofCfwy2xoO6GRBED6Yb-uCtm1: 	 <a href="#">Active ▾</a>

Copied!



## Settings

User Management

**Identity Provider**

Terms & Conditions

## ← Identity Provider

### Create new

IDP Type

Okta

Name

FileWave\_Okta\_Integration

Authentication for:

☐ Enrollment



Use this provider to enroll registered Devices

☐ Admin



Use this provider to import registered Admins

### Login Redirect URLs

Copy URLs to your IDP settings in order to get responses from IDP.

[Get URLs](#)

Client ID ⓘ

Ooaegc849xrdkvdIK697

Client Secret ⓘ

.....

Domain ⓘ

Your domain name

API Token ⓘ

.....

☒ Organization authorization server ☐ Custom authorization server

Cancel

Create

## 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.

Settings

User Management

Identity Provider

Terms & Conditions

← Identity Provider

Create new

IDP Type

Okta

Name

FileWave\_Okta\_Integration

Authentication for:

☐ Enrolment
 

Use this provider to enroll registered Devices

☐ Admin
 

Use this provider to import registered Admins

Login Redirect URLs

Copy URLs to your IDP settings in order to get responses from IDP.

Get URLs

Client ID

Ooae849xrdkdlK697

Client Secret

.....

Domain

Your domain name

API Token

.....

☒ Organization authorization server
 ☐ Custom authorization server

Cancel

Create

## 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)

okta

Get Started

Dashboard

Directory

Applications

Security

Workflow

Reports

Settings

My Apps

← Back to Applications

okta\_app\_1

Active

View Logs

General

Sign On

Assignments

Okta API Scopes

Client Credentials

Client ID

Ooab1ka6

Client secret

.....

General Settings

Okta domain

f .okta.com

APPLICATION

Application name

okta\_app\_1

Application type

Web

Allowed grant types

Client acting on behalf of itself

☐ Client Credentials
 ☒ Authorization Code
 ☐ Refresh Token
 ☐ Implicit (Hybrid)

Ready to code

You can download a preconfigured sample app.

Download sample app

To get started using your custom app integration, see the "Sign Users In" section in the Okta Developer's guide

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



**Settings**

User Management

**Identity Provider**

Terms & Conditions

**Create new**

IDP Type: **Okta**

Name: FileWave\_Okta\_Integration

Authentication for:

☐ Enrollment ☐ Admin

Use this provider to enroll registered Devices ☐ Use this provider to import registered Admins ☐

Client ID: 00aegc849xrdkvdIK697

Client Secret: .....

Domain: **filewave.com**

API Token: .....

☒ Organization authorization server ☐ Custom authorization server

Login Redirect URLs

Copy URLs to your IDP settings in order to get responses from IDP. [Get URLs](#)

[Cancel](#) [Create](#)

## 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.

**Settings**

**Identity Provider**

**Edit Identity Provider**

IDP Type: Okta

Name: Okta Test

Authentication for:

☒ Enrollment ☒ Admin

Use this provider to enroll registered Devices ☒ Use this provider to import registered Admins ☒

Client ID: 00abe1ka6

Client Secret: .....

API Token: .....

Domain: f.okta.com

☒ Organization authorization server ☐ Custom authorization server

Login Redirect URLs

Copy URLs to your IdP settings in order to get responses from IdP. [Get URLs](#)

[Cancel](#) [Remove](#) [Save](#)

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.

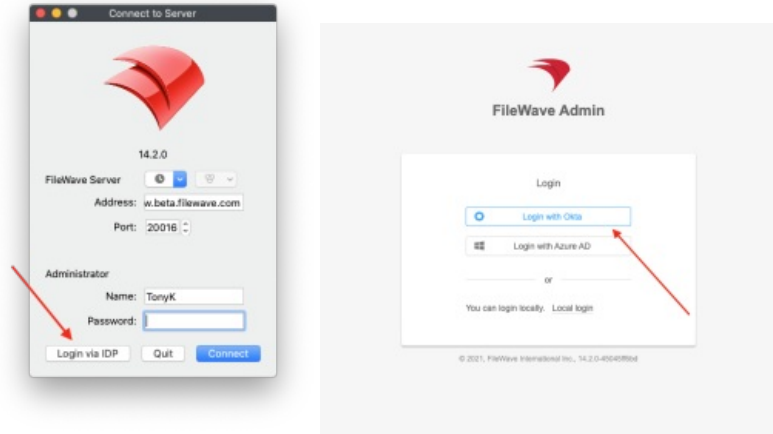
- See: [Adding IdP Groups for FileWave Authentication](#)

## 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