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.

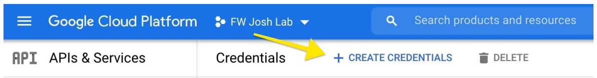
NOTE: CANNOT be IP Address or self-signed cert. Must be FQDN - Instructions Linked Here

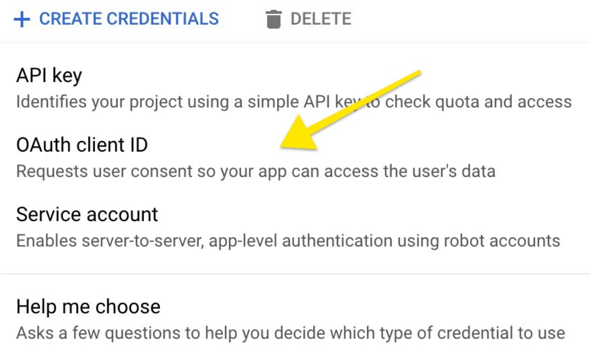
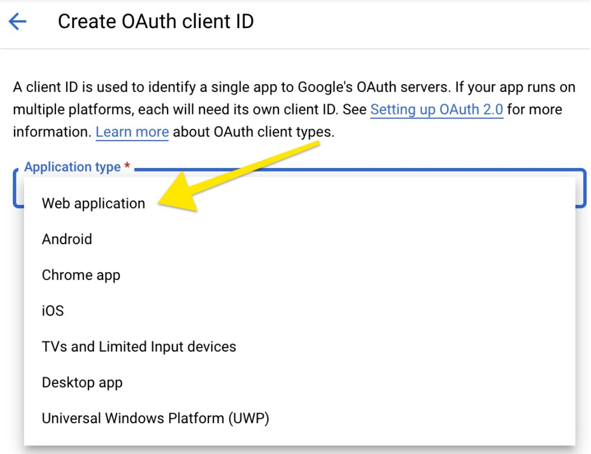
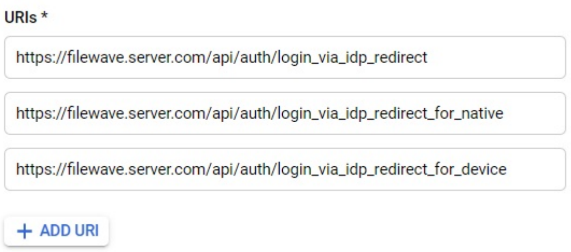
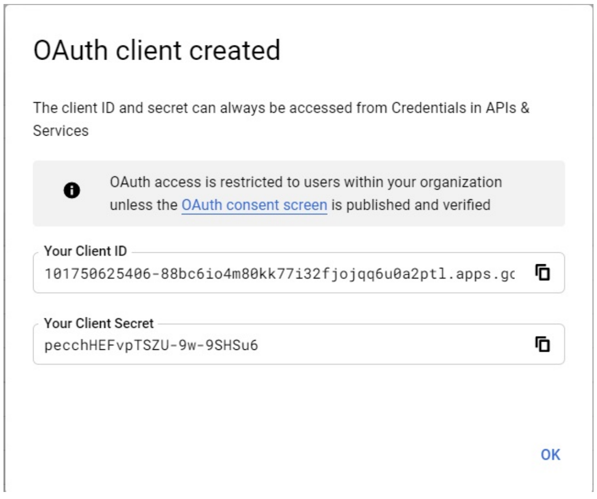
Domain verification

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)

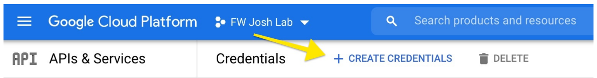
Below is an excerpt on how to obtain a Client ID and client secret. For a more detailed tutorial and additional information, check the documentation.

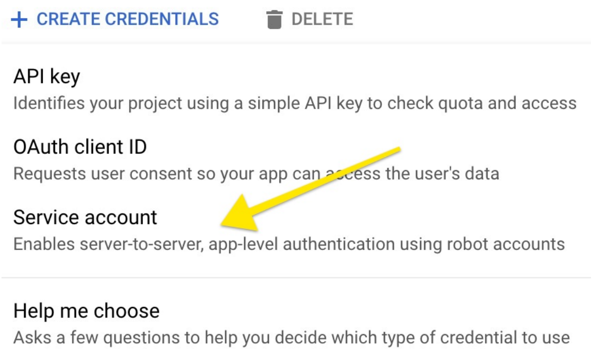
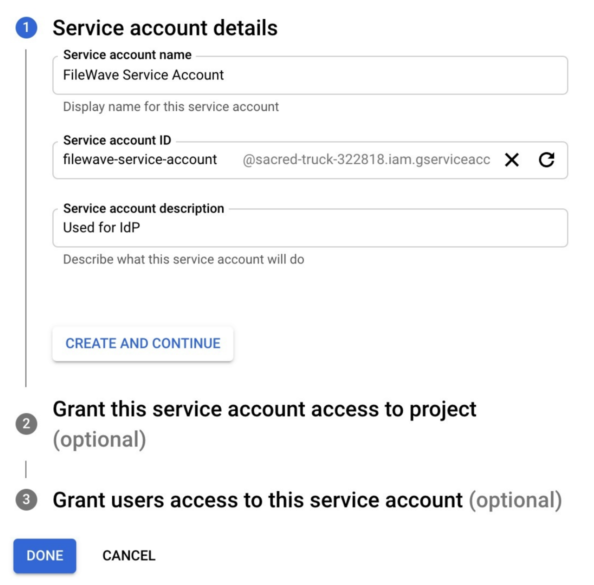
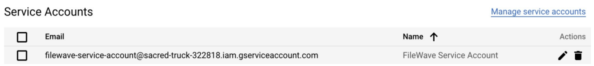
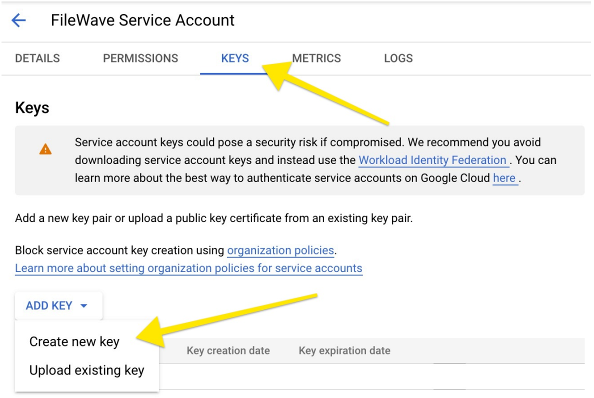
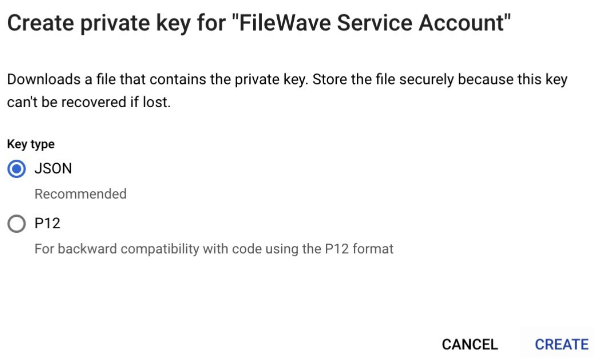
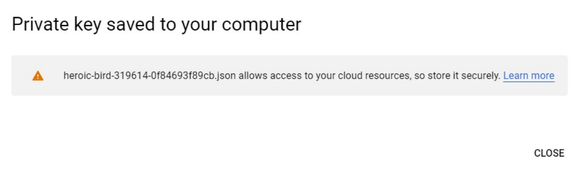
Step	Example screenshot
(Step 1) - Navigate to https://console.cloud.google.com/apis/credentials	/
(Step 2) - Click on "Create credentials"	 Google Cloud Platform FW Josh Lab Search products and resources API APIs & Services Credentials + CREATE CREDENTIALS DELETE
(Step 3) - Choose "OAuth client ID"	

	 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
(Step 4) - In the next screen, choose "Web application"	Create OAuth client ID 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. Application type * Web application Android Chrome app iOS TVs and Limited Input devices Desktop app Universal Windows Platform (UWP)
(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	URIs * 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
(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.	OAuth client created The client ID and secret can always be accessed from Credentials in APIs & Services OAuth access is restricted to users within your organization unless the OAuth consent screen is published and verified Your Client ID 101750625406-88bc6io4m80kk77i32fjojqq6u0a2ptl.apps.gc Your Client Secret pecchHEFvpTSZU-9w-9SHSu6

Creating a service account (Google)

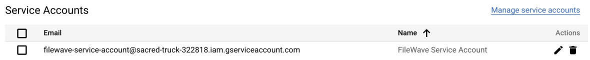
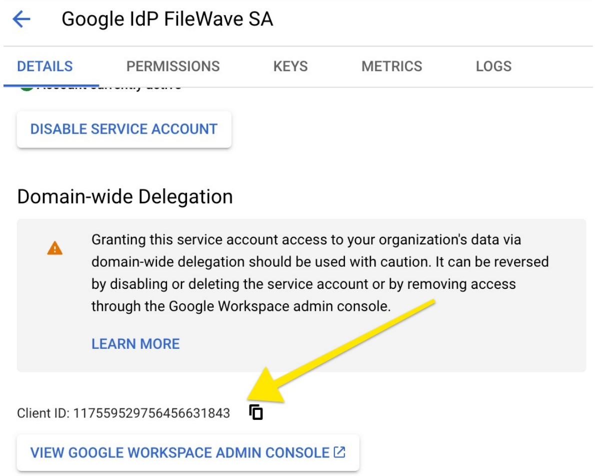
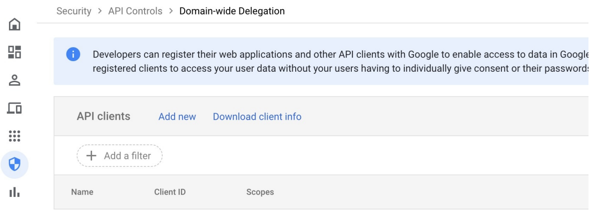
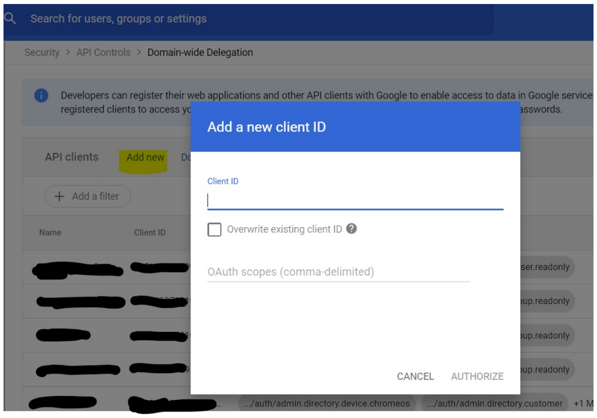
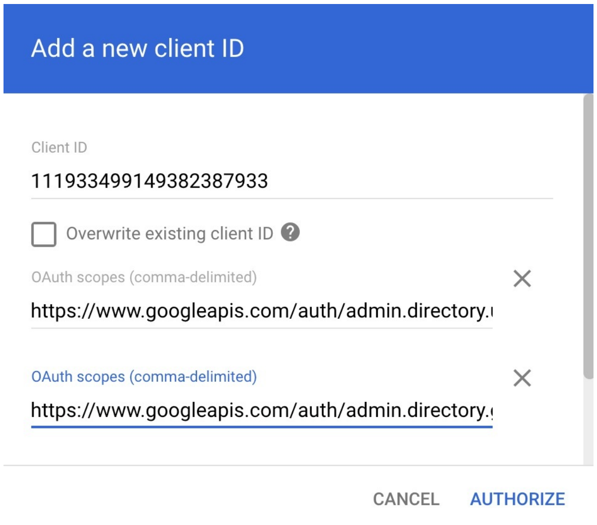
To support server-to-server interactions, first create a service account for your project in the API Console. - Google documentation

Step	Example screenshot
(Step 7) - Navigate to https://console.cloud.google.com/apis/credentials	/
(Step 8) - Click on "Create credentials"	 Google Cloud Platform FW Josh Lab Search products and resources API APIs & Services Credentials CREATE CREDENTIALS DELETE
(Step 9) - Choose "Service account"	

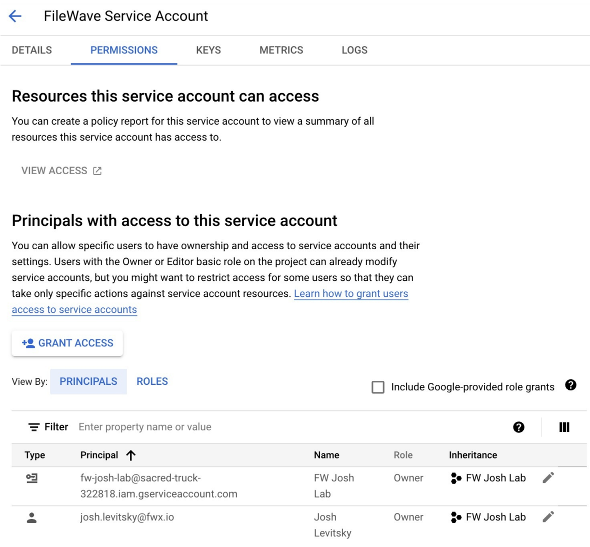
	 + CREATE CREDENTIALS DELETE API key Identifies your project using a simple API key to check quota and access OAuth client ID Requests user consent so your app can access the user's data Service account Enables server-to-server, app-level authentication using robot accounts Help me choose Asks a few questions to help you decide which type of credential to use
(Step 10) - Input required details and click "DONE". NOTE Skip optional steps 2 and 3, we will take care of it later.	 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 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
(Step 11) - Newly created service account should now be visible in the list of service accounts. (it might take few minutes)	 Service Accounts Manage service accounts □ Email Name ↑ Actions □ filewave-service-account@sacred-truck-322818.iam.gserviceaccount.com FileWave Service Account
(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".	 ← 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
(Step 13) - Click on "Create new key", select JSON type and click "Create".	 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
(Step 14) - Service key is now downloading to your computer. Save it, as it's needed in further configuration.	 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

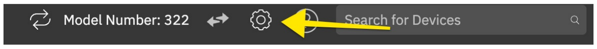
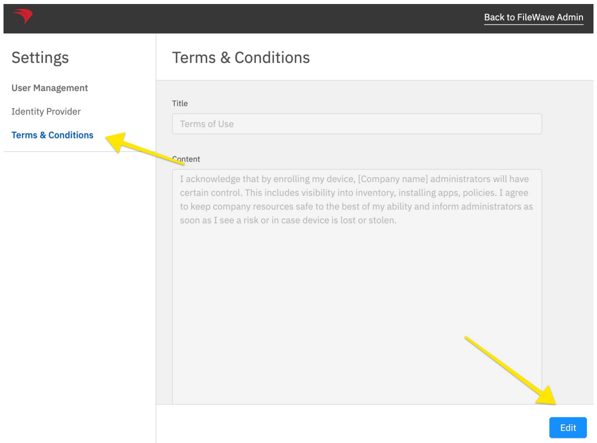
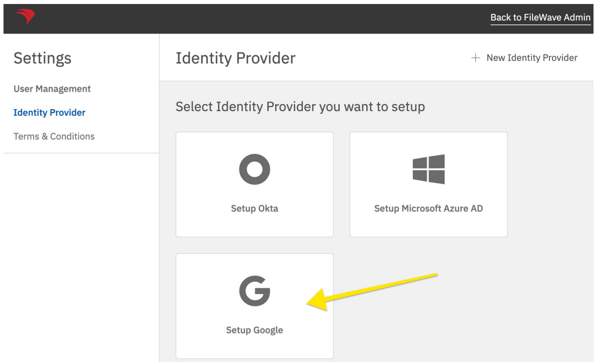
If you want to access user data for users in your Google Workspace account, then delegate domain-wide access to the service account. - Google documentation

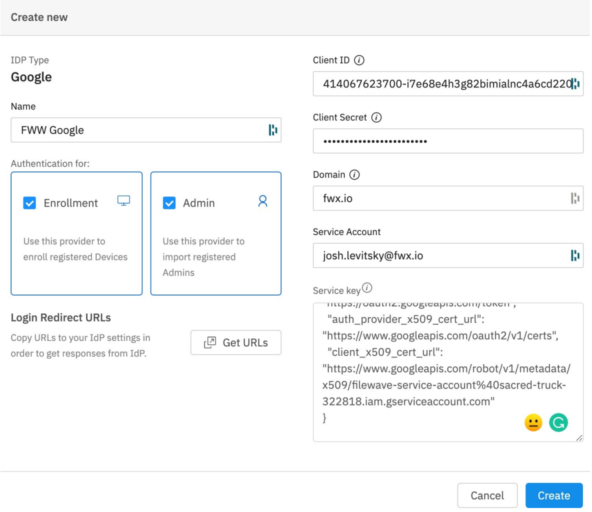
Step	Screenshot
(Step 15) - Navigate to https://console.cloud.google.com/apis/credentials	 Service Accounts Manage service accounts □ Email · Name ↑ · Actions □ filewave-service-account@sacred-truck-322818.iam.gserviceaccount.com · FileWave Service Account
(Step 16) - Open newly created service account details, by clicking on the service account name. Click SHOW ADVANCED SETTINGS. Save Client ID as it will be used later on..	 Google IdP FileWave SA DETAILS · PERMISSIONS · KEYS · METRICS · LOGS DISABLE SERVICE ACCOUNT Domain-wide Delegation Granting this service account access to your organization's data via domain-wide delegation should be used with caution. It can be reversed by disabling or deleting the service account or by removing access through the Google Workspace admin console. LEARN MORE Client ID: 117559529756456631843 VIEW GOOGLE WORKSPACE ADMIN CONSOLE
(Step 17) - Navigate to https://admin.google.com/ac/owl/domainwidedelegation	 Security > API Controls > Domain-wide Delegation Developers can register their web applications and other API clients with Google to enable access to data in Google registered clients to access your user data without your users having to individually give consent or their passwords API clients · Add new · Download client info + Add a filter Name · Client ID · Scopes
(Step 18) - Click on "Add New" to create a new domain delegation. NOTE You will need super administrator permissions for this step.	 Search for users, groups or settings Security > API Controls > Domain-wide Delegation Developers can register their web applications and other API clients with Google to enable access to data in Google service registered clients to access yo … asswords. API clients · Add new · Do + Add a filter Name · Client ID [redacted] [redacted] … ser.readonly [redacted] [redacted] … up.readonly [redacted] [redacted] … up.readonly [redacted] [redacted] … up.readonly [redacted] [redacted] … .../auth/admin.directory.device.chromeos · .../auth/admin.directory.customer · +1 M Add a new client ID Client ID □ Overwrite existing client ID OAuth scopes (comma-delimited) CANCEL · AUTHORIZE
(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.ı OAuth scopes (comma-delimited) https://www.googleapis.com/auth/admin.directory.(CANCEL · AUTHORIZE

Service account and permissions

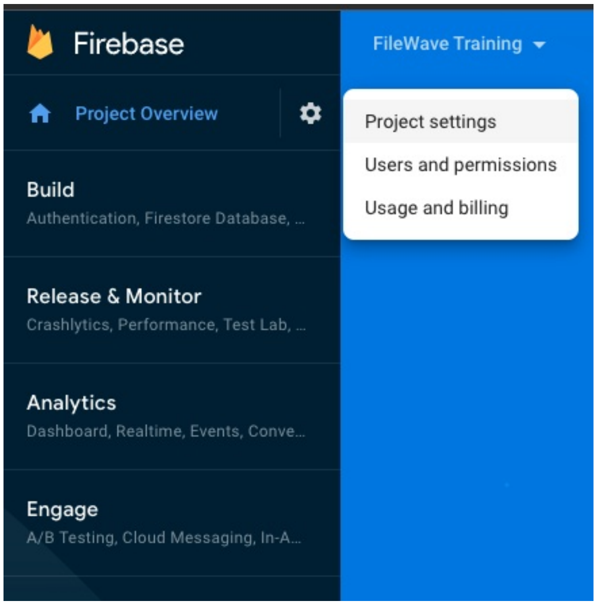
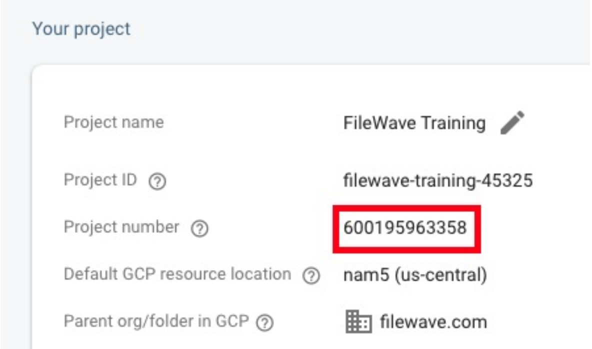
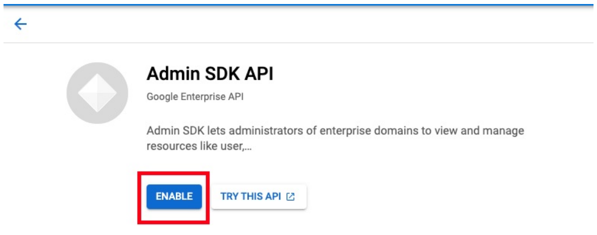
Step	Screenshot
(Step 20) - The next to last piece is setting up a service account. A service account is a user, that is going to be used in order to access resources. In order to add a user to a service account, navigate to https://console.cloud.google.com/apis/credentials and then click the service account you created, click on the Permissions tab, and add a user you'd like to use for accessing Google Workspace resources. NOTE Make sure the user has at least read access to the User and Group resource.	 FileWave Service Account DETAILS PERMISSIONS KEYS METRICS LOGS **Resources this service account can access** You can create a policy report for this service account to view a summary of all resources this service account has access to. VIEW ACCESS **Principals with access to this service account** 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 GRANT ACCESS View By: PRINCIPALS ROLES □ Include Google-provided role grants Filter Enter property name or value Type | Principal | Name | Role | Inheritance fw-josh-lab@sacred-truck-322818.iam.gserviceaccount.com | FW Josh Lab | Owner | FW Josh Lab josh.levitsky@fwx.io | Josh Levitsky | Owner | FW Josh Lab
The selected user's email becomes your service account token.	Example "josh.levitsky@fwx.io"

Configure Filewave server to use Google as IdP (Filewave)

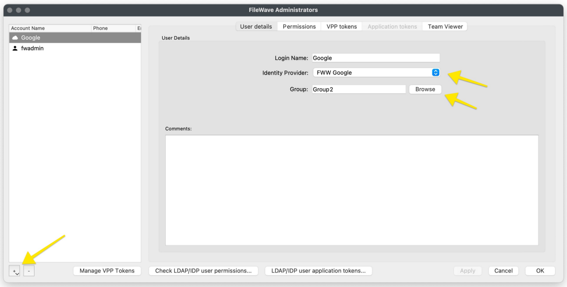
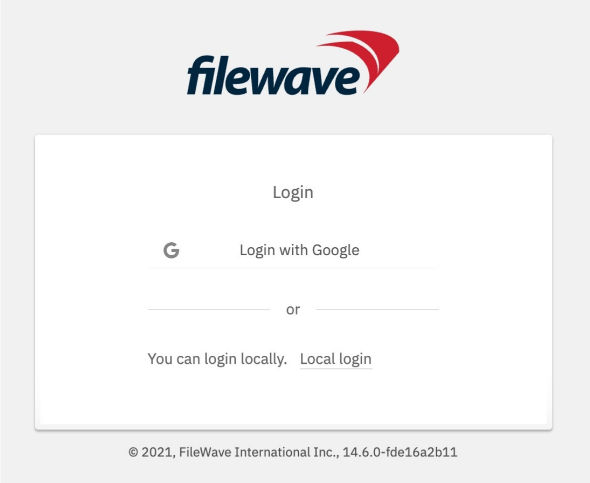
Step	Screenshot
(Step 21) - The last piece of the puzzle is setting up Filewave to talk to Google. Navigate to https://filewave.server.com replacing the address with your FileWave server. Login as fwadmin to be sure you will have proper permissions to make the next changes. Click on the Settings gear icon at the top of the page.	 Model Number: 322 Search for Devices
(Step 22) - Edit the Terms & Conditions to have appropriate text for your organization. This text is displayed when using an IdP to enroll devices.	 Back to FileWave Admin Settings User Management Identity Provider Terms & Conditions Terms & Conditions Title Terms of Use Content I acknowledge that by enrolling my device, [Company name] administrators will have certain control. This includes visibility into inventory, installing apps, policies. I agree to keep company resources safe to the best of my ability and inform administrators as soon as I see a risk or in case device is lost or stolen. Edit
(Step 23) - Click Setup Google or if you already have another IdP setup then click New Identity Provider on the top right because this screen will look different.	 Back to FileWave Admin Settings User Management Identity Provider Terms & Conditions Identity Provider + New Identity Provider Select Identity Provider you want to setup Setup Okta Setup Microsoft Azure AD Setup Google
(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.	 Create new IDP Type Google Name FWW Google 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 414067623700-i7e68e4h3g82bimialnc4a6cd220 Client Secret •••••••••••••••••••••••• Domain fwx.io Service Account josh.levitsky@fwx.io Service key "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs", "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/filewave-service-account%40sacred-truck-322818.iam.gserviceaccount.com" } Cancel Create

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

Step	Screenshot
(Step 25) - Now we need to enable the Admin SDK API for your project. Navigate to https://console.developers.google.com/apis/api/admin.googleapis.com/overview?project=<project-number> Fill in <project-number> is from Firebase/Project settings/General/Project number If you are unsure what this is you can find it via logging into http://console.firebase.google.com/ > click your Firebase Project > Click the gear icon at the top left to the right of "Project Overview" > Project Settings	 Firebase FileWave Training Project Overview Project settings Users and permissions Usage and billing Build Authentication, Firestore Database, ... Release & Monitor Crashlytics, Performance, Test Lab, ... Analytics Dashboard, Realtime, Events, Conve... Engage A/B Testing, Cloud Messaging, In-A...
(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	 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,...

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

Step	Screenshot
(Step 28) - Now that you have configured FileWave to talk to Google for Admin you need to go into the Native Admin to enable admins to actually log in and set their permissions. Launch the Native Admin and go to Assistants → Manage Administrators.	
(Step 29) - Click the + on the lower-left corner and pick IdP Group Account. On this screen, it is important to clarify that you are not defining a user here but a group of users. The Login Name is misleading here, and should be thought of as the name of the group of users so you might put something like Google - Desktop Techs and then for Identity Provider make sure your Google connection is selected that you set up in the prior steps. For Group click the Browse button and select the group that includes all of the users who will have access. If you will give all of your users the same level of permissions then you can use one group for all of your FileWave admins, but if you will use different levels of access then make an IdP Group Account on this window to define each of your groups of FileWave admins. In the image, you see a single entry for Google which might be appropriate if all of the FileWave admins are in a single group on the Google side.	 FileWave Administrators Account Name: Google Account Name: fwadmin User Details Login Name: Google Identity Provider: FWW Google Group: Group2 Comments: Phone User details Permissions VPP tokens Application tokens Team Viewer Browse + - Manage VPP Tokens Check LDAP/IDP user permissions... LDAP/IDP user application tokens... Apply Cancel OK
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.	 Login You can login locally. © 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

Revision #6
Created 21 June 2023 20:18:49 by Josh Levitsky
Updated 31 May 2024 19:24:19 by Josh Levitsky