# Gmail API Search and Delete Tool (SAD Tool)

[Summary](#h.1lvpigum1u8r)

[Platform requirements](#h.r1gvltbtxm5w)

[Admin Authentication](#h.fp4d1bcbm3lj)

[Data Access Restrictions](#h.hwwkuz4s7jwi)

[Search Functionality](#h.acnq3tqzcdkz)

[Delete Functionality](#h.ihnwh0nez915)

[Logging Functionality](#h.2h4khh3ryc5s)

[Web GUI](#h.t1zjuam2o01i)

[GUI Workflows-Authenticate](#h.bblttji2sc2l)

[GUI Workflows-Search/Deletion of Mail](#h.8sriggqugp3d)

[GUI Workflows-Results](#h.feez8r8becqp)

[GUI Workflows-Log Search](#h.t9ydfiv5r1s0)

[GUI Workflows-Export](#h.gl7aeappukym)

[Authorization Model](#h.ci1bzebwiu1z)

[End User Authorization](#h.qd7ztypqzzhh)

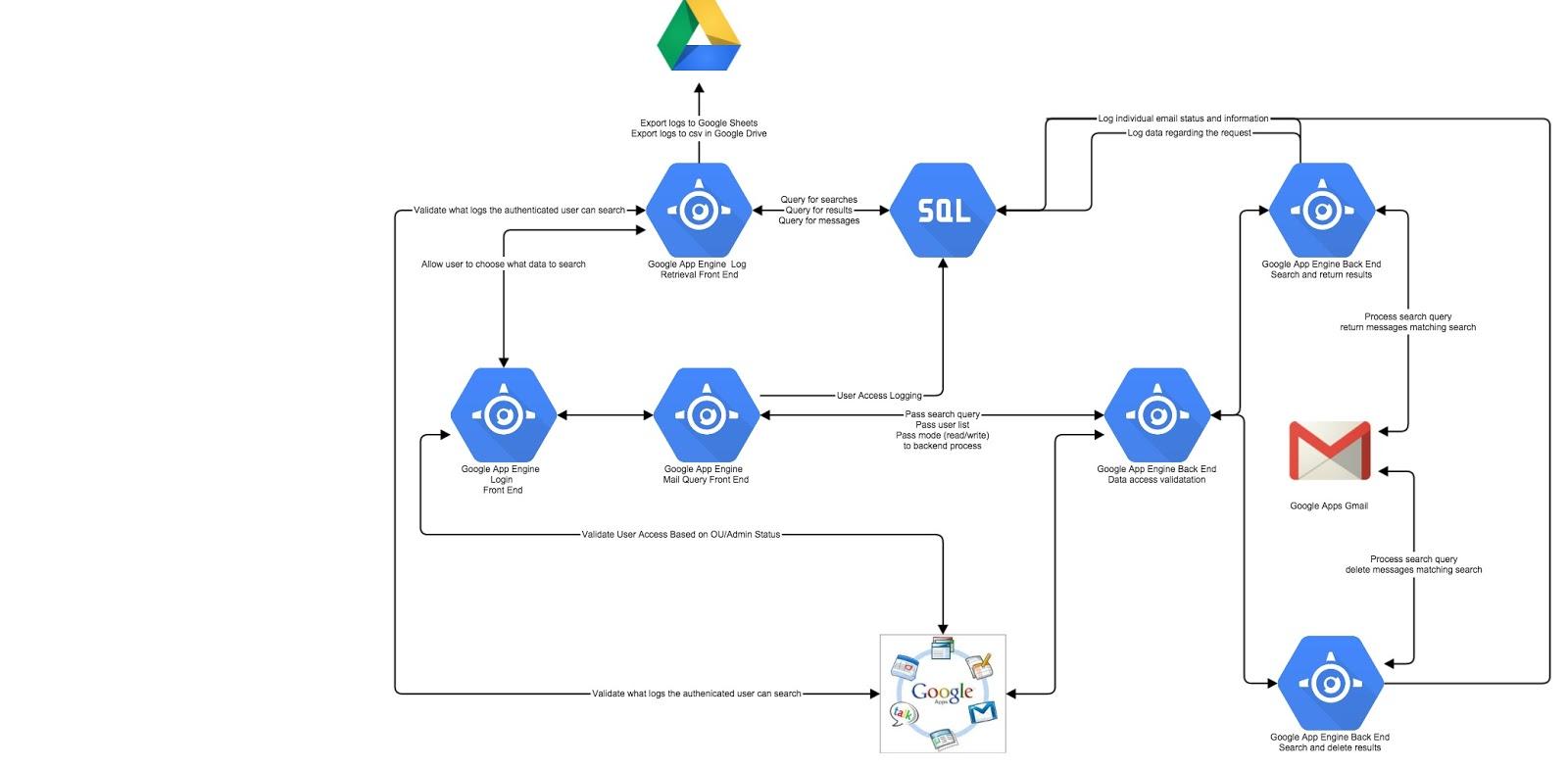
[Service Account Authorization](#h.wbslzb5o706g)

[Validating Data Access](#h.3rtrubspd8lp)

[Backend: Search and Delete](#h.oq2y893yr9e8)

# 

# Summary

The The Gmail API Search and Delete Tool is an administrative tool that can search for and delete messages in a Google Apps user’s Gmail account. This application will also be responsible for OU based authorization and logging of applications actions.

## Platform requirements

* 1. Google App Engine
  2. Google CloudSQL
  3. Java
  4. Java Google Client Library

## Admin Authentication

* 1. Tool will require users to login with their Google Apps credentials.
  2. Tool will limit access based on delegated administrative status.
  3. Tool will access end user mailboxes via Oauth 2.0 service account and delegated access.

## Data Access Restrictions

* 1. Tool will track the organizational unit hierarchy of the authenticated user.
  2. Tool will prevent the authenticated user from searching, deleting or reviewing the logs that are applicable to users outside of their organizational unit hierarchy.

## Search Functionality

* 1. Tool will provide the ability for authenticated users to search through multiple mailboxes using Gmail syntax.
  2. Tool will log each search activity (the user who conducted the search, time, search term, number of users.)
  3. Tool will log the total number of search results for each user being searched.
  4. Tool will log every message returned by the search (indexed by messageId.)

## Delete Functionality

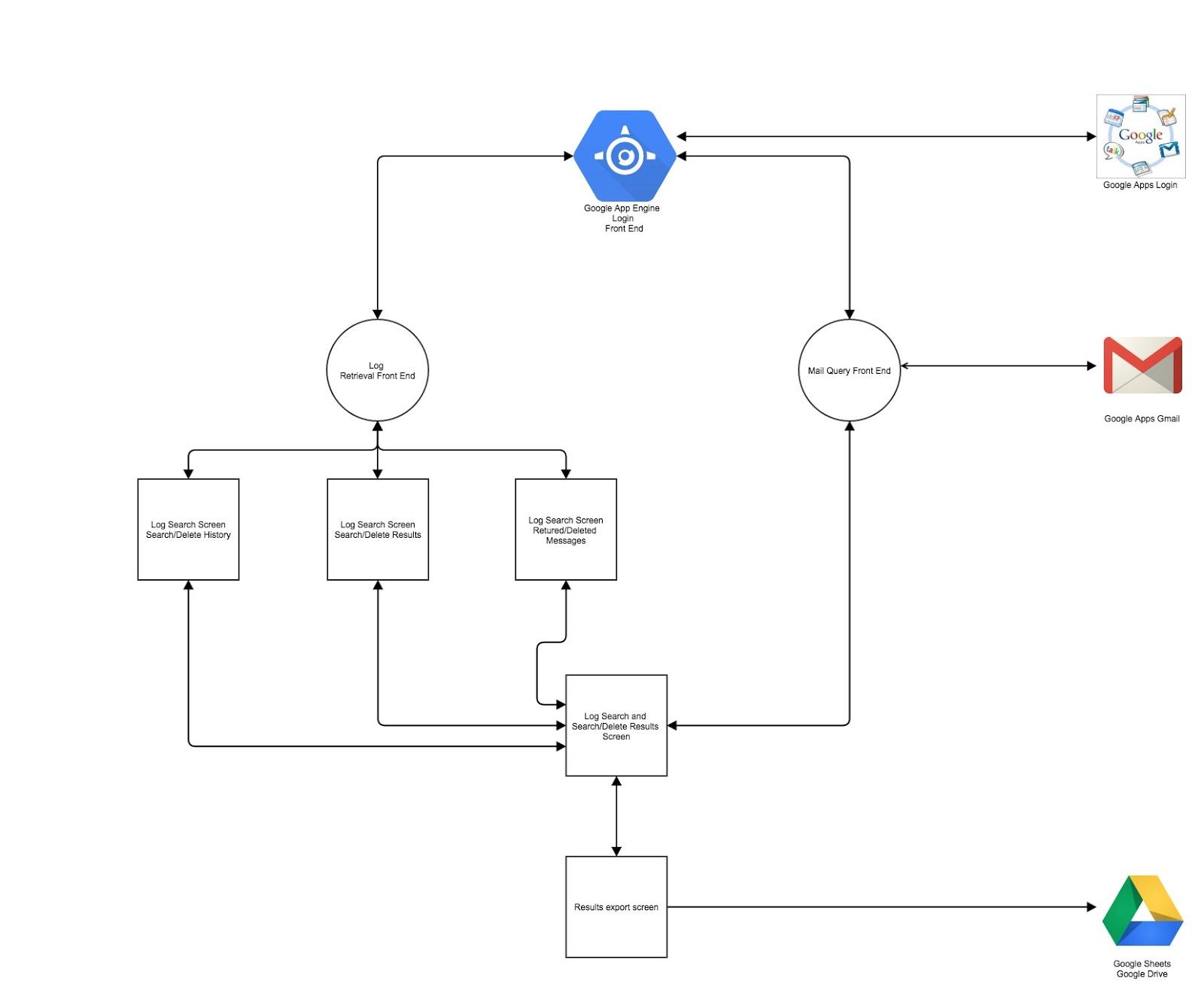
* 1. Tool with provide the ability for authenticated users to search through multiple mailboxes using Gmail syntax and delete the return messages.
  2. Tool will log each delete activity (the user who conducted the deletion, time, search term, number of users.)
  3. Tool will log the total number of search results for each user being searched and the total number of successfully deleted message.
  4. Tool will log every message returned by the search (indexed by messageId.)

## Logging Functionality

* 1. Tool will provide the ability to search deletion and search requests.
  2. Tool will provide the ability to search deletion and search results by user/message.
  3. Tool will provide the ability to export any log search as csv or pdf.
  4. Tool will provide the ability to export to Google Sheets.

# Web GUI

The tool’s web GUI will be hosted on App Engine and Java. The web GUI should be built on a common framework for future revisions and development. The web GUI should provide the flexibility to brand various visual elements of the site.



## GUI Workflows-Authenticate

When a user first visits the application they will be prompted to sign into their Google Apps account if not already signed in.The user will be validated against a list of approved users. Otherwise the user is presented with two options: search logs or conduct a search/deletion of mail.

## GUI Workflows-Search/Deletion of Mail

The end user will be presented with a screen providing the ability to select between searching and deleting message. The user will be presented with a “build a search” functionality as well as a free-text search box. The user will be presented with a dialog to upload a list of users to run the search against. The user must submit a list of users and a search query before they can submit the form. The page will update the status of the search or deletion: the total number of users being searched, the total number of users not being searched due to restrictions and the total number of users left to be searched. After the process has been finished the user will be forwarded to the results screen.

## GUI Workflows-Results

The user will be provided with statistics regarding the previous search query or deletion request. The end user will have the option to export the data, conduct a new action or search logs.

## GUI Workflows-Log Search

The user will be presented with two options for searching logs.

* The first option is to search the access logs, these looks include details on search/deletion requests.
* The second option returns per user logs across search or deletion requests. Data included in these logs is the parent search ID, the user email of the data being searched, total number of messages returned by the search and if applicable the total number of messages deleted in the action.

## GUI Workflows-Export

The user will be provided with options for exporting log results to Google Drive in native Google Sheets or csv format. Csv should be formated as that it can be imported in Excel.

# Authorization Model

The tool will require a complex authorization model that will give the tool and user appriorate access to user and domain content.

## End User Authorization

The tool will authenticate the user via the Google + sign in API and authorize all necessary data access scopes at this time. The scopes include Drive edit and file creation scopes as well as the ability to read the user’s email address.

## Service Account Authorization

The tool will utilize an oauth 2.0 service account to act on behalf of users. This tool will use this authorization flow to act as cPanel admin to retrieve information from the Admin SDK Directory API and when accessing the Gmail API on behalf of users. The tool should allow for multiple service accounts to be authorized for highly thread operations.

## Validating Data Access

The tool must prevent users part of one organizational unit hierarchy from accessing logs, searching messages or deleting messages. Prior to conducting each activity the tool should verify the authenticated user’s OU to confirm what data they have access to.

* Searching logs: when a user searches logs data on searches/deletions conducted by admins in other OUs should not be returned.
* Searching mailboxes: when a user submits a csv as part of the search process the tool should conduct a check against each user confirming that they are part of the same organizational unit hierarchy as the authenticated user.
* Deleting messages:when a user submits a csv as part of the deletion process the tool should conduct a check against each user confirming that they are part of the same organizational unit hierarchy as the authenticated user.

# Backend: Search and Delete

The tool will make calls to the Gmail API to search and delete messages from users’ mailboxes.

The tool will provide the ability for end users to search a list of users’ mailboxes via the Gmail API. By default searches should include the Trash and Spam labels in user’s mailboxes. Once a search has been conducted the tool will collect the search results in two tables that will be created in the CloudSQL instance:

* Action Tracking: this database will track every request to delete or search for content within users’ accounts. It will store data specific to each query.
* User Tracking: this database will track every message requested in a given mailbox across multiple searches or deletions. This includes the title of the message and other envelope information, as well as the mail snippet. It will also track whether the message was deleted and list the unique idea of each action that returned the message.