User/Administrator Manual for Team Envolution's Secure File Sharing

Donald Tran, Rolland Goodenough, Tyler Huckeba, Spencer Wirth

Capstone Project Spring 2023

The University of West Florida

26 April 2023

CIS4595

Dr. Owsnicki-Klewe

Secure File Share

Product Functions and Capabilities

For teams, organizations, and businesses alike, Envolution's Secure Document Sharer is a practical and secure solution for sharing documents between multiple users. The purpose of this product is to provide a way to share files with a group in a secure manner. The product allows users to upload and share files into a secure environment, with the ability to see files in groups/clusters based on individual user permissions.

With the Secure File Sharing web application, users will be able to set up group systems in which specific users may be granted access to files and resources. Additionally, the Secure File Sharing web application has capabilities set up for administrators to manage their groups and its files. Administrators of respective groups get privileged abilities such as the ability to remove members from their group and to delete files from their group drives.

Product Features and Function

The web-based application for Secure File Sharing incorporates a variety of functionalities that facilitate the effortless storage, retrieval, and deletion of digital files. These functionalities encompass the following attributes:

1) **Account Setup (Register and Login)**

   The web-based application allows users the ability to create an account through the log-in screen of the web applkication. The Secure File Sharing web application utilizes Google's authentication system, therefore, users may effortlessly log-in using their Google accounts. If the user does not have an account, they may register an account through Google and use that to log in. The utilization of Google's authentication system ensures that user log in through the File Sharing web application is secure through the usage of CAPTCHA technology and two-step verification.

   Account Registering:
   1. The user selects the "Login to Envolution" button.
   2. The user clicks on the "Sign Up" button through Google's authentication.

3. The user is prompted to enter their Google account credentials, such as their email and password.
4. Google's authentication system verifies the user's credentials, and the account is created.

Account Login:

1. The user is redirected back to the Google's authentication login page.
2. The user enters in their Google account credentials and clicks "Log In". Depending on the user's Google account security, they may have to go through a two-factor authentication.

2) Personal File Storage

Users can upload files from their local machine to their personal file storage on the web-application. Furthermore, the user may download the file uploaded as well as delete the file from their drives.

Personal File Upload:

1. The user navigates to the "My Drive" view of the web application through the navigation button on the web-application sidebar.
2. The user clicks on the "Upload New File" button from the web-application sidebar.
3. The user clicks "Choose File" to choose a file from their local machine.
4. The user clicks "Submit" to upload to file to their personal drive.

Personal File Download:

1. To download files from their personal drive, the user clicks on the respective file in their My Drive document table view.

Personal File Deletion:

1. To delete files from their personal drive, the user right clicks on the file to bring up the "Delete" menu option and then click "Delete" to delete the file.

3) Shared File Storage

Users can upload files from their local machine to their shared file storage on the web-application. Furthermore, the user may download the file uploaded.

Shared File Upload:

1. The user navigates to the “Shared With Me” view of the web application through the navigation button on the web-application sidebar.
2. The user clicks on the “Upload New File” button from the web-application sidebar.
3. The user clicks “Choose File” to choose a file from their local machine.
4. The user selects a group to share to the file to from the “Select A Group To Share With” drop down menu.
5. The user clicks “Submit” to upload to file to the selected group drive.

Shared File Download:

1. To download files from their group drive, the user clicks on the respective file in their Shared With Me document table view.

4) Group Operations

By clicking on the “Create Group” button, users are able to create groups. When groups are created, other users can be invited to the group and the user who created the group becomes the group admin and can administer the group. Users can also view all of the groups they belong to.

Group Creation:

1. The User clicks on the "Create Group" button.
2. The User enters in the name of the group.
3. The User may enter in the email addresses of users they would like to initially invite to the group when it is created.
4. The User clicks “Create Group” button to create the group.

Group and Group Member Viewing:

1. The User clicks on the “View Group” button.
2. The User clicks on the “eye” icon next to the respective group they would like to view the group members of.

5) Group Admin Priviledge

Admins of groups has extra privileges within their respective groups. Group admins have the ability to kick other members from the group as well as delete files from the group drive.

Shared File Deletion:

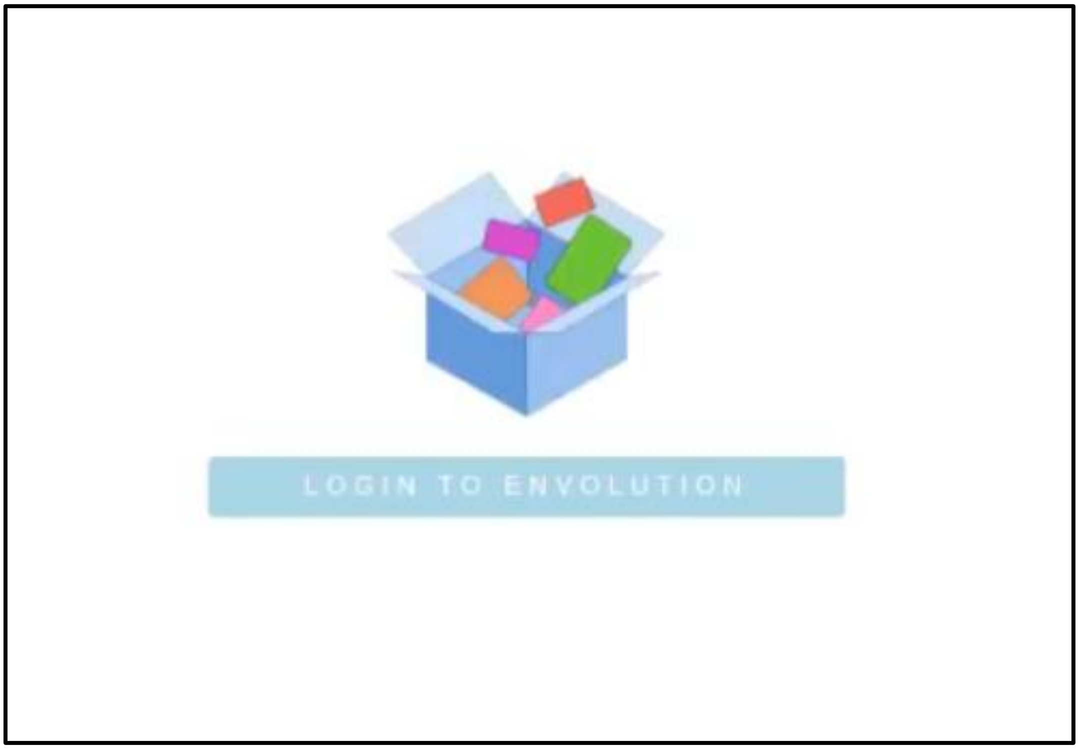
1. To delete files from their shared group drive, the user must be the admin to group in which the file was shared to. If so, the user right clicks on the file to bring up the "Delete" menu option and then click "Delete" to delete the file.

Kick Member:

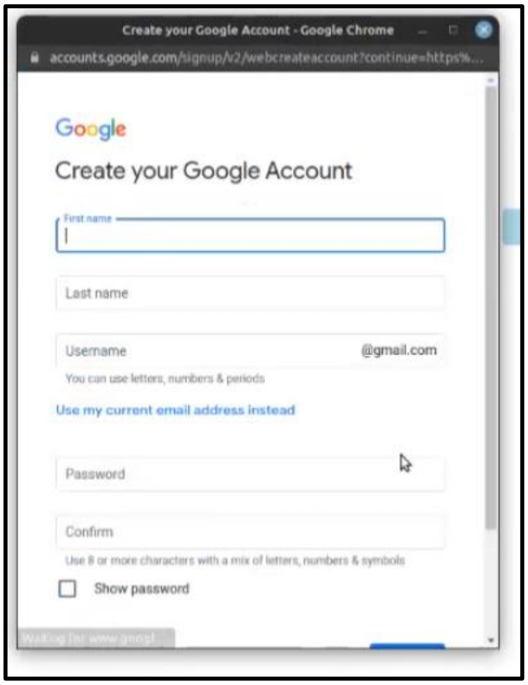
1. The admin clicks on the 'View Groups" button on the sidebar to view all of the groups they belong to.
2. The admin chooses the group that they are the admin to by clicking on the "eye" icon next to it.
3. The admin clicks on the "X" button next to the name of the user within the group that they would like to kick.

Product Walkthrough

The first thing that you will want to do is launch the application. Once the web application is running, the user is presented with the the login page:



In order to gain access to the web-application features, the user must first register an account. If the User already has an account created with Google, they may use that account to login, otherwise, Users can register through Google's authentication:



Create your Google Account - Google Chrome
accounts.google.com/signup/v2/webcreateaccount?continue=https%...
Google

Create your Google Account

First name
Last name
Username
@gmail.com

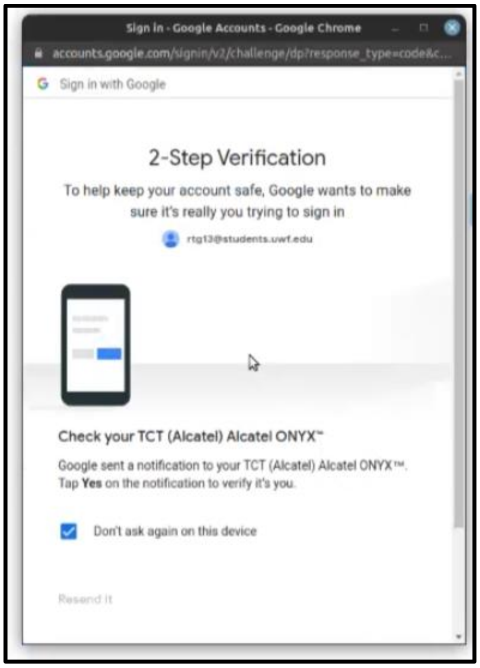
You can use letters, numbers & periods

Use my current email address instead
Password
Confirm

Use 8 or more characters with a mix of letters, numbers & symbols

□ Show password

When an account has been registered, the user may log in with their newly created account by entering the appropriate credentials and pressing log in. If the user has two-factor authentication enabled, they will need to authenticate:



Sign in - Google Accounts - Google Chrome
accounts.google.com/signin/v2/challenge/dp?response_type=code&c...
Sign in with Google

2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

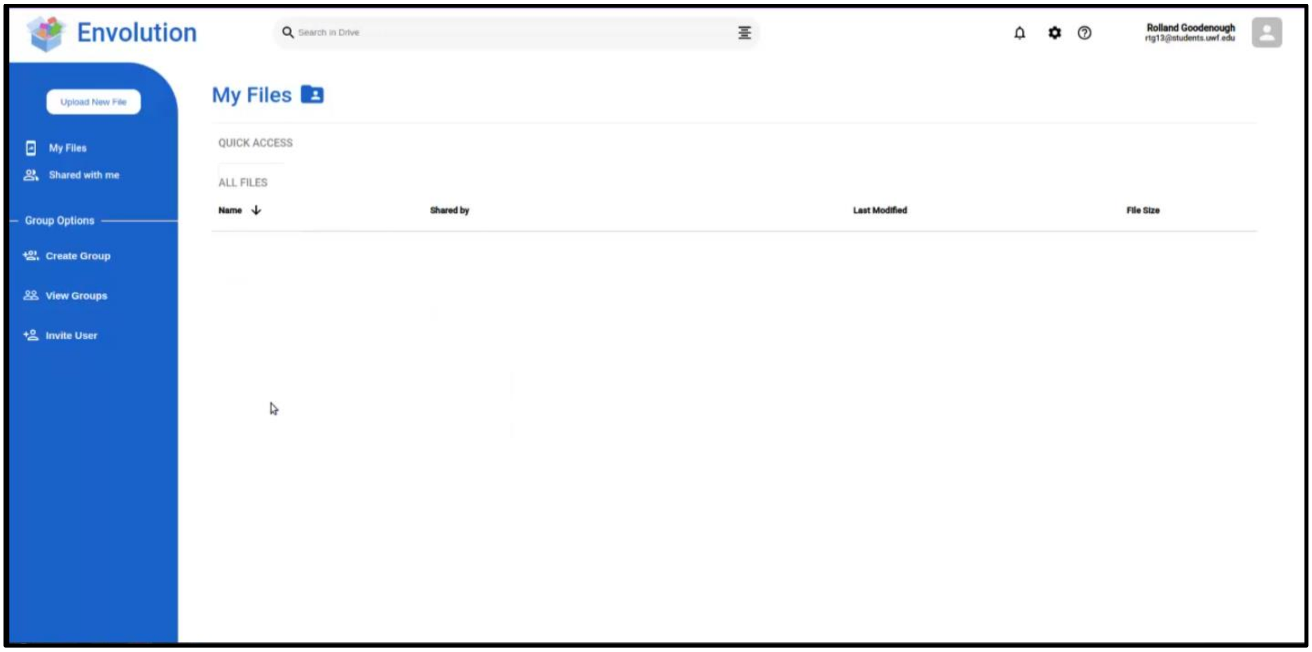
rtg13@students.uwf.edu

Check your TCT (Alcatel) Alcatel ONYX™

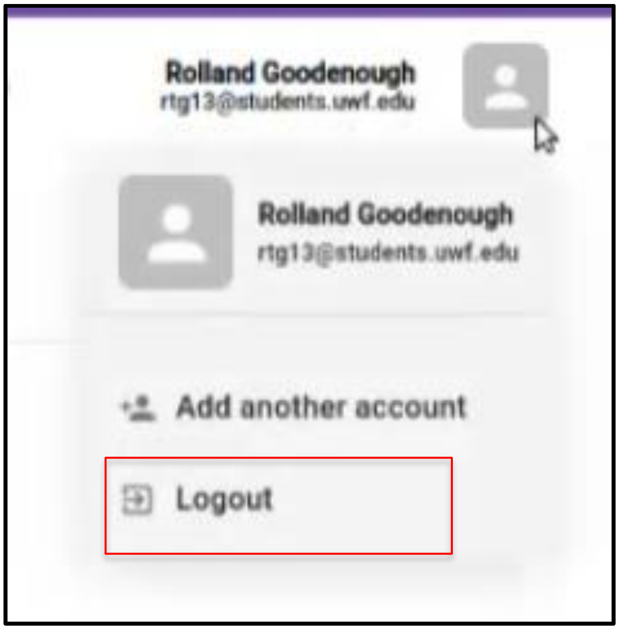
Google sent a notification to your TCT (Alcatel) Alcatel ONYX™. Tap **Yes** on the notification to verify it's you.

☑ Don't ask again on this device

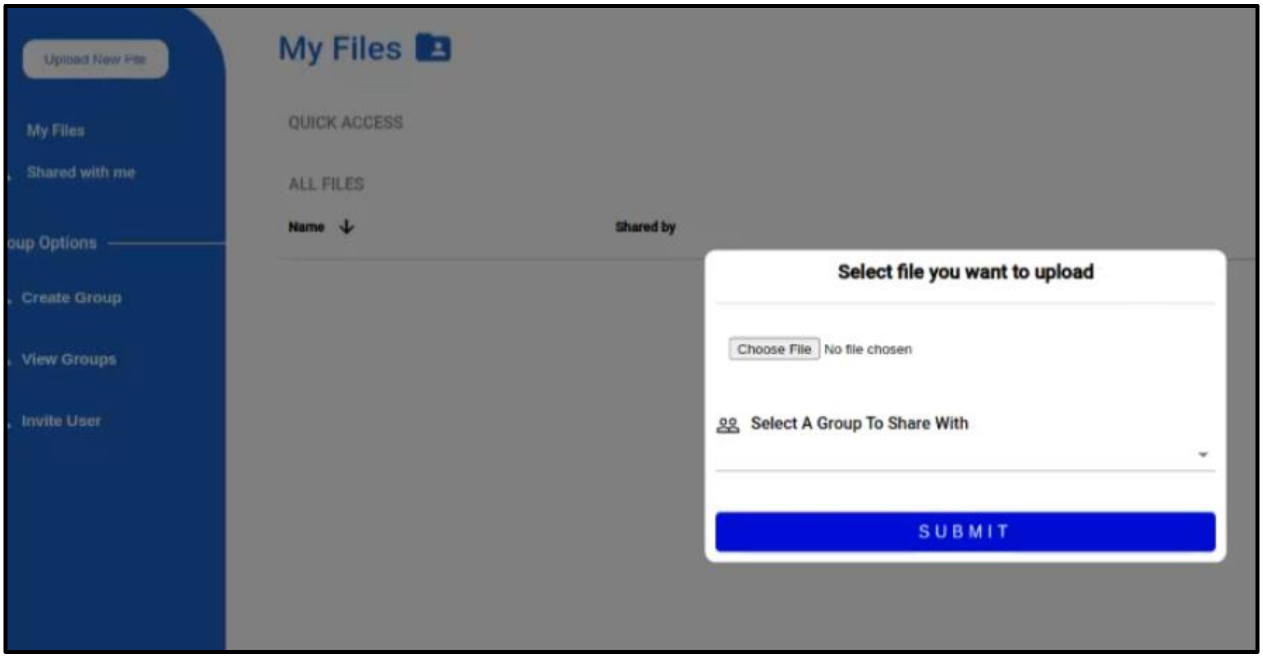
Once logged in, the user gains access to the web-application's dashboard:



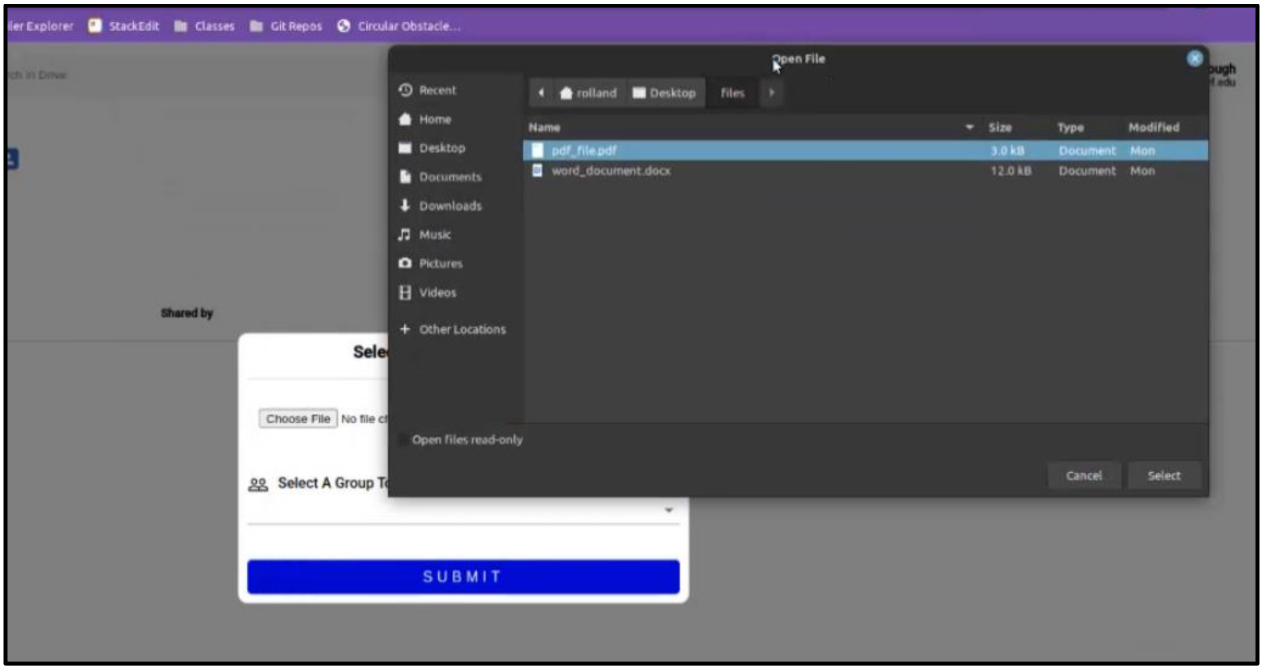
To log out of their account. The user can click on their user profile picture within the header on the top right corner of ther web-application. From there, the user will be prompted with the option to logout. The user can click on the "Logout" button to log out of their account:



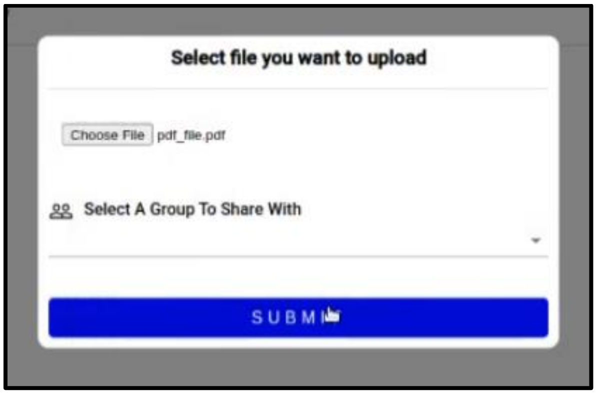
To upload a file to the personal drive, the User may click on the “Upload New File” button on the sidebar to bring up the Document Upload Modal:



The user clicks on the “Choose File” button to choose a file from their local machine to upload to their personal drive on the web application:

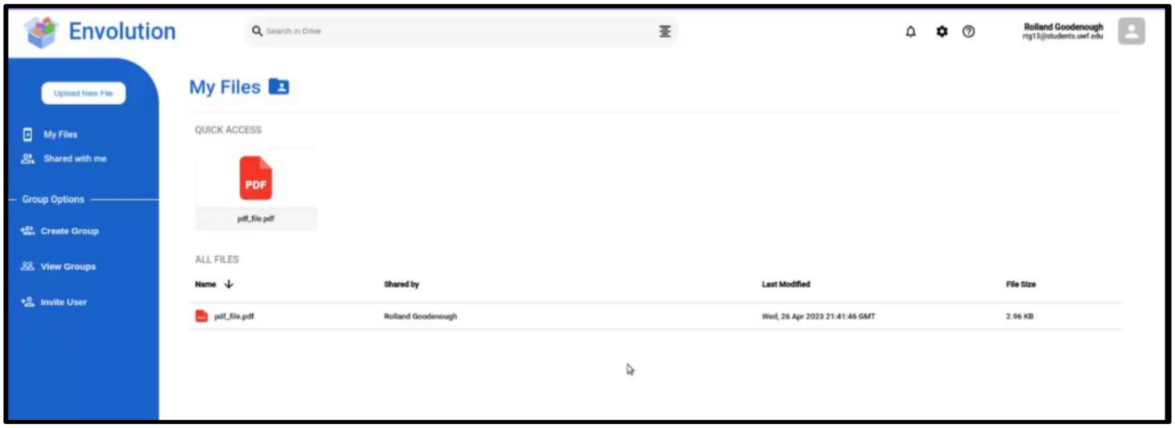


The User clicks on the “Submit” button to upload the file:



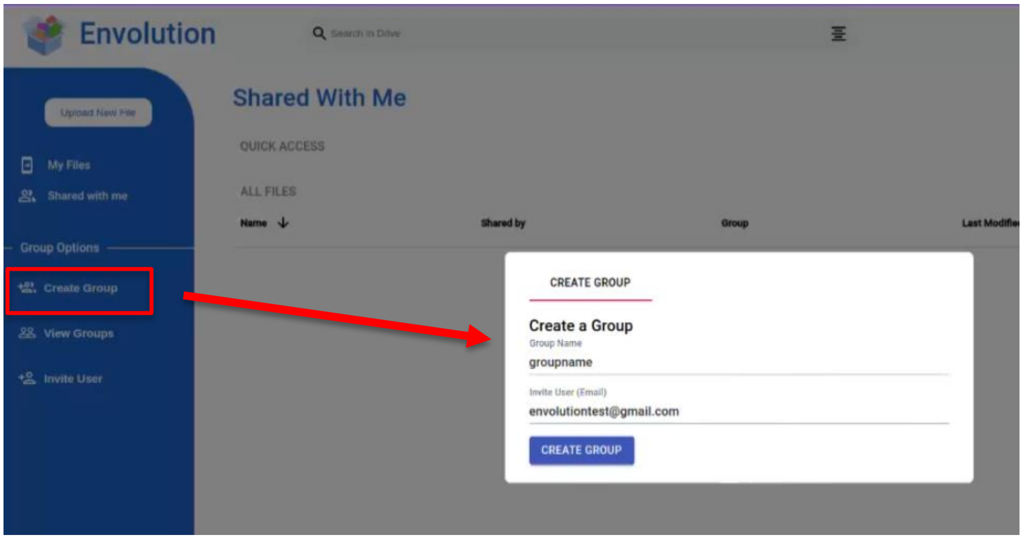
pdf_file.pdf

The file that was selected and uploaded now displays in the user’s personal drive:



Name ↓	Shared by	Last Modified	File Size
pdf_file.pdf	Rolland Goodenough	Wed, 26 Apr 2023 21:41:46 GMT	2.96 KB

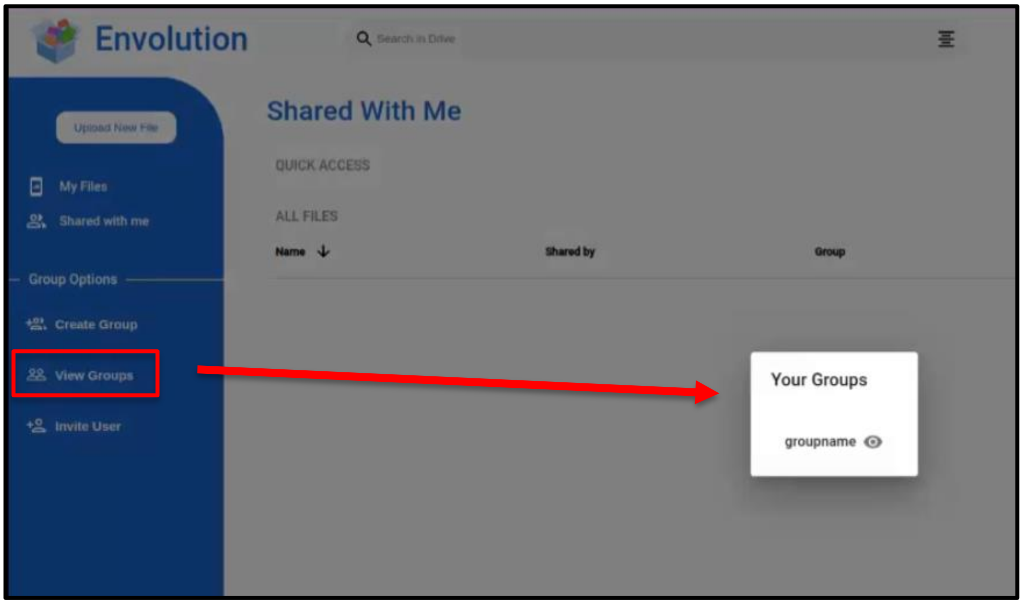
To create a group, the user clicks on the “Create Group” button to bring up the group creation modal. Then the user enters in the group name and the email of users to invite:



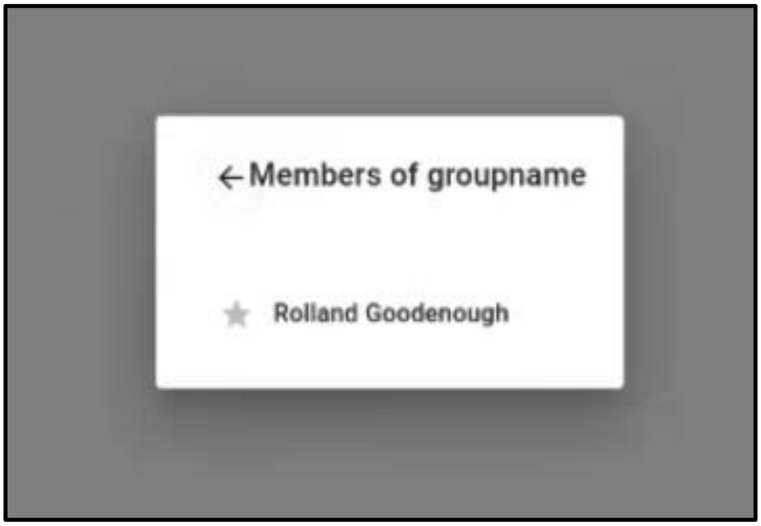
Group Name
groupname

Invite User (Email)
envolutiontest@gmail.com

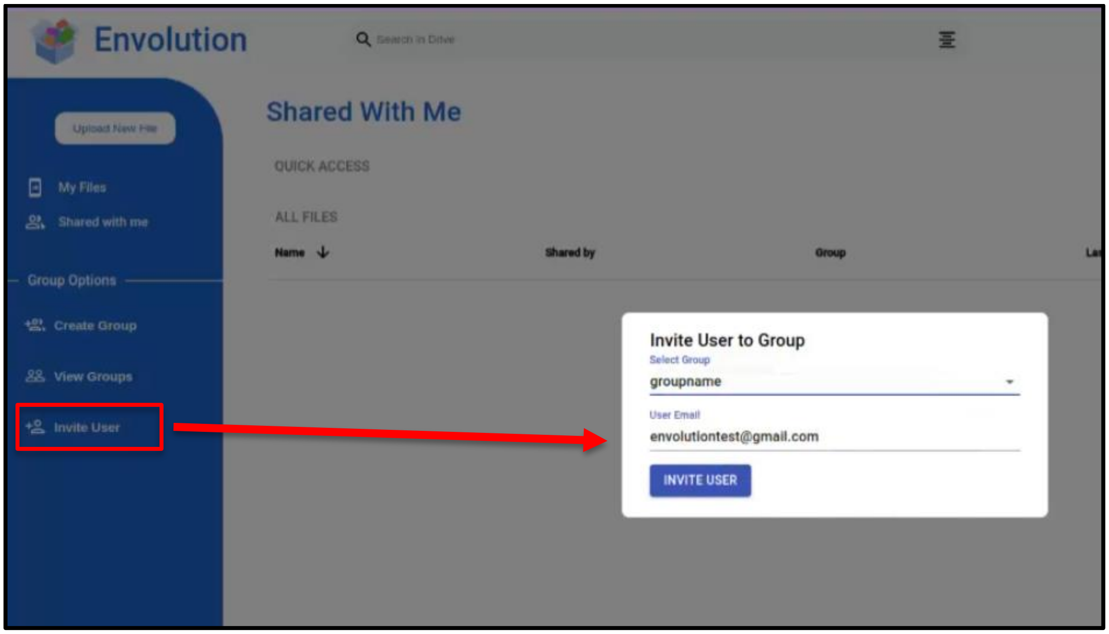
Once the user clicks on the “Create Group” button, the group is created, and the user may view the group from the “View Groups” button which displays all groups the user belongs to:



By clickin the “eye” icon next to the group, the user can view all members within that group:



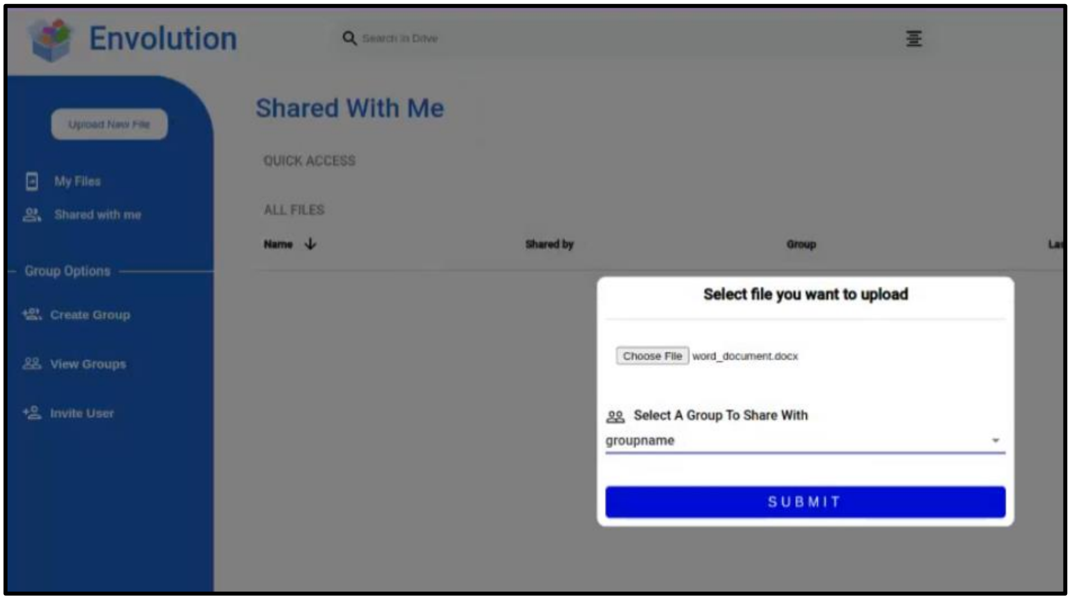
If a user wants to invite additional users to their group, the user can click on the “Invite User” button. From there, they can select the group they want to invite the user to from a group selector drop down menu, and then enter in the user’s email address in the User Email field. The User then clicks the “Invite User” button to send the invite:



Select Group
groupname

User Email
envolutiontest@gmail.com

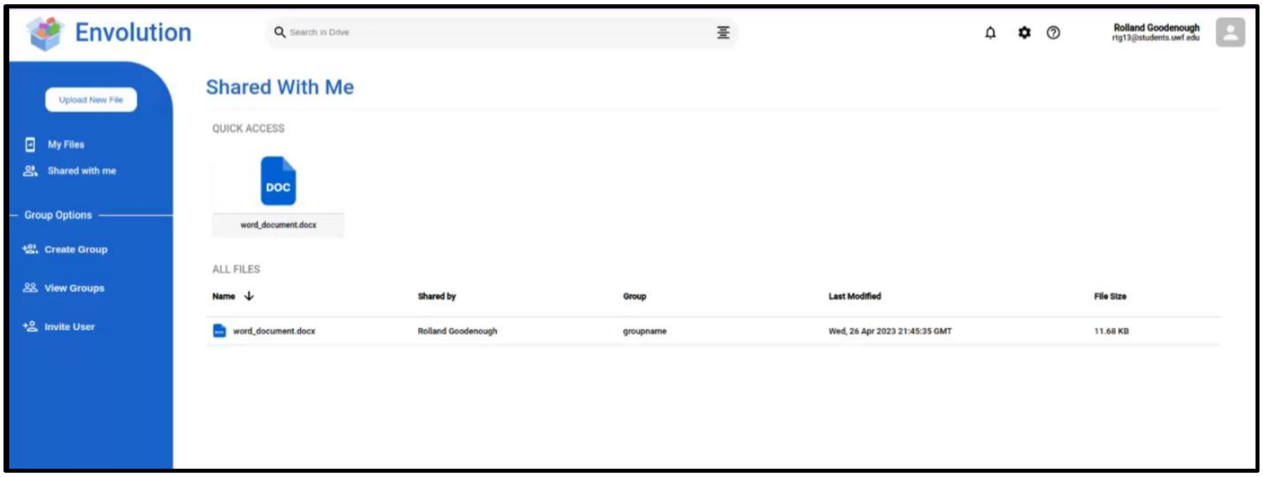
Once a user is in a group, they have the ability to upload files to their group drive. The method is the same as uploading files to their personal drive, except this time, the user will have to select the group to upload the file to from the “Select A Group To Share With” selector drop down menu:



word_document.docx

Select A Group To Share With
groupname

Once the “Submit” button is clicked to upload to file to the group drive, the file will be viewable through the Share With Me view, which displays all shared files from all groups. The group the file is shared to is denoted from the “Group” column:



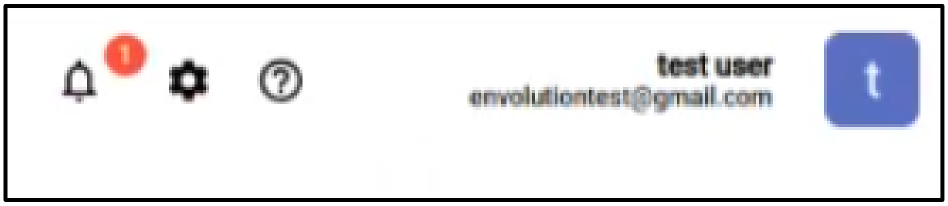
Shared With Me

QUICK ACCESS

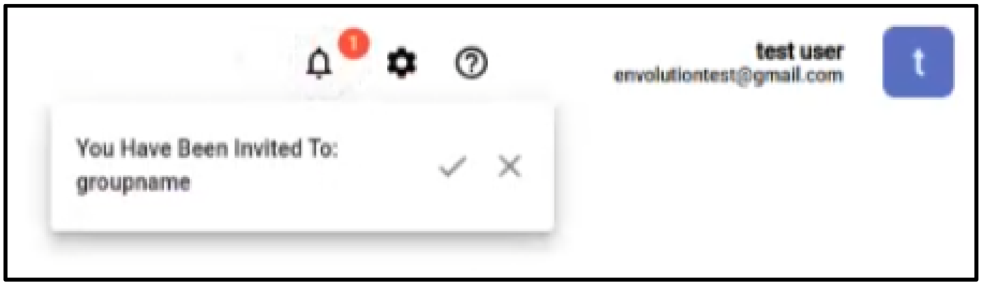
ALL FILES

Name ↓	Shared by	Group	Last Modified	File Size
word_document.docx	Rolland Goodenough	groupname	Wed, 26 Apr 2023 21:45:35 GMT	11.68 KB

If you have received an invite to a group, you can view the invite from the alerts button on the website header:



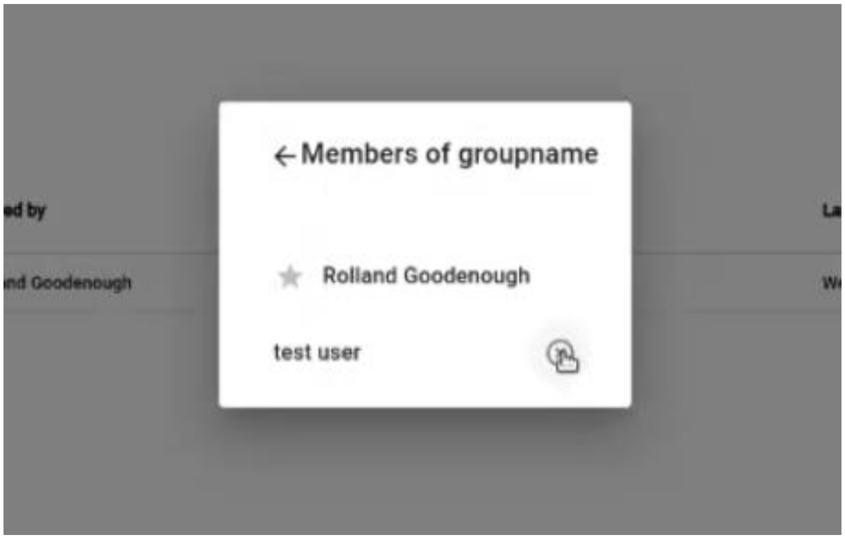
Clicking on the alerts button will bring up all of the invites you have received. You can click on the accept or decline button to either accept or decline the invite:



You Have Been Invited To:
groupname

✓ ✕

If you are the admin of a group, you can kick members out of your respective group by clicking on the “View Groups” button, then clicking on the “eye” icon next to the group you are the admin of, and then clicking on the kick button next to the name of the user you would like to kick. The star next to a user’s name indicates that they are the admin of the group:

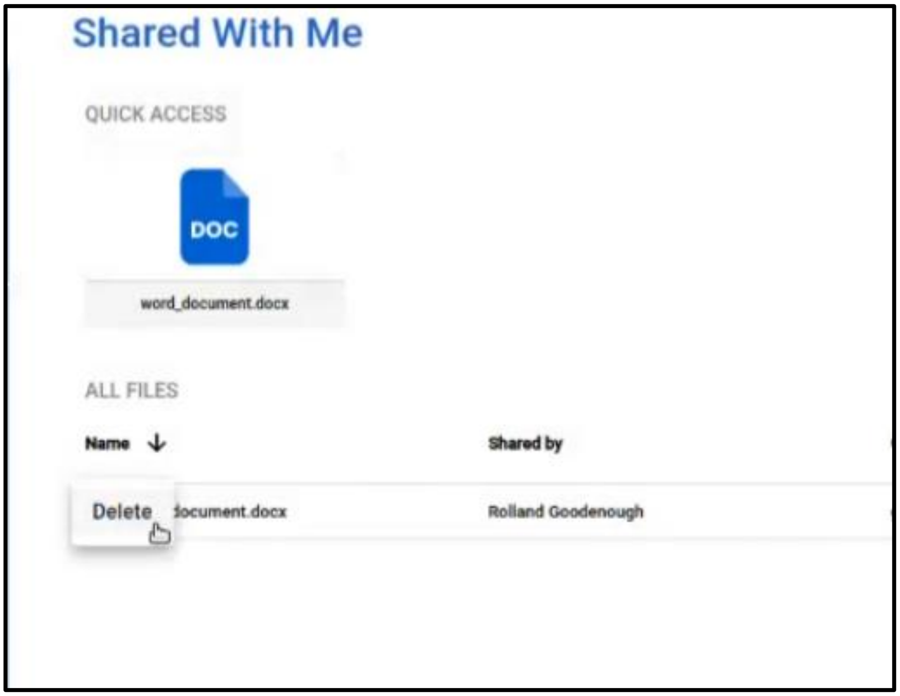


← Members of groupname

★ Rolland Goodenough

test user

If you are the admin of a group, you can also delete files from the group’s drive. This is done simply by right clicking on the file, and then clicking delete:



Shared With Me

QUICK ACCESS

word_document.docx

ALL FILES

Name ↓	Shared by
Delete locument.docx	Rolland Goodenough

Installation of the Software

In order to install this application, you will first need to go to the github repository at this link (which should already be shared to you):
Envolution-Capstone/secureFilePlatform (github.com)

Clone the repository into your IDE. The recommended IDE to use is Visual Studio Code, as the software was developed with Visual Studio Code and this entire installation tutorial will be based off of Visual Studio Code.

Before Running the application there are several set-up steps that must be followed, starting with ensuring that all project dependencies and requirements are present and working.

This software requires the following programs:

1) NodeJS
2) Npm (comes with NodeJS)
3) Gcloud CLI

To install NodeJS, the most convenient way is to install via a package manager at the following link. Simply follow the instructions on the package manager and you will have NodeJS installed, along with npm:
Download Node.js (nodejs.dev)

With NodeJs installed, if you have Make, the following setup is easy:

1. run the command `make setup` in the base directory

If you do not have Make:

1. enter the `server/` directory and run `npm install -y --force --silent`
2. enter the `client/` directory and run `npm install -y --force --silent`

To install gcloud CLI, all you have to do is to install the Google Cloud CLI, and then initialize the glcoud CLI. The instructions to install gcloud CLI can be found through the gcloud CLI documentation link:
Install the gcloud CLI | Google Cloud

Select the correct operating system you utilize and follow the installation instructions. Once you have installed gcloud CLI, the last thing you need to do is initialize gcloud CLI by running the following command through your terminal or command prompt:

```
gcloud init
```

Database Setup

NOTE: For the security of our web application, we would NEVER expose our Firebase configuration nor include the .env file in a real-world application. However, since this project is purely for demonstration purposes and is privated, we have included the .env file for the Firebase database configuration already for ease of use.

This project utilizes a cloud-hosted NoSQL database through Google's Firebase, therefore, it is not neccessary to setup the database through SQL commands. This project is currently set up using our group's own Firebase project configuration, therefore, the database connection is established by utilizing our Firebase configuration object containing keys and identifiers for our app:

```
 apiKey: "AIzaSyA7ROErICF1bCa4earw2UoglBq_POrwBrA",
 authDomain: "file-storage-e6537.firebaseapp.com",
 projectId: "file-storage-e6537",
 storageBucket: "file-storage-e6537.appspot.com",
 messagingSenderId: "68930784514",
 appId: "1:68930784514:web:65d2623bfbc3da3f27c61b"
```

The Firebase configuration is to be utilized within a .env file in the /server/ directory.

If you want to set up and utilize your own Firebase database, follow the official Firebase documentation for adding Firebase to a web application.

Once your Firebase project is created and the application is registered, navigate to your project settings through your Firebase console on your web browser, scroll down to SDK setup and configuration, select 'Config' and copy and paste your Firebase configuration into a .env file on the /sever/ directory.

Running the Application

Once you have finished installing all necessary requirements as well as setting up the database (it is already preset for you), you can run the program through two methods:

With Make:

1) Run the command ‘make run’ in the base directory

Without Make:

1) Enter the ‘server/’ directory and run ‘npm start’
2) Enter the ‘client/’ directory and run ‘npm start’

Troubleshooting Problems

Ensure that there are no missing npm modules

If the software does not run, try installing all of the required NPM modules:

In `/server/`:
run `npm install -y --force --silent`

In `/client/`:
run `npm install -y --force --silent`

Ensure that the correct NodeJS version is being used

Having an out-of-date versiona of Node JS can cause issues.
Follow https://nodejs.org/en/download/current for getting the newest version.

Ensure that you are not missing the .env and Service Credential files

The server requires .env and service-account-credentials.json files to be in the /server/ directory. These files should be on the repo *(though if this were a real product they would not be)* If the files are missing, copy and paste the following in to the respective file in /server/.

```
// .env
PORT=9000
APIKEY="AIzaSyA7ROErICF1bCa4earw2UoglBq_POrwBrA"
AUTHDOMAIN="file-storage-e6537.firebaseapp.com"
PROJECTID="file-storage-e6537"
STORAGEBUCKET="file-storage-e6537.appspot.com"
MESSAGINGSENDERID="68930784514"
APPID="1:68930784514:web:65d2623bfbc3da3f27c61b"
```

```
// service-account-credentials.json
{
  "type": "service_account",
  "project_id": "file-storage-e6537",
  "private_key_id": "c473669f0358a8f8d842e1cc3a9df8cad81c26a3",
  "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCxZ/b6JELEZw
n1\nj/OfphMg77X2bMIs98TOjN1Y0Lh/rvANWpRfAjbiwRqgEKMiBvjDLwwtzaJC0n3F
\nukNKDflANJcIFahcEiiji1qAkruT1eyeBhA+MvGIJcC/ng6t0oSZw1BQ5nU7WCf5\ncm
FdNXueWkhLSmLZ0WguGXBjgNA4tnmVqDTr3Ed0v3HQxA0z2JYVtt5cnQyql5Rx\nu
YAx7TaaOQFMUPxvlnpYDLTGjTulsRWcuu4AdkXJyLSwTMFV6xpME+gLF5BOHeEK\
nPX1f2aYSpP8S4QL//nSIMfo9NguCOoQnlsXafsshT0BGiL49HZQMvrc+g2O2kY+e\n
R1ytM9BRAgMBAAECggEACGF48Wg1H0Ie3lLml2wpCy1H01Rf9+/chEVzT3bMwHtr\
nK7ZTvAlGvn+Q2m7uxfS+W7olQSStvapj9qtN8nmmhLn3SJJ9WZwh/1fd9qT354v7\n
mZt/uPB/KIdgC61T1DJVwU3QxYGdmCgZ+1bD8rtME7cAIo5oTQ+q9EKPZKP5MjSY\
nSFAxdej9oGdQw//rqfPqnciTVPOp986teM6La+fvS+VNCEth8KyagDEWlVY3empF\nl
s8gT6ZDNIlWOtIfI8FP8hglTjYciZUumRki8c6k9iznbjHWv7itpmWtCas97/K5\nbNHST
MnpJiA6GJe5L+r55kj8z+wgClJH/QGGmxCRYQKBgQDz3QWDLt0xumKCzQQM\nLH
W7rwgVHsTzFLvPT7NLNwNO5+e6MxIICXjPCLwq6sBcKhR5UdwKjoUMg+AR1JC9\n
/LvoF0jkZhueZrIISYDLLI2ydMWOH9O871svohwvCqNKXazB95C85c4ua8Mx/tKF\nZj
p5oo9wmH0fN5z4drGbivQFBwKBgQC6PDwD68KYluUbD5mnN7XS++rj5+6uIrRO\n
GxO/sTW2bc2QD/Nb6zKTGW+68JJDUSGSR9WzQcVUKcAOVr5/OWUiDG8dlCoFxj
RE\nDtDeRwKgh+ObsMwJvVYXVPEjlcZiSOJnw+5LOHng1yt1Z/mMN8h+MaFLNCtQ
iAZC\niq9BFb/B5wKBgG6+lrxGUgk9PXNtK0NkBWtgR2lf+czyQ4AYD7I+n2/7/M4gVz
Xz\nJzvOGbXbudOhAH8/34+jvWQ7l0xBniHJXoQ93spqXGyI8py01Jpv90FtqjGq3ntU
\nr7JoCiiKyjEBbW0AwmgmbIXERnaz5GLUVAXdVjwp49iDZvOm421howONAoGARIt
Q\n53yJddHr5wbZ3cLSaCISNOmzXmIljK3ImgAmLcvCIejNACLTzXJKPjq3CpG80nM
g\nA0cM0so/BsgEexzrzRlYeEGFKfTmXbo6Q+VM4TrCmhX7MwZ9vj6kNh21E42RzvE
9\nLnBN42QueZrYLTSG1XN80woTeyNlcm5KzKCtoDcCgYEAti4+UZ8r2DnRrCoQ/TE
1\nJzbJ1oRcYCA7UKcF8Vxj3WtAXTnNukso JDX1yVkvIU3/03qB959M826CTb1Qc2sW
\nzx1WHz2TnBIT+QPbHXX8Kp2J1cZ+Fw8rW4+OUNcmL1TSl/zJQtc8Ke924tD6e44y
\nA4pMqJxQiCVQbnEDcvS2LEQ=\n-----END PRIVATE KEY-----\n",
  "client_email": "firebase-adminsdk-bjgpc@file-storage-
e6537.iam.gserviceaccount.com",
  "client_id": "115410691965466141057",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url":
"https://www.googleapis.com/robot/v1/metadata/x509/firebase-adminsdk-
bjgpc%40file-storage-e6537.iam.gserviceaccount.com"
}
```