February 2022

Google Workspace Data Subject Requests (DSR) Guide

Disclaimer

This guide applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of February 2022 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Intended Audience

This guide is intended to help Google Workspace customers better understand how to use Google Workspace services and settings to assist them in responding to data subject requests (DSRs) under data protection legislation. We recommend that you consult with a legal expert to obtain guidance on the specific requirements applicable to your organization, as this guide does not constitute legal advice.

Google Cloud

Introduction

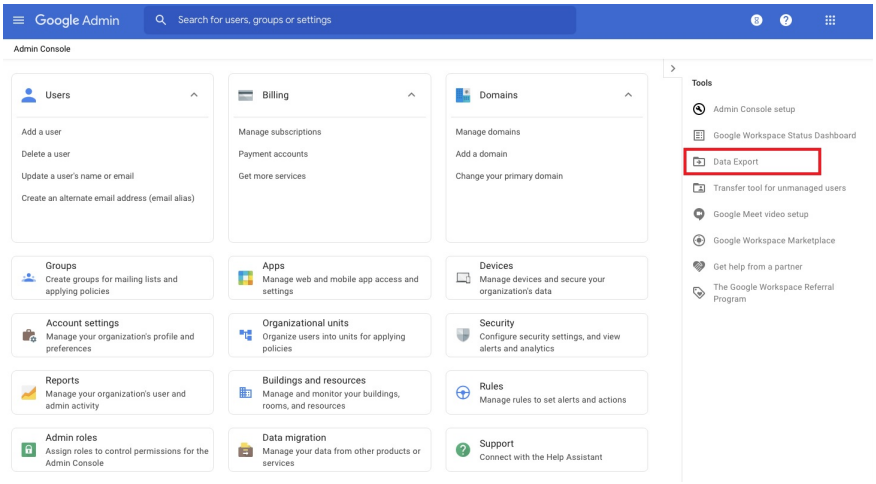
As a Google Workspace customer, Google Cloud provides you with transparency and control over the use of your data, and protects it throughout its lifecycle. This guide provides details on how a Google Workspace Administrator can use Google Workspace Admin Console features to help you fulfill potential obligations related to Data Subject[1] Requests (DSRs) as may be required under applicable data protection laws. This guide will cover how we support some of the actions you may have to take when responding to a DSR, such as access, export, and data deletion.

Part 1: Access & Export

Google Workspace provides functions for both Google Workspace Admins and data subjects to access and export your customer personal data from our products directly. Google Workspace Admins can use **Admin Data Export** to export organization level data, and use **Google Vault** for targeted user-based searches and export. On the other hand, data subjects can utilize our **Google Takeout** interface to directly access and export all customer personal data by themselves.

Export via Administrator Console and APIs

Data Export tool available in your Google Workspace Admin Console enables administrators to export core services[2] customer data for the entire organization. To export activity data about what actions a user has taken, an administrator may use APIs from the Google Workspace Admin SDK or functionality provided in the Admin Console. For example, the Reports API can be used to generate a summary of a user's usage activity. Details of specific actions taken by a user can be obtained from audit logs.

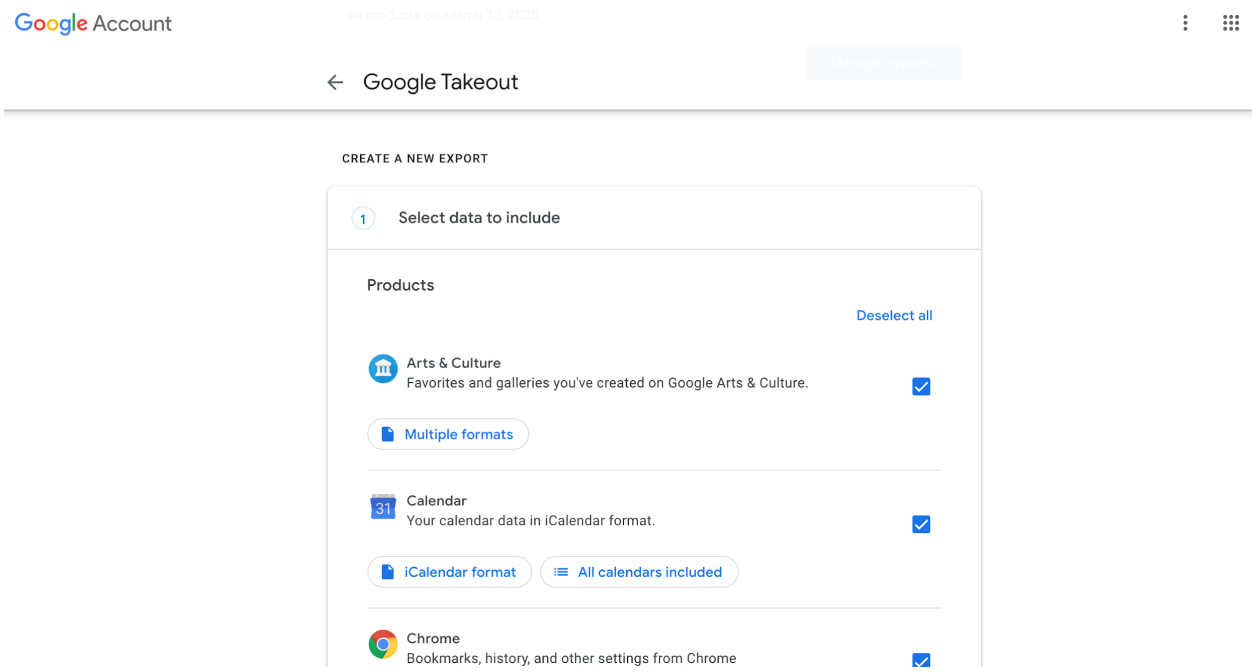


User Takeout

[1] Data subjects are individuals who may have broad statutory rights regarding "personal data" relating to them which is held by the organizations; that is, any information by which the requestor may be identified or identifiable. Data subjects could include current or former employees, as well as individuals who provide personal data through interactions with your organization.

[2] Google Workspace Core Services https://workspace.google.com/terms/user_features.html

Google Takeout allows data subjects to export and download their data from the Google products they use, including Google Workspace services like Gmail, Google Calendar, and Google Derive if permitted by their Google Workspace Admin. In just a few steps, users create an archive to retain for their records or to use in another service, choosing which data to include in the archive and how it's formatted. Scheduling a routine export is also an option.



If you're an administrator of Google accounts for an organization, you can control who uses Takeout from their account by turning the service on or off at the organizational unit level or access group level in the Admin Console. When Takeout is turned on for a user by their Google Workspace Admin, they download a copy of the data in their accounts. Review Turn Takeout off or on for users to choose settings for your end users.

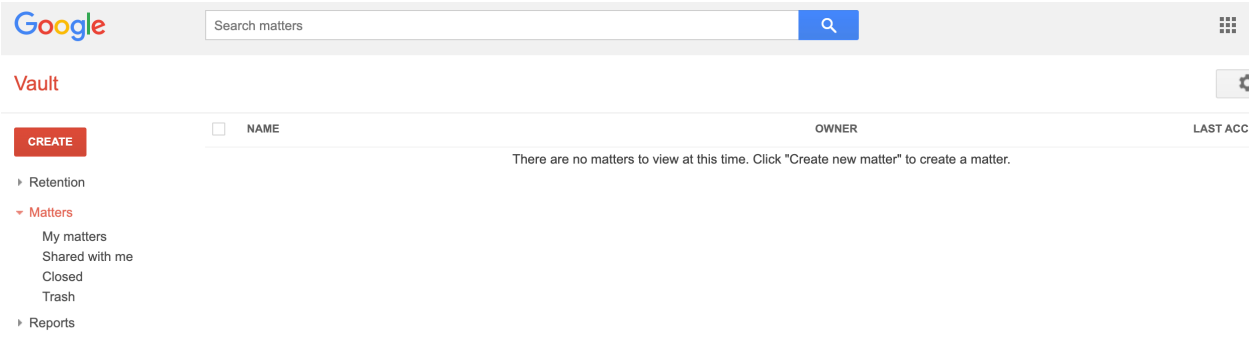
Vault Search & Export

Google Workspace's flagship eDiscovery product, Google Vault[3], streamlines the ability for customers to search and export for information required to meet DSR obligations or other compliance needs. When configured for your organization, Google Workspace administrators with Vault privileges can use Vault to

[3] Vault is included with Google Workspace Enterprise Plus, Google Workspace Business Plus, Google Workspace for Education Fundamentals, Google Workspace for Education Plus, and Drive Enterprise editions, or you can buy add-on Vault licenses for Google Workspace Basic and Frontline.

search across Google Workspace[4] to find data including documents, chats, and email items. Using Google Vault, customers can:

- Search by user account, organizational unit, date, or keyword to discover data relevant to a DSR, even from suspended accounts
- Use queries to find just the messages needed. For example, you can find or exclude messages that contain specific words, exclude deleted messages, or find specific types of attachments. See how you can use operators to refine a search in Vault
- Search results can then be reviewed and further filtered so you can tailor exports to the relevant information to meet the compliance requirements of the applicable DSR



After Vault locates the messages or files you need, you're ready to export them for further analysis. The export functionality of Google Vault is designed to provide you with:

- A comprehensive copy of all the data that matches your search criteria
- The metadata you need to link the exported data to individual users in your domain. See the metadata included in Gmail, Chat, and Groups and Drive Vault export XML files
- The corroborating information required to prove that the exported data matches the data stored on Google's servers

When you export data from Vault, you can choose to store the export file in a specific geographic location. Administrators who are using data region policies can select this option for any users with Google Workspace Enterprise Plus or Google Workspace Business licenses. Vault Export files are available for 15 days after you start the export. Get started with Vault export to learn more.

The Vault API provides the same functionality as the Vault user interface for organizations that want to programmatically retain, search, and export user data. Learn more about Vault API to get started.

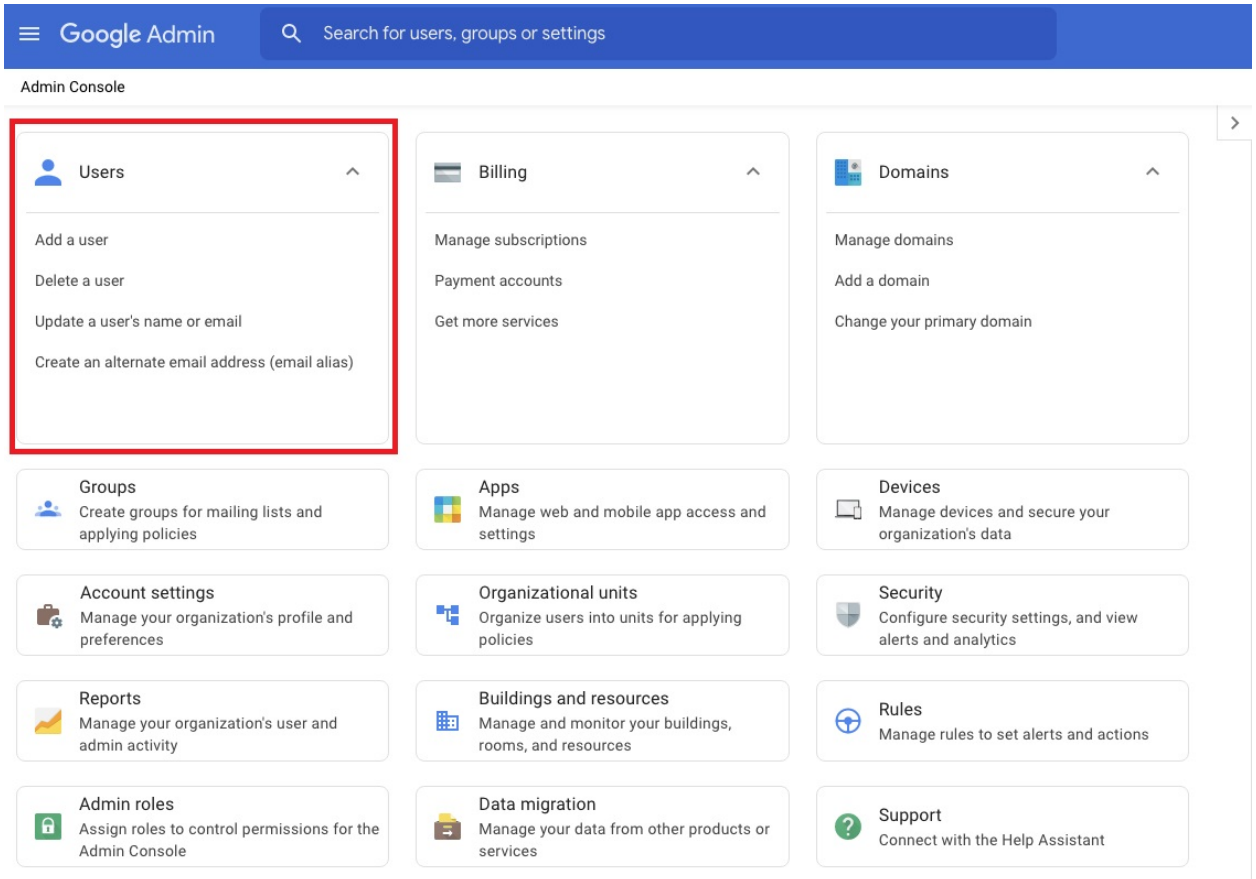
[4] See supported products and data types here.

Part 2: Data Retention & Deletion

Google Workspace administrators can manage user accounts through the Google Admin console, including deleting an account or removing customer personal data from mobile devices and products.

Deleting a user

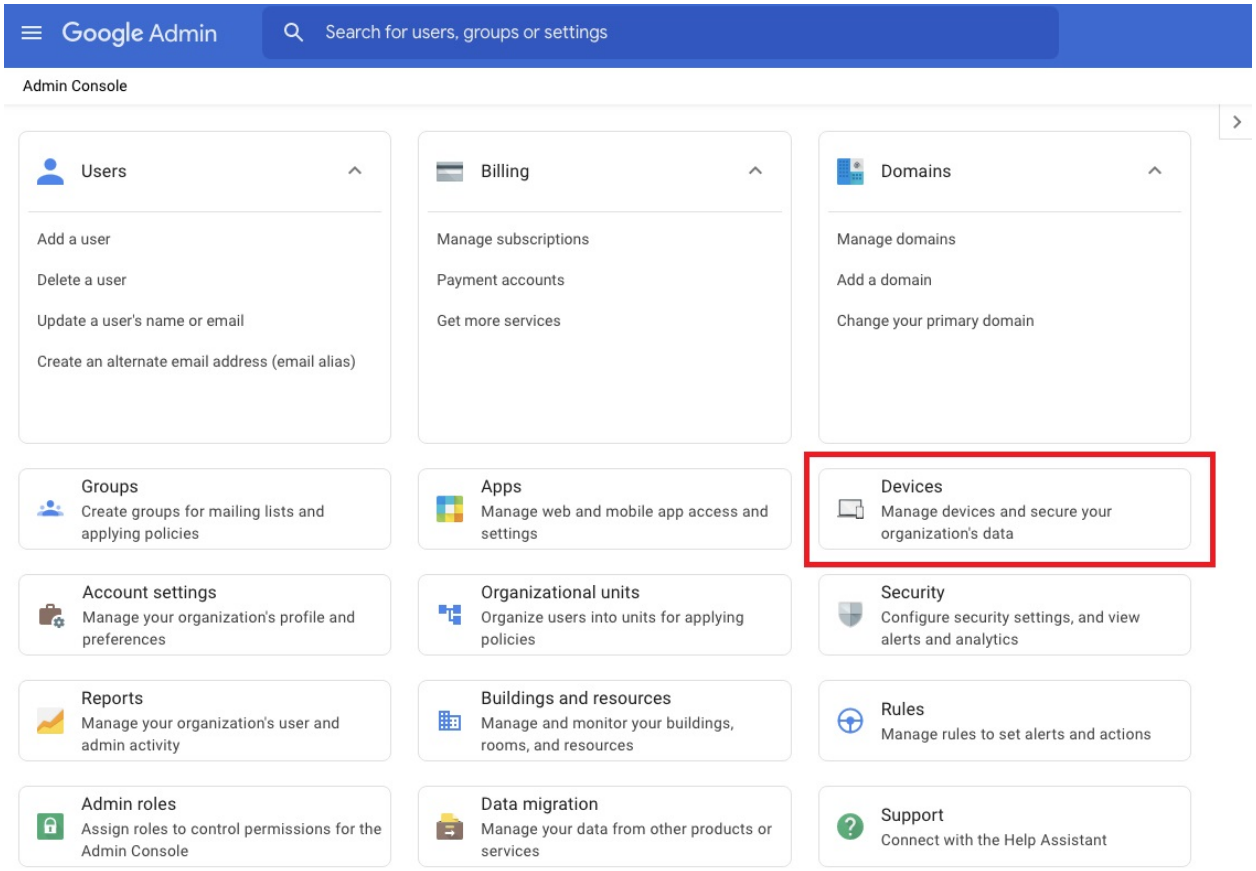
If you delete a user — for example, when they leave your organization —they will no longer have access to any of your organization's Google Workspace services. As an administrator, you can transfer files and data owned by the user (files that the user doesn't own are not affected). If content ownership isn't transferred upon account deletion, the content will be deleted. Deletion can take up to 24 hours to complete. Review Delete a user from your organization for instructions on deleting or restoring a user, and details about what data is deleted.



Managing customer personal data on devices

As an admin, you can control which devices can sync customer personal data. With basic or advanced mobile management, you can delete a device to prevent it from syncing data. You can also approve, block, or unblock a device using the Admin console. Furthermore, with advanced mobile management, you can control which apps can sync customer personal data on Android and iOS devices (i.e., if a user can access their work Calendar on their device).

Note: When you delete a device, the device stops syncing data, but no information is removed from it. If you want to remove data from the device, wipe the account from the device or wipe the entire device before you delete it. For details, see Remove corporate data from a mobile device.



Delete customer data

Google Workspace allows you to delete customer data at any time, using options like “Move to trash” and “Delete”. Once data is removed from Google Workspace— for example, when a deleted email can no longer be recovered from the trash — data is permanently deleted according to your Customer Agreement and our Privacy Policy unless you set retention rules on data from certain Google Workspace apps using Google Vault (see section below for more details on Google Vault).

When our customers delete data in Google Workspace, we immediately start the process of removing it from the product and our systems. First, we aim to immediately remove it from view. We then begin a process designed to safely and completely delete the data from our storage systems. Each Google storage system from which data gets deleted has its own detailed process for safe and complete deletion. This might involve repeated passes through the system to confirm all data has been deleted. Our services also use encrypted backup storage as another layer of protection to help recover from potential disasters. Data can remain on these systems for up to 6 months.

Below are some commonly asked questions regarding data deletion and recovery. Review the Google Workspace Help Center for more information.

- How do I delete and restore files in Google Drive? (data subjects)
- How do I restore deleted shared drives or their files? (Google Workspace Admin)
- How do I delete or recover deleted Gmail messages?
- How do I delete or restore my site?

Vault Retention & Deletion

Vault also allows Admins to enforce retention policies. Retention allows domains to set the life cycle for customer data:

- **Keep data for as long as you need it**: If your organization is required to preserve data for a period of time, you can configure Vault to retain it even if users delete messages and files, and then empty their trash.
- **Remove data when you no longer need it**: If your organization is required to delete sensitive data after a period of time, you can configure Vault to remove it from user accounts and expunge it from all Google systems.

However, if you delete a user, you can't search or export any of their data from Vault and any retention rules or holds places on the user's data no longer apply.

Conclusion

Meeting regulatory compliance requirements is a top priority for us and our customers. Google is committed to helping you meet your privacy and data protection obligations by offering tools and building robust privacy and security protections into our services and contracts. For more information, please visit our GDPR Compliance resource center and CCPA Compliance resource center, where you can find our GDPR whitepaper, CCPA whitepaper, and Google Workspace Data Protection Implementation Guide.