

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](#)
- [IdP Setup: Microsoft Entra ID](#)
- [IdP Setup: Okta](#)
- [IdP Setup: Google](#)
- [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](#)
- [Troubleshooting](#)
 - [Directory data synchronization between IdP and FW is not supported](#)
- [Renaming Azure Active Directory \(Azure AD\) to Microsoft Entra ID](#)

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 3 IdP providers with version 14.6.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](#)
- [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

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

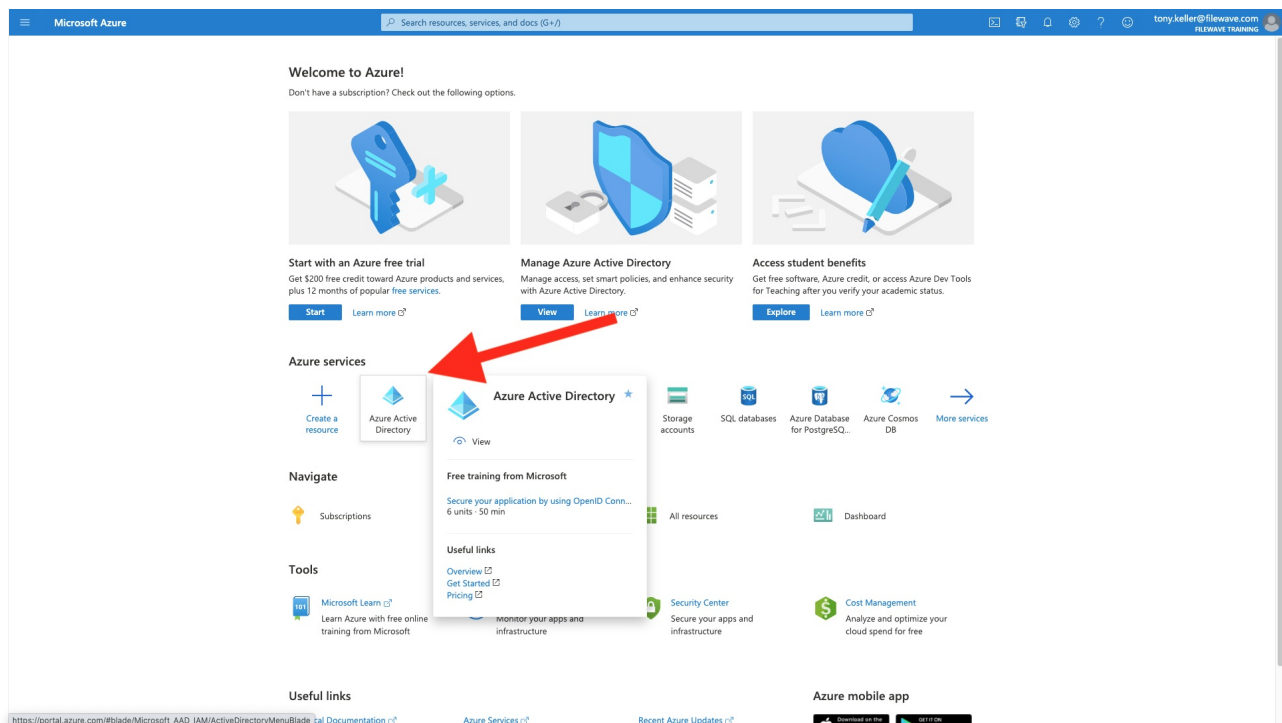
This configuration is required if you want to use AzureAD for authentication during device enrollment or during login to the FileWave Web and Native administrator consoles.

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:

The screenshot shows the Microsoft Azure portal interface for the FileWave Training tenant. The left sidebar contains navigation links for Overview, Manage, and Monitoring. The main content area shows the 'FileWave Training' overview, including a search bar for tenants, a 'Tenant information' card, and an 'Azure AD Connect' card. The 'Tenant information' card displays details such as the role (Global administrator), license (Azure AD Free), tenant ID (00487120-4139-4b67-b1db-962...), and primary domain (fwtraining.onmicrosoft.com). A red arrow points to the primary domain field. Below this, there is a 'Sign-ins' graph showing a peak of 15 sign-ins around December 20th. At the bottom, there are 'Create' buttons for User, Guest user, Group, Enterprise application, and App registration, along with 'Featured services'.

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":

The screenshot shows the Microsoft Azure portal interface for the FileWave Training tenant, specifically the 'App registrations' page. The left sidebar shows the 'App registrations' link highlighted. The main content area shows a 'New registration' button and a table of applications. A red arrow points to the 'New registration' button. The table lists three applications: 'FileWave Integration', 'FW Beta', and 'FW Beta'. The 'FileWave Integration' application is the first one listed.

Display name	Application (client) ID	Created on	Certificates & secrets
FileWave Integration	065ccb0e-86cd-4887-a54c-b8b08a086a2c	2/14/2020	-
FW Beta	34a993c3-fb0c-4900-83f1-bc2d98d0a6bb	12/28/2020	-
FW Beta	61a5f712-3c20-4b88-878d-ce9214a99166	1/13/2021	Current

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

Microsoft Azure

Search resources, services, and docs (Cmd+I)

Home > FileWave Training > FW Beta 2

Register an application

* Name

The user-facing display name for this application (this can be changed later).

FW Beta 2

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (FileWave Training only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Register

Created on	Certificates & secrets
2/14/2020	-
12/28/2020	-
1/13/2021	Current

Part 3: Add a Platform and URI Addresses

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

Microsoft Azure

Search resources, services, and docs (Cmd+I)

Home > FileWave Training > FW Beta 2

FW Beta 2 | Authentication

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (FileWave Training only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

Yes No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

Configure platforms

Web applications

Web

Build, host, and deploy a web server application. .NET, Java, Python

Single-page application

Configure browser client applications and progressive web applications. Javascript.

Mobile and desktop applications

iOS / macOS

Objective-C, Swift, Xamarin

Android

Java, Kotlin, Xamarin

Mobile and desktop applications

Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

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

FileWave Admin

Model Number: 108

Search for Devices

TonyK

Settings

Go to Dashboard

Devices

Android ChromeOS iOS macOS tvOS Windows Other/Unknown All

Groups	Name	Groups	Asset Tag	Comment	User	Model	IP Addr
Root	3183a5776d58cee0	SG Mixed, SG Mixed 1 (test), ...					
All iOS (non-inv)	ARKONE	All Windows (inv), FileWave Cl...			Administrator	16	99.203...
All macOS (inv)	DESKTOP-T3SL865	All Windows (inv), FileWave Cl...			joe	0	184.19...
All Windows (inv)	Rewave's Mac	All macOS (inv), FileWave Cle...			filewave	11	184.19...
BAM Devices	FOUNDRY1	All Windows (inv), FileWave Cl...	FW-ASSET		keller90	83	172.58...
Chromebooks	FW-DMP891ZTHG5...	All iOS (non-inv), TK Client De...					172.58...
FileWave Client Version	lpad Main	All iOS (non-inv), Have Asset T...	FW-657394				172.58...
FileWave Client Version 42	PesCee-McPC	All Windows (inv), FileWave Cl...					172.58...
Have Asset Tags	Surface-McPC	All Windows (inv), FileWave Cl...	Mine		sk_fir	105	172.58...
SG Mixed	Tony Keller MBPro	All macOS (inv), FileWave Cle...	FW-123456		keller90	108	172.58...
SG Mixed 1 (test)							
Test Android							
TK Client Devices							

14.2.0-27a6c524a

Then choose an Microsoft Entra ID IDP Provider

Settings

Identity Provider

Back to FileWave Admin

+ New Identity Provider

Select Identity Provider you want to setup

Setup Okta

Setup Microsoft Azure AD

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

Settings

Identity Provider

Back to FileWave Admin

+ New Identity Provider

Identity Provider

Create new

IDP Type

Azure AD

Name

FW Beta Example

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

Paste Client ID

Required

Client Secret

Required

Domain

Your domain name

Cancel

Create

Settings

Identity Provider

Back to FileWave Admin

+ New Identity Provider

Identity Provider

Create new

IDP Type

Azure AD

Name

FW Beta Example

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

Paste Client ID

Required

Client Secret

Required

Domain

Your domain name

Cancel

Create

Login redirect URLs

Copy the URLs below to your IDP provider settings

https://fw.beta.filewave.com:4...

Copy

https://fw.beta.filewave.com:4...

Copy

https://fw.beta.filewave.com:4...

Copy

Close

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

Microsoft Azure

Home > FileWave Training > FW Beta 2

FW Beta 2 | Authentication

Search (Cmd+J)

Save Discard Got feedback?

Overview Quickstart Integration assistant

Manage

Branding Authentication Certificates & secrets Token configuration API permissions Expose an API App roles | Preview Owners Roles and administrators | Preview Manifest

Support + Troubleshooting Troubleshooting New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (FileWave Training only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

Yes No

• App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)

• No keyboard (Device Code Flow) [Learn more](#)

• SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

Configure Web

All platforms Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https://fw.beta.filewave.com:443/api/auth/login_via_idp_redirect

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. <https://myapp.com/logout>

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more.](#)

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☐ ID tokens (used for implicit and hybrid flows)

Configure Cancel

And then add the other two from here:

Microsoft Azure

Home > FileWave Training > FW Beta 2

FW Beta 2 | Authentication

Search (Cmd+J)

Save Discard Got feedback?

Overview Quickstart Integration assistant

Manage

Branding Authentication Certificates & secrets Token configuration API permissions Expose an API App roles | Preview Owners Roles and administrators | Preview Manifest

Support + Troubleshooting Troubleshooting New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https://fw.beta.filewave.com:443/api/auth/login_via_idp_redirect

https://fw.beta.filewave.com:443/api/auth/login_via_idp_redirect_for_native

https://fw.beta.filewave.com:443/api/auth/login_via_idp_redirect_for_device

Add URI

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. <https://myapp.com/logout>

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more.](#)

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☐ ID tokens (used for implicit and hybrid flows)

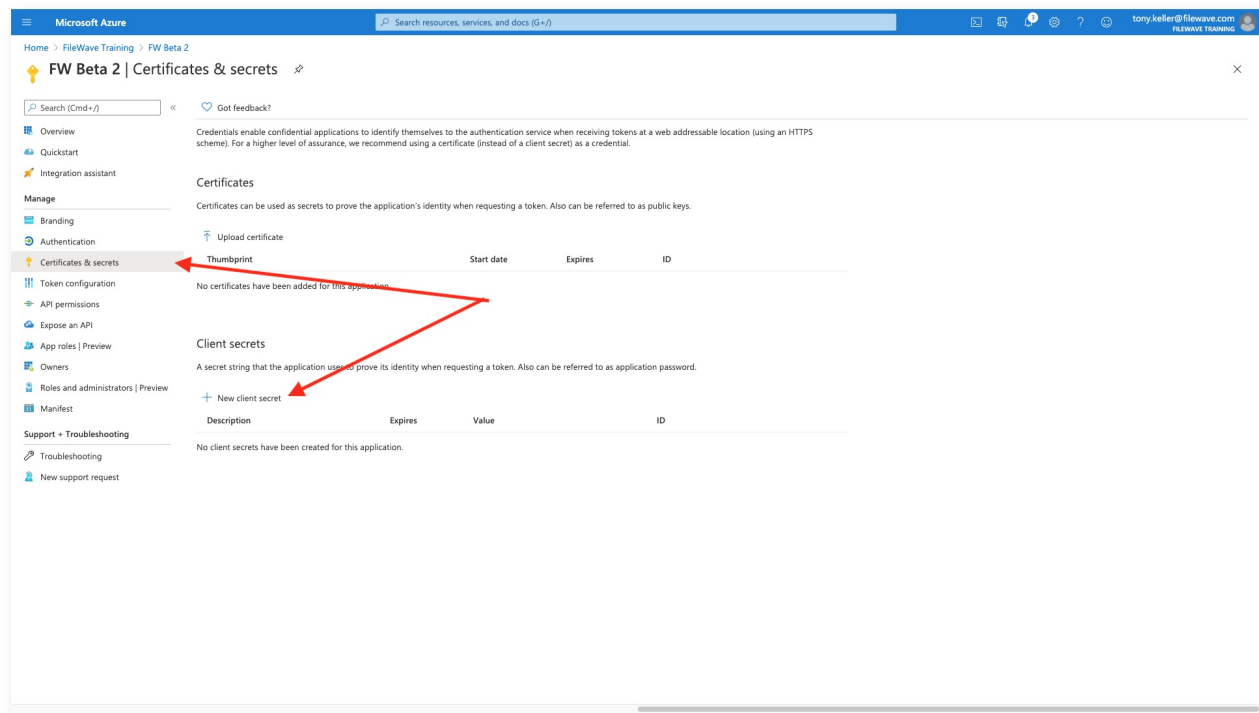
Supported account types

Who can use this application or access this API?

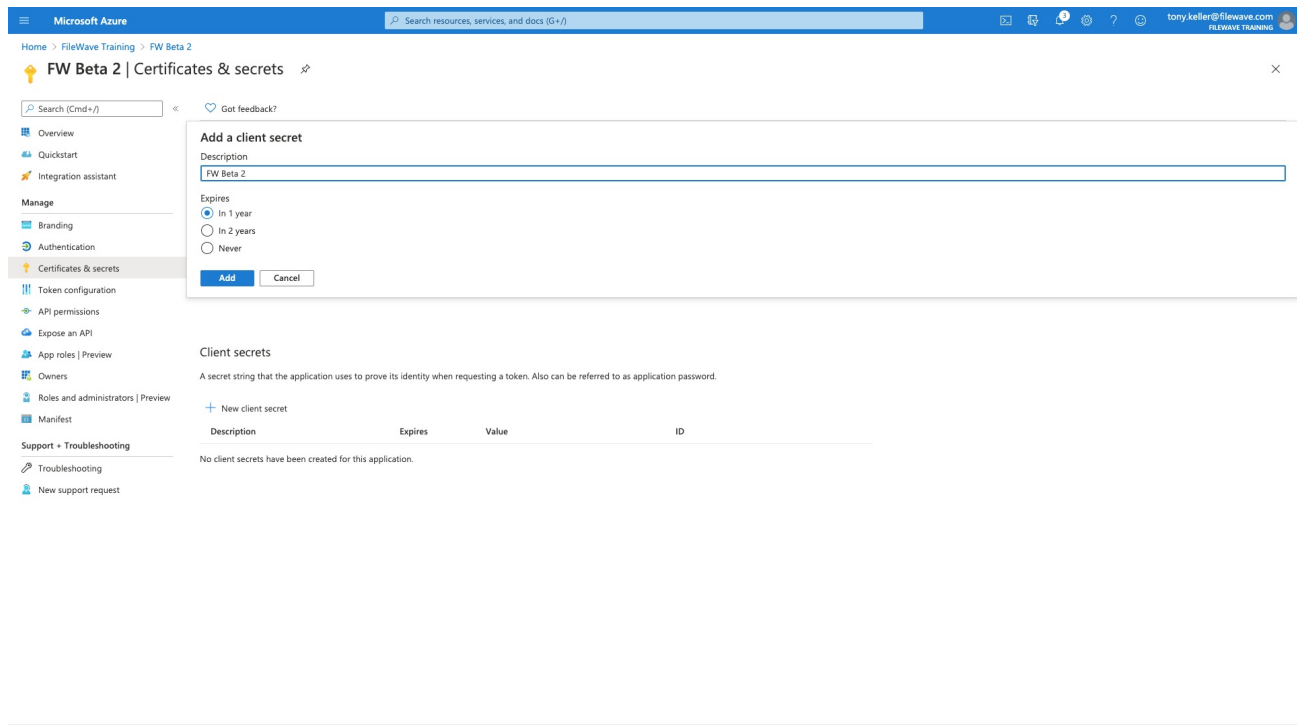
Make sure to hit Save at the top after you have entered all three.

Part 4: Cert & Secrets

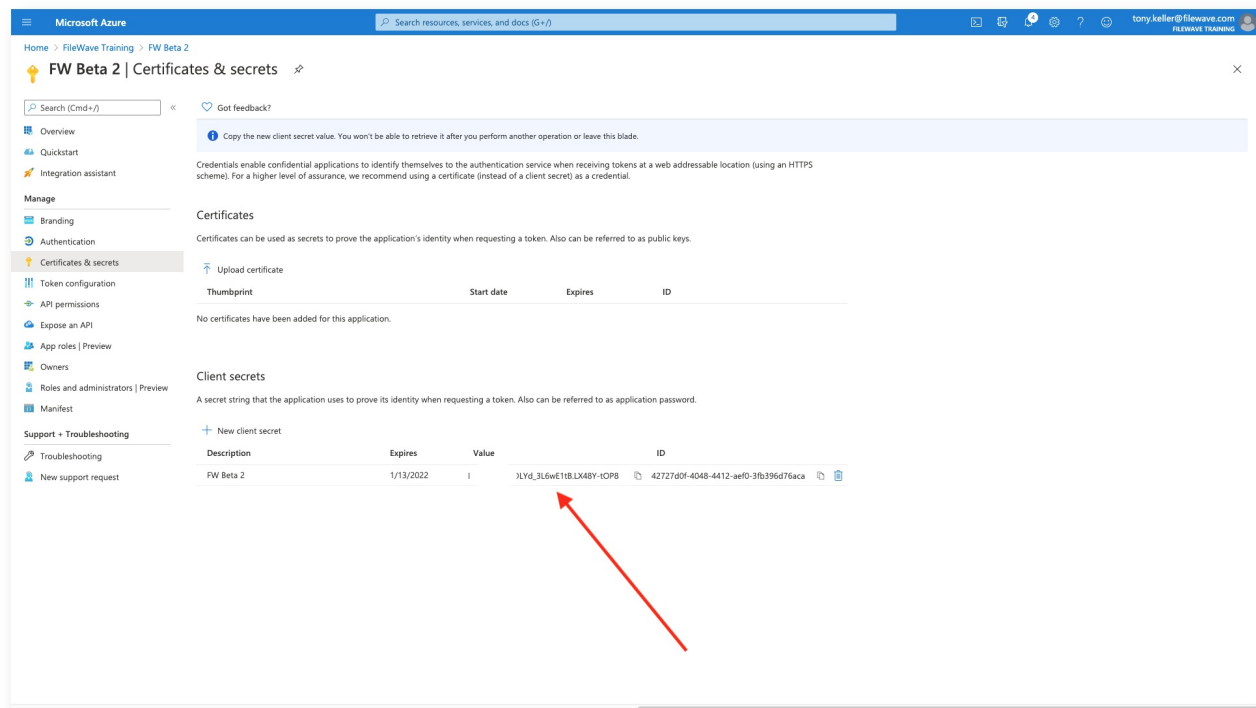
Now we are going to go to Certificates & Secrets to provide a way for FileWave to authentication to our new application. Click on New client secret



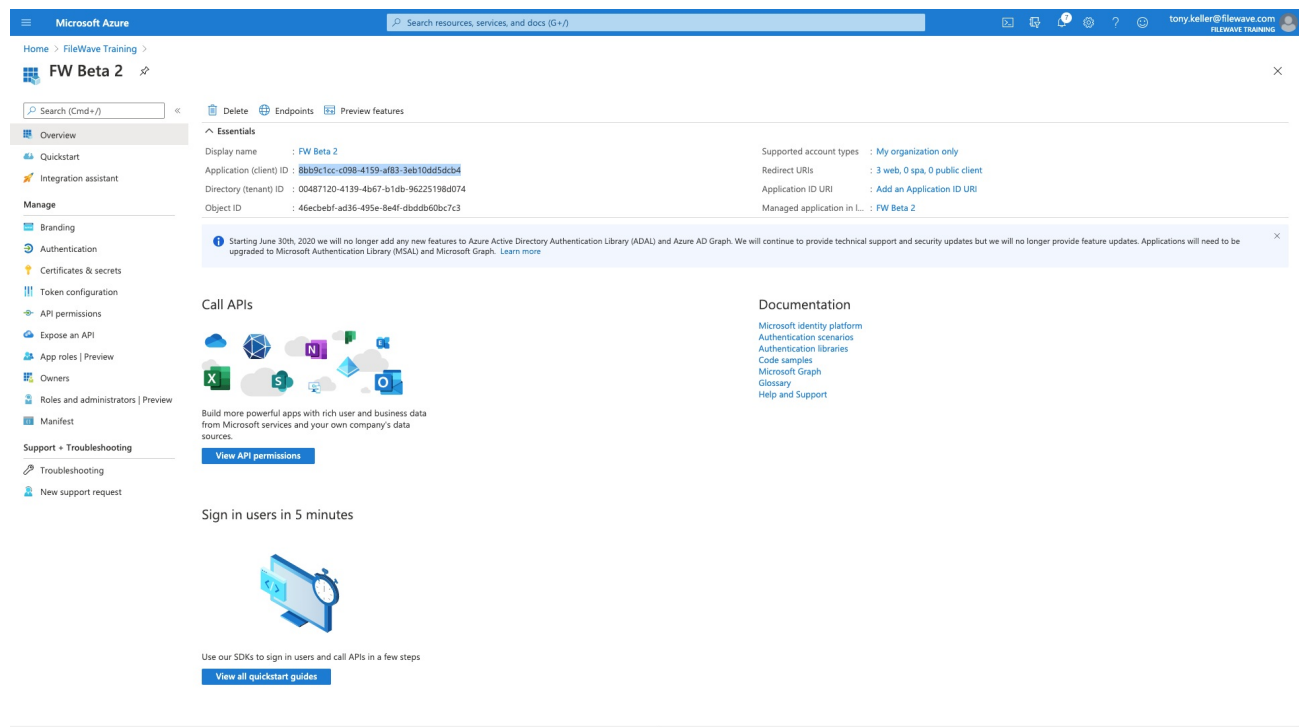
Then we give it a descriptive name:



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



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:

Settings

Identity Provider

Identity Provider

Create new

IDP Type

Azure AD

Name

FW Beta Example

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

42727d0f-4048-4412-ae00-3fb396d76aca

Client Secret

Domain

fwtraining.onmicrosoft.com

Cancel

Create

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

Microsoft Azure

Search resources, services, and docs (G+)

Home > FileWave Training > FW Beta 2

FW Beta 2 | API permissions

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles | Preview

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Search (Cmd+/)

Refresh

Got feedback?

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

Add a permission

Grant admin consent for FileWave Training

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User.read	Delegated	Sign in and read user profile	-	...

To view and manage permissions and user consent, try [Enterprise applications](#).

Our permissions are going to be for Microsoft Graph

Microsoft Azure | Search resources, services, and docs (G+)

Home > FileWave Training > FW Beta 2

FW Beta 2 | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for FileWave Training

API / Permissions name	Type	Description	Admin consent req...
▼ Microsoft Graph (1)			
User Read	Delegated	Sign in and read user profile	-


To view and manage permissions and user consent, try [Enterprise applications](#).


Request API permissions


Select an API


Microsoft APIs APIs my organization uses My APIs


Commonly used Microsoft APIs


**Microsoft Graph**
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.


**Azure Rights Management Services**
Allow validated users to read and write protected content


**Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal

**Dynamics 365 Business Central**
Programmatic access to data and functionality in Dynamics 365 Business Central


**Intune**
Programmatic access to Intune data


**Office 365 Management APIs**
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs


**SharePoint**
Interact remotely with SharePoint data


**Skype for Business**
Integrate real-time presence, secure messaging, calling, and conference capabilities


More Microsoft APIs


**Azure Batch**
Schedule large-scale parallel and HPC applications in the cloud

**Azure Data Catalog**
Programmatic access to Data Catalog resources to register, annotate and search data assets

**Azure Data Explorer**
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

**Azure Data Explorer (with Multifactor Authentication)**
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

**Azure Data Lake**
Access to storage and compute for big data analytic scenarios

**Azure DevOps**
Integrate with Azure DevOps and Azure DevOps server

We'll start with an application permission:

Microsoft Azure | Search resources, services, and docs (G+)

Home > FileWave Training > FW Beta 2

FW Beta 2 | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of all the permissions the application needs. [Learn more about permissions and consent](#)


+ Add a permission ✓ Grant admin consent for FileWave Training

API / Permissions name	Type	Description	Admin consent req...
▼ Microsoft Graph (1)			
User Read	Delegated	Sign in and read user profile	-

To view and manage permissions and user consent, try [Enterprise applications](#).

Request API permissions

< All APIs

**Microsoft Graph**
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Add permissions Discard

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

Microsoft Azure | Search resources, services, and docs (G+)

Home > FileWave Training > FW Beta 2

FW Beta 2 | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for FileWave Training

API / Permissions name	Type	Description	Admin consent req...
▼ Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

To view and manage permissions and user consent, try [Enterprise applications](#).

Request API permissions

< All APIs

- EdUAssignments
- EduRoster
- EntitlementManagement
- ExternalItem
- Files
- Group (1)
- Group.Create ○ Create groups Yes
- Group.Read.All ○ Read all groups Yes
- Group.ReadWrite.All ○ Read and write all groups Yes
- GroupMember
- IdentityProvider
- IdentityRiskEvent
- IdentityRiskyUser
- IdentityUserFlow
- InformationProtectionPolicy
- MailboxSettings
- Mail

Add permissions Discard

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

Microsoft Azure | Search resources, services, and docs (G+)

Home > FileWave Training > FW Beta 2

FW Beta 2 | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for FileWave Training

API / Permissions name	Type	Description	Admin consent req...
▼ Microsoft Graph (3)			
Group.Read.All	Application	Read all groups	Yes
User.Read	Delegated	Sign in and read user profile	-
User.Read.All	Application	Read all users' full profiles	Yes

To view and manage permissions and user consent, try [Enterprise applications](#).

Request API permissions

< All APIs

Microsoft Graph <https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Start typing a reply url to filter these results

Permission	Admin consent required
▼ Openid permissions (2)	
email ○ View users' email address	-
offline_access ○ Maintain access to data you have given it access to	-
openid ○ Sign users in	-
profile ○ View users' basic profile	-
AccessReview	
AdministrativeUnit	
AgreementAcceptance	
Agreement	
Analytics	
APICConnectors	

Add permissions Discard

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

Microsoft Azure

Home > FileWave Training > FW Beta 2

FW Beta 2 | API permissions

Search (Cmd+/) Refresh Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ☒ Grant admin consent for FileWave Training

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (5)				
Group.Read.All	Application	Read all groups	Yes	Not granted for FileWav...
openid	Delegated	Sign users in	-	
profile	Delegated	View users' basic profile	-	
User.Read	Delegated	Sign in and read user profile	-	
User.Read.All	Application	Read all users' full profiles	Yes	Not granted for FileWav...

To view and manage permissions and user consent, try [Enterprise applications](#).

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

Microsoft Azure

Home > FileWave Training > FW Beta 2

FW Beta 2 | API permissions

Search (Cmd+/) Refresh Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ☒ Grant admin consent for FileWave Training

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (5)				
Group.Read.All	Application	Read all groups	Yes	Not granted for FileWav...
openid	Delegated	Sign users in	-	
profile	Delegated	View users' basic profile	-	
User.Read	Delegated	Sign in and read user profile	-	
User.Read.All	Application	Read all users' full profiles	Yes	Not granted for FileWav...

To view and manage permissions and user consent, try [Enterprise applications](#).

When they show as green, we are all done!

Microsoft Azure

Home > FileWave Training > FW Beta

FW Beta | API permissions

Search (Cmd+J) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

Branding Authentication Certificates & secrets Token configuration API permissions Expose an API App roles | Preview Owners Roles and administrators | Preview Manifest

Support + Troubleshooting Troubleshooting New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for FileWave Training

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (5)				...
Group.Read.All	Application	Read all groups	Yes	Granted for FileWave Tr... ✓
openid	Delegated	Sign users in	-	Granted for FileWave Tr... ✓
profile	Delegated	View users' basic profile	-	Granted for FileWave Tr... ✓
User.Read	Delegated	Sign in and read user profile	-	Granted for FileWave Tr... ✓
User.Read.All	Application	Read all users' full profiles	Yes	Granted for FileWave Tr... ✓

To view and manage permissions and user consent, try [Enterprise applications](#).

Part 6: App Registration Renewal

At some point the Certificate of the App will expire and a new certificate should be generated.

From the App Registration view, expired certificates may be observed

Overview Preview features Diagnose and solve problems

Manage

Users Groups External Identities Roles and administrators Administrative units Delegated admin partners Enterprise applications Devices App registrations

+ New registration Endpoints Troubleshooting Refresh Download Preview features Got feedback?

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

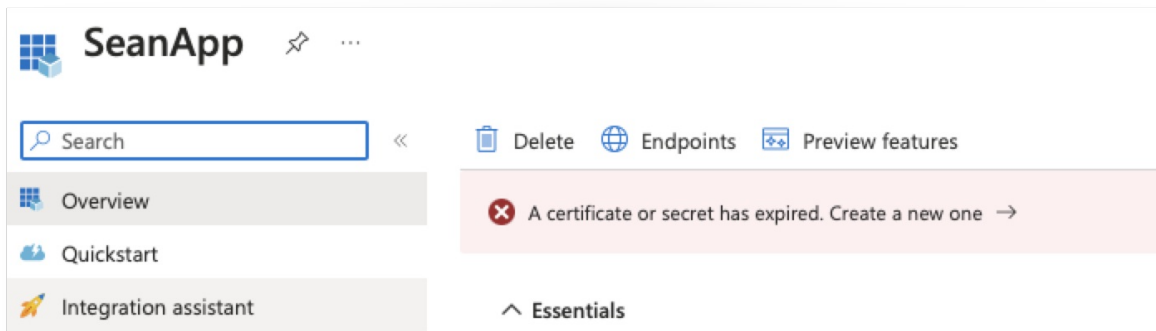
All applications Owned applications Deleted applications

Start typing a display name or application (client) ID to filter these r... Add filters

2 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
SeanApp		2/8/2022	Expired
SeanXcredApp		11/29/2022	-

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 ID

This time though, Edit the current IdP in FileWave Anywhere:

- Open Settings in the FileWave Admin
- Choose Edit from the selected IdP
- Paste in the new Client Secret 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

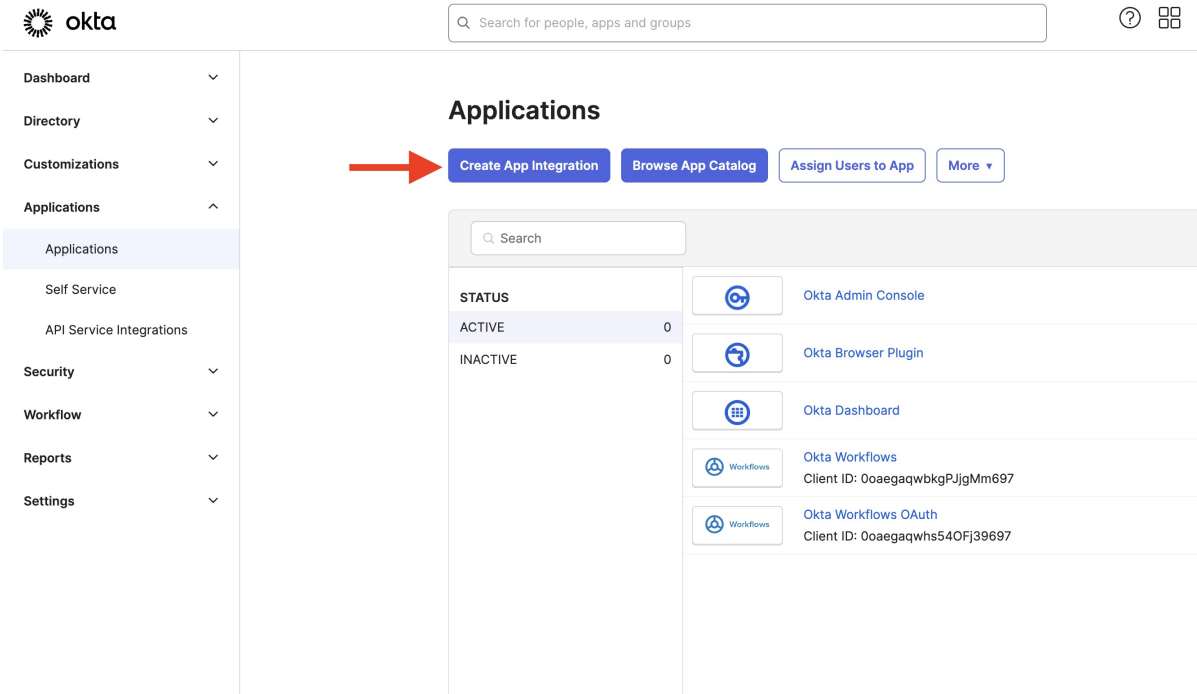
Begin by logging in to the Okta Admin Portal with an administrator's account. (<https://example-admin.okta.com/admin>)

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.

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_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.

New Web App Integration

General Settings

App integration name FileWave_Okta_Integration

Logo (Optional)



Grant type

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

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

+ Add URI

Sign-out redirect URIs (Optional)

http://localhost:8080

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

+ Add URI

Trusted Origins

Base URIs (Optional)

+ Add URI

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.

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)



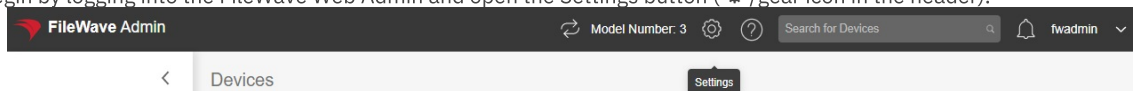
Require PKCE as additional verification

Part 3: Configure the Okta App in FileWave

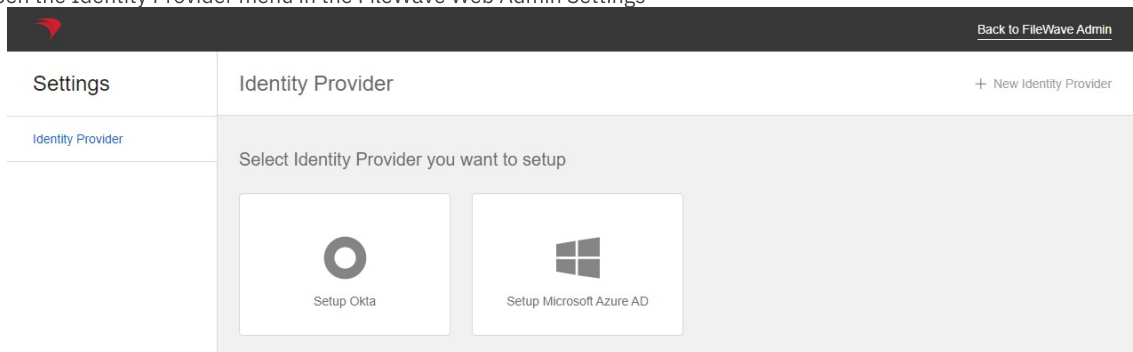
Configure an Okta App in the FileWave Web Admin Console

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




1. 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

Ooae8c849xrdkvdIK697



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: 	<div>Copied!</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.



Client ID ⓘ

Ooae8c849xrdkvdIK697

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.

Okta Admin Console interface showing the API Tokens tab. The left sidebar highlights the Security and API sections. The main content area displays the API Tokens tab with a 'Create token' button. Below this, a table shows token details, including token types (All, Health check, Suspicious tokens) and a list of tokens with their values, creation dates, and expiration dates. A search bar is available to find specific tokens.

Token types	Token name	Created	Expires	Last used
All	0			
Health check				
Suspicious tokens	0			

- Click the Create Token button in the Tokens tab.
- Input a meaningful name in the API token's Name field.
- 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.)

Create token

Token created successfully!

Please make a note of this token as it will be the only time that you will be able to view it. After this, it will be stored as a hash for your protection.

Token Value

007XemtReA_QHd-ygrVqc8EK-KaUW7oHhNbg6HjiK

OK, got it

- 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

Ooagc849xrdkdlK697

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

Edit

Client ID

Ooabek6

Client secret

.....

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](#)

General Settings

Edit

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

Client acting on behalf of a user

☒ Authorization Code

☐ Refresh Token

☐ Implicit (Hybrid)

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

Use this provider to enroll registered Devices

☐ Admin

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

Use this provider to enroll registered Devices

☒ Admin

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.

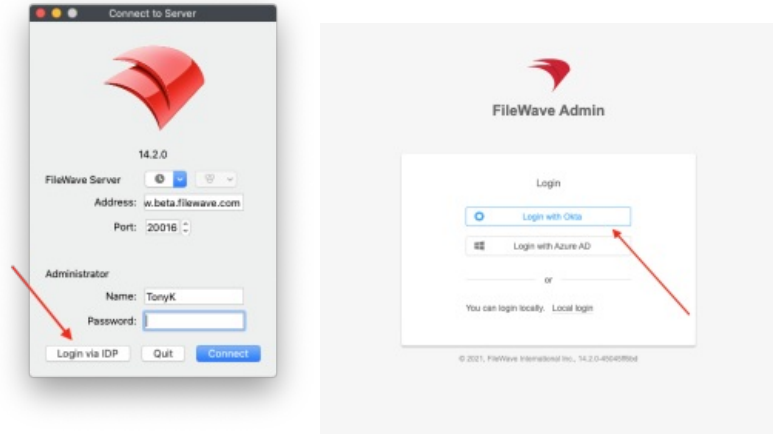
- See: [Adding IdP Groups for FileWave Authentication](#)

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](#)

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.

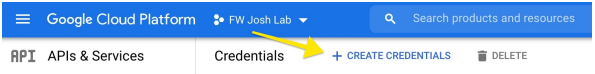
NOTE: CANNOT be IP Address or self-signed cert. Must be FQDN - [Instructions Linked Here](#)



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)

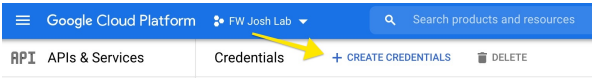
Below is an excerpt on how to obtain a Client ID and client secret. For a more detailed tutorial and additional information, [check the documentation](#).

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"	

	<div> + CREATE CREDENTIALS  DELETE </div> <div> API key Identifies your project using a simple API key to check quota and access </div> <div> OAuth client ID Requests user consent so your app can access the user's data </div> <div> Service account Enables server-to-server, app-level authentication using robot accounts </div> <div> Help me choose Asks a few questions to help you decide which type of credential to use </div>
(Step 4) - In the next screen, choose "Web application"	<div> ← Create OAuth client ID </div> <div> A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See Setting up OAuth 2.0 for more information. Learn more about OAuth client types. </div> <div> <div>Application type *</div> <div> Web application Android Chrome app iOS TVs and Limited Input devices Desktop app Universal Windows Platform (UWP) </div> </div>
(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. https://filewave.server.com/api/auth/login_via_idp_redirect https://filewave.server.com/api/auth/login_via_idp_redirect_for_native https://filewave.server.com/api/auth/login_via_idp_redirect_for_device	<div>URIs *</div> <div> https://filewave.server.com/api/auth/login_via_idp_redirect </div> <div> https://filewave.server.com/api/auth/login_via_idp_redirect_for_native </div> <div> https://filewave.server.com/api/auth/login_via_idp_redirect_for_device </div> <div> + ADD URI </div>
(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.	<div> OAuth client created </div> <div> The client ID and secret can always be accessed from Credentials in APIs & Services </div> <div> <div>  OAuth access is restricted to users within your organization unless the OAuth consent screen is published and verified </div> <div> Your Client ID 101750625406-88bc6io4m80kk77i32fjojqq6u0a2ptl.apps.gcp </div> <div> Your Client Secret pecchHEFvpTSZU-9w-9SHS6 </div> <div>OK</div> </div>

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.

[+ CREATE CREDENTIALS](#) [DELETE](#)

API key

Identifies your project using a simple API key to check quota and access

OAuth client ID

Requests user consent so your app can access the user's data

Service account

Enables server-to-server, app-level authentication using robot accounts

Help me choose

Asks a few questions to help you decide which type of credential to use

1 Service account details

Service account name

FileWave Service Account

Display name for this service account

Service account ID

filewave-service-account @sacred-truck-322818.iam.gserviceacc X ↺

Service account description

Used for IdP

Describe what this service account will do

[CREATE AND CONTINUE](#)

2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

[DONE](#)

[CANCEL](#)

Service Accounts

[Manage service accounts](#)

<input type="checkbox"/>	Email	Name ↑	Actions
<input type="checkbox"/>	filewave-service-account@sacred-truck-322818.iam.gserviceaccount.com	FileWave Service Account	✎ ✖

FileWave Service Account

[DETAILS](#) [PERMISSIONS](#) [KEYS](#) [METRICS](#) [LOGS](#)

Keys

⚠ Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the [Workload Identity Federation](#). You can learn more about the best way to authenticate service accounts on Google Cloud [here](#).

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).

[Learn more about setting organization policies for service accounts](#)

[ADD KEY](#) ▾

Create new key

Upload existing key

Key creation date Key expiration date

Create private key for "FileWave Service Account"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

☒ JSON

Recommended

☐ P12

For backward compatibility with code using the P12 format

[CANCEL](#)

[CREATE](#)

Private key saved to your computer

⚠ heroic-bird-319614-0f84693f89cb.json allows access to your cloud resources, so store it securely. [Learn more](#)

[CLOSE](#)

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".	

Add a new client ID

Client ID

111933499149382387933

☐ Overwrite existing client ID ?

OAuth scopes (comma-delimited) ×

https://www.googleapis.com/auth/admin.directory.!

OAuth scopes (comma-delimited) ×


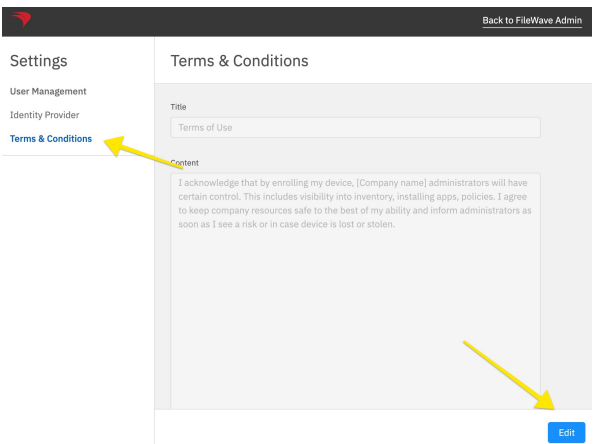
https://www.googleapis.com/auth/admin.directory.!

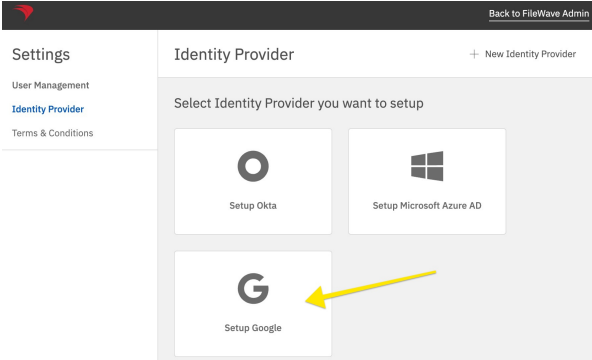
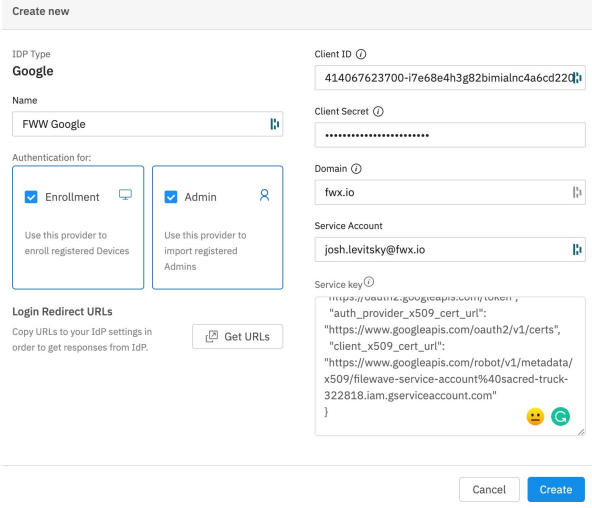
CANCEL
AUTHORIZE

Service account and permissions

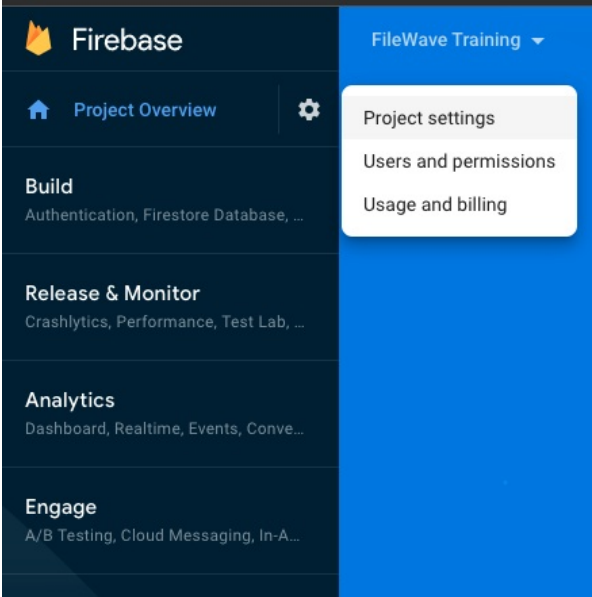
Step	Screenshot															
<p>(Step 20) - The next to last piece is setting up a service account. A service account is a user, that is going to be used in order to access resources. In order to add a user to a service account, navigate to https://console.cloud.google.com/apis/credentials and then 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.</p> <p>NOTE</p> <p>Make sure the user has at least read access to the User and Group resource.</p>	<div><div><div><div>←</div><div>FileWave Service Account</div></div><div><div>DETAILS</div><div>PERMISSIONS</div><div>KEYS</div><div>METRICS</div><div>LOGS</div></div></div><div><div>Resources this service account can access</div><div>You can create a policy report for this service account to view a summary of all resources this service account has access to.</div><div>VIEW ACCESS</div></div><div><div>Principals with access to this service account</div><div>You can allow specific users to have ownership and access to service accounts and their settings. Users with the Owner or Editor basic role on the project can already modify service accounts, but you might want to restrict access for some users so that they can take only specific actions against service account resources. Learn how to grant users access to service accounts</div><div><div>GRANT ACCESS</div></div><div><div>View By: <div>PRINCIPALS</div>ROLES</div><div><input type="checkbox"/> Include Google-provided role grants</div></div><div><div><div>Filter</div><div>Enter property name or value</div></div><table><thead><tr><th>Type</th><th>Principal ↑</th><th>Name</th><th>Role</th><th>Inheritance</th></tr></thead><tbody><tr><td></td><td>fw-josh-lab@sacred-truck-322818.iam.gserviceaccount.com</td><td>FW Josh Lab</td><td>Owner</td><td><div><div><div></div></div><div>FW Josh Lab</div><div></div></div></td></tr><tr><td></td><td>josh.levitsky@fwx.io</td><td>Josh Levitsky</td><td>Owner</td><td><div><div><div></div></div><div>FW Josh Lab</div><div></div></div></td></tr></tbody></table></div></div></div>	Type	Principal ↑	Name	Role	Inheritance		fw-josh-lab@sacred-truck-322818.iam.gserviceaccount.com	FW Josh Lab	Owner	<div><div><div></div></div><div>FW Josh Lab</div><div></div></div>		josh.levitsky@fwx.io	Josh Levitsky	Owner	<div><div><div></div></div><div>FW Josh Lab</div><div></div></div>
Type	Principal ↑	Name	Role	Inheritance												
	fw-josh-lab@sacred-truck-322818.iam.gserviceaccount.com	FW Josh Lab	Owner	<div><div><div></div></div><div>FW Josh Lab</div><div></div></div>												
	josh.levitsky@fwx.io	Josh Levitsky	Owner	<div><div><div></div></div><div>FW Josh Lab</div><div></div></div>												
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
<p>(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.</p> <p>Click on the Settings gear icon at the top of the page.</p>	 <p>The screenshot shows the top of the FileWave Admin interface. A yellow arrow points to the 'Settings' gear icon in the top navigation bar. Another yellow arrow points to the 'Search for Devices' button.</p>
<p>(Step 22) - Edit the Terms & Conditions to have appropriate text for your organization. This text is displayed when using an IdP to enroll devices.</p>	 <p>The screenshot shows the 'Terms & Conditions' page in the FileWave Admin interface. A yellow arrow points to the 'Terms & Conditions' link in the left sidebar. Another yellow arrow points to the 'Edit' button at the bottom right of the content area.</p>
(Step 23) - Click Setup Google or if you already have another IdP setup then	


<p>click New Identity Provider on the top right because this screen will look different.</p>	
<p>(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. 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.</p>	


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

Step	Screenshot
<p>(Step 25) - Now we need to enable the Admin SDK API for your project. Navigate to <a href="https://console.developers.google.com/apis/api/admin.googleapis.com/overview?project=<project-number>">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</p>	
<p>(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</p>	


Your project

Project name


FileWave Training 

Project ID 


filewave-training-45325


Project number 

600195963358


Default GCP resource location 

nam5 (us-central)

Parent org/folder in GCP 

 filewave.com

(Step 27) Click the Enable button




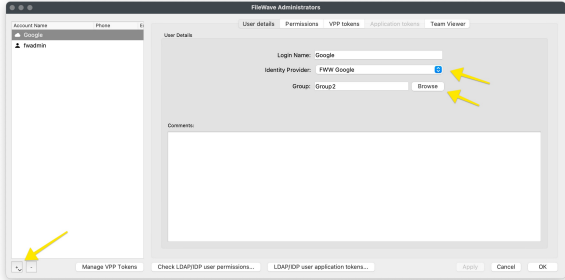
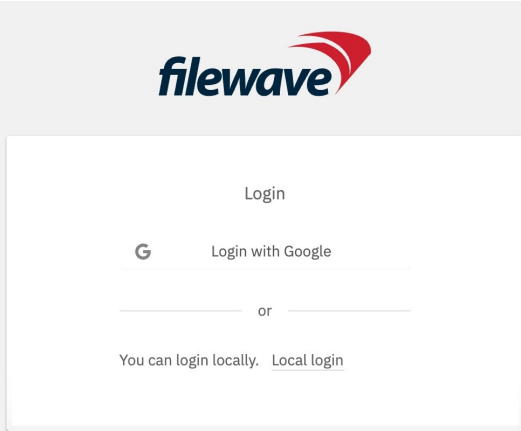
Admin SDK API

Google Enterprise API

Admin SDK lets administrators of enterprise domains to view and manage resources like user,...

ENABLE

TRY THIS API 

Step	Screenshot
<p>(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.</p> <p>Launch the Native Admin and go to Assistants → Manage Administrators.</p> <p>(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.</p>	
<p>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.</p>	

Login

 Login with Google

or

You can login locally. Local login

© 2021, FileWave International Inc., 14.6.0-fde16a2b11

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: https://www.googleapis.com/oauth2/v3/certs` 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

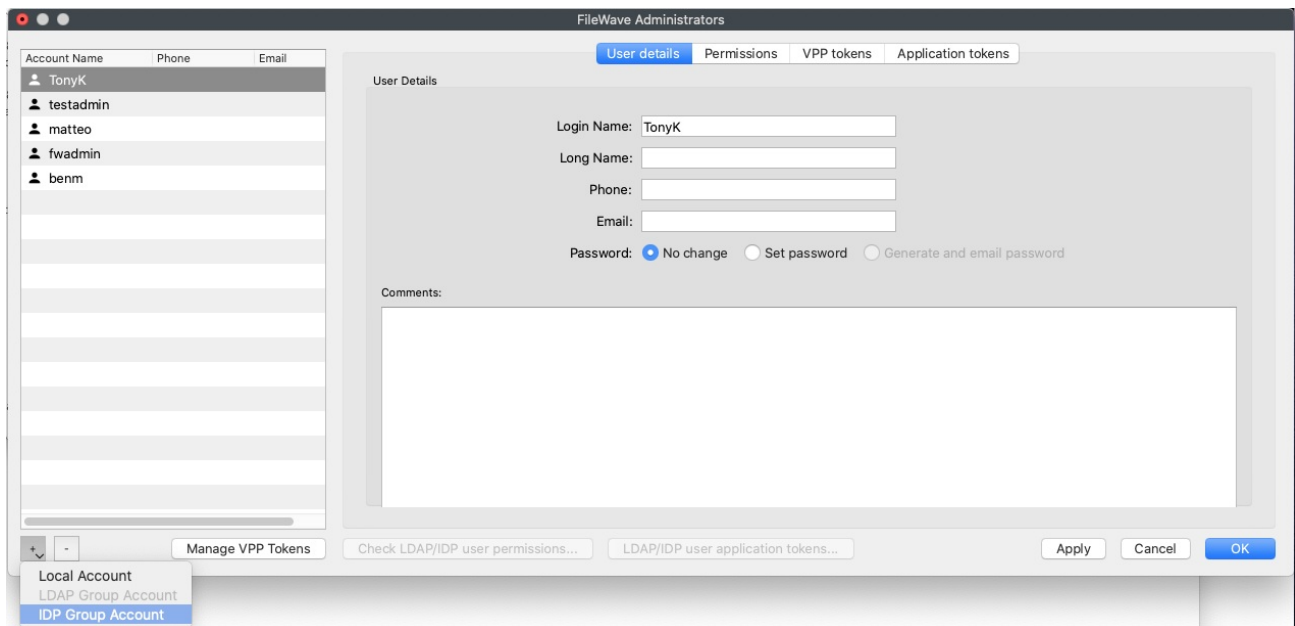
We'll use this as the configuration for admins to login, and to assign permissions. This method is especially helpful if you require 2 Factor Authentication through your IdP.

How

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

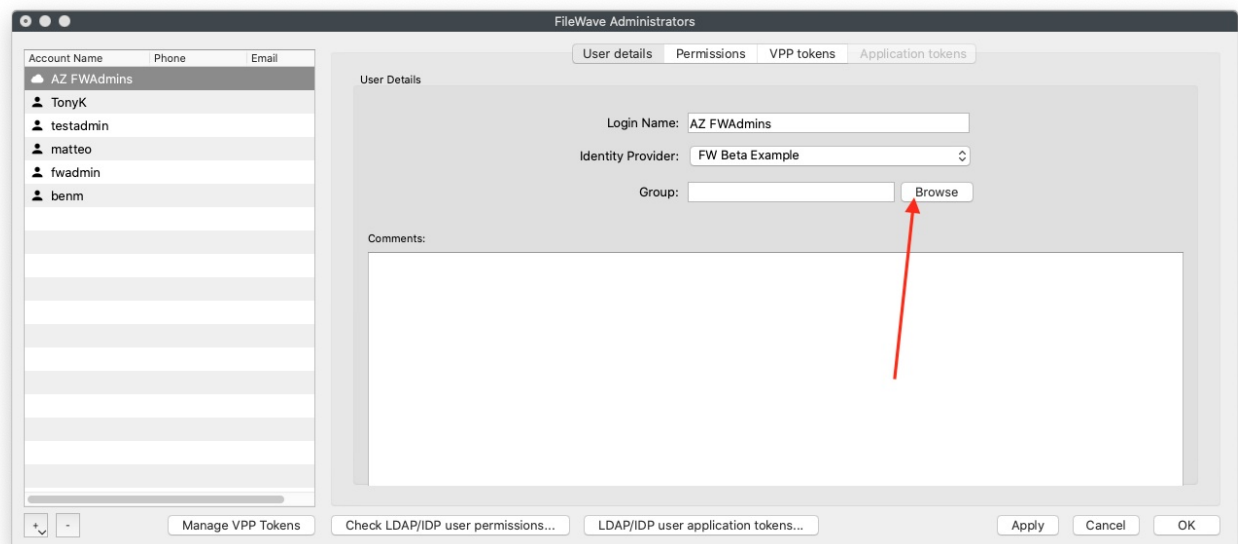
Assistants→ Manage Administrators

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

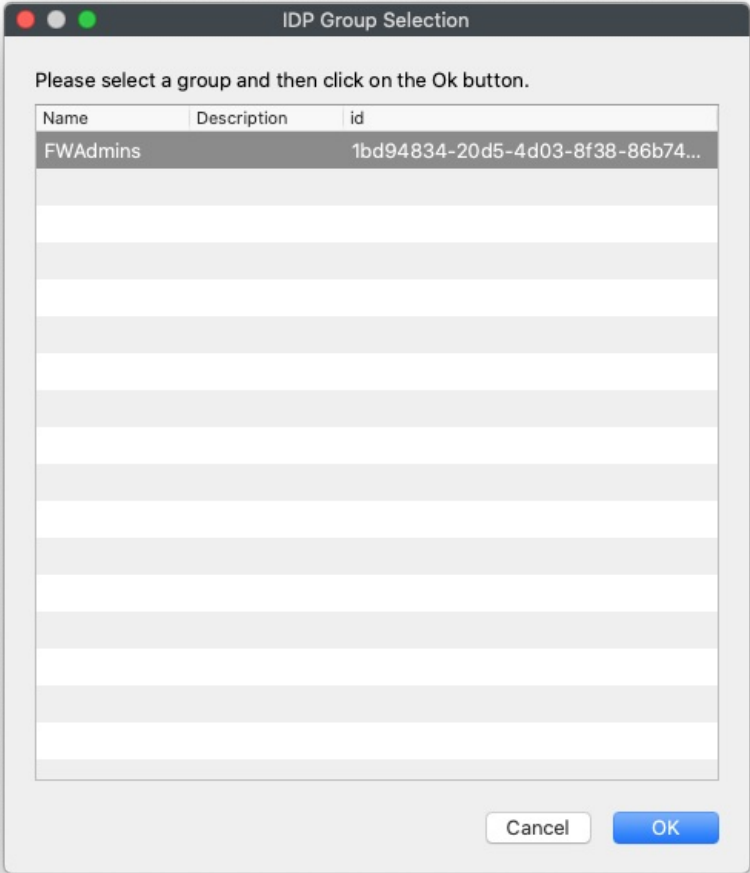


Give the group a name, and assign permissions as you would any normal local or LDAP based account.

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

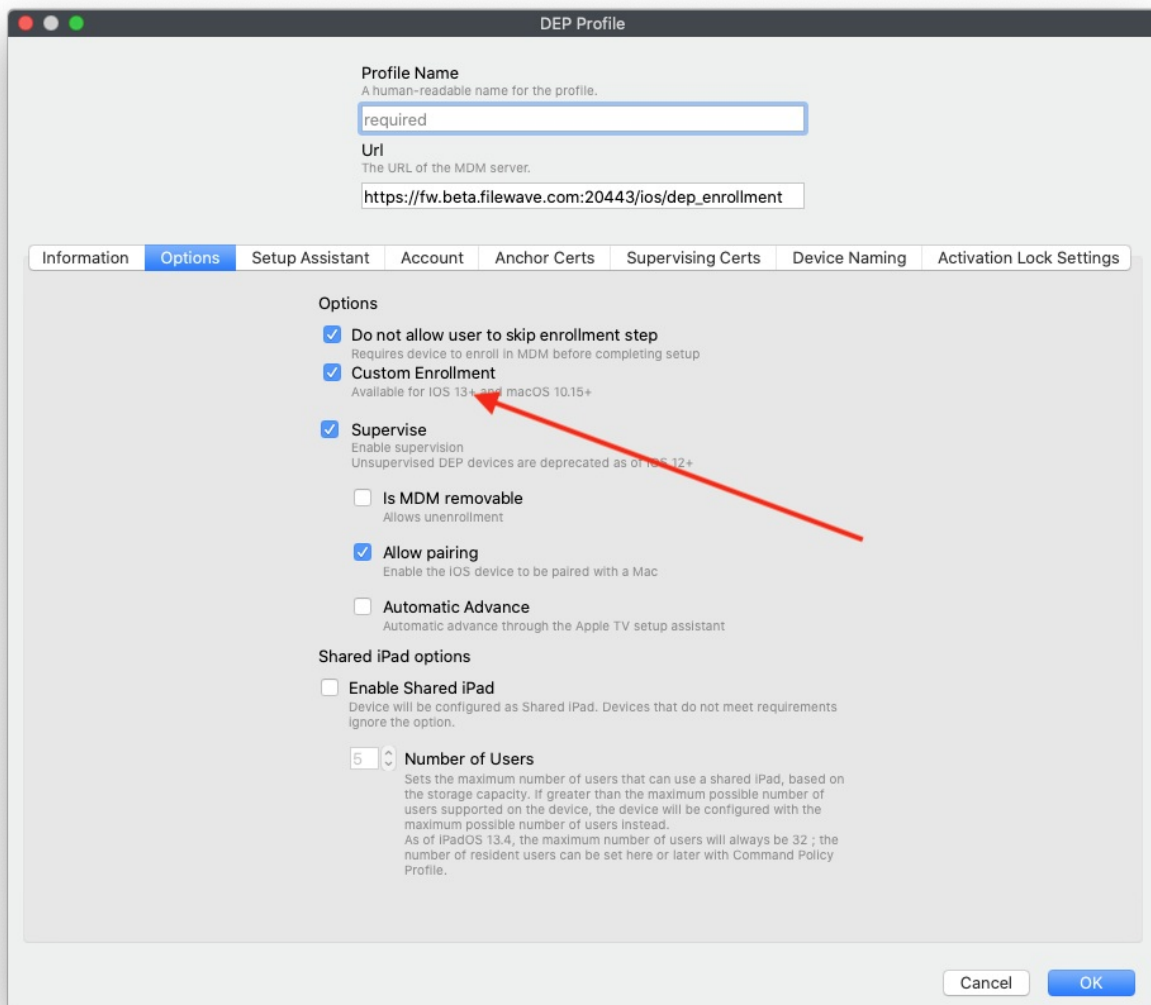
Configuring Apple Devices DEP Profiles to use IDP authentication.


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):



New DEP Profile 

Cancel

Save

General

Assigned devices

MDM Options

MDM Server

URL Address

https://fw.beta.filewave.com:20443/ios/dep_enrollment

Enrollment and supervise

☒ Required MDM enrollment ⓘ

☒ Custom enrollment ⓘ

☒ Supervision ⓘ

☐ Removable enrollment ⓘ

☒ Allow pairing ⓘ

☐ Automatic advance ⓘ

☐ Shared iPad (Only for Apple School Manager) ⓘ

Device naming

Naming policy only renames the devices without changing its client name.

New Devices

Rename Using the Name Template

Re-enrolled Devices (Same auth username)

Rename Using the Name Template

Re-enrolled Devices (New auth username)

Rename Using the Name Template

Name Template

%SerialNumber%

Use any inventory, custom, or LDAP attribute to include their values. [See full list](#)

Activation Lock Configuration

iCloud

MDM Options

Accounts

Setup Assistant

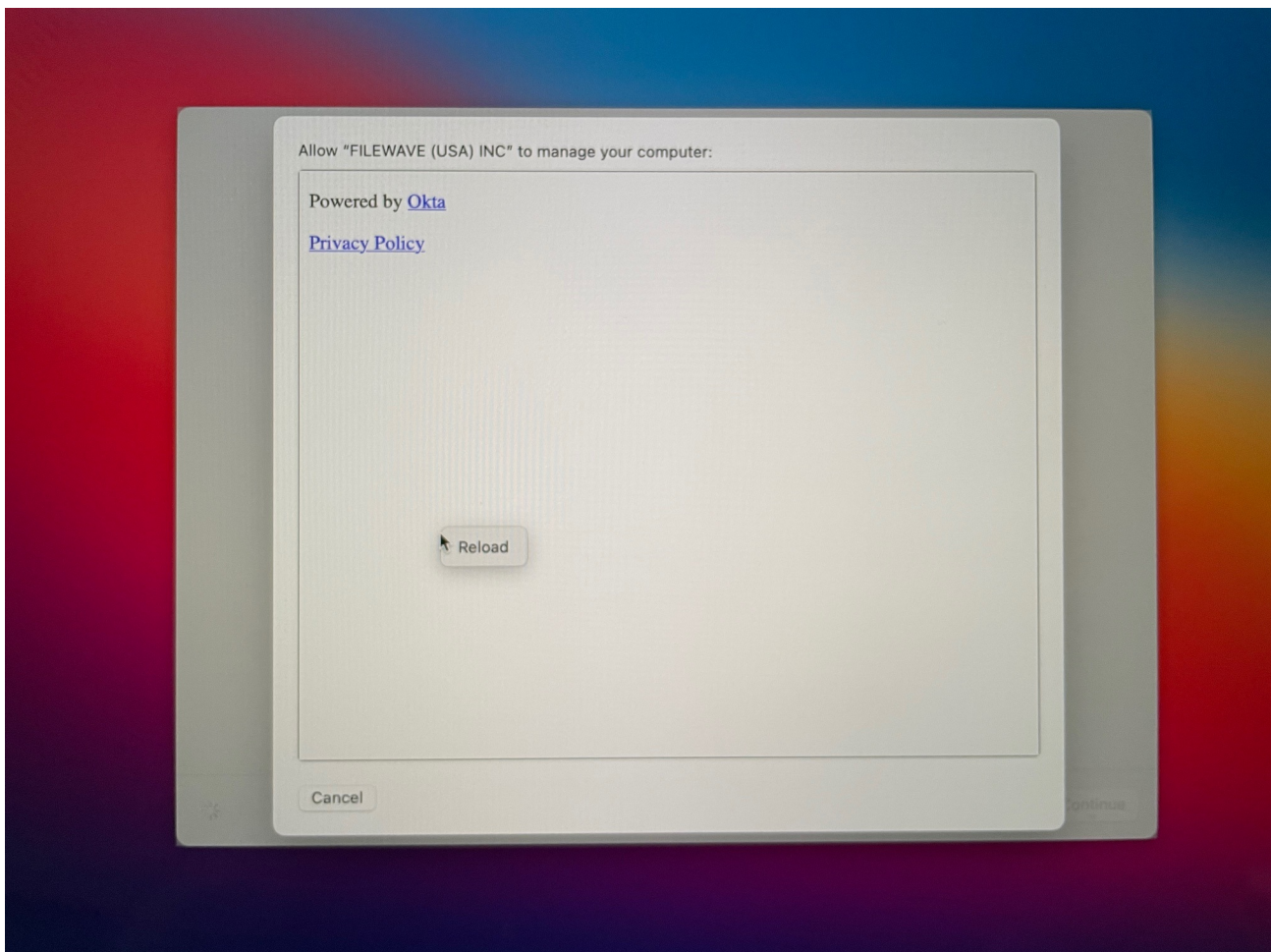
Certificates

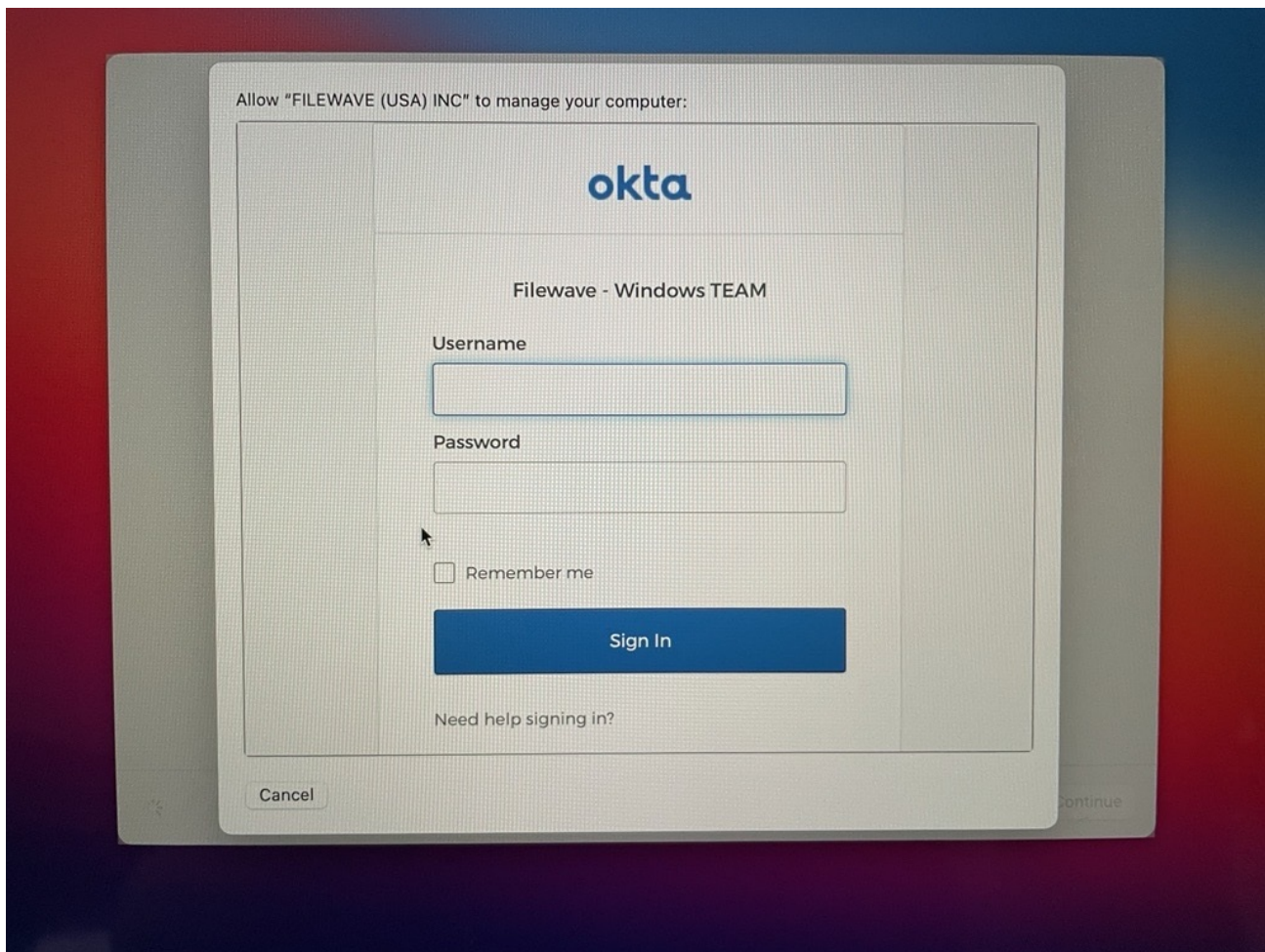
Information

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

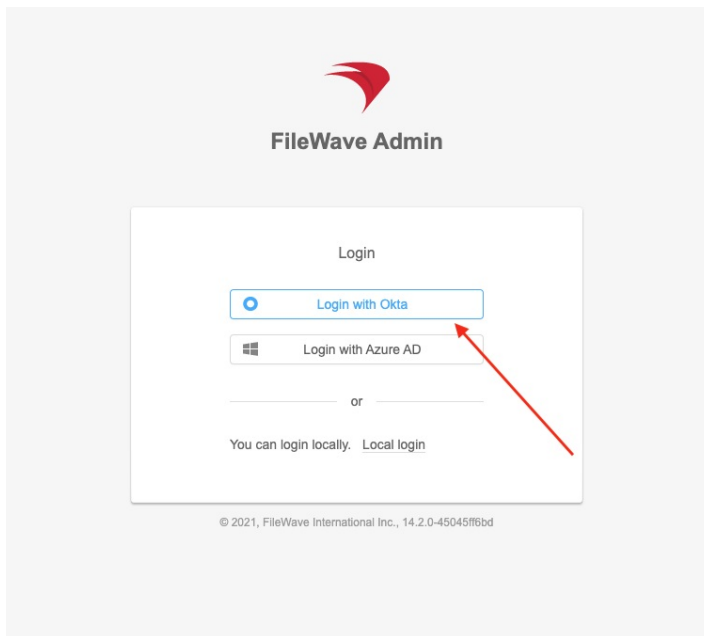
You'll notice some new options now for login once an IdP provider is specified.

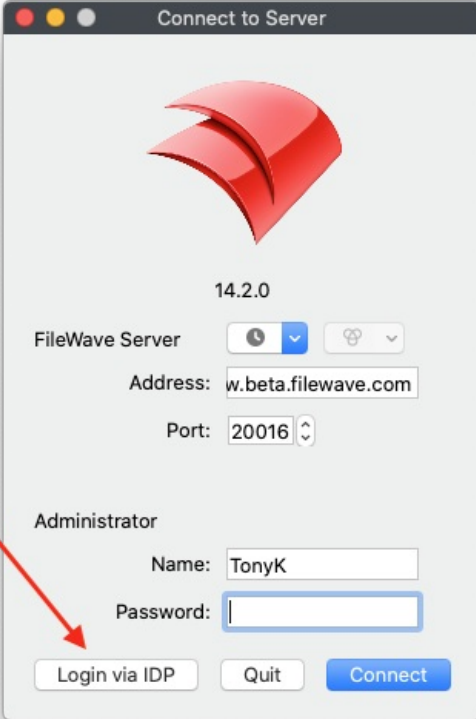
When/Why

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:





The image shows a 'Connect to Server' dialog box with a red ribbon icon at the top. Below the icon is the version number '14.2.0'. The 'FileWave Server' section includes a status indicator (a clock icon and a blue checkmark) and a dropdown menu. The 'Address' field contains 'w.beta.filewave.com' and the 'Port' field contains '20016'. The 'Administrator' section has a 'Name' field with 'TonyK' and a 'Password' field. A red arrow points to the 'Login via IDP' button at the bottom left, which is next to 'Quit' and 'Connect' buttons.

Connect to Server

14.2.0

FileWave Server

Address: w.beta.filewave.com

Port: 20016

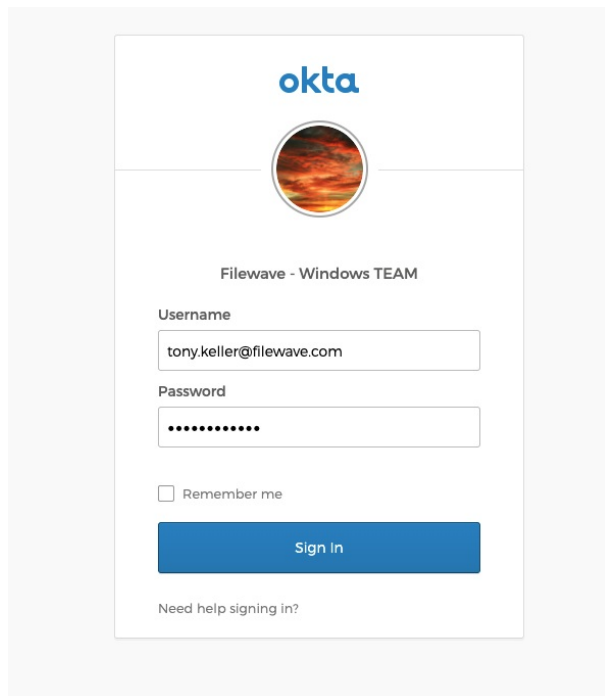
Administrator

Name: TonyK

Password:

Login via IDP Quit Connect

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



The image shows an Okta login page. At the top is the Okta logo. Below it is a circular profile picture of a person. The text 'Filewave - Windows TEAM' is displayed. The 'Username' field contains 'tony.keller@filewave.com' and the 'Password' field is masked with dots. There is a 'Remember me' checkbox and a blue 'Sign in' button. At the bottom, there is a link that says 'Need help signing in?'.

okta

Filewave - Windows TEAM

Username

tony.keller@filewave.com

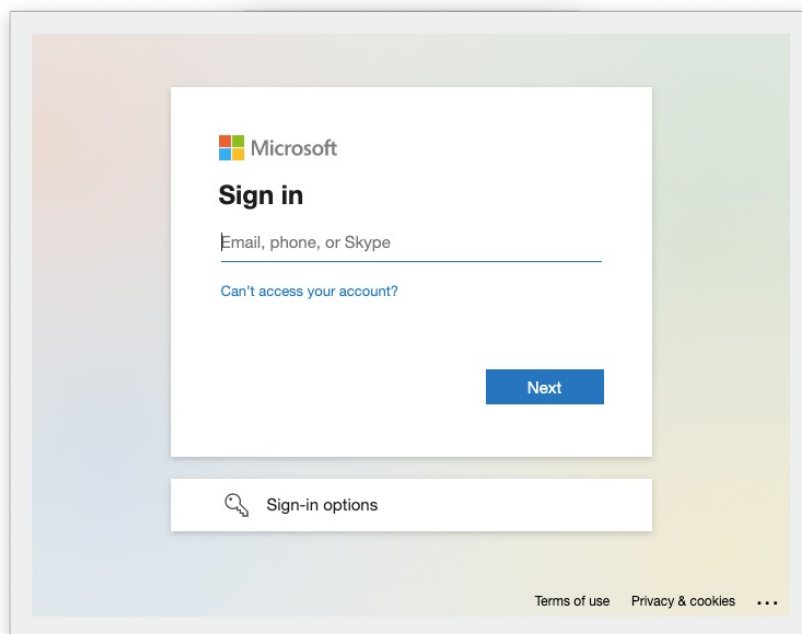
Password

.....

☐ Remember me

Sign in

Need help signing in?



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

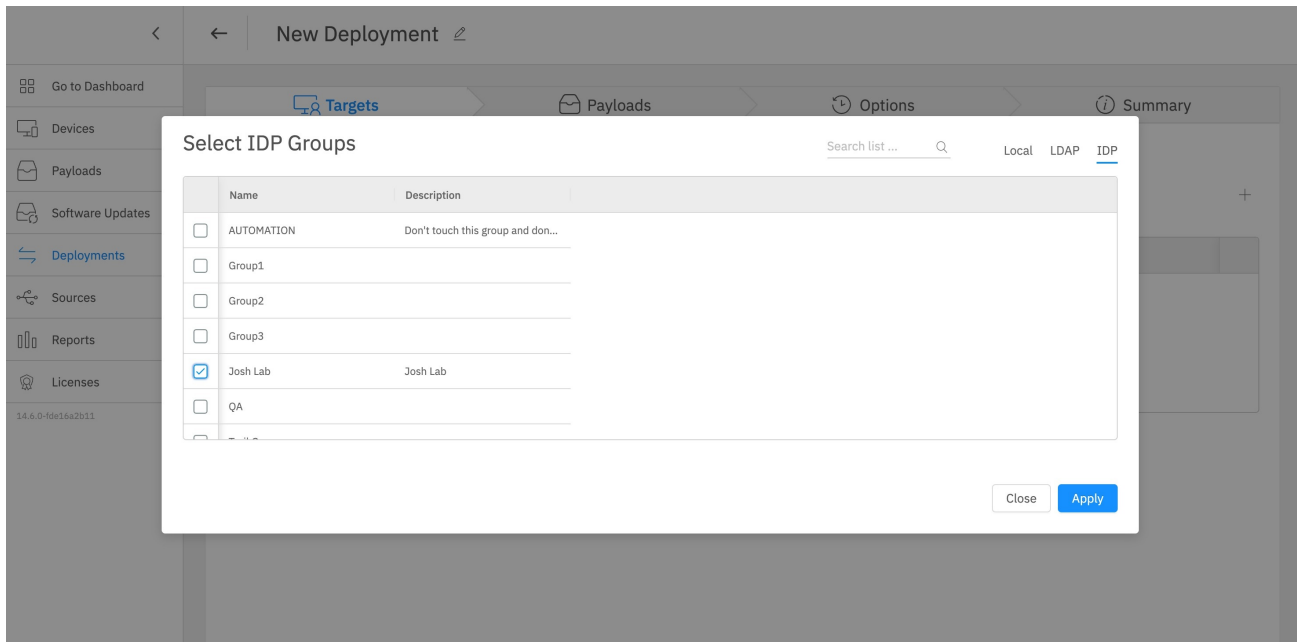
As a FileWave administrator using IdP enrollment of devices, I need to report on what groups devices are a part of in order to report on them and target software.

When/Why

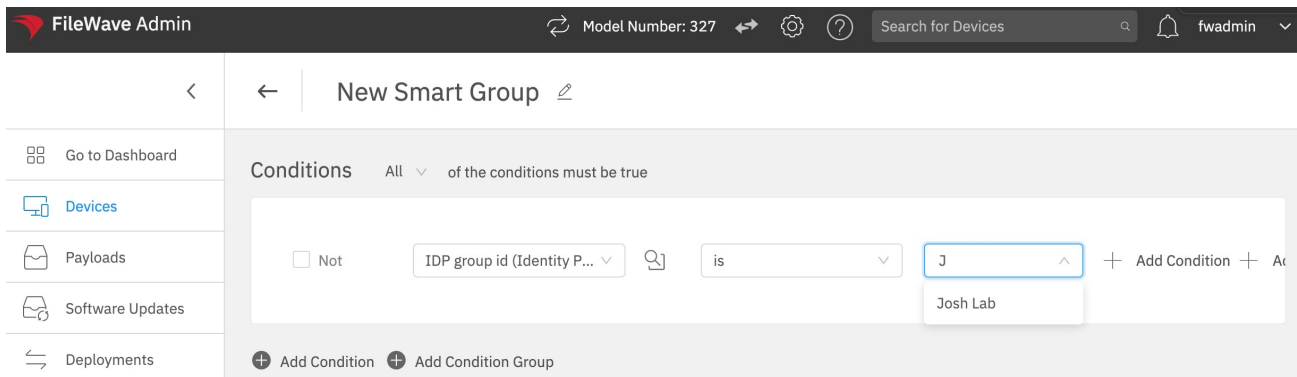
There is a new field that is populated which you can use for targeting deployments in the Web Admin, and for reporting queries both in Web Admin and the Native Admin.

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

Q

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

CriteriaFieldsClients

All of these expressions must be true

☐ Not in Groups for smart groups / IDP group id

is

02koq65640u05wc

+ - Add Group

Move upMove downMove in next groupMove before parent

CancelSave

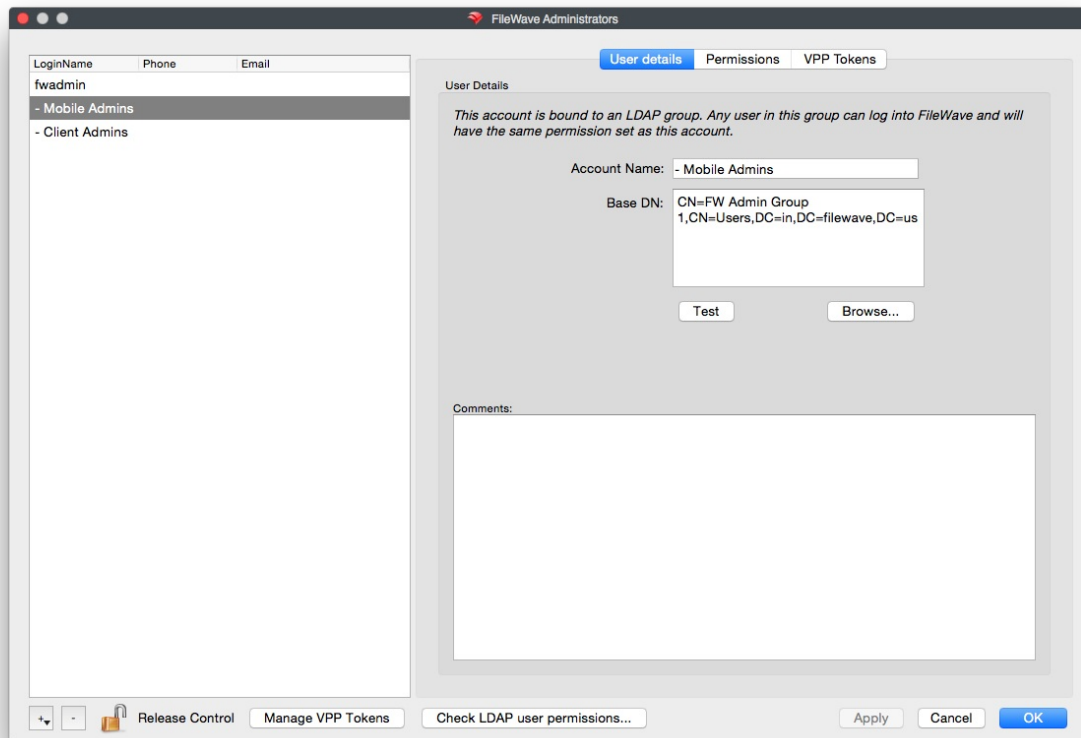
LDAP Admin Integration

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:

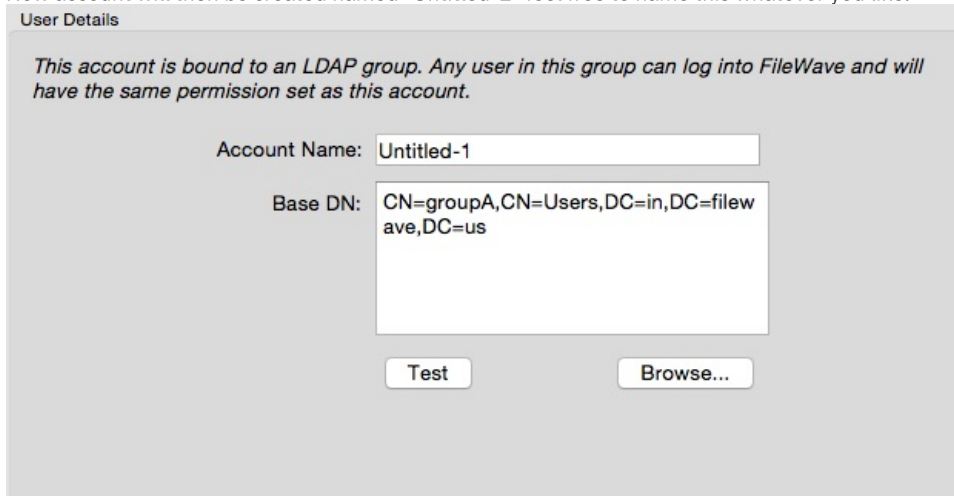
1. Open the FileWave Administrators window by navigating to the Assistants menu, and then selecting Manage Administrators. Once in the FileWave Administrators window, hit the "+" button at the bottom left of the window.



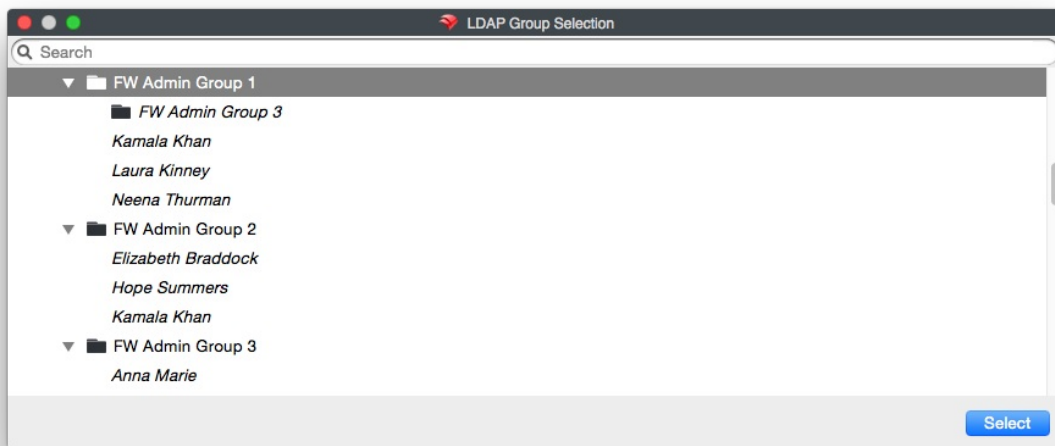
2. Select LDAP Group Account

Local Account
LDAP Group Account

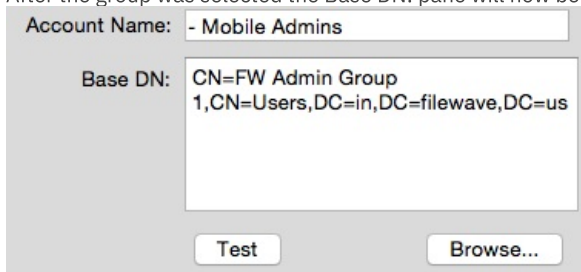
3. New account will then be created named "Untitled-1" feel free to name this whatever you like.



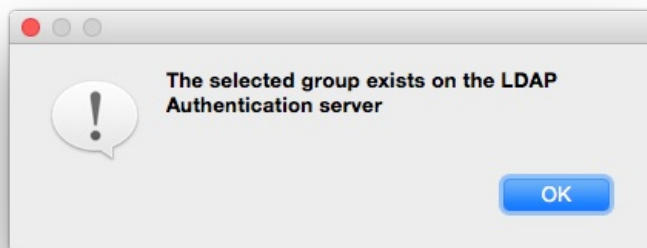
4. Once you have named your account, locate and click the Browse... button at the bottom right of the Base DN: pane
5. You will now be prompted with the LDAP browser where you can now find and hit Select for the group you want to associate. This will associate all the users in your specified group. As 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.

User details Permissions **VPP Tokens**

Server/Model

☒ Update Model ☐ Activation Keys
☒ Revert Model ☐ Auditing

User Administration

☐ Can administer users

Clients and Groups

☒ Modify Clients/Groups ☐ Set Permissions
☐ Clear Fileset Status

Filesets and Groups

☒ Modify Filesets ☒ Export Fileset/Template
☒ Show Fileset Report ☒ Manage VPP codes
☐ Set Permissions

Associations

☒ Modify Associations ☒ Approve Software Updates
☐ Modify Imaging Associations

DEP

☒ Edit Profiles
☒ Assign Profiles

Dashboard

☐ Configure dashboard

Select None Select All

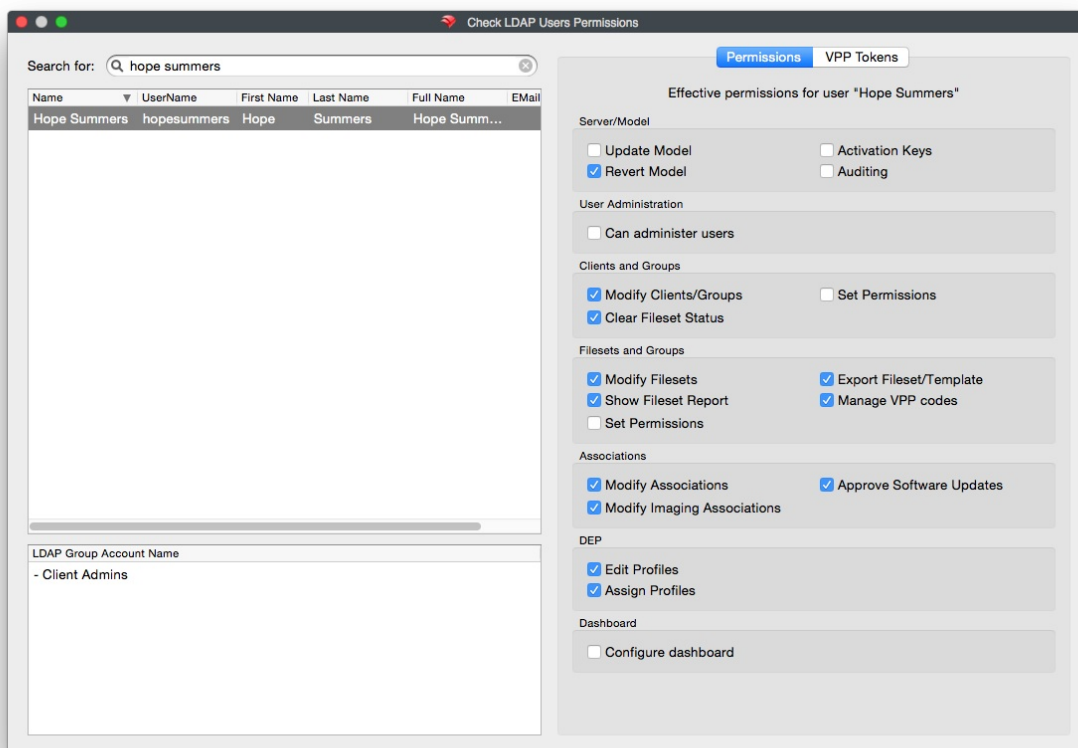
9. The final tab is called VPP Tokens. These will be the VPP Tokens that this group of users can manage in FileWave. To add or remove VPP token access for users and groups, click Manage VPP Tokens, and hit the check box for each token you want each user to manage.

User details Permissions **VPP Tokens**

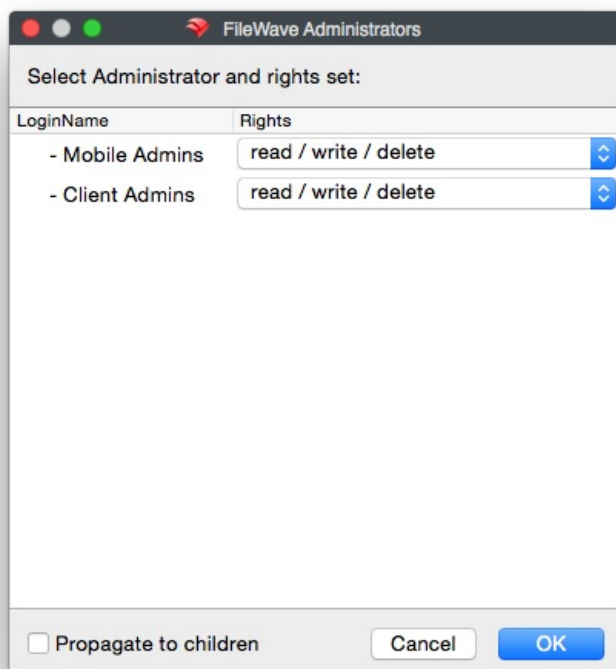
VPP Token name

vpp

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 synchronization 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.

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](#)