IBM Storage Protect for Cloud Google Workspace

User Guide

IBM

Contents

Note:

Before you use this information and the product it supports, read the information in “Notices” on page 130.

Edition Notice (June 2024)

This edition applies to IBM® Storage Protect for Cloud Google Workspace (product number 5900-AP6) all subsequent releases and modifications until otherwise indicated in new editions.

About this publication

This publication provides overview, planning, and user instructions for IBM® Storage Protect for Cloud.

Who should read this publication

This publication is intended for administrators and users who are responsible for implementing a backup and recovery solution with IBM® Storage Protect for Cloud Google Workspace in one of the supported environments.

System administrators can use this guide to help start the application, manage users, and catalog resource information. Users can find procedures on how to search and browse for objects, generate and interpret reports, schedule jobs, and orchestrate backup and restore jobs.

What's new

Learn about new features and updates in IBM® Storage Protect for Cloud Google Workspace.

Release Date: November 2, 2025

New features and updates

- **Data management** now includes support for Vault.

Updates in previous versions

Release Date: September 3, 2025

- On the **Storage consumption** report, add Gmail (Vault), Drive (Vault), and Shared drives (Vault) for the Vault data protection.
  If your organization uses the BYOS (Bring your own storage) subscription and has enabled Vault protection, you can contact IBM support to add this report for your tenant.
- The API method for retrieving job information has been enhanced to support filtering for Google Vault (including Gmail, Drive, and shared drives).

Release Date: July 6, 2025

- In **Data management**, backup data for shared drives can now be deleted.
- In **Job monitor**, the UI for downloading exported content has been enhanced. After selecting **Download content**, the relevant panel appears with step-by-step instructions: first retrieve the password for decrypting the exported data, then click **Download** to download the content.
- For organizations who use their own storage locations to store backup data, IBM® Storage Protect for Cloud Google Workspace now displays a message prompt recommending storage firewall configuration to ensure the backup service can access your storage.
- On the **Dashboard**, the **Vault** tab now displays additional content, including **Users in protected matters** and **Subscription information**
- Updated links in IBM® Storage Protect for Cloud Google Workspace interfaces, job reports, and related emails to direct users to the content-sensitive pages.

Release Date: May 11, 2025

- IBM® Storage Protect for Cloud Google Workspace now supports backing up and exporting Google Vault data (Gmail, Drive, and shared drives). If your organization wants to enable the Vault protection add-on in the Google Workspace module, contact your IBM representative to enable this feature in your tenant's subscription to IBM® Storage Protect for Cloud Google Workspace.
- Administrators can now add multiple users into a restore queue in IBM® Storage Protect for Cloud Google Workspace, allowing bulk restores for the users' Gmail, Drive, Calendar, and Contacts backup data. Users can be selected in **Calendar mode** or imported via CSV file upload.
- New navigation updates are being rolled out, delivering a more intuitive, consistent, and efficient user experience. In IBM® Storage Protect for Cloud Google Workspace, the left navigation pane has the following key updates:
  - Renamed the following options:

New	Previous
Dashboard	Overview
Reporting	Report center
Unusual activities analysis	Google Workspace unusual activities analysis
Subscription	Subscription consumption

  - Moved **System auditor** and **Subscription** to the **System** section.

- IBM Storage Protect for Cloud Google Workspace now supports selecting Chat backup data via the **Calendar mode**.
- The **Last Modified By** column has been added to the list of files with unusual activities, showing the email addresses of users who last added or modified the files.
- In **Settings** > **General** > **Backup settings**, you can now configure the **Advanced labels exclusion** setting to exclude more labels from the **Gmail** backup scope, and configure the **Advanced folders exclusion** setting to exclude more folders from the **Drive** or **Shared drives** backup scope.
- Google Workspace Chat is now fully supported.

Release Date: March 3, 2025

The left navigation pane in IBM® Storage Protect for Cloud Google Workspace and IBM® Storage Protect for Cloud Recovery Portal has been streamlined for improved usability. Here are the key updates:

- In the left navigation pane of IBM® Storage Protect for Cloud Google Workspace, the **Activity** and **System** sections have been added. The **Activity** section includes **Report center** (renamed from **Report**) and **Job monitor**, and the **System** section includes **Settings** and **System auditor**.
- In IBM® Storage Protect for Cloud Recovery Portal, the **Contact admin** () button is now located under the System section.

In **Settings** > **General**, administrators can now enable the approval process for data deletion requests from **Manually delete backup data** and **Data subject access requests**. With the **Approval process for data deletion** setting enabled, data deletion requests and email notifications will be sent to administrators. Upon approval, deletion jobs will proceed. After the approval process has been enabled, you must contact IBM technical support if you want to disable this setting.

IBM® Storage Protect for Cloud Google Workspace now supports retrieving job information via IBM® Storage Protect for Cloud modern APIs. By invoking the API method with the **gsuite.graph.read.all** permission, you can gain in-depth insights and data on specific job reports, improving your organization's ability to manage and analyze job information effectively.

The retention logic for IBM® Storage Protect for Cloud Google Workspace subscription renewals has been improved. If your updated subscription has a shorter retention period than your current configuration, retention periods will be automatically adjusted to match the new subscription limits. If the updated subscription has the same or longer retention period, no changes will be made. To verify your configuration and ensure you are aware of any changes, refer to **Settings** > **General** > **Retention policy**.

Release Date: January 12, 2025

In **Settings** > **General**, the **Retention policy** section has the following improvements:

- Enhanced the user interface by replacing drop-down lists with textboxes, simplifying the process for users to set retention period values.
- You can now select the **Use a custom retention policy for each container**option, and then customize retention policies for containers.

When you use a Google account to access the IBM® Storage Protect for Cloud Google Workspace environment via the direct URL for the first time, a pop-up window will appear if you signed up for IBM® Storage Protect for Cloud with a local account. In the pop-up window, you can choose to link the local account with your Google account to enable single sign-on.

You can now invoke the **GetProductConsumptionDetails** API (provided by IBM) to get reports of customers' protected data size and consumed storage size of using IBM® Storage Protect for Cloud Google Workspace.

Release Date: November 11, 2024

You can now view and select backup data for recovery via a **Calendar mode** view, making it easier to drill down to a specific recovery point in time.

Users utilizing multi-geo storage can now specify data center locations for shared drive data. This enhancement provides flexibility to manage and store your data according to your preferences, whether for compliance with federal regulations or internal best practices.

For organizations that use a custom Google app, if you want to set conditions of the **Organizational units** rule to scan shared drives via the scan profiles configured in IBM® Storage Protect for Cloud > **Auto discovery**, the **https://www.googleapis.com/auth/admin.directory.orgunit.readonly** permission scope must be added to the custom app.

In **Settings** > **Notification**, you can now manage multiple notification profiles.

The date format in IBM® Storage Protect for Cloud Google Workspace can now be customized. You can navigate to IBM® Storage Protect for Cloud > **Administration** > **General settings** > **Culture settings** to select a desired date format option.

You can now apply conditions on the **ID** filter when searching for backup data of folders/files, allowing you to locate folders or files based on their unique IDs.

Release Date: August 25, 2024

In **Report** > **System auditor**, you can now customize a time range to export the report.

In **Settings** > **Notification** > **Job notification**, the master switch **Email notification for job completion status** has been added. It is enabled by default. If you want to disable job notification settings, you can turn off the toggle.

The user interface of the **System auditor** reports has been optimized to provide a more intuitive and user-friendly experience.

In notification emails, you can now click **Learn more about IBM Storage Protect for Cloud Google Workspace** to open the documentation center at https://www.ibm.com/docs/en/spfc

Release Date: June 23, 2024

IBM® Storage Protect for Cloud Google Workspace has a brand-new redesigned UI!

IBM® Storage Protect for Cloud Google Workspace now supports customers with Multi-Geo enabled to configure mappings between Google Workspace geo locations and IBM® Storage Protect for Cloud data centers.

Release Date: April 28, 2024

The **Account Management** function now is available for the Google Classroom module.

You can now choose to rerun the jobs for just the failed items, rather than running the entire job again. This can help you ensure that your data is recovered as quickly as possible. In **Job Monitor**, you can rerun a job by clicking the **Rerun** () button.

If your organization's subscription is **Bring your own storage** (BYOS) and the custom storage type is **Microsoft Azure Blob Storage**, IBM® Storage Protect for Cloud Google Workspace can now move the backup data to the archive tier on the storage for saving your storage cost. When performing a restore job, you can choose **Automatically rehydrate if backup data is in Azure archive storage tier**. The administrator can navigate to **Settings** > **Self-service Settings** > **End-user Restore** settings and control whether to allow end-users to restore backup data on the Archive tier. If you want to disable the archive setting, you can contact IBM support for help.

IBM® Storage Protect for Cloud Google Workspace now supports the **Storage Consumption** report. The report provides an overview of storage consumption by different service types, the history and trends of storage usage, and utilization information of containers. If you want to add this report, you can contact IBM support for help.

Release Date: March 3, 2024

You can now configure multi-geo storage locations for your backup data. These settings can be customized at the container level to better fit your data requirements.

IBM® Storage Protect for Cloud Google Workspace now offers support for custom app profiles, allowing for more flexible protection of your environment.

The exported job reports now contain the **Error Code** column. The **Error Code** column displays the error codes related to the failed jobs. You can click the link in the **Error Code** column to open the user guide for troubleshooting.

Release Date: January 7, 2024

The following new features and improvements are made to the new experience of the IBM® Storage Protect for Cloud Google Workspace:

- In **Data Management** > **Data Subject Access Requests** > **Discover & Delete**, IBM® Storage Protect for Cloud Google Workspace now supports deleting multiple users at a time.

About IBM® Storage Protect for Cloud Google Workspace

IBM® Storage Protect for Cloud Google Workspace can protect your Google Workspace data (including Gmail, Drive, Calendar, Contacts, and shared drives), Google Vault data (including Gmail, Drive, and shared drives), and Google Classroom data by offering automatic backups and flexible restores that enable fast recovery from errors, attacks, and failures.

Google Workspace and Google Classroom

Google Workspace and Google Classroom are individual modules. To use each module, ensure that your organization has purchased the module in the subscription of IBM® Storage Protect for Cloud Google Workspace. Suppose your organization has both Google Workspace and Google Classroom modules. In that case, the following pages distinguish the two modules via the **Google Workspace** and **Google Classroom** tabs: **Dashboard**, **Protection**, **Restore**, and **Subscription**.

- The following functions are only available for organizations with the Google Workspace module in the subscription of IBM® Storage Protect for Cloud Google Workspace: **Data management**, **Self-service** (for IBM® Storage Protect for Cloud Recovery Portal), and **Unusual activities analysis**

For more information on the data types that are supported or unsupported, refer to the following sections:

Google Vault Protection

Protection for the Google Vault data is an addon in the Google Workspace module. If your organization needs the protection for Vault, contact the IBM representative to enable this feature in your tenant's subscription to IBM® Storage Protect for Cloud Google Workspace. Once the Vault protection has been enabled, the following pages will display the **Google Workspace** and **Vault** tabs to distinguish the two protections: **Dashboard**, **Protection**, and **Restore**. For additional details, see Vault Data Protection.

Helpful Notes

Note the following:

- IBM® Storage Protect for Cloud Recovery Portal is a portal where invited Google users can restore or export their data that is protected by IBM® Storage Protect for Cloud Google Workspace, as well as view and download job reports. You can click **Go to IBM® Storage Protect for Cloud Recovery Portal** to access the portal. For additional details, refer to the IBM® Storage Protect for Cloud Recovery Portal User Guide. Recovering Google Classroom data hasn't been supported in IBM® Storage Protect for Cloud Recovery Portal.
- When a backup job needs to back up a large number of objects, to not affect the next backups, IBM® Storage Protect for Cloud Google Workspace can split the backup into sub jobs to shorten the time of the backup job.
- For files and folders in drives or shared drives, if a file/folder was backed up before it has been moved to a new location, without any changes to its content, the file/folder couldn't be backed up again in the new location.

Language Support

IBM® Storage Protect for Cloud Google Workspace supports the following languages: English, French, and German.

Supported Browsers

The following table provides the required browser versions:

Browser	Version
Google Chrome	The latest version
Microsoft Edge ( )	The latest version
Microsoft Edge based on Chromium ( )	The latest version

Use IBM® Storage Protect for Cloud Google Workspace Graph APIs

You can use the Graph APIs to do the following:

- Retrieve audit records for activities within your IBM® Storage Protect for Cloud tenant. For details, open IBM Graph Modern API Overview page and navigate to **Services and Features** > **IBM® Storage Protect for Cloud** > **Audits**.
- Retrieve job information from IBM® Storage Protect for Cloud Google Workspace and IBM® Storage Protect for Cloud Recovery Portal. For details, open IBM Graph Modern API Overview page and navigate to **Services and Features** > **IBM® Storage Protect for Cloud Google Workspace** > **Jobs**.

Integration with Microsoft Azure Event Hubs

If you want to build an integration between a hub in Microsoft Azure Event Hubs and the audit records from IBM® Storage Protect for Cloud Google Workspace, refer to the instructions in the IBM® Storage Protect for Cloud user guide.

Data Export Service

Data Export Service is provided for organizations who want to remove their backup data as they plan to end the subscription to IBM® Storage Protect for Cloud Google Workspace. For more details, see Data Export Service.

> **Note:** If you only want to export a smaller sample set of data to plain file format, use the **Export** button in the restore wizard. For details on downloading exported data, refer to Download Data of Export Jobs.

Subscription and Licensing Information

To find out how IBM® Storage Protect for Cloud Google Workspace, refer to Subscription and Licensing Information.

> **Note:** Suspended users and Archived users are not in the scope of counting licenses for charge.

Storage Location for Backup Data

You can choose to store the backup data in the default storage location provided by IBM® Storage Protect for Cloud or your custom storage location. The storage type of the default storage location is Microsoft™ Azure Blob Storage. The storage type of the custom storage location can be one of the following: Google Cloud Storage, Amazon S3, Amazon S3-Compatible Storage, Microsoft™ Azure Blob Storage, IBM® Storage Protect - S3, and IBM® Cloud Object Storage.

If your backup data is currently on the default storage location and you want to use your own storage afterward, you can contact IBM Software Support to update your subscription to **Bring Your Own Storage** (BYOS) and change the storage location to your own storage. For details about configuring a custom storage location, refer to “Configure Custom Storage Location for Your Backup Data” on page 23.

If you use your own storage location at the beginning but you want to change to the default storage location, you can also contact IBM® Storage Protect for Cloud support to update your subscription and the storage location.

If you are using the default **Microsoft Azure Blob Storage** storage and you want to change to another default storage type, note the following:

- The legacy backup data will remain on the old default storage and can be restored.
- The new default storage can only store the data that is backed up after you switch to the new default storage type.
- Both default storage types will be covered in the retention jobs.

If you want to use a custom storage location, the storage type can be one of the following: **Amazon S3**, **Amazon S3-Compatible Storage**, **Microsoft Azure Blob Storage**, **IBM Storage Protect – S3**, and **IBM Cloud Object Storage**. Note the following:

- If you use your own storage location at the beginning but you want to change to the default storage location, you can also contact IBM Software Support to update your subscription and the storage location.

Retention Policy of Backup Data

If you use your custom storage location to store backup data, you can navigate to **Settings** > **General** > **Retention policy** to customize the retention period for the backup data.

You can also customize the **Retention policy** setting if you use the default storage location with the **Unlimited retention** subscription.

For details about configuring the **Retention policy** setting, refer to Configure the Retention Policy Setting.

> **Note:** If your storage location for the backup data has been changed from a custom storage location to the IBM default storage location, only the backup data on the IBM default storage will be deleted according to the retention policy.

Multi-Geo Support (for Enterprise Subscription)

If your Google organization has **No preference**, **United States**, or **Europe** data regions and wants to store backup data on separate storages based on the different data regions, the administrator can contact the IBM representative to enable the Multi-Geo function in your tenant's enterprise subscription of IBM® Storage Protect for Cloud Google Workspace. With the Multi-Geo support, you can configure data regions for user containers or shared drive containers in IBM® Storage Protect for Cloud Google Workspace.

Refer to the following instructions to complete settings related to the Multi-Geo support:

1. You must first configure mappings between your Google Workspace geo locations and IBM® Storage Protect for Cloud data centers.
   Note the following:
   - The **No preference** region is mapped to the IBM data center where your primary tenant initially signed up.
   - The **United States** region is mapped to the **East US (Virginia)** data center.
   - The **Europe** region is mapped to the **UK South (London)** data center by default. If you want to change this mapping, select a data center from the drop-down list.
   - After you click **Continue**, the initialization for your multi-geo environment starts and you can no longer go back to change the mappings.
2. When you follow the steps on the wizard for the initial backup and you select containers to be protected, you can click **Configure data region** to configure data regions for the selected containers.

   > **Note:** For **Classroom** containers, the data region is **No preference** and cannot be changed.

3. If your tenant's subscription is BYOS (Bring your own storage), you must configure a storage location for each selected data region.
4. Service administrators and Application administrators have permission to all data regions. Standard users, when added to security groups within a specific data region, are limited to accessing only those containers that fall under their assigned security groups. Standard users' access is restricted to the confines of that particular data region.
   When users with permissions to multiple data regions access IBM® Storage Protect for Cloud Google Workspace, they need to select a region to continue.

   In IBM® Storage Protect for Cloud Google Workspace, if they want to switch to another region, they can select a region from the drop-down list.

> **Note:** The **Subscription** and **Self-service** pages do not have the data region drop-down list, as they are global settings. The data region drop-down list on the **Protection** page contains the **All** option, which makes it easy for the administrators to have a global view when they configure data regions.

5. On the **Protection** page, when administrators configure the protected scope, they can configure data regions for containers.

Data Encryption Methods

Data encryption can be divided into two scenarios: data transmission (data in transit) encryption and data storage (data at rest) encryption.

For data transmission encryption, IBM® Storage Protect for Cloud Google Workspace is deployed on the Microsoft Azure / Google Cloud Platform framework to make outbound Google API calls and internal communications over HTTPS/TLS encrypted channels. Certificate-based authentication is used for internal communications.

For data storage encryption, IBM® Storage Protect for Cloud Google Workspace encrypts all the Google Workspace data obtained by calling Google APIs with AES 256 using keys unique to each tenant (either default keys or BYOK). The encryption happens before the data is transmitted to storage.

When transmitting the encrypted data to storage, the data transmission encryption will leverage their own data transmission encryption algorithm or protocols applied of the target storage's available protocols.

Vault Data Protection

IBM® Storage Protect for Cloud Google Workspace supports backing up and exporting Google Vault data (Gmail, Drive, and shared drives). If your organization wants to enable the Vault protection add-on in the Google Workspace module, contact the IBM representative to enable this feature in your tenant's subscription to IBM® Storage Protect for Cloud Google Workspace.

Below is a quick checklist for organizations who enabled Vault protection:

1. To enable protection for the Vault service, it is necessary to configure a custom Google app. For additional details, see Custom Google App.
2. Navigate to IBM® Storage Protect for Cloud > **Auto discovery** > **Scan profiles**, and configure scan profiles to automatically scan Google Vault matters into containers for backup. For additional details, see the Auto Discovery for Google Workspace section in the IBM® Storage Protect for Cloud user guide.
3. Only users in the **Administrators** group can back up and export Vault data. To manage users in the **Administrators** group, navigate to **Settings** > **User management**, select the **Administrator** group and click **Edit**.
4. For the Vault protection, **Back up now** is supported and the next backup job will back up the incremental data of the same user in the last backup job. To back up Vault data, refer to the steps below:
   a. Go to **Protection** and click the **Vault** tab.
   b. Select containers and click **Configure protected scope**.
   c. Select the services that you want to protect.

      > **Note:** Vault protection does not back up the drafts in Gmail (Vault), for avoiding the duplicate drafts generated by the Google Vault.

   d. Click **Back up now**.

   When you click **Back up now**, the system will trigger a backup job and you can check the job status in **Job monitor**.

> **Note:** The Vault protection would not support to back up shared drives that were deleted from Google Workspace.

5. You can use the **Search mode** to select Vault backup data to export. For additional details, see Export Google Vault Data.

> **Note:** The following settings are currently unsupported for Vault protection: **Backup settings** and **Retention policy**.

Data Export Service

The Data Export Service is provided to organizations in the following instance:

- Organizations who plan to end their subscription to IBM® Storage Protect for Cloud Google Workspace and remove their backup data

Additionally, the operation of Data Export Service depends on your organization's storage location of backup data:

- For organizations using IBM-provided default storage
  IBM will retain the backup data in IBM storage for 60 days, subject to the terms of your service agreement if the subscription to IBM® Storage Protect for Cloud Google Workspace service ends. The backup data in IBM storage can be exported to your own storage as a paid service. Contact your sales representative if you wish to export data from IBM Storage.
- For BYOS organizations
  If your subscription is the BYOS type, ending the subscription will not delete the backup data stored in your own storage. You do not need to pay an export fee.

The backup data is encrypted and stored in IBM format rather than as pure copies of Google Workspace data. The encryption keys are required when converting encrypted backup data to readable content. Before leaving this product, ensure you export the encryption keys, as you will lose access to the product's interface once your subscription ends. For more details, refer to Export Encryption Keys. By default, exporting encryption keys is not available to organizations using IBM-provided default storage. If your organization uses IBM default storage, you can contact IBM Software Support to enable this feature if needed.

Get Started

Follow the instructions below to complete the preparations in IBM® Storage Protect for Cloud:

1. Sign in to the IBM® Storage Protect for Cloud environment with your account.
2. After you get a subscription of IBM® Storage Protect for Cloud Google Workspace, you can accept the subscription agreement of IBM® Storage Protect for Cloud Google Workspace.
3. Connect your Google tenant in IBM® Storage Protect for Cloud > **Management** > **Tenant management**. For additional details, refer to the Connect your Tenants to IBM® Storage Protect for Cloud section in the IBM® Storage Protect for Cloud user guide.
4. Refer to the instructions below to prepare an app in your Google Workspace environment:
   - Custom Google app – If your organization has specific requirements, refer to the Custom Google App to configure a custom Google app.
     Note that a custom Google app is required in the following scenarios:
     - When using the default service app **(IBM Tenant Management)**, you may encounter throttling issues caused by Google quota limits. If performance is a concern, consider configuring a custom Google app for your organization.
     - If your organization wants to enable protection for the Chat/Vault service, it is necessary to configure a custom Google app.
   - Default service app – You can search and install the **IBM Tenant Management** app from the Google Workspace Marketplace. For the permissions requested by the **IBM Tenant Management** apps, see the IBM® Storage Protect for Cloud Google Workspace sections in the IBM® Storage Protect for Cloud user guide.

     > **Note:** If your organization has configured both the default **IBM Tenant Management** app and a custom Google app, only the custom Google app will be used in backup and restore jobs.
5. In IBM® Storage Protect for Cloud, create an app profile for Google Workspace. For additional details, see the Create an App Profile section in the IBM® Storage Protect for Cloud user guide.

   > **Note:** Managing an app profile requires the Super Admin account in Google Workspace. Ensure that the Super Admin account has been assigned with the required licenses:
   > - The Google Workspace module requires licenses for the Gmail, Calendar, Contacts, Drive, and Chat services. The following additional licenses are only needed for managing specific services: Shared drive for shared drives and Vault for Vault matters.
   > - The Google Classroom module requires licenses for the Classroom service.
6. Navigate to IBM® Storage Protect for Cloud > **Auto discovery**, and create scan profiles to automatically scan Google Workspace objects into containers for backup. For additional details, see the Auto Discovery for Google Workspace section in the IBM® Storage Protect for Cloud user guide.

   > **Note:** For each scanned shared drive to be backed up, ensure there is at least one member with the **Manager** permission. Otherwise, the shared drive cannot be successfully backed up.
7. You can add users into IBM® Storage Protect for Cloud and grant permissions for them to perform backup and restore. For additional details, see the Manage Users section in the IBM® Storage Protect for Cloud user guide.
8. In IBM® Storage Protect for Cloud, to access IBM® Storage Protect for Cloud Google Workspace, click **Backup** on the left navigation, and then click **Google Workspace** from the drop-down list. You can also

My Services on the left navigation, and then click **IBM® Storage Protect for Cloud Google Workspace** under the **All services** or **My favorite services** tab.

In IBM® Storage Protect for Cloud Google Workspace, refer to the sections below to get started with your data protection:

1. Complete your customization for backup jobs. For details, refer to the Configure General Settings for Backup and Change the Protected Scope sections.
2. Manage security groups / user access to control users' permissions for data recovery. For details, refer to the Account Management and Configure Self-service Settings for Recovery Portal sections.

   > **Note:** For additional methods about deleting users' backup data due to security/GDPR concerns, refer to Data Management.

3. Configure notification profiles to receive email alerts when there are job exceptions or unusual activities detected. For details, refer to Configure Job Status Notification Settings.
4. Perform data recovery for Google Workspace, Google Vault, or Google Classroom data. For details, refer to Recover Google Workspace Data, Export Google Vault Data, and Recover Google Classroom Data.
5. Monitor jobs, view job reports, and download exported data. For details, refer to Monitor Jobs and Download Job Reports and Download Data of Export Jobs.
6. Check reports in Cloud Backup for Google Workspace. For details, refer to View Reports.
7. View user activities in IBM® Storage Protect for Cloud Google Workspace and IBM® Storage Protect for Cloud Recovery Portal. For details, refer to Audit User Activities in System Auditor.
8. View your organization's subscription information, including utilization, top consumers, and usage history. For details, refer to View Subscription Information.

Custom Google App

Configuring a custom Google app is required in the following scenarios:

- When using the default service app (**IBM Tenant Management**), you may encounter throttling issues caused by Google quota limits. If performance is a concern, consider configuring a custom Google app for your organization.
- If your organization wants to enable protection for the Chat/Vault service, it is necessary to configure a custom Google app.
- If your organization has configured both the default **IBM Tenant Management** app and a custom Google app, only the custom Google app will be used in backup and restore jobs.

Follow the instructions below to configure a custom Google app and create an app profile to consent to the custom app:

1. Configure a custom Google app by referring to the Create a Custom Google App section in the IBM® Storage Protect for Cloud user guide.
2. Refer to the information below to enable the required APIs:
   - **Admin SDK API** must be enabled for common functionalities.
   - **Gmail API** must be enabled if you want to protect the Gmail data.
   - **Google Drive API** must be enabled if you want to protect drives and shared drives.
   - **Drive Labels API** must be enabled if you want to protect labels for drives and shared drives.
   - **Google Calendar API** must be enabled if you want to protect calendars.
   - **Google People API** must be enabled if you want to protect contacts.
   - **Google Chat API** must be enabled if you want to protect chats. After enabling the Google Chat API at Google Cloud Console, you need to configure the app information under its **CONFIGURATION** tab by following the steps below. (Note that the Chat apps are required to access Chat data but are invisible to Google users.)

a. Configure the following application information:
    - **App Name** – Enter the name of the app.
    - **Avatar URL** – Provide an icon for the app. Any valid URL is acceptable.
    - **Description** – Write a brief description of the app.

b. Disable the **Enable Interactive features** option.

c. Click **Save**.

- **Google Vault API** and **Google Cloud Storage JSON API** must be enabled if you want to protect the Vault data.
- **Google Classroom API** must be enabled if you want to protect the Classroom data.

3. Refer to the following information to configure the related **OAuth scopes**:
    - To protect the Google Workspace data (including Gmail, Drive, Drive labels, Calendar, Contacts, Chat, and shared drives), you can copy and paste the following to the **OAuth scopes**:
      https://www.googleapis.com/auth/admin.directory.group.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.reports.usage.readonly,https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://mail.google.com/,https://www.googleapis.com/auth/drive,https://www.googleapis.com/auth/drive.admin.labels,https://www.googleapis.com/auth/drive.labels,https://www.googleapis.com/auth/calendar,https://www.googleapis.com/auth/contacts.other.readonly,https://www.googleapis.com/auth/contacts,https://www.googleapis.com/auth/chat.spaces.readonly,https://www.googleapis.com/auth/chat.memberships.readonly,https://www.googleapis.com/auth/chat.messages.readonly
    - To protect the Google Workspace data (including Gmail, Drive, Drive labels, Calendar, Contacts, Chat, and shared drives) and the Google Vault data (including Gmail, Drive, and shared drives), you can copy and paste the following to the **OAuth scopes**:
      https://www.googleapis.com/auth/admin.directory.group.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.reports.usage.readonly,https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://mail.google.com/,https://www.googleapis.com/auth/drive,https://www.googleapis.com/auth/drive.admin.labels,https://www.googleapis.com/auth/drive.labels,https://www.googleapis.com/auth/calendar,https://www.googleapis.com/auth/contacts.other.readonly,https://www.googleapis.com/auth/contacts,https://www.googleapis.com/auth/chat.spaces.readonly,https://www.googleapis.com/auth/chat.memberships.readonly,https://www.googleapis.com/auth/chat.messages.readonly,https://www.googleapis.com/auth/ediscovery,https://www.googleapis.com/auth/devstorage.read_only
    - To protect the Google Classroom data, you can copy and paste the following to the OAuth scopes:
      https://www.googleapis.com/auth/admin.directory.group.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.reports.usage.readonly,https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/classroom.courses,https://www.googleapis.com/auth/classroom.announcements,https://www.googleapis.com/auth/classroom.coursework.me,https://www.googleapis.com/auth/classroom.coursework.students,https://www.googleapis.com/auth/classroom.courseworkmaterials,https://www.googleapis.com/auth/classroom.rosters,https://www.googleapis.com/auth/classroom.profile.emails,https://www.googleapis.com/auth/classroom.topics,https://www.googleapis.com/auth/classroom.topics.readonly,https://www.googleapis.com/auth/classroom.guardianlinks.students

Refer to the table below for details about why we need the scopes:

Service	API	Scope	Purpose
Common	Admin SDK API	https://www.googleapis.com/auth/admin.directory.group.readonly	Retrieve groups in your domain.
		https://www.googleapis.com/auth/admin.directory.user.readonly	Retrieve users in your domain.

Service	API	Scope	Purpose
		https://www.googleapis.com/auth/admin.reports.usage.readonly	Retrieve your organization subscription usage for backup admins to monitor their subscription in the app.
		https://www.googleapis.com/auth/admin.directory.orgunit.readonly	Retrieve organization units in your workspace
Gmail	Gmail API	https://mail.google.com/	Back up emails and labels in Gmail for future recovery.
Drive	Google Drive API	https://www.googleapis.com/auth/drive	Back up folders and files under My Drive and Shared Drives for future recovery.
Drive label	Drive Labels API	https://www.googleapis.com/auth/drive.admin.labels	Retrieve all information of labels on files in Drives for backup and restore.
		https://www.googleapis.com/auth/drive.labels	Back up and restore properties of labels on files in Drives.
Calendar	Google Calendar API	https://www.googleapis.com/auth/calendar	Back up calendars and events from Google Calendar for future recovery.
Contacts	Google People API	https://www.googleapis.com/auth/contacts.other.readonly	Back up **Other contacts** data.
		https://www.googleapis.com/auth/contacts	Back up contact groups and contacts from Google Contacts for future recovery.
Chat	Google Chat API	https://www.googleapis.com/auth/chat.spaces.readonly	Retrieve all chat spaces.
		https://www.googleapis.com/auth/chat.memberships.readonly	Retrieve the membership of each chat space.
		https://www.googleapis.com/auth/chat.messages.readonly	Back up chats and related attachments.
Vault	Google Vault API	https://www.googleapis.com/auth/ediscovery	Use this API to export Google Vault data.
	Google Cloud Storage JSON API	https://www.googleapis.com/auth/devstorage.read_only	Download the exported Google Vault data.
Classroom	Google Classroom API	https://www.googleapis.com/auth/classroom.courses	Back up and restore classes.
		https://www.googleapis.com/auth/classroom.announcements	Back up and restore announcements in classes.

Service	API	Scope	Purpose
		https://www.googleapis.com/auth/classroom.coursework.me	Back up classwork in classes
		https://www.googleapis.com/auth/classroom.coursework.students	Restore classwork in classes.
		https://www.googleapis.com/auth/classroom.courseworkmaterials	Back up and restore classwork materials.
		https://www.googleapis.com/auth/classroom.rosters	Back up and restore students and teachers in classes.
		https://www.googleapis.com/auth/classroom.profile.emails	Retrieve email addresses in classes.
		https://www.googleapis.com/auth/classroom.topics	Back up and restore topics in classes.
		https://www.googleapis.com/auth/classroom.topics.readonly	Retrieve information of topics.
		https://www.googleapis.com/auth/classroom.guardianlinks.students	Retrieve guardians of students in classes.

After you finish configuring scopes for the custom Google app, go to IBM® Storage Protect for Cloud and navigate to **Management** > **App management** to create an app profile and consent to the custom Google app. For more details, refer to the Consent to Custom Apps section in the IBM® Storage Protect for Cloud user guide.

View Dashboard

To glance at the protected scope, backup points, and subscription information in your IBM® Storage Protect for Cloud Google Workspace, click the **Overview**() tab on the left pane. The **Overview** page appears.

On the **Overview** page, you can perform the following:

- To view the protected scope and backup points of a service, click the service tab at the top of the page. Refer to the following scenarios to perform your actions:
  - If a service hasn't been protected, you can click **Protect Now** and configure the protection scope for the service by referring to "Configure Protected Scope" on page 32
  - If a service already has been protected, you can do the following:
    - To change the protected scope of the service, click the number of protected/unprotected/total objects and refer to "Configure Protected Scope" on page 32
    - To view details of backup points, click **More Details**. The details page appears. You can click the **Backup Details** and **Restore Details** tab to view a summary of backup and restore jobs. Clicking **View Details** will direct you to **Job Monitor** where you can view details of a job and get the job report by referring to "Monitor Jobs and Download Job Reports" on page 91.
- Under the **Vault** tab, you can use the **Users in protected matters** section to check which users' data has been backed up in the protected matters. Clicking the number in the **Protected matters** column will open the panel with these matters' details.
- The **Subscription Information** section shows the following basic information about your subscription:
  - The number of resources that your organization has purchased, the number of resources that your organization has assigned/consumed, and the number of available resources.
  - The date when your subscription will expire.

To view more subscription information, click the arrow button to go to the **Subscription Consumption** page. For more information, see IBM Storage Protect for Cloud Microsoft 365.

Configure General Settings for Backup

The **General** settings are only available to users in the **Administrators** group of this product. To configure **General settings**, click **Settings** () tab on the left navigation and click **General** in the drop-down menu. The **General** page appears, and you can configure the following:

- To configure additional settings for backup jobs, click **Backup settings**. For additional details , see "Configure Backup Settings" on page 22
- To configure the schedule for backup jobs, click **Backup schedule**. For additional details , see Configure the Backup Schedule "Configure the Backup Schedule" on page 23.
- To avoid accidental data loss, you can enable the approval process by turning on the **Approval process for data deletion** toggle. With this feature enabled, when requesters are going to delete data in **Data subject access requests** or **Manually delete backup data**, data deletion requests and email notifications will be sent to the administrators. Once the requests are approved, the deletion jobs will start to delete data. For additional details, see Data Management.

  > **Note:** Once the **Approval process for data deletion** is enabled, you must contact IBM Software Support if you want to disable the setting.

- To manage information about the storage location, click **Storage location**. For additional details, see "Configure Custom Storage Location for Your Backup Data" on page 23.
- To manage the retention period for the backup data on the storage location, click **Retention policy**. For additional details , see "Configure the Retention Policy Setting" on page 29.
- To generate and download the encryption keys which will be used to convert your exported backup data into readable content, click **Encryption keys**. For additional details, see Export Encryption Keys.

Configure Backup Settings

To improve performance, special labels/folders/files can be excluded from the protected scope. If you want to update the protected scope, navigate to **Settings** > **General**, and click **Backup settings**. The **Backups settings** pane appears, and you can configure the following:

> **Note:** The settings related to Google Workspace objects are available only when the Google Workspace module is included in your subscription. These backup settings do not take effect on the Vault protection.

- **Encryption profile** – View the encryption profile information. For more information, refer to the Manage Encryption Profiles section in the IBM® Storage Protect for Cloud user guide.
- **Gmail** – By default, the **Trash** and **Spam** special labels are not in the protected scope. If you want to add **Trash** or **Spam** to the protected scope, select the corresponding checkbox.
  If you want to exclude more from the protected scope, you can enter specific labels in the **Advanced labels exclusion** text box. When adding multiple items, press **Enter** on the keyboard to separate them. The maximum limit is 100 labels.
- **Drive** – By default, the **Shared with me** and **Trash** special folders are not in the protected scope. If you want to add **Shared with me** or **Trash** to the protected scope, select the corresponding checkbox.
  When the **Shared with me** folder is included in the backup scope, note the following:
  - The orphaned files, which are in shared folders but have lost their parent folders, can be backed up as shared objects.
  - The shared objects can be restored only when they have been backed up by the owner.

If you want to exclude more from the protected scope, you can enter specific folders in the **Advanced folders exclusion** text box. When adding multiple items, press **Enter** on the keyboard to separate them. The maximum limit is 100 folders.

- **Shared drives** – By default, the **Trash** special folder is not in the protected scope. If you want to add **Trash** to the protected scope, select the corresponding checkbox.
  If you want to exclude more from the protected scope, you can enter specific folders in the **Advanced folders exclusion** textbox. When adding multiple items, press **Enter** on the keyboard to separate them. The maximum limit is 100 folders.
- **Exclude special file types** (for drives and shared drives only) – By default, the following file types are in the protected scope: `avi`, `mov`, `mp4`, `m4v`, `wmv`, `flv`, `vmdk`, and `iso`. If you want to exclude specific file types from the protected scope, use the checkboxes to select file types.
- **Back up labels on files** (for drives and shared drives only) – To enable this setting, select the **Back up labels on files in drives and shared Drives** option.
  Note the following:
  - Labels will be included in both the initial backup and subsequent incremental backups. Note that enabling this setting will significantly impact performance.
  - If your organization installed the IBM® Storage Protect for Cloud app before January 8, 2023, to use the **Back up labels on files** feature, you must navigate to Google Admin console > **Apps** > **Google Workspace Marketplace apps** > **Apps list**, click the **IBM® Storage Protect for Cloud** app, and click **Grant access** to add the following permissions to the app: **drive.admin.labels** and **drive.labels**.

Click **Save** at the bottom of the pane to apply the backup settings. The updates will take effect from the next backup job.

Configure the Backup Schedule

By default, IBM® Storage Protect for Cloud will run one backup job per day. If you want to change the backup schedule, navigate to **Settings** > **General** and click **Backup schedule**. The **Backup schedule** pane appears and you can configure the following:

- **Number of backup jobs per day** – Select a number to define how many backup jobs you want to run per day.
- **Time of the first backup job** – The default value is the time when you start the initial backup job. You can change the time to define when the first backup job starts per day, and the time of the rest backup jobs will be automatically calculated and displayed.

Click **Save** at the bottom of the pane to apply the backup schedule to the next backup cycle.

> **Note:** For the Vault protection, the backup schedule is unsupported, and you can only click **Back up now** to trigger a backup job when you configure the protected scope.

Configure Custom Storage Location for Your Backup Data

To view the information about the storage location where your backup data resides, navigate to **Settings** > **General** > **Storage location**.

If you are currently using the **Default storage location** and you want to use your own storage afterward, you can contact IBM® Storage Protect for Cloud support to update your subscription, and then follow the steps below to change the storage location to your own storage.

> **Note:** The changes from the default storage to a custom storage cannot be reverted, and the custom storage cannot be changed to another custom storage once saved.

1. In your own storage location, for security concerns, the storage firewall may have been set up to only allow trusted clients. To ensure the IBM® Storage Protect for Cloud service can access your storage, you

must complete the corresponding settings in "Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account" on page 24.

2. Navigate to **Settings › General › Storage location** and click **Change to my own storage**.
3. In the **Change to my own** storage pop-up window, to decide how to handle the existing backup data on the default storage, choose an option from the following:
   - **Retain all backup data currently stored in IBM® Storage Protect for Cloud's storage until the retention time expires** – The backup data in the default storage location will be retained until the retention time expires. The next backup job for each of the services in the protected scope will store the backup data in the configured custom storage location.
   - **Remove all backup data from IBM® Storage Protect for Cloud's storage** – The backup data will be removed from the default storage location, and you cannot use the previous backup data for restore. After the storage location is changed, the backup jobs for services in the protected scope will start in a few seconds. The backup data will be stored in the configured custom storage location.

   > **Note:** After you have changed the storage location, the backup data on the previous storage location will follow the current **Retention policy**.

4. Click **OK** to save the settings.

Refer to the instructions in the following sections to configure the custom storage location.

> **Note:** For the best network performance, we strongly recommend you use the Azure storage that is in the same data center as one of your tenants in IBM® Storage Protect for Cloud. Using other storages may cause higher network costs for restore.

Allow IBM® Storage Protect for Cloud Agent Servers to Access Your Storage Account

Complete the following settings based on your scenario:

> **Note:** If you are using a trial subscription and the storage account you want to use in the trial has a firewall enabled, read the conditions below and contact IBM Software Support for the corresponding reserved IP addresses or ARM VNet IDs.

- For custom storage locations of the Microsoft™ Azure Blob Storage type, configure the settings required by the conditions below:
  - If your storage account is in the same data center as the one you use to sign up for IBM® Storage Protect for Cloud or your storage account is in its paired region, add the Azure Resource Manager (ARM) VNet subnets where the IBM® Storage Protect for Cloud agents are running on to your storage networking. You can find additional details in the Microsoft article Grant access from a virtual network. To get the ARM VNet subnet IDs for your data center, navigate to IBM® Storage Protect for Cloud > **Administration** > **Security**. For detailed instructions, refer to the following **Add ARM Virtual Networks** section.
  - For conditions other than the above, you need to add all the reserved IP addresses to the Azure storage firewall. For details, refer to the following **Add Reserved IP Addresses** section.
- For custom storage locations for other types, follow the steps in the following **Add Reserved IP Addresses** section to add the reserved IP addresses to your storage firewall.

Add Reserved IP Addresses

Follow the steps below:

1. Navigate to **IBM® Storage Protect for Cloud** interface > **Administration** > **Security** to download the list of reserved IP addresses of IBM® Storage Protect for Cloud. For details, refer to the Download a List of Reserved IP Addresses section in the IBM® Storage Protect for Cloud user guide.
2. Navigate to the storage account that you want to secure.
3. Select **Networking** on the menu.
4. Check that you've selected to allow access from **Selected networks**.
5. Enter the IP address or address range under **Firewall** > **Address Range**.
6. Select **Save** to apply your changes.

Add ARM Virtual Networks

You can refer to the Download ARM VNet IDs section in the IBM® Storage Protect for Cloud user guide to get the VNet IDs for your data center.

There are two ways to add ARM virtual networks:

- Use the Azure CLI tool (https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest)

```
## Use the Azure CLI tool

# Step 1 (Optional): If you have multiple Azure subscriptions, please switch to the
correct subscription
# This command sets the active subscription to the specified subscription ID.
az account set --subscription xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy

# Step 2 (Optional): Confirm whether the subscription switch is correct
# This command displays the current subscription information in a table format.
az account show --output table

# Step 3: Get the IBM® Storage Protect for Cloud network subnet resource ID
# This variable stores the resource ID of the subnet in the virtual network.
# Replace with the Azure Resource Manager (ARM) VNet ID downloaded from
your IBM® Storage Protect for Cloudtenant.
$SUBNETID="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy/resourceGroups/
ResourceGroupName/providers/Microsoft.Network/virtualNetworks/VirtualNetworkName/
subnets/SubnetName"

# Step 4: Set your resource group name
# This variable stores the name of the resource group where your storage account is
located.
$DESTRG="customer_resource_group_name"

# Step 5: Set your storage account name
# This variable stores the name of the storage account to which you want to add the
network rule.
$DESTSTA="customer_storage_account_name"

# Step 6: Add the firewall virtual network rule to grant access to IBM® Storage Protect
for Cloud
# This command adds a network rule to the specified storage account, allowing access
from the specified subnet.
az storage account network-rule add --resource-group $DESTRG --account-name $DESTSTA --
subnet $SUBNETID

# Step 7: List the current network rules for the storage account to verify the addition
# This command lists the virtual network rules for the specified storage account.
az storage account network-rule list --resource-group $DESTRG --account-name $DESTSTA
--query virtualNetworkRules

# Step 8 (Optional): Disable the public access to storage account
# This command updates the storage account to deny public network access.
az storage account update --resource-group $DESTRG --name $DESTSTA --default-action
Deny

# Step 9 (Optional): Verify that the default action for network rules is set to Deny
# This command shows the network rule set for the specified storage account, including
the default action.
az storage account show --resource-group $DESTRG --name $DESTSTA --query
networkRuleSet.defaultAction
```

- Use the Azure Az PowerShell (https://learn.microsoft.com/en-us/powershell/azure/install-azure-powershell?view=azps-14.2.0)

```
## Use Azure PowerShell (Az Module)

# Step 1: Sign in to Azure with your Azure Admin account

Connect-AzAccount

# Step 2 (Optional): If you have multiple Azure subscriptions, please switch to the
correct subscription
# This command sets the active subscription to the specified subscription ID.

Set-AzContext -SubscriptionId "xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy"


# Step 3: Get the IBM® Storage Protect for Cloud network subnet resource ID
# This variable stores the resource ID of the subnet in the virtual network.
# Replace with the Azure Resource Manager (ARM) VNet ID downloaded from
your IBM® Storage Protect for Cloud tenant.

$SUBNETID="/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-yyyyyyyyyyyy/resourceGroups/
ResourceGroupName/providers/Microsoft.Network/virtualNetworks/VirtualNetworkName/
subnets/SubnetName"

# Step 4: Set resource group name
# This variable stores the name of the resource group where your storage account is
located.

$DESTRG="customer_resource_group_name"

# Step 5: Set storage account name
# This variable stores the name of the storage account to which you want to add the
network rule.

$DESTSTA="customer_storage_account_name"

# Step 6: Add the firewall virtual network rule to grant access to IBM® Storage Protect
for Cloud
# This cmdlet adds a network rule to the specified storage account, allowing access
from the specified subnet.
Add-AzStorageAccountNetworkRule -ResourceGroupName $DESTRG -Name $DESTSTA
-VirtualNetworkResourceId $SUBNETID

# Step 7: Verify the newly added network rule

# This cmdlet retrieves the network rule set for the specified storage account.

Get-AzStorageAccountNetworkRuleSet -ResourceGroupName $DESTRG -AccountName
```

You will see the virtual network rules in Azure Portal, as the screenshot below shows. You may also notice that a warning message “Insufficient Permission...” is displayed. It is because the subnet is not in your subscription. You can ignore it.

Amazon S3

Note that IBM® Storage Protect for Cloud will store your backup data to the S3 Standard storage class automatically. You can move the backup data from S3 Standard to S3 Standard-IA, S3 One Zone-IA, or S3 Intelligent-Tiering, and IBM® Storage Protect for Cloud Google Workspace can restore the backup data of those storage classes. However, it is not recommended to activate the archive access tier if you are using S3 Intelligent-Tiering. Activating the archive access tier will cause data object files that have not yet been accessed for 90 days to be archived, and IBM® Storage Protect for Cloud Google Workspace cannot access the archived data in your Amazon S3 storage.

Procedure

Follow the instructions below:

1. **Storage type** – Select **Amazon S3** from the drop-down list.
2. **Bucket name** – Enter a name for the bucket you want to access or create.
3. **Access key ID** – Enter the corresponding access key ID to access the specified bucket. You can view the access key ID from your AWS account.
4. **Secret access key** – Enter the corresponding secret key ID to access the specified bucket. You can view the secret key ID from your AWS account.

5. **Storage region** – Select the storage region of this bucket from the drop-down list.
6. **Advanced** – If you want to configure extended parameters, select the **Advanced** option. Refer to the instructions below to configure **Extended parameters**, and note that if you have multiple parameters to enter, use the semicolon (;) to separate the parameters.
    - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer from 0 to 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, and it can reconnect at most 6 times.
      If you do not configure this parameter, the value is 6 by default.
    - **RetryMode** – Customize the retry mode for the requests not being completed successfully. If this parameter is not configured or configured incorrectly, the **Legacy** will be applied as the default value. You can also set the value to **Standard** or **Adaptive**. **Standard** represents the standardized request retry strategy which is consistent across all SDKs; **Adaptive** represents an experimental request retry strategy that builds on the Standard strategy and introduces congestion control through client-side rate limiting.
7. Click **Save** to save the custom storage location.

Amazon S3-Compatible Storage

Follow the instructions below:

Procedure

1. **Storage type** – Select **Amazon S3-Compatible Storage** from the drop-down list.
2. **Bucket name** – Enter a name for the bucket you want to access or create.
3. **Access key ID** – Enter the corresponding access key ID to access the specified bucket.
4. **Secret access key** – Enter the corresponding secret access key to access the specified bucket.
5. **Endpoint** – Enter the URL used to connect to the place where you want to store the data.
6. **Advanced** – If you want to configure extended parameters, select the **Advanced** option. Refer to the instructions below to configure **Extended parameters**, and note that if you have multiple parameters to enter, use the semicolon (;) to separate the parameters.
    - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer from 0 to 2147483646. For example, RetryCount=6 represents when the network connection is interrupted, it can reconnect at most 6 times.
      If you do not configure this parameter, the value is 6 by default.
    - **RetryMode** – Customize the retry mode for the requests not being completed successfully. If this parameter is not configured or configured incorrectly, the **Legacy** will be applied as the default value. You can also set the value to **Standard** or **Adaptive**. **Standard** represents the standardized request retry strategy which is consistent across all SDKs; **Adaptive** represents an experimental request retry strategy that builds on the Standard strategy and introduces congestion control through client-side rate limiting.
7. Click **Save** to save the custom storage location.

Microsoft Azure Blob Storage

Follow the instructions below:

About this task

> **Note:** Before adding the storage account to the IBM® Storage Protect for Cloud Google Workspace interface, ensure IBM® Storage Protect for Cloud Agents have access to your storage. For details, refer to "Allow IBM Storage Protect for Cloud Agent Servers to Access Your Storage Account" on page 24.

Procedure

1. **Storage type** – Select **Microsoft™ Azure Blob Storage** from the drop-down list.
2. **Access point** – Enter the URL for the Blob Storage Service. The default URL is *https://blob.core.windows.net*.
3. **Container name** – Enter the name for the container you wish to access.
4. **Account name** – Enter the corresponding account name to access the specified container.
5. **Account key** – Enter the corresponding account key to access the specified container.
6. **Advanced** – If you want to configure extended parameters, select the **Advanced** option. Refer to the instructions below to configure **Extended parameters**, and note that if you have multiple parameters to enter, use the semicolon (;) to separate the parameters.
   - **RetryInterval** – Customize the retry interval when the network connection is interrupted. You are allowed to enter any positive integer from 0 to 2147483646 (the unit is in milliseconds). For example, RetryInterval=30000 means that it will try to reconnect every 30000 milliseconds.
     If you do not configure this parameter, the value is 30000 milliseconds by default.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. You are allowed to enter any positive integer from 0 to 2147483646. For example, RetryCount=10 represents when the network connection is interrupted, it can reconnect at most 10 times.
     If you do not configure this parameter, the value is 6 by default.
7. Click **Save** to save the custom storage location.

IBM® Storage Protect - S3

Follow the instructions below:

Before you begin

The IBM Storage Protect Object client (S3) must be installed and configured before setting up IBM® Storage Protect for Cloud. Refer to, Sending data from other object clients to IBM Storage Protect.

Procedure

1. **Storage type** – Select IBM® Storage Protect - S3 from the drop-down list.
2. **Bucket name** – Enter the bucket name you wish to access.

   > **Note:** The entered name must match an existing bucket. For details on creating a bucket, see How to create an S3 bucket in IBM Storage Protect.

3. **Access key ID** – Enter the corresponding access key ID to access the specified bucket.
4. **Secret access key** – Enter the corresponding secret key ID to access the specified bucket.
5. **Endpoint** – Enter the URL used to connect to the place where you want to store the data.

   > **Note:** The URL must begin with `http://` or `https://`.

6. **Advanced** – If you want to configure extended parameters, select the **Advanced** option. Refer to the instructions below to configure **Extended parameters**, and note that if you have multiple parameters to enter, use the semicolon (;) to separate the parameters.
   - **Use_PathStyle=true** – This parameter is required to ensure the IBM® Storage Protect for Cloud Google Workspace can work with your storage properly.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer from 0 to 2147483646. For example, **RetryCount=6** represents when the network connection is interrupted, and it can reconnect at most 6 times.
     If you do not configure this parameter, the value is 6 by default.

- **RetryMode** – Customize the retry mode for the requests not being completed successfully. If this parameter is not configured or configured incorrectly, the **Legacy** will be applied as the default value. You can also set the value to **Standard** or **Adaptive**. **Standard** represents the standardized request retry strategy which is consistent across all SDKs; **Adaptive** represents an experimental request retry strategy that builds on the Standard strategy and introduces congestion control through client-side rate limiting.
- **Allow_Insecure_SSL** – By default, the storage client expects an SSL certificate issued by a public trusted certificate authority over HTTPS transport to ensure integrity. A self-signed certificate on the storage server side will fail the certificate validation. If you choose to use a self-signed certificate, you can set the **Allow_Insecure_SSL** to **true** in the Extended parameters to bypass the certificate validation.
- **Cert_thumbprint** – If you use a self-signed certificate on the storage server side and you want to pass the certificate validation with a specific thumbprint, set the value to the thumbprint string. By default, the **Cert_thumbprint** parameter is not configured.

7. Click **Save** to save the custom storage location.

IBM® Cloud Object Storage

Follow the instructions below:

Procedure

1. **Storage type** – Select **IBM® Cloud Object Storage** from the drop-down list.
2. **Bucket name** – Enter the bucket name you wish to access.
3. **Access key ID** – Enter the corresponding access key ID to access the specified bucket.
4. **Secret access key** – Enter the corresponding secret key ID to access the specified bucket.
5. **Endpoint** – Enter the URL used to connect to the place where you want to store the data.

   > **Note:** The URL must begin with `http://` or `https://`.

6. **Advanced** – If you want to configure extended parameters, select the **Advanced** option. Refer to the instructions below to configure **Extended parameters**, and note that if you have multiple parameters to enter, use the semicolon (;) to separate the parameters.
   - **RetryCount** – Customize the reconnection times after the network connection is interrupted. Enter any positive integer from 0 to 2147483646. For example, RetryCount=6 represents when the network connection is interrupted. It can reconnect at most 6 times.
     If you do not configure this parameter, the value is 6 by default.
   - **RetryMode** – Customize the retry mode for the requests not being completed successfully. If this parameter is not configured or configured incorrectly, the **Legacy** will be applied as the default value. You can also set the value to Standard or **Adaptive**. **Standard** represents the standardized request retry strategy which is consistent across all SDKs; **Adaptive** represents an experimental request retry strategy that builds on the Standard strategy and introduces congestion control through client-side rate limiting.
7. Click **Save** to save the custom storage location.

Configure the Retention Policy Setting

You can customize the retention period for backup data if your storage location meets one of the following scenarios:

- Use custom storage location to store backup data.
- Use the default IBM® Storage Protect for Cloud storage location and the retention policy configured in the subscription is **Unlimited retention**.

- Use the default IBM® Storage Protect for Cloud storage location and the retention policy configured in the subscription is a specific period longer than one year.

Refer to the following instructions to configure a retention policy:

1. Navigate to **Settings › General › Retention policy**.
2. Choose a policy from the following options:
   - **Set a default retention period for all services**
   - **Use a custom retention policy for each service**
   - **Use a custom retention policy for each container**
     Note the following:
     - Retention policy is currently unsupported for Vault service.
     - If you select the **Use a custom retention policy for each container** option, click the **Expand** ( ) button to expand the container list, and then set a retention policy for each container. If there are backup data of objects that are currently not in any containers, the configured **Retention policy for backup data not in a container** setting will be applied to these backup data.
3. Refer to the following information to configure the retention period (measured in years):
   - If your organization uses a custom storage location, you can enter an integer from 1 to 99 to set a retention period.
   - If your organization uses the default IBM storage location with the **Unlimited retention** subscription, the default retention period value is **Unlimited retention**, and you can also set an integer (from 1 to 99) as the retention period when necessary.
   - If you use the default IBM storage location with a specific retention period (longer than one year) in the subscription, you can enter an integer, which is not longer than the retention policy in the subscription, as the retention period.
4. Click **Save** to update the retention policy setting. You can monitor retention jobs in **Job monitor**. For details, see "Monitor Jobs and Download Job Reports" on page 91.

> **Note:** If your storage location for the backup data has been changed from a custom storage location to the IBM® Storage Protect for Cloud default storage location, only the backup data on the IBM® Storage Protect for Cloud default storage will be deleted according to the retention policy.

When I renew my IBM® Storage Protect for Cloud Google Workspace subscription, what will happen to my data retention settings?

Upon subscription renewal, your data retention settings will be adjusted based on a comparison between the new and previous retention period:

- **If the new subscription has a shorter retention period:** Your retention periods will be automatically adjusted to match the new subscription limits.
- **If the new subscription has the same or longer retention period:** No changes will be made to your existing retention settings.

To verify your configuration and ensure you are aware of any changes, refer to **Settings** > **General** > **Retention policy**. Additionally, you will receive notification emails 90 days, 60 days, and 30 days before any data deletion. Upon subscription renewal, a notification email will advise you to check and update your retention settings in IBM® Storage Protect for Cloud Google Workspace as needed.

Export Encryption Keys

The backup data generated by IBM® Storage Protect for Cloud Google Workspace is encrypted. If you have chosen our Data Export Service, the encryption keys are necessary when converting encrypted backup data into readable content. Note the following:

- By default, exporting encryption keys is not available to organizations using IBM-provided default storage. If your organization uses IBM default storage, you can contact IBM Software Support to enable this feature if needed.
- You must export encryption keys before leaving this product, as you will lose access to the product's interface once your subscription ends.

To export encryption keys, follow the steps below:

1. Navigate to **Settings** > **General** > **Encryption keys**.
2. Before generating encryption keys, you must first set a password for encryption keys and click **Apply** to apply the password. The password is used to access the encryption keys when restoring exported data via the standalone tool.
   If your subscription is the BYOS type, you can also configure whether to allow IBM® Storage Protect for Cloud Google Workspace to copy the encryption keys to your BYOS storage weekly.
3. To generate and download the encryption keys for the service types for which you have performed a backup, click **Generate** to generate the key, and then click **Download** to download the ZIP file and save it to your local computer.
   If you have performed backups or updated the password after the last time you generated the key, click **Regenerate** to regenerate the keys and download the file again.

Configure Protected Scope

To configure the protected scope, follow the steps below:

Procedure

1. Click the **Protection** () on the left navigation. The **Protection** page appears.
2. If your organization has multiple modules, select your desired module by clicking the **Google Workspace** , **Vault**, or **Google Classroom** tab.

   > **Note:** If your organization installed the IBM® Storage Protect for Cloud app before August 2023 release, to protect Google Classroom data, you must navigate to the Google Admin console > **Apps** > **Google Workspace Marketplace apps** > **Apps list**, click the **IBM® Storage Protect for Cloud** app, and click **Grant access** to add the required permissions to the app. For details on the required permissions, refer to the IBM Storage Protect for Cloud Google Workspace section in the IBM® Storage Protect for Cloud user guide.

3. In the Google Workspace module, based on the container type where you want to configure the protected scope, click the **User Services** or **Shared Drives** tab at the top of the page.
4. On the **Protection** page, the table under each tab will list all containers. The icon of a protected service will be colorful, and the icon of an unprotected service will be grey. If you want to search for desired containers, you can click **Filters** or use the search box.

   > **Note:** With a trial subscription, you can protect up to 5 items across the following container types: user, group, shared drive, and classroom.

5. If you want to view items in a container, click the expand () button next to the container.
6. To configure the protected scope for one or multiple containers, select the containers. If you want to select all containers at a time, click **Select all**.
7. Click **Configure protected scope**. The **Configure protected scope** pane appears on the right of the page.
8. Select the services that you want to protect. Note the following:
   - For each scanned shared drive to be backed up, ensure there is at least one member with the **Manager** permission. Otherwise, the shared drive cannot be successfully backed up.
   - If your organization has enabled the Multi-Geo function, you can configure the **Data region** setting for user containers and shared drive containers.
   - If your organization wants to enable protection for the Chat/Vault service, it is necessary to configure a custom Google app. For details, see Custom Google App.
   - Vault protection does not back up the drafts in Gmail (Vault), to avoid duplicate drafts generated by the Google Vault.
9. Click **Save**. The new protected scope will take effect in the next backup job.

   > **Note:** For the Vault protection, you can select services and click **Back up now** to start a backup job. For additional details, see Vault Data Protection.

User Management

User management provides centralized management of security groups, which controls what standard users can restore/export in IBM® Storage Protect for Cloud Google Workspace. You can configure security groups with different permission scopes assigned, and then add standard users to security groups. Standard users added to a security group will be granted permissions of the security group, and they can restore/export objects contained in the security group.

To manage security groups, navigate to **Settings** > **User management**. All configured security groups are listed on the **User management** page. The Administrators group is the built-in group and cannot be deleted. The Administrators group has all permissions and containers, and you can only manage users/groups in this group.

> **Note:** The users who have been designated as application administrators of IBM® Storage Protect for Cloud Google Workspace will be automatically synchronized to the Administrators group. If a user is demoted from an application administrator to a standard user, it is recommended to remove this user from the **Administrators** group. If service administrators contain groups, you must manually add the groups into the Administrators group when needed.

On the **User management** page, you can take the following actions to manage security groups:

- To create a security group, click **Create security group**. In the **Create security group** pane, you can refer to the following **Create a Security Group** section to configure settings.
- To view details of a security group, click group name.
- To edit details of a security group, click the more actions (•••) button and click **Edit** from the drop-down menu, or select the group and click the **Edit** ( ) button.
- To delete a security group, click the more actions (•••) button and click **Delete** from the drop-down menu. You can also select one or multiple groups and click the **Delete** ( ) button.

Create a Security Group

Follow the instructions below to create a security group:

1. Navigate to **Settings** > **User management**.
2. Click **Create security group**. The **Create security group** pane appears on the right of the page.
3. **Security group name** – Enter a name for the group.
4. **Description** – Enter an optional description.
5. **Invite users/groups** – Enter users or groups that you want to add to this group. Note that the entered users and groups must exist in your tenant and they must have access to IBM® Storage Protect for Cloud Google Workspace.
6. **Grant permissions** – Grant permissions to this security group by selecting desired options from the following:
   - Restore the data to its original location
   - Restore the data to another location
   - Export

   You can refer to the information in the table below when you grant permissions to a security group.

Object types			Restore options		
			Restore the data to its original location	**Restore the data to another location**	**Export**
User Services	Selected items	Gmail Calendar Contacts Drive > My Drive	Supported	Supported	Supported
		Drive > Shared with me	Unsupported	Supported	Supported
	Full account		Supported	Supported	Supported
Shared drive			Supported	Supported	Supported
Classroom	Selected items	Announcement Classwork People	Supported	Unsupported	Supported
		Grades	Unsupported	Unsupported	Supported
		Drive	Unsupported	Supported	Supported
	Whole class		Supported	Unsupported	Supported

Note: The protection for Vault service is only available to users in the **Administrators** group.

7. **Select permission scope** – To select permission scope for a service type, turn on the toggle in the **Type** column, and then click the **Select container** ( ) button in the **Action** column. In the pane, select desired containers and click **Save**. If you want to go back to the last step without saving changes, click **Cancel**. In each security group, you can configure permission scope for more than one object type.
8. Click **Save**.

Recover Google Workspace Data

IBM® Storage Protect for Cloud Google Workspace provides the following ways to recover your lost Google Workspace data:

- Restore backup data to its original location or another location.
  For more information on the supported and unsupported data types of Google Workspace, refer to:
  - “Gmail Data Types” on page 105
  - “Drive Data Types” on page 106
  - “Calendar Data Types” on page 108
  - “Contacts Data Types” on page 111
  - “Shared Drive Data Types” on page 111
  - Chat Data Types (for **Export** only)
- Export and download specific backup data.

To select the backup data that you want to recover, you can choose **Search mode** or **Calendar mode**:

- **Search mode** – In this mode, you can choose the **Selected items** method, configure search conditions based on the properties of the objects that you want to recover, and then select your desired backup data from the search results to perform a data recovery.
  In the **Search mode**, you can also choose the **Full account** method to restore Gmail, Drive, Calendar, or Contacts backup data at the service-level for a specific Google user. For details, refer to Restore Gmail, Drive, Calendar, or Contacts Data for a User.
- **Calendar mode** – In this mode, you can browse backup jobs via a calendar view, and then select your desired recovery points to drill down to the specific objects that you want to recover.
  In the **Calendar mode**, Administrators can add multiple top-level objects in to a restore queue to perform a bulk restore. For details, refer to Bulk Restore for Gmail, Drive, Calendar, or Contacts and Bulk Restore for Shared Drives.

Restore Gmail, Drive, Calendar, or Contacts Data for a User

If you want to restore Gmail, Drive, Calendar, or Contacts data for a Google user, follow the steps below:

Procedure

1. Click the **Restore** () tab on the left pane.
2. > **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has the Google Classroom module.

   On the **Restore** page, select the **Search mode** tab and select the **User services** option.
3. To search for a Google user, enter keywords of the username in the **Search by email address** field and select the desired user’s email address from the drop-down list.
4. Click **Search**. The **Select and restore the user data** page will appear. The **Email address** field displays the email address of the selected user.
5. On the right of the **Email address** field, choose the **Full account** option.
6. Click the **Backup time range** field and set a time range to search for the backup data you want to recover.
7. Click **Search**. The search results table list services that have been backed up in the selected backup time range.
8. In the drop-down list under the **Recovery point** column, select a time when the data you want to recover has been backed up.

9. To restore data for one or multiple services, select the checkboxes next to the services, and click **Restore** above the table.
10. After you click **Restore**, the **Restore** pane appears on the right. Refer to the instructions below to configure settings:
    - If you select multiple services to restore, refer to Configure Settings.
    - If you select only one service to restore, refer to Restore Gmail, Restore Drive, Restore Calendar, or Restore Contacts.

Configure Settings

If you want to restore multiple services in batch, configure the following settings:

Procedure

1. Choose where you would like to restore the selected backup data.
    - **Restore the data to its original location** – Restore the data to where it was backed up.
    - **Restore the data to another location** – Restore the data to another destination.
2. Configure the following settings based on your scenario:
    - If you choose **Restore the data to its original location**, configure the following settings:
        a. Select a container level conflict resolution from the following:
            - **Skip** – The destination container settings will remain unchanged.
            - **Merge** – The backup container settings and the content will be merged with the destination container.

        b. The resolution of the content-level conflict will be the following:
            - **Skip** (for Gmail, Drive, and Calendar) – Existing data in the destination will remain unchanged. For emails, the associated labels will be restored.
            - **Append** (for Contacts only) – All contacts included will be recovered as new contacts.

        c. If **Drive** is included in the restore scope, the job will restore all content and security.
    - If you choose **Restore the data to another location**, configure the following settings:
        a. Enter keywords of the destination account's email address, and then select the destination account from the drop-down list.

        > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

        b. The data of the selected services will be restored as follows in the destination:
            - Restore Gmail data to a new label.
            - Restore Drive data to a new folder.
            - Restore Calendar data and add a suffix to its name.
            - Restore Contacts data and add a suffix to its name.

        The default value of the new label/folder/suffix is displayed in the textbox, and you can customize the value. If the name of the restored item conflicts with the name of another item in the destination, the restored item's name will be appended with "**_1**".
3. If necessary, you can enter your comments in the **Description** field for this restore job.
4. Click **Next** to have an overview of the restore settings.
5. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

What to do next

If you want to restore a specific service, you can refer to the following sections to configure restore settings.

- "Restore Gmail" on page 37
- "Restore Drive" on page 37
- "Restore Calendar" on page 39
- "Restore Contacts" on page 40

Restore Gmail

To restore Gmail data for a user, configure the following settings:

Procedure

1. Choose where you would like to restore the selected backup data.
   - **Restore the data to its original location** – Restore the data to where it was backed up.
   - **Restore the data to another location** – Restore the data to another destination.
2. Configure the following settings based on your scenario:
   - If you choose **Restore the data to its original location**, configure the following settings:
     a. Select a container level conflict resolution from the following:
        - **Skip** – The destination container settings will remain unchanged.
        - **Merge** – The backup container settings and the content will be merged with the destination container.

     b. Select a content-level conflict resolution from the following:
        - **Skip** – Existing data in the destination will remain unchanged, and the associated labels will be restored.
        - **Overwrite** – Existing data will be replaced by the backup data.
   - If you choose **Restore the data to another location**, configure the following settings:
     a. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

     > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

     b. View the default name of the new label where the selected data will be restored to the destination. You can customize the name of the new label. If this label name conflicts with another label name in the destination, this label name will be appended with "**_1**".
3. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.
4. If necessary, you can enter your comments in the **Description** field for this restore job.
5. Click **Next** to have an overview of the restore settings.
6. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Restore Drive

Choose where you would like to restore the selected backup data:

- **Restore the data to its original location** – Restore the data to where it was backed up.
- **Restore the data to another location** – Restore the data to another destination.

Based on your scenario, refer to the sections below to continue.

I Want to Restore the Data to Its Original Location

After you choose **Restore the data to its original location**, configure the following settings:

1. Choose to **Restore all content and security** or **Restore content only**.

   > **Note:** The default option is **Restore content only**, which will not restore file labels and the locked status.

2. Choose how to handle container-level conflict for the restore.
   - **Skip** – The destination container settings will remain unchanged.
   - **Merge** – The backup container settings and the content will be merged with the destination container.
3. Choose how to handle content-level conflict for the restore.
   - **Skip** – Existing data in the destination will remain unchanged.
   - **Overwrite** – Existing data will be replaced by the backup data.
   - **Append a number prefix to the file name** – All data will remain untouched, and backup data will be restored with a sequential number prefix.
4. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

5. If necessary, you can enter your comments in the **Description** field for this restore job.
6. Click **Next** to have an overview of the restore settings.
7. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

I Want to Restore the Data to Another Location

After you choose **Restore the data to another location**, configure the following settings:

1. Choose to **Restore all content and security** or **Restore content only**.

   > **Note:** The default option is **Restore content only**, which will not restore file labels and the locked status.

2. Enter the keywords of the destination account's address, and then select the destination account from the drop-down list.

   > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

3. View the default name of the new folder where the selected data will be restored to the destination. You can customize the name of the new folder. If this folder name conflicts with another folder name in the destination, this folder name will be appended with "**_1**".

4. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

5. If necessary, you can enter your comments in the **Description** field for this restore job.
6. Click **Next** to have an overview of the restore settings.
7. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Restore Calendar

To restore Calendar data for a user, configure the following settings:

Procedure

1. Choose where you would like to restore the selected backup data.
   - **Restore the data to its original location** – Restore the data to where it was backed up.
   - **Restore the data to another location** – Restore the data to another destination.

     > **Note:** If you performed a job to restore a user's primary calendar to another destination, after the restore, the primary calendar would be restored as a custom calendar in the destination, and guest users cannot update their replies to events on the restored calendar.

2. Configure the following settings based on your scenario:
   - If you choose **Restore the data to its original location**, configure the following settings:
     a. Select a container level conflict resolution from the following:
        - **Skip** – The destination container settings will remain unchanged.
        - **Merge** – The backup container settings and the content will be merged with the destination container.

     b. Select a content-level conflict resolution from the following:
        - **Skip** – Existing data in the destination will remain unchanged.
        - **Merge** – The backup data will be merged with the destination data.
   - If you choose **Restore the data to another location**, configure the following settings:
     a. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

        > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

     b. View the default suffix, which will be added to the name of the data after the restore in the destination. You can customize this suffix. If the name of the restored item conflicts with the name of another item in the destination, this restored item's name will be appended with "**_1**".
3. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

> **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

4. If necessary, you can enter your comments in the **Description** field for this restore job.
5. Click **Next** to have an overview of the restore settings.
6. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Restore Contacts

To restore Contacts data for a user, configure the following settings:

Procedure

1. Choose where you would like to restore the selected backup data.
   - **Restore the data to its original location** – Restore the data to where it was backed up.
   - **Restore the data to another location** – Restore the data to another destination.
2. Configure the following settings based on your scenario:
   - If you choose **Restore the data to its original location**, configure the following settings:
     a. The resolution for container-level conflict is **Skip**. After the restore, the destination container settings will remain unchanged.
     b. The resolution for content-level conflict is **Append**. After the restore, all contacts included will be recovered as new contacts.

     > **Note:** With the **Append** content-level conflict resolution, there may be duplicate contacts after the restore, and you can use the **Merge duplicates** method in Google Contacts to deal with the duplicates.

   - If you choose **Restore the data to another location**, configure the following settings:
     a. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

     > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

     b. View the default suffix, which will be added to the name of the data after the restore in the destination. You can customize this suffix. If the name of the restored item conflicts with the name of another item in the destination, this restored item's name will be appended with "**_1**".
3. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

> **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

4. If necessary, you can enter your comments in the **Description** field for this restore job.
5. Click **Next** to have an overview of the restore settings.
6. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Bulk Restore for Gmail, Drive, Calendar, or Contacts

About this task

As a user in the **Administrators** group, if you want to add multiple users in a restore queue to perform a bulk restore, refer to the steps below:

Procedure

1. Click **Restore** () on the left navigation.
2. On the **Restore** page, select the **Calendar mode** tab.

   > **Note:** On the **Restore** page, select the **Google Workspace** tab if your organization also has other modules.

3. Select the **Gmail**, **Drive**, **Calendar**, or **Contacts** option from the drop-down list at the top of the calendar.
4. By default, only the successful backup jobs are displayed on the calendar. If you also want to check backup jobs with exceptions, select the **Include jobs with partial backup data** option.
5. Each recovery point on the calendar represents the start time of a backup job. By default, the calendar displays the current month's page. You can click components on the calendar to find the month page which lists your desired recovery points.
6. Click a recovery point, and you are directed to the table listing users who are in the backup scope.

   > **Note:** By default, the scope contains historical backup data. If you want to recover contents that were just backed up by the selected backup job, select the **Include data from this backup only** option.

7. Select the users that you want to add to a restore queue, and then click **Add to restore queue**. You can use the search box on the upper-right corner to search for users. If you want to import users via uploading a CSV file, click the **Restore queue** () icon and see Bulk Import for more details.
   The users in the restore queue will be labeled as **Added to queue**, and the number shown on the **Restore queue** icon indicates the total users in the queue.

   Note the following:

   - The restore queue has a maximum limit of 100 users.
   - If you want to upload a CSV file to bulk import users, the file size cannot exceed 10 MB.

8. Click the **Restore queue** () icon. The **Restore queue** panel appears.
9. In the **Restore queue** panel, manage users in the queue.

   - **Remove** – If you want to remove users from the restore queue, you can click the **Remove** () button to remove a single user, or you can select multiple users and click **Remove** at the top of the panel.
   - **Bulk import** – You can also use the Bulk Import function to add multiple users by uploading a CSV file.

10. In the **Restore queue** panel, select users and click **Restore**. The **Restore** panel appears. Refer to the Configure Settings for Bulk Restore section to configure restore settings.

Bulk Import

About this task

The **Bulk import** function is only available to users in the **Administrators** group. After clicking **Bulk import** in the **Restore queue** panel, the **Bulk import** panel appears. In the **Bulk import** panel, you can do the following:

Procedure

1. Click **Download CSV template**.
2. Configure the downloaded CSV template to add the users whom you want to add to the restore queue. Note the following:
   - The restore queue has a maximum limit of 100 users.
   - The CSV file size cannot exceed 10 MB.
   - Ensure the added users' backup data are covered by the selected recovery point.
3. Click **Upload** and select the configured CSV file.
4. Click **Import**.
5. The system will check objects imported via uploading a CSV file. In the **Restore queue** panel, an error message will be displayed under each invalid object. You can click **Remove all invalid objects** to clear them.
6. In the **Restore queue** panel, select users and click **Restore**. The **Restore** panel appears. Refer to the Configure Settings for Bulk Restore section to configure restore settings.

Configure Settings for Bulk Restore

After you select users and click **Restore** in the **Restore queue** panel, the **Restore** panel appears. Refer to the following sections to configure restore settings.

Gmail

Refer to the following instructions to configure restore settings for Gmail.

1. Choose where you would like to restore the selected backup data. Then, complete the following steps based on your choice.
   - **Restore the data to its original location** – Restore the data to where it was backed up. Follow the steps below to continue with this choice:
     a. Choose how to handle container level conflict for the restore.
        - **Skip** – The destination container settings will remain unchanged.
        - **Merge** – The backup container settings and the content will be merged with the destination container.

     b. Choose how to handle content level conflict for the restore.
        - **Skip** – Existing data in the destination will remain unchanged, and the associated labels will be restored.
        - **Overwrite** – Existing data will be replaced by the backup data.
   - **Restore the data to another location** – Restore the data to another destination. Follow the steps below to continue with this choice:
     a. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

     > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

     b. View the default name of the new label where the selected data will be restored to the destination. You can customize the name of the new label. If this label name conflicts with another label name in the destination, this label name will be appended with "**_1**".
2. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

3. If necessary, you can enter your comments in the **Description** field for this restore job.
4. Click **Next** to have an overview of the restore settings.
5. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Drive

Refer to the following instructions to configure restore settings for Drive.

1. Choose where you would like to restore the selected backup data. Then, complete the following steps based on your choice.
   - **Restore the data to its original location** – Restore the data to where it was backed up. Follow the steps below to continue with this choice:
     a. Choose to **Restore content only** or **Restore all content and security**.

     > **Note:** The default option is **Restore content only**, which will not restore file labels and the locked status.

     b. Choose how to handle container level conflict for the restore.
        - **Skip** – The destination container settings will remain unchanged.
        - **Merge** – The backup container settings and the content will be merged with the destination container.

     c. Choose how to handle content level conflict for the restore.
        - **Skip** – Existing data in the destination will remain unchanged.
        - **Overwrite** – Existing data will be replaced by the backup data.
        - **Append a number prefix to the file name** – All data will remain untouched, and backup data will be restored with a sequential number prefix.
   - **Restore the data to another location** – Restore the data to another destination. Follow the steps below to continue with this choice:
     a. Choose to **Restore content only** or **Restore all content and security**.

     > **Note:** The default option is **Restore content only**, which will not restore file labels and the locked status.

     b. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

     c. View the default name of the new folder where the selected data will be restored to the destination. You can customize the name of the new folder. If this folder name conflicts with another folder name in the destination, this folder name will be appended with "**_1**".
2. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

3. If necessary, you can enter your comments in the **Description** field for this restore job.
4. Click **Next** to have an overview of the restore settings.

5. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Calendar

Refer to the following instructions to configure restore settings for Calendar.

1. Choose where you would like to restore the selected backup data. Then, complete the following steps based on your choice.
   - **Restore the data to its original location** – Restore the data to where it was backed up. Follow the steps below to continue with this choice:
     a. Choose how to handle container level conflict for the restore.
        - **Skip** – The destination container settings will remain unchanged.
        - **Merge** – The backup container settings and the content will be merged with the destination container.

     b. Choose how to handle content level conflict for the restore.
        - **Skip** – Existing data in the destination will remain unchanged.
        - **Merge** – The backup data will be merged with the destination data.
   - **Restore the data to another location** – Restore the data to another destination. Follow the steps below to continue with this choice:

     > **Note:** If you performed a job to restore a user's primary calendar to another destination, after the restore, the primary calendar would be restored as a custom calendar in the destination, and guest users cannot update their replies to events on the restored calendar.

     a. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

        > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

     b. View the default suffix, which will be added to the name of the data after the restore in the destination. You can customize this suffix. If the name of the restored item conflicts with the name of another item in the destination, this restored item's name will be appended with "**_1**".
2. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.
3. If necessary, you can enter your comments in the **Description** field for this restore job.
4. Click **Next** to have an overview of the restore settings.
5. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Contacts

Refer to the following instructions to configure restore settings for Contacts.

1. Choose where you would like to restore the selected backup data. Then, complete the following steps based on your choice.
   - **Restore the data to its original location** – Restore the data to where it was backed up. Follow the steps below to continue with this choice:

a. The resolution for container level conflict is **Skip**. After the restore, the destination container settings will remain unchanged.

b. The resolution for content level conflict is **Append**. After the restore, all contacts included will be recovered as new contacts.

> **Note:** With the **Append** content level conflict resolution, there may be duplicate contacts after the restore, and you can use the **Merge duplicates** method in Google Contacts to deal with the duplicates.

- **Restore the data to another location** – Restore the data to another destination. Follow the steps below to continue with this choice:

  a. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

  > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

  b. View the default suffix, which will be added to the name of the data after the restore in the destination. You can customize this suffix. If the name of the restored item conflicts with the name of another item in the destination, this restored item's name will be appended with "**_1**".

2. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

3. If necessary, you can enter your comments in the **Description** field for this restore job.
4. Click **Next** to have an overview of the restore settings.
5. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**

Bulk Restore for Shared Drives

About this task

As a user in the **Administrators** group, if you want to add multiple shared drives into a restore queue to perform a bulk restore, refer to the steps below:

Procedure

1. Click **Restore** () on the left navigation.
2. On the **Restore** page, select the **Calendar mode** tab.

   > **Note:** On the **Restore** page, select the **Google Workspace** tab if your organization also has other modules.

3. Select the **Shared drives** option from the drop-down list at the top of the calendar.
4. By default, only the successful backup jobs are displayed on the calendar. If you also want to check backup jobs with exceptions, select the **Include jobs with partial backup data** option.

5. Each recovery point on the calendar represents the start time of a backup job. By default, the calendar displays the current month's page. You can click components on the calendar to find the month page which lists your desired recovery points.
6. Click a recovery point, and you are directed to the table listing shared drives in the backup scope.

   > **Note:** By default, the scope contains historical backup data. If you want to recover contents that were just backed up by the selected backup job, select the **Include data from this backup only** option.

7. Select the shared drives that you want to add to a restore queue, and then click **Add to restore queue**. You can use the search box on the upper-right corner to search for shared drives. If you you want to import shared drives via uploading a CSV file, click the **Restore Queue** () icon and see Bulk Import Shared Drives for more details.
   The shared drives in the restore queue will be labeled as **Added to queue**, and the number shown on the **Restore queue** icon indicates the total shared drives in the queue.

   Note the following:

   - The restore queue has a maximum limit of 100 objects.
   - If you want to upload a CSV file to bulk import shared drives, the file size cannot exceed 10 MB.

8. Click the **Restore queue** () icon. The **Restore queue** panel appears.
9. In the **Restore queue** panel, manage shared drives in the queue.
   - **Remove** – If you want to remove shared drives from the restore queue, you can click the **Remove** () button to remove a single item, or you can select multiple shared drives and click **Remove** at top of the panel.
   - **Bulk import** – You can also use this function to add multiple shared drives by uploading a CSV file. For details, refer to Bulk Import Shared Drives.
10. In the **Restore queue** panel, select shared drives and click **Restore**. The **Restore** panel appears. Refer to the Configure Settings to Bulk Restore Shared Drives section to configure restore settings.

Bulk Import Shared Drives

About this task

The **Bulk import** function is only available to users in the **Administrators** group. After clicking **Bulk import** in the **Restore queue** panel, the **Bulk import** panel appears. In the **Bulk import** panel, you can do the following:

Procedure

1. Click **Download CSV template**.
2. Configure the downloaded CSV template to add the shared drives to be included in the restore queue. Note the following:
   - The restore queue has a maximum limit of 100 objects.
   - The CSV file size cannot exceed 10 MB.
   - Ensure the added objects' backup data are covered by the selected recovery point.
3. Click **Upload** and select the configured CSV file.
4. Click **Import**.
5. The system will check objects imported via uploading a CSV file. In the **Restore queue** panel, an error message will be displayed under each invalid object. You can click **Remove all invalid objects** to clear them.

6. In the **Restore queue** panel, select shared drives and click **Restore**. The **Restore** panel appears. Refer to the Configure Settings to Bulk Restore Shared Drives section to configure restore settings.

Configure Settings to Bulk Restore Shared Drives

About this task

Refer to the following instructions to configure restore settings.

Procedure

1. Choose where you would like to restore the selected backup data. Then, complete the following steps based on your choice.
    - **Restore the data to its original location** – Restore the data to where it was backed up. Follow the steps below to continue with this choice:
        a. Choose to **Restore content only** or **Restore all content and security**.

        > **Note:** The default option is **Restore content only**, which will not restore file labels and the locked status.

        b. Choose how to handle container level conflict for the restore.
            - **Skip** – The destination container settings will remain unchanged.
            - **Merge** – The backup container settings and the content will be merged with the destination container.

        c. Choose how to handle content level conflict for the restore.
            - **Skip** – Existing data in the destination will remain unchanged.
            - **Overwrite** – Existing data will be replaced by the backup data.
            - **Append a number prefix to the file name** – All data will remain untouched, and backup data will be restored with a sequential number prefix.
    - **Restore the data to another location** – Restore the data to another destination. Follow the steps below to continue with this choice:
        a. Choose to **Restore content only** or **Restore all content and security**.

        > **Note:** The default option is **Restore content only**, which will not restore file labels and the locked status.

        b. Enter keywords of the destination shared drive's name, and then select the destination shared drive from the drop-down list.

        > **Note:** The drop-down list only displays shared drives scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

        c. View the default name of the new folder where the selected data will be restored to the destination. You can customize the name of the new folder. If this folder name conflicts with another folder name in the destination, this folder name will be appended with "**_1**".
2. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

> **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

3. If necessary, you can enter your comments in the **Description** field for this restore job.
4. Click **Next** to have an overview of the restore settings.
5. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Restore or Export Gmail Data

To restore or export Gmail data, refer to the instructions below:

1. First you Select Gmail Data via Search Mode or Select Gmail Data via Calendar Mode
2. Configure the related settings to proceed with the data recovery:
   - **Restore** – Configure Settings to Restore Gmail Data
   - **Export** – Export Gmail Data

> **Note:** To improve performance, special labels/folders/files can be excluded from the protected scope. If you want to update the protected scope, refer to Configure Backup Settings.

Select Gmail Data via Search Mode

Procedure

To search specific items in a user's Gmail to restore or export, follow the steps below:

1. Click **Restore** ( ) on the left navigation.
2. On the **Restore** page, select the **Search mode** tab and select the **User services** option.

> **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. To search for a Google user, enter keywords of the username in the **Search by email address** field and select the desired user's email address from the drop-down list.
4. Click **Search**. The **Select and restore the user data** page appears. The **Email address** field displays the email address of the selected user.
5. Keep the **Selected items** option selected on the right of the **Email address** field, and then click the **Gmail** tab.
6. In the **Level** drop-down list, select one of the following options based on the object type you want to recover:
   - If you want to restore or export Gmail data for the user, select **User**.
   - If you want to search for specific labels to restore or export, select **Label**.
   - If you want to search for specific emails to restore or export, select **Mail**.
7. Based on the level you select, configure the search conditions to search for the specific data you want to recover:
   - If you select **User**, click the **Backup time range** field and set a time range to search for the backup data you want to recover.
   - If you select **Label**, configure the following conditions to search for backup labels:

- **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.
- **Label name** – In this field, you can enter keywords of label names to search for labels.

- If you select **Mail**, configure the following conditions to search for backup emails:
  - **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.
  - **Label name** – In this field, you can enter keywords of label names to search for emails.
  - **Subject** – In this field, you can enter keywords of subjects to search for emails.
  - **Date sent** – You can click this field and set a time range to search for emails.
  - **Sent from**, **Sent to**, or **Sent cc** – You can also enter information in these fields to search for emails.

8. Click **Search** to search for the backup data you want to recover.
9. In the search results table, find the item you want to recover. To select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery point** column.
   Note the following:
   - The **Hierarchy** column shows the information on the latest time in **Recovery point**.
10. You can take the following actions to recover data:
    - To restore items, select the checkboxes next to the items, and click **Restore** above the table. For additional details, see Configure Settings to Restore Gmail Data.
    - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table. For additional details, see Export Gmail Data.

Select Gmail Data via Calendar Mode

Procedure

To restore/export backup Gmail data from a specific recovery point, follow the steps below:

1. Click **Restore** () on the left navigation.
2. On the **Restore** page, select the **Calendar mode** tab.

   > **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. Select the **Gmail** option from the drop-down list at the top of the calendar.
4. By default, only the successful backup jobs are displayed on the calendar. If you also want to check backup jobs with exceptions, select the **Include jobs with partial backup data** option.
5. Each recovery point on the calendar represents the start time of a backup job. By default, the calendar displays the current month's page. You can click components on the calendar to find the month page which lists your desired recovery points.
6. Click a recovery point, and you are directed to the table listing users who are in the backup scope of the Gmail service.

   > **Note:** By default, the scope contains historical backup data. If you want to recover contents that were just backed up by the selected backup job, select the **Include data from this backup only** option.

7. Backup objects can be listed into the following levels: **User** (), **Label** (), and **Mail** (). Note the following:
    - When you hover the mouse over an item with sub-level items, you can click that item and continue to select sub-level items as needed.
    - When you select a parent-level item, all sub-level items will also be selected. If you only want to recover some of the sub-level items, you can return to the parent-level item and deselect it.
8. You can take the following actions to recover data:
    - To restore items, select the checkboxes next to the items, and click **Restore** above the table. For additional details, see Configure Settings to Restore Gmail Data.
    - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table. For additional details, see Export Gmail Data.

> **Note:** If you select items of different levels to restore/export, the restore/export settings will follow the selected parent-level items.

Configure Settings to Restore Gmail Data

To restore data in a user's Gmail, configure the following settings:

Procedure

1. Choose where you would like to restore the selected backup data.
    - **Restore the data to its original location** – Restore the data to where it was backed up.
    - **Restore the data to another location** – Restore the data to another destination.
2. Configure the following settings based on your scenario:
    - If you choose **Restore the data to its original location**, configure the following settings:
        a. If you select **User** or **Label** level to restore data, select a container level conflict resolution from the following:
            - **Skip** – The destination container settings will remain unchanged.
            - **Merge** – The backup container settings and the content will be merged with the destination container.

        b. Select a content-level conflict resolution from the following:
            - **Skip** – Existing data in the destination will remain unchanged, and the associated labels will be restored.
            - **Overwrite** – Existing data will be replaced by the backup data.

        c. If you select the **Label** level to restore data, choose whether to restore additional labels that are applied to items under the labels you want to restore.
    - If you choose **Restore the data to another location**, configure the following settings:
        a. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

        > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

        b. View the default name of the new label where the selected data will be restored to the destination. You can customize the name of the new label. If this label name conflicts with another label name in the destination, this label name will be appended with "**_1**".

3. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

> **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

4. If necessary, you can enter your comments in the **Description** field for this restore job.
5. Click **Next** to have an overview of the restore settings.
6. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Export Gmail Data

Procedure

After you click **Export**, the **Export** pop-up window appears. Refer to the instructions below:

1. Choose a format for the data you want to export:
   - **EML** – This file format represents email messages saved using Outlook and other relevant applications.
   - **MBOX** – The most common format for storing email messages.
   - **PST** – Files with .PST extension represent Outlook Personal Storage Files (also called Personal Storage Table) that store a variety of user information.
2. Click **Export** to start the export job.
3. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

Restore or Export Drive Data

Procedure

To restore or export Drive data, refer to the instructions below:

1. First you Select Drive Data via Search Mode or Select Drive Data via Calendar Mode.
2. Configure the related settings to proceed with the data recovery:
   - **Restore data in My Drive** – Configure Settings to Restore Data in My Drive
   - **Restore data shared with me** – Configure Settings to Restore Shared Data
   - **Export** – Export Drive Data

> **Note:** To improve performance, special labels/folders/files can be excluded from the protected scope. If you want to update the protected scope, refer to Configure Backup Settings

Select Drive Data via Search Mode

Procedure

To search specific items in a user's Drive (including items in My Drive and Shared with me) to restore or export, follow the steps below:

1. Click **Restore** () tab on the left navigation.

2. On the **Restore** page, select the **Search mode** tab and select the **User services** option.

> **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. To search for a Google user, enter keywords of the username in the **Search by email address** field and select the desired user's email address from the drop-down list.
4. Click **Search**. The **Select and restore the user data** page appears. The **Email address** field displays the email address of the selected user.
5. Keep the **Selected items** option selected on the right of the **Email address** field, and then click the **Drive** tab.
6. Choose a source where the data you want to recover resides:
   - If you want to recover the data in the user's Drive, click **My Drive**.
   - If you want to recover the data shared with this user, click **Shared with me**.
     Note the following:
     - The **Shared with me** tab only shows backup data when this folder is in the protected scope and has been backed up. For details about adding this folder to the protected scope, see "Configure Backup Settings" on page 22. If you select **Shared with Me**, you can restore backup data to a new folder in the user's My Drive.
     - Under the **Shared with me** tab, the shared objects can be restored only when they have been backed up by the owner, and restoring multiple objects in batch is only supported when they belong to the same owner. You can contact the owner before the restore.
7. In the **Level** drop-down list, select one of the following options based on the object type you want to recover:
   - Under the **My Drive** tab, if you want to recover Drive data for the user, select **User**.
   - Under the **My Drive** or **Shared with me** tab, if you want to search for specific folders to restore or export, select **Folder**.
   - Under the **My Drive** or **Shared with me** tab, if you want to search for specific files to restore or export, select **File**.
8. Based on the level you select, configure the search conditions to search for the specific data you want to recover:
   - If you select **User**, click the **Backup time range** field and set a time range to search for the backup data you want to recover.
   - If you select **Folder**, configure the following conditions to search for backup folders:
     - **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.
     - **Owner** – If you want to recover folders under the **Shared with me** tab, you must enter keywords of the username in this field and select the owner from the drop-down list.
     - **Folder name** – In this field, you can enter keywords of folder names to search for backup folders.
     - **ID** – In this field, you can enter keywords to search for backup folders using their unique IDs.

> **Note:** When there are folders with the same name in the backup data, you can configure the **ID** condition to locate the folder that you want to recover. The unique ID of a folder is a part of the folder's URL.

   - If you select **File**, configure the following conditions to search for backup files:
     - **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.

- **Owner** – If you want to search and recover files under the **Shared with me** tab, you must enter keywords of the username in this field and select the owner from the drop-down list.
- **Folder name** – In this field, you can enter keywords of folder names to search for files.
- **File name** – In this field, you can enter keywords of file names to search for files.
- **Label name** – In this field, you can enter keywords of labels on files to search for files.

  > **Note:** Labels can only be backed up when the **Back up labels on files** setting has been enabled, but enabling this setting will significantly impact performance. For additional details, see Configure Backup Settings.

- **ID** – In this field, you can enter keywords to search for backup files using their unique IDs.

  > **Note:** When there are files with the same name in the backup data, you can configure the **ID** condition to locate the file that you want to recover. The unique ID of a file is a part of the file's URL.

- **Created date** – You can click this field and set a time range to search for files.
- **Modified by** – In this field, you can enter keywords of usernames to search for files.
- **File size** – Under the **My Drive** tab, you can set a range of file sizes to search for files.

9. Click **Search** to search for the backup data you want to recover.
10. In the search results table, find the item you want to recover. To select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery point** column.
11. You can take the following actions to recover data:
    - To restore items, select the checkboxes next to the items, and click **Restore** above the table.
      - If you restore data in **My Drive**, see Configure Settings to Restore Data in My Drive.
      - If you restore data in **Shared with me**, see Configure Settings to Restore Shared Data.
    - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table. For more details, see Export Drive Data.

Select Drive Data via Calendar Mode

Procedure

To restore/export backup Drive data from a specific recovery point, follow the steps below:

1. Click **Restore** () on the left navigation.
2. On the **Restore** page, select the **Calendar mode** tab.

   > **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. Select the **Drive** option from the drop-down list at the top of the calendar.
4. By default, only the successful backup jobs are displayed on the calendar. If you also want to check backup jobs with exceptions, select the **Include jobs with partial backup data** option.
5. Each recovery point on the calendar represents the start time of a backup job. By default, the calendar displays the current month's page. You can click components on the calendar to find the month page which lists your desired recovery points.

6. Click a recovery point, and you are directed to the table listing users who are in the backup scope of the Drive service.

> **Note:** By default, the scope contains historical backup data. If you want to recover contents that were just backed up by the selected backup job, select the **Include data from this backup only** option.

7. Backup objects can be listed into the following levels: **User** (), **Folder** (), and **File** (). The table below shows the relationship between different levels.

<table>
<tr><th colspan="5">Level</th><th>Note</th></tr>
<tr><td colspan="5">User</td><td>When you select users at this level to recover backup data, the data in Shared with me will not be included in the recovery scope.</td></tr>
<tr><td rowspan="3">Type</td><td>My Drive</td><td>Folder</td><td colspan="2">File</td><td></td></tr>
<tr><td>Trash</td><td colspan="3">Folder/File</td><td></td></tr>
<tr><td>Folder/File</td><td>Owner</td><td>Folder</td><td>File</td><td>If you want to recover shared data, click Shared with me to drill down and specify an owner to define the recovery scope.</td></tr>
</table>

Note the following:

- When you hover the mouse over an item with sub-level items, you can click that item and continue to select sub-level items as you needed.
- When you select a parent-level item, all sub-level items will also be selected. If you only want to recover some of the sub-level items, you can return to the parent-level item and deselect it.

8. You can take the following actions to recover data:
   - To restore items, select the checkboxes next to the items, and click **Restore** above the table.
     - If you restore data in **My Drive** or **Trash**, see Configure Settings to Restore Data in My Drive.
     - If you restore data in **Shared with me**, see Configure Settings to Restore Shared Data.
   - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table. For more details, see Export Drive Data.

> **Note:** If you select items of different levels to restore/export, the restore/export settings will follow the selected parent-level items.

Configure Settings to Restore Data in My Drive

Choose where you would like to restore the selected backup data.

- **Restore the data to its original location** – Restore the data to where it was backed up.
- **Restore the data to another location** – Restore the data to another destination.

Based on your scenario, refer to the sections below to continue.

I Want to Restore the Data to Its Original Location

After you choose **Restore the data to its original location**, configure the following settings:

1. Choose to **Restore all content and security** or **Restore content only**.

   > **Note:** The default option is **Restore content only**, which will not restore file labels and the locked status.

2. If you restore data at **User** or **Folder** level, choose how to handle container level conflict for the restore.
   - **Skip** – The destination container settings will remain unchanged.
   - **Merge** – The backup container settings and the content will be merged with the destination container.
3. Choose how to handle content-level conflict for the restore.
   - **Skip** – Existing data in the destination will remain unchanged.
   - **Overwrite** – Existing data will be replaced by the backup data.
   - **Append a number prefix to the file name** – All data will remain untouched, and backup data will be restored with a sequential number prefix.
4. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

5. If necessary, you can enter your comments in the **Description** field for this restore job.
6. Click **Next** to have an overview of the restore settings.
7. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

I Want to Restore the Data to Another Location

After you choose **Restore the data to another location**, configure the following settings:

1. Choose to **Restore all content and security** or **Restore content only**.

   > **Note:** The default option is **Restore content only**, which will not restore file labels and the locked status.

2. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

   > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

3. View the default name of the new folder where the selected data will be restored to the destination. You can customize the name of the new folder. If this folder name conflicts with another folder name in the destination, this folder name will be appended with "**_1**".
4. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

5. If necessary, you can enter your comments in the **Description** field for this restore job.
6. Click **Next** to have an overview of the restore settings.
7. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Configure Settings to Restore Shared Data

To restore the data shared with a user, configure the following settings:

Procedure

1. The selected items will be restored to a new folder in the user's My Drive, and the **Restore to a new folder in My Drive** field will show the default folder name. You can change the folder name.
2. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

3. If necessary, you can enter your comments in the **Description** field for this restore job.
4. Click **Next** to have an overview of the restore settings.
5. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Export Drive Data

After you click **Export**, the **Export** pop-up window appears. The selected backup data will be exported as a **ZIP** file. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

Restore or Export Calendar Data

Procedure

To restore or export Calendar data, refer to the instructions below:

1. First you Select Calendar Data via Search Mode or Select Calendar Data via Calendar Mode.
2. Configure the related settings to proceed with the data recovery:
   - **Restore** – Configure Settings to Restore Calendar Data
   - **Export** – Export Calendar Data

> **Note:** To improve performance, special labels/folders/files can be excluded from the protected scope. If you want to update the protected scope, refer to Configure Backup Settings.

Select Calendar Data via Search Mode

Procedure

To search for specific items in a user's Calendar to restore or export, follow the steps below:

1. Click **Restore** () tab on the left navigation.
2. On the **Restore** page, select the **Search mode** tab and select the **User services** option.

   > **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. To search for a Google user, enter keywords of the username in the **Search by email address** field and select the desired user's email address from the drop-down list.
4. Click **Search**. The **Select and restore the user data** page appears. The **Email address** field displays the email address of the selected user.
5. Keep the **Selected items** option selected on the right of the **Email address** field, and then click the **Calendar** tab.
6. In the **Level** drop-down list, select one of the following options based on the object type you want to recover:
   - If you want to restore or export Calendar data for the user, select **User**.
   - If you want to search for specific calendars to restore or export, select **Calendar**.
7. Based on the level you select, configure the search conditions to search for the specific data you want to recover:
   - If you select **User**, click the **Backup time range** field and set a time range to search for the backup data you want to recover.
   - If you select **Calendar**, configure the following conditions to search for backup calendars:
     - **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.
     - **Calendar name** – In this field, you can enter keywords of calendar names to search for calendars.
8. Click **Search** to search for the backup data you want to recover.
9. In the search results table, find the item you want to recover. To select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery point** column.
10. You can take the following actions to recover data:
    - To restore items, select the checkboxes next to the items, and click **Restore** above the table. For additional details, see "Configure Settings to Restore Calendar Data" on page 58.
    - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table . For additional details, see Export Calendar Data.

Select Calendar Data via Calendar Mode

Procedure

To restore/export backup Calendar data from a specific recovery point, follow the steps below:

1. Click **Restore** ( ) on the left navigation.
2. On the **Restore** page, select the **Calendar mode** tab.

> **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. Select the **Calendar** option from the drop-down list at top of the calendar.
4. By default, only the successful backup jobs are displayed on the calendar. If you also want to check backup jobs with exceptions, select the **Include jobs with partial backup data** option.
5. Each recovery point on the calendar represents the start time of a backup job. By default, the calendar displays the current month's page. You can click components on the calendar to find the month page which lists your desired recovery points.
6. Click a recovery point, and you are directed to the table listing users who are in the backup scope of the Calendar service.

> **Note:** By default, the scope contains historical backup data. If you want to recover contents that were just backed up by the selected backup job, select the **Include data from this backup only** option.

7. Backup objects can be listed into the following levels: **User** ( ) and **Calendar** ( ). Note the following:
   - When you hover the mouse over an item with sub-level items, you can click that item and continue to select sub-level items as needed.
   - When you select a parent-level item, all sub-level items will also be selected. If you only want to recover some of the sub-level items, you can return to the parent-level item and deselect it.
8. You can take the following actions to recover data:
   - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table. For additional details, see Export Calendar Data.

> **Note:** If you select items of different levels to restore/export, the restore/export settings will follow the selected parent-level items.

Configure Settings to Restore Calendar Data

To restore data in a user's Calendar, configure the following settings:

Procedure

1. Choose where you would like to restore the selected backup data.
   - **Restore the data to its original location** – Restore the data to where it was backed up.
   - **Restore the data to another location** – Restore the data to another destination.

> **Note:** If you performed a job to restore a user's primary calendar to another destination, after the restore, the primary calendar would be restored as a custom calendar in the destination, and guest users cannot update their replies to events on the restored calendar.

2. Configure the following settings based on your scenario:

- If you choose **Restore the data to its original location**, configure the following settings:
  a. Select a container level conflict resolution from the following:
     - **Skip** – The destination container settings will remain unchanged.
     - **Merge** – The backup container settings and the content will be merged with the destination container.
  b. Select a content-level conflict resolution from the following:
     - **Skip** – Existing data in the destination will remain unchanged.
     - **Merge** – The backup data will be merged with the destination data.
- If you choose **Restore the data to another location**, configure the following settings:
  a. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

     > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

  b. View the default suffix, which will be added to the name of the data after the restore in the destination. You can customize this suffix. If the name of the restored item conflicts with the name of another item in the destination, this restored item's name will be appended with "**_1**".

3. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

4. If necessary, you can enter your comments in the **Description** field for this restore job.
5. Click **Next** to have an overview of the restore settings.
6. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Export Calendar Data

After you click **Export**, the **Export** pop-up window appears. The selected backup data will be exported as **iCalendar (.ics)** file. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

> **Note:** The following data of events are unsupported due to Google API limitations:
> - Does not support exporting events' Join with Google Meet, Join by phone, Time zone, Guest, Guest permissions, and attachments properties.
> - In the exported data, the format of events' Location and Room information cannot be kept.

Restore or Export Contacts Data

Procedure

To restore or export Contacts data, refer to the instructions below:

1. First you Select Contacts Data via Search Mode or Select Contacts Data via Calendar Mode.
2. Configure the related settings to proceed with the data recovery:

- **Restore** – Configure Settings to Restore Contacts Data
- **Export** – Export Contacts Data

> **Note:** To improve performance, special labels/folders/files can be excluded from the protected scope. If you want to update the protected scope, refer to Configure Backup Settings.

Select Contacts Data via Search Mode

Procedure

To search specific items in a user's Contacts to restore or export, follow the steps below:

1. Click **Restore** () on the left navigation.
2. On the **Restore** page, select the **Search mode** tab and select the **User services** option.

   > **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. To search for a Google user, enter keywords of the username in the **Search by email address** field and select the desired user's email address from the drop-down list.
4. Click **Search**. The **Select and restore the user data** page appears. The **Email address** field displays the email address of the selected user.
5. Keep the **Selected items** option selected on the right of the **Email address** field, and then click the **Contacts** tab.
6. In the **Level** drop-down list, select one of the following options based on the object type you want to recover:
   - If you want to restore or export Contacts data for the user, select **User**.
   - If you want to search for specific labels to restore or export, select **Label**.
   - If you want to search for specific contacts to restore or export, select **Contact**.
7. Based on the level you select, configure the search conditions to search for the specific data you want to recover:
   - If you select **User**, click the **Backup time range** field and set a time range to search for the backup data you want to recover.
   - If you select **Label**, configure the following conditions to search for backup labels:
     - **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.
     - **Label name** – In this field, you can enter keywords of label names to search for labels.
     - If you select **Contact**, configure the following conditions to search for backup contacts:
     - **Label name** – In this field, you can enter keywords of label names to search for contacts.
     - **Contact name** – In this field, you can enter keywords of users' names to search for contacts.
     - **Email** – In this field, you can enter keywords of email addresses to search for contacts.
8. Click **Search** to search for the backup data you want to recover.
9. In the search results table, find the item you want to recover. To select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery point** column.
   Note the following:
   - The **Hierarchy** column shows information of the latest time in **Recovery point**.

- For the external users in **Other contacts**, their display names cannot be retrieved due to the Google API limitation, and their addresses will be displayed in the **Name** column of the search results table.

10. You can take the following actions to recover data:
    - To restore items, select the checkboxes next to the items, and click **Restore** above the table.
    - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table. For additional details, see Export Contacts Data.

Select Contacts Data via Calendar Mode

Procedure

To restore/export backup Contacts data from a specific recovery point, follow the steps below:

1. Click **Restore** () on the left navigation.
2. On the **Restore** page, select the **Calendar mode** tab.

> **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. Select the **Contacts** option from the drop-down list at the top of the calendar.
4. By default, only the successful backup jobs are displayed on the calendar. If you also want to check backup jobs with exceptions, select the **Include jobs with partial backup data** option.
5. Each recovery point on the calendar represents the start time of a backup job. By default, the calendar displays the current month's page. You can click components on the calendar to find the month page which lists your desired recovery points.
6. Click a recovery point, and you are directed to the table listing users who are in the backup scope of the Contacts service.

> **Note:** By default, the scope contains historical backup data. If you want to recover contents which were just backed up by the selected backup job, select the **Include data from this backup only** option.

7. Backup objects can be listed into the following levels: **User** (), **Label** (), and **Contacts** (). Note the following:
    - When you hover the mouse over an item with sub-level items, you can click that item and continue to select sub-level items as you needed.
    - When you select a parent-level item, all sub-level items will also be selected. If you only want to recover some of the sub-level items, you can return to the parent-level item and deselect it.
8. You can take the following actions to recover data:
    - To restore items, select the checkboxes next to the items, and click **Restore** above the table. For additional details, see Configure Settings to Restore Contacts Data.
    - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table. For additional details, see Export Contacts Data.

> **Note:** If you select items of different levels to restore/export, the restore/export settings will follow the selected parent-level items.

Configure Settings to Restore Contacts Data

To restore data in a user's Contacts, configure the following settings:

Procedure

1. Choose where you would like to restore the selected backup data.
   - **Restore the data to its original location** – Restore the data to where it was backed up.
   - **Restore the data to another location** – Restore the data to another destination.
2. Configure the following settings based on your scenario:
   - If you choose **Restore the data to its original location**, configure the following settings:
     a. If you select **User** or **Label** level to restore data, the resolution for container level conflict is **Skip**. After the restore, the destination container settings will remain unchanged.
     b. The resolution for content-level conflict is **Append**. After the restore, all contacts included will be recovered as new contacts.

     > **Note:** With the **Append** content-level conflict resolution, there may be duplicate contacts after the restore, and you can use the **Merge duplicates** method in Google Contacts to deal with the duplicates.

     c. If you select the **Label** level to restore data, choose whether to restore additional labels that are applied to items under the labels you want to restore.
   - If you choose **Restore the data to another location**, configure the following settings:
     a. Enter keywords of the destination account's address, and then select the destination account from the drop-down list.

     > **Note:** The drop-down list only displays Google users scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

     b. View the default suffix, which will be added to the name of the data after the restore in the destination. You can customize this suffix. If the name of the restored item conflicts with the name of another item in the destination, this restored item's name will be appended with "**_1**".
3. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

4. If necessary, you can enter your comments in the **Description** field for this restore job.
5. Click **Next** to have an overview of the restore settings.
6. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Export Contacts Data

Procedure

After you click **Export**, the **Export** pop-up window appears. Refer to the instructions below:

1. Choose a format for the data you want to export:

- **Outlook CSV** – If you select this format, the job will export all data and convert names to the default character encoding.
- **Google CSV** – If you select this format, the job will export all data and use Unicode to preserve international characters. Note that some email programs such as Outlook do not support Unicode.
- **vCard (.vcf file)** – This is an internet standard that is supported by many email programs and contact managers such as OS X Mail and Contacts.

2. Click **Export** to start the export job.
3. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

> **Note:** Due to Google API limitations, the following contact properties are unsupported for export: photo, File as, Internet call, and Custom field.

Restore or Export Shared Drives Data

Procedure

To restore or export shared drives data, refer to the instructions below:

1. First you Select Shared Drives Data via Search Mode or Select Shared Drives Data via Calendar Mode.
2. Configure the related settings to proceed with the data recovery:
   - **Restore** – Configure Settings to Restore Data in Shared Drives
   - **Export** – Export Shared Drives Data

> **Note:** To improve performance, special labels/folders/files can be excluded from the protected scope. If you want to update the protected scope, refer to Configure Backup Settings.

Select Shared Drives Data via Search Mode

Procedure

To search for shared drives data to restore or export, follow the steps below:

1. Click **Restore** () on the left navigation.
2. On the **Restore** page, select the **Search mode** tab and select the **Shared drive** option.

> **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. To search for a shared drive, enter keywords of the shared drive name in the **Search by shared drive name** field and select the shared drive from the drop-down list.
4. Click **Search**. The **Select and restore the shared drive data** page appears. The **Shared drive** field displays the name of the shared drive.
5. In the **Level** drop-down list, select one of the following options based on the object type you want to recover:
   - If you want to restore or export data in the Shared Drive, select **shared drive**.
   - If you want to search for specific folders to restore or export, select **Folder**.
   - If you want to search for specific files to restore or export, select **File**.

6. Based on the level you select, configure the search conditions to search for the specific data you want to recover:
    - If you select **Shared drive**, click the **Backup time range** field and set a time range to search for the backup data you want to recover.
    - If you select **Folder**, configure the following conditions to search for backup folders:
        - **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.
        - **Folder name** – In this field, you can enter keywords of folder names to search for backup folders.
        - **ID** – In this field, you can enter keywords to search for backup folders using their unique IDs.

          > **Note:** When there are folders with the same name in the backup data, you can configure the **ID** condition to locate the folder that you want to recover. The unique ID of a folder is a part of the folder's URL.
    - If you select **File**, configure the following conditions to search for backup files:
        - **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.
        - **Folder name** – In this field, you can enter keywords of folder names to search for files.
        - **File name** – In this field, you can enter keywords of file names to search for files.
        - **Label name** – In this field, you can enter keywords of labels on files to search for files.

          > **Note:** Labels can only be backed up when the **Back up labels on files** setting has been enabled, but enabling this setting will significantly impact performance. For additional details, see Configure Backup Settings.
        - **ID** – In this field, you can enter keywords to search for backup files using their unique IDs.

          > **Note:** When there are files with the same name in the backup data, you can configure the **ID** condition to locate the file that you want to recover. The unique ID of a file is a part of the file's URL.
        - **Created date** – You can click this field and set a time range to search for files.
        - **Modified by** – In this field, you can enter keywords of usernames to search for files.
        - **File size** – In this field, you can set a range of file sizes to search for files.
7. Click **Search** to search for the backup data you want to recover.
8. In the search results table, find the item you want to recover. To select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery point** column.
9. You can take the following actions to recover data:
    - To restore items, select the checkboxes next to the items, and click **Restore** above the table. For additional details, see Configure Settings to Restore Data in Shared Drives.
    - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table. For additional details, see Export Shared Drives Data.

Select Shared Drives Data via Calendar Mode

Procedure

To restore/export backup shared drives data from a specific recovery point, follow the steps below:

1. Click **Restore** ( ) on the left navigation.
2. On the **Restore** page, select the **Calendar mode** tab.

> **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. Select the **Shared drives** option from the drop-down list at the top of the calendar.
4. By default, only the successful backup jobs are displayed on the calendar. If you also want to check backup jobs with exceptions, select the **Include jobs with partial backup data** option.
5. Each recovery point on the calendar represents the start time of a backup job. By default, the calendar displays the current month's page. You can click components on the calendar to find the month page which lists your desired recovery points.
6. Click a recovery point, and you are directed to the table listing shared drives that are in the backup scope.

> **Note:** By default, the scope contains historical backup data. If you want to recover contents that were just backed up by the selected backup job, select the **Include data from this backup only** option.

Backup objects can be listed into the following levels: **Shared drive** ( ), **Folder** ( ), and **File** ( ). The table below shows the relationship between different levels.

Summary for complex table

Level			
Shared drive			
Type	Shared drive	Folder	File
	Trash	Folder/File	

Note the following:

- When you hover the mouse over an item with sub-level items, you can click that item and continue to select sub-level items as needed.
- When you select a parent-level item, all sub-level items will also be selected. If you only want to recover some of the sub-level items, you can return to the parent-level item and deselect it.

7. You can take the following actions to recover data:
   - To restore items, select the checkboxes next to the items, and click **Restore** above the table. For additional details, see Configure Settings to Restore Data in Shared Drives.
   - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table. For additional details, see Export Shared Drives Data.

> **Note:** If you select items of different levels to restore/export, the restore/export settings will follow the selected parent-level items.

Configure Settings to Restore Data in Shared Drives

Choose where you would like to restore the selected backup data.

- **Restore the data to its original location** – Restore the data to where it was backed up.

- **Restore the data to another location** – Restore the data to another destination.

Based on your scenario, refer to the sections below to continue.

I Want to Restore the Data to Its Original Location

After you choose **Restore the data to its original location**, configure the following settings:

1. Choose to **Restore all content and security** or **Restore content only**.

   > **Note:** The default option is **Restore content only**, which will not restore file labels and the locked status.

2. If you restore data at **Shared drive** or **Folder** level, choose how to handle container level conflict for the restore:
   - **Skip** – The destination container settings will remain unchanged.
   - **Merge** – The backup container settings and the content will be merged with the destination container.
3. Choose how to handle content-level conflict for the restore:
   - **Skip** – Existing data in the destination will remain unchanged.
   - **Overwrite** – Existing data will be replaced by the backup data.
   - **Append a number prefix to the file name** – All data will remain untouched, and backup data will be restored with a sequential number prefix.
4. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

5. If necessary, you can enter your comments in the **Description** field for this restore job.
6. Click **Next** to have an overview of the restore settings.
7. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

I Want to Restore the Data to Another Location

After you choose **Restore the data to another location**, configure the following settings:

1. Choose to **Restore all content and security** or **Restore content only**.

   > **Note:** The default option is **Restore content only**, which will not restore file labels and the locked status.

2. Enter keywords of the destination shared drive's name, and then select the destination shared drive from the drop-down list.

   > **Note:** The drop-down list only displays shared drives scanned via **Auto discovery** in IBM® Storage Protect for Cloud.

3. View the default name of the new folder where the selected data will be restored in the destination. You can customize the name of the new folder. If this folder name conflicts with another folder name in the destination, this folder name will be appended with "**_1**".

4. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

5. If necessary, you can enter your comments in the **Description** field for this restore job.
6. Click **Next** to have an overview of the restore settings.
7. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Export Shared Drives Data

After you click **Export**, the **Export** pop-up window appears. The selected backup data will be exported as a **ZIP** file. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

Export Chat Data

Refer to the following sections to export Chat backup data via the **Search mode** or **Calendar mode**.

- **Search mode** – In this mode, you can configure search conditions based on the properties of Chat data, and then select your desired backup data from the search results to export.
- **Calendar mode**– In this mode, you can browse backup jobs via a calendar view, and then select your desired recovery points to drill down to the specific objects that you want to export.

Export Chat Data via Search Mode

To search specific items in a user's Chat to export, follow the steps below:

1. Click **Restore** ( ) on the left navigation.
2. On the **Restore** page, select the **Search mode** tab and select the **User** option.

   > **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules

3. To search for a Google user, enter keywords of the username in the **Search by email address** field and select the desired user's email address from the drop-down list.
4. Click **Search**. The **Select and restore the user data** page appears. The **Email address** field displays the email address of the selected user.
5. Keep the **Selected items** option selected on the right of the **Email address** field, and then click the **Chat** tab.
6. In the **Level** drop-down list, select one of the following options based on the object type you want to recover.
   - If you want to export Chat data for the user, select **User**.
   - If you want to search for specific spaces and direct messages to export, select **Space and direct message**.
   - If you want to search for specific chats to export, select **Chat**
7. Based on the level you select, configure the search conditions to search for the specific data you want to recover:

- If you select **User**, click the **Backup time range** field and set a time range to search for the backup data you want to recover.
- If you select **Space and direct message**, configure the following conditions to search for backup spaces and direct messages:
  - **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.
  - **Space name** (for space chats only) – In this field, you can enter keywords of space names to search for space chats.
  - **Member** – In this field, you can enter keywords of a username to search for spaces / direct messages which this member has participated. This field does not support searching for external users.
- If you select **Chat**, configure the following conditions to search for backup chats:
  - **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.
  - **Space name** (for space chats only) – In this field, you can enter keywords of space names to search for space chats.
  - **Sender** – In this field, you can enter keywords of a username to search for chats sent by this user. This field does not support searching for external users.
  - **Keywords** – In this field, you can enter keywords to search for chat messages. Note that the search is limited to the 500 characters of a message.
  - **Date sent** – You can click this field and set a time range to search for chats.

8. Click **Search** to search for the backup data you want to recover.
9. In the search results table, find the item you want to recover. To select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery point** column.
10. To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
11. The **Export** pop-up window appears. The selected backup data will be exported as an **HTML** file. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

Export Chat Data via Calendar Mode

To export backup Chat data from a specific recovery point, follow the steps below:

1. Click **Restore** () on the left navigation.
2. On the **Restore** page, select the **Calendar mode** tab.

> **Note:** On the **Restore** page, click the **Google Workspace** tab if your organization also has other modules.

3. Select the **Chat** option from the drop-down list at the top of the calendar.
4. By default, only the successful backup jobs are displayed on the calendar. If you also want to check backup jobs with exceptions, select the **Include jobs with partial backup data** option.
5. Each recovery point on the calendar represents the start time of a backup job. By default, the calendar displays the current month's page. You can click components on the calendar to find the month page which lists your desired recovery points.
6. Click a recovery point, and you are directed to the table listing users who are in the backup scope of the Chat service.

> **Note:** By default, the scope contains historical backup data. If you want to recover contents which were just backed up by the selected backup job, select the **Include data from this backup only** option

7. Backup objects can be listed into the following levels: **User**, **Direct messages** / **Spaces**, and **Chat**. Note the following:
   - When you hover the mouse over an item with sub-level items, you can click that item and continue to select sub-level items as needed.
   - When you select a parent-level item, all sub-level items will also be selected. If you only want to recover some of the sub-level items, you can return to the parent-level item and deselect it.
8. To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
9. The **Export** pop-up window appears. The selected backup data will be exported as an **HTML** file. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

Export Google Vault Data

Follow the instructions below to export your desired Vault backup data:

1. Click **Restore** () on the left navigation.
2. On the **Restore** page, select the **Vault** tab.
3. Select the **User services** or **Shared drive** option according to the content that you want to export:
   - To export the backup data of Gmail/Drive in Vault, select the **User services** option.
   - To export the backup data of shared drives in Vault, select the **Shared drive** option.
4. To search for a Google user or a shared drive, enter keywords of the object name in the **Search by email address** / **Search by shared drive name** field, and then select the desired object from the drop-down list.

   > **Note:** To search for a shared drive deleted from Google Workspace, you could only enter the shared drive ID to search it.

5. Click **Search**. The configuration page appears, and you can refer to the following sections to select the backup Vault data to be exported.

Gmail (Vault)

Select the **Gmail (Vault)** tab, and refer to the steps below to select and export backup data:

1. In the **Level** drop-down list, select one of the following options based on the object type you want to export:
   - If you want to export Gmail data for the user, select **User**.
   - If you want to search for specific emails to export, select **Mail**.
2. Based on the level you select, configure the search conditions to search for the specific data you want to export:
   - If you select **User**, click the **Backup time range** field and set a time range to search for the backup data you want to export.
   - If you select **Mail**, configure the following conditions to search for backup emails:
     - **Backup time range** – Click this field and set a time range to search for the backup data you want to export.
     - **Subject** – In this field, you can enter keywords of subjects to search for emails.
     - **Date sent** – You can click this field and set a time range to search for emails.
     - **Sent from**, **Sent to**, and **Sent cc** – You can also enter information in these fields to search for emails.
3. Click **Search** to search for the backup data you want to export.
4. In the search results table, find the item you want to export. To select the status you want to export for this item, select a backup job time in the drop-down list under the **Recovery point** column.
5. To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
6. The **Export** pop-up window appears. Choose a format for the data you want to export:
   - **EML** – This file format represents email messages saved using Outlook and other relevant applications.
   - **MBOX** – The most common format for storing email messages.
   - **PST** – Files with .PST extension represent Outlook Personal Storage Files (also called Personal Storage Table) that store a variety of user information.

7. Click **Export** to start the export job
8. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

Drive (Vault)

Select the **Drive (Vault)** tab, and refer to the steps below to select and export backup data:

1. Choose a source where the data you want to export resides:
   - If you want to export the data in the user's Drive, click **My Drive**.
   - If you want to export the data shared with this user, click **Shared with me**.

     > **Note:** Under the **Shared with me** tab, the shared objects can be restored only when they have been backed up by the owner, and restoring multiple objects in batch is only supported when they belong to the same owner. You can contact the owner before the restore.

2. In the **Level** drop-down list, select one of the following options based on the object type you want to export:
   - Under the **My Drive** tab, select **User** if you want to export Drive data for the user, or select **File** if you want to search for specific files to export.
   - Under the **Shared with me** tab, select **File**.
3. Based on the level you select, configure the search conditions to search for the specific data you want to export:
   - If you select **User**, click the **Backup time range** field and set a time range to search for the backup data you want to export.
   - If you select **File**, configure the following conditions to search for backup files:
     - **Backup time range** – Click this field and set a time range to search for the backup data you want to export.
     - **Owner** – If you want to search and export files under the **Shared with me** tab, you must enter keywords of the username in this field and select the owner from the drop-down list.
     - **File name** – In this field, you can enter keywords of file names to search for files.
     - **ID** – In this field, you can enter keywords to search for backup files using their unique IDs.

       > **Note:** When there are files with the same name in the backup data, you can configure the **ID** condition to locate the file that you want to export. The unique ID of a file is a part of the file's URL.

     - **Created date** – You can click this field and set a time range to search for files.
     - **File size** – Under the **My Drive** tab, you can set a range of file sizes to search for files.
4. Click **Search** to search for the backup data you want to export.
5. In the search results table, find the item you want to export. To select the status you want to export for this item, select a backup job time in the drop-down list under the **Recovery point** column.
6. To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
7. The **Export** pop-up window appears. The selected backup data will be exported as a **ZIP** file. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

Shared drives (Vault)

Refer to the steps below to select and export backup data of shared drives in Vault:

1. In the **Level** drop-down list, select one of the following options based on the object type you want to export:
    - If you want to export the shared drive backup data, select **Shared drive**.
    - If you want to search for specific files to export, select **File**.
2. Based on the level you select, configure the search conditions to search for the specific data you want to export:
    - If you select **Shared drive**, click the **Backup time range** field and set a time range to search for the backup data you want to export.
    - If you select **File**, configure the following conditions to search for backup files:
        - **Backup time range** – Click this field and set a time range to search for the backup data you want to recover.
        - **File name** – In this field, you can enter keywords of file names to search for files.
        - **ID** – In this field, you can enter keywords to search for backup files using their unique IDs.

          > **Note:** When there are files with the same name in the backup data, you can configure the **ID** condition to locate the file that you want to recover. The unique ID of a file is a part of the file's URL.

        - **Created date** – You can click this field and set a time range to search for files.
        - **File size** – In this field, you can set a range of file sizes to search for files.
3. Click **Search** to search for the backup data you want to export.
4. In the search results table, find the item you want to export. To select the status you want to export for this item, select a backup job time in the drop-down list under the **Recovery point** column.
5. To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
6. The **Export** pop-up window appears. The selected backup data will be exported as a **ZIP** file. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

Recover Google Classroom Data

To select the backup data that you want to recover, you can choose **Search mode** or **Calendar mode**:

- **Search mode** – In this mode, you can configure search conditions based on the properties of the objects that you want to recover, and then select your desired backup data from the search results to perform a data recovery.
  In the **Search mode**, you can refer to the following instructions to recover data: Recover a Whole Class via Search Mode and Recover Selected Items in a Class via Search Mode.
- **Calendar mode**– In this mode, you can browse backup jobs via a calendar view, and then select your desired recovery points to drill down to the specific objects that you want to recover.
  In the **Calendar mode**, you can refer to the following instructions to recover data: Recover Classroom Data via Calendar Mode and Bulk Restore for Classes.

For more information on the data types that are supported or unsupported, see Classroom Data Types.

> **Note:** The Grades data can only be recovered through the **Export** method.

Recover a Whole Class via Search Mode

Procedure

If you want to use the search mode to select a class and recover Announcements, Classwork, People, Grades, and Drive data for the whole class, follow the steps below:

1. Click **Restore** () on the left navigation.

   > **Note:** On the **Restore** page, click the **Google Classroom** tab if your organization also has other modules.

2. Select the **Search mode** tab.
3. To search for a class, enter keywords of the class name in the **Search by class name** field and select a class from the drop-down list.
4. Click **Search**. The **Select and restore the Google Classroom data** page appears. The **Class name** field displays the name of the selected class.
5. On the right of the **Class name** field, select the **Whole class** option.
6. After you select the **Whole class** option, click the **Backup time range** field and set a time range to search for the backup data you want to recover.
7. Click **Search**. The search results table will list the class if it has been backed up in the selected backup time range.
8. In the drop-down list under the **Recovery point** column, select a time when the data you want to recover has been backed up.
9. You can choose one of the following methods to recover data:

   > **Note:** The Grades data can only be recovered through the **Export** method.

   - **Restore** – To restore data of a class, select the class in the search results table, and click **Restore** above the table. The **Restore** pane appears on the right. Refer to the following instructions to configure settings:

a. The restore method is **Restore the data to its original location**, and the related drive files will also be restored.

b. The content-level conflict resolution is **Skip**. After the restore, existing data in the destination will remain unchanged.

c. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

> **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

d. If necessary, enter your comments in the **Description** field for this restore job.

e. Click **Next** to have an overview of the restore settings.

f. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

- **Export** – To export data of a class, select the checkbox next to the class, and click **Export** above the table. The **Export** pop-up window appears, and the data will be exported as the **ZIP** format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

> **Note:** The Grades data can only be recovered through the **Export** method.

10. After the restore or export job is finished, you can navigate to **Job monitor** to view job details and download job reports. For details, see Monitor Jobs and Download Job Reports.

Recover Selected Items in a Class via Search Mode

If you want to recover specific items in Announcements, Classwork, People, Grades, or Drive, follow the steps below:

1. Click **Restore** () on the left navigation.

> **Note:** On the **Restore** page, click the **Google Classroom** tab if your organization also has other modules.

2. Select the **Search mode** tab.
3. To search for a class, enter keywords of the class name in the **Search by class name** field and select a class from the drop-down list.
4. Click **Search**. The **Select and restore the Google Classroom data** page appears. The **Class name** field displays the name of the selected class.
5. On the right of the **Class name** field, select the **Selected items** option.
6. Based on the object type you want to recover, select the **Announcements**, **Classwork**, **People**, **Grades**, or **Drive** tab. Then, refer to the following sections to proceed.

Announcements

Under the **Announcements** tab, follow the steps below to search and recover specific items:

1. To search for the specific items, refer to the following instructions to configure search conditions:
   - **Backup time range** – Click this field and set a time range to search for the backup data that you want to recover.

- **Announcement** – In this field, you can enter keywords of announcement content text.
- **Created by** – In this field, you can enter keywords of users' email addresses.
- **Created date** – You can click this field and set a time range.

2. Click **Search**.
3. In the search results table, find the item you want to recover. In order to select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery Point** column.
4. You can take the following actions to recover data:
   - To restore items, select the checkboxes next to the items, and click **Restore** above the table.
   - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
5. To configure settings for restore or export, follow the instructions below.
   - After you click **Restore**, the **Restore** pane appears on the right. Refer to the following instructions to configure restore settings:
     a. The restore method is **Restore the data to its original location**, and the related drive files will be restored together.
     b. Refer to the information below to select a content-level conflict resolution:
        - **Skip** – Existing data in the destination will remain unchanged.
        - **Append** – All announcements included will be recovered as new announcements. This option has the best performance but may result in duplicate announcements if they already exist.
     c. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

        > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

     d. If necessary, enter your comments in the **Description** field for this restore job.
     e. Click **Next** to have an overview of the restore settings.
     f. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.
   - After you click **Export**, the **Export** pop-up window appears, and the data will be exported as the ZIP format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see "Download Data of Export Jobs" on page 92.
6. After the restore or export job is finished, you can navigate to **Job monitor** to view job details and download job reports. For details, see "Monitor Jobs and Download Job Reports" on page 91.

Classwork

Under the **Classwork** tab, follow the steps below to search and recover specific items:

1. To search for the specific items, refer to the following instructions to configure search conditions:
   - **Backup time range** – Click this field and set a time range to search for the backup data that you want to recover.
   - **Type** – Select **All**, **Assignment**, **Short answer**, **Multiple choice**, or **Material** from the drop-down list.
   - **Title** – In this field, you can enter keywords of classwork titles.
   - **Created by** – In this field, you can enter keywords of users' email addresses.
   - **Created date** – You can click this field and set a time range.
2. Click **Search**.

3. In the search results table, find the item you want to recover. To select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery point** column.
4. You can take the following actions to recover data:
   - To restore items, select the checkboxes next to the items, and click **Restore** above the table.
   - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
5. To configure settings for restore or export, follow the instructions below.
   - After you click **Restore**, the **Restore** pane appears on the right. Refer to the following instructions to configure settings:
     a. The restore method is **Restore the data to its original location**, and the related drive files will be restored together.
     b. Refer to the information below to select a content-level conflict resolution:
        - **Skip** – Existing data in the destination will remain unchanged.
        - **Append** – All classwork included will be recovered as new classwork. This option has the best performance but may result in duplicate classwork if they already exist.
     c. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

        > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

     d. If necessary, enter your comments in the **Description** field for this restore job.
     e. Click **Next** to have an overview of the restore settings.
     f. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.
   - After you click **Export**, the **Export** pop-up window appears, and the data will be exported as the ZIP format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see "Download Data of Export Jobs" on page 92.
6. After the restore or export job is finished, you can navigate to **Job Monitor** to view job details and download job reports. For details, see "Monitor Jobs and Download Job Reports" on page 91.

People

Under the **People** tab, follow the steps below to search and recover specific items:

1. a. To search for the specific items, refer to the following instructions to configure search conditions:
      - **Backup time range** – Click this field and set a time range to search for the backup data that you want to recover.
      - **Role** – Select **All**, **Student**, or **Teacher** from the drop-down list.
      - **User name** – In this field, you can enter keywords of users' names.
      - **User email address** – In this field, you can enter keywords of users' email addresses.
2. Click **Search**.
3. In the search results table, find the item you want to recover. In order to select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery point** column.
4. You can take the following actions to recover data:
   - To restore items, select the checkboxes next to the items, and click **Restore** above the table.
   - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.

5. To configure settings for restore or export, follow the instructions below.
    - After you click **Restore**, the **Restore** pane appears on the right. Refer to the following instructions to configure settings:
        a. The restore method is **Restore the data to its original location**.
        b. The content-level conflict resolution is **Skip**. After the restore, existing data in the destination will remain unchanged.
        c. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

        > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

        d. If necessary, enter your comments in the **Description** field for this restore job.
        e. Click **Next** to have an overview of the restore settings.
        f. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.
    - After you click **Export**, the **Export** pop-up window appears, and the data will be exported as the ZIP format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see "Download Data of Export Jobs" on page 92.
6. After the restore or export job is finished, you can navigate to **Job Monitor** to view job details and download job reports. For details, see "Monitor Jobs and Download Job Reports" on page 91.

Grades

Under the **Grades** tab, follow the steps below to search and recover specific items:

1. To search for the specific items, refer to the following instructions to configure search conditions:
    - **Backup time range** – Click this field and set a time range to search for the backup data that you want to recover.
    - **Student email address** – In this field, you can enter keywords of students' email addresses.
    - **Classwork title** – In this field, you can enter keywords of classwork titles.
2. Click **Search**.
3. In the search results table, find the item you want to export. In order to select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery point** column.
4. To export backup data, select the checkboxes next to the items, and click **Export** above the table.
5. After you click **Export**, the **Export** pop-up window appears, and the data will be exported as the ZIP format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see "Download Data of Export Jobs" on page 92.
6. After the export job is finished, you can navigate to **Job monitor** to view job details and download job reports. For details, see "Monitor Jobs and Download Job Reports" on page 91.

Drive

Under the **Drive** tab, follow the steps below to search and recover specific items:

1. To search for the specific items, refer to the following instructions to configure search conditions:
    - **Level** – Based on the object type that you want to recover, select **Folder** or **File** from the drop-down list.
    - **Backup time range** – Click this field and set a time range to search for the backup data that you want to recover.
    - **Owner email address** – You must specify an owner of folders or files according to your selected level. Enter keywords of owners' email addresses, and then select an owner from the drop-down

list. The email addresses in the drop-down list are retrieved from the backup data of Classroom Drive.

- **Folder name** – In this field, you can enter keywords of folders' names.
- **ID** – In this field, you can enter keywords to search for backup folders using their unique IDs.

> **Note:** When there are folders with the same name in the backup data, you can configure the **ID** condition to locate the folder that you want to recover. The unique ID of a folder is a part of the folder's URL.

If you select the **File** level, you can also configure the following conditions:

- **File name** – In this field, you can enter keywords of files' names.
- **ID** – In this field, you can enter keywords to search for backup files using their unique IDs.

> **Note:** When there are files with the same name in the backup data, you can configure the **ID** condition to locate the file that you want to recover. The unique ID of a file is a part of the file's URL.

- **Created date** – You can click this field and set a time range.
- **File size** – You can set a range of file sizes to search for files.

2. Click **Search**.
3. In the search results table, find the item you want to recover. In order to select the status you want to recover for this item, select a backup job time in the drop-down list under the **Recovery point** column.
4. You can take the following actions to recover data:
   - To restore items, select the checkboxes next to the items, and click **Restore** above the table.
   - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
5. To configure settings for restore or export, follow the instructions below.
   - After you click **Restore**, the **Restore** pane appears on the right. Refer to the following instructions to configure settings:
     a. The selected items will be restored to a new folder in the class owner's drive. If necessary, you can change the default folder name in the **Restore to a new folder in the class owner's drive** field.

     > **Note:** If this folder name conflicts with another folder name in the destination, this folder name will be appended with "**_1**".

     b. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

     > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

     c. If necessary, enter your comments in the **Description** field for this restore job.
     d. Click **Next** to have an overview of the restore settings.
     e. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

- After you click **Export**, the **Export** pop-up window appears, and the data will be exported as the ZIP format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see "Download Data of Export Jobs" on page 92.

6. After the restore or export job is finished, you can navigate to **Job Monitor** to view job details and download job reports. For details, see "Monitor Jobs and Download Job Reports" on page 91.

Recover Classroom Data via Calendar Mode

To restore/export backup Classroom data from a specific recovery point, follow the steps below:

1. To restore/export backup Classroom data from a specific recovery point, follow the steps below:
2. Click **Restore** ( ) on the left navigation.

> **Note:** On the **Restore** page, click the **Google Classroom** tab if your organization also has other modules.

3. Select the **Calendar mode** tab.
4. By default, only the successful backup jobs are displayed on the calendar. If you also want to check backup jobs with exceptions, select the **Include jobs with partial backup data** option.
5. Each recovery point on the calendar represents the start time of a backup job. By default, the calendar displays the current month's page. You can click components on the calendar to find the month page which lists your desired recovery points.
6. Click a recovery point, and you are directed to the table listing classes that are in the backup scope.

> **Note:** By default, the scope contains historical backup data. If you want to recover contents which were just backed up by the selected backup job, select the **Include data from this backup only** option.

7. The table below shows the relationship between different levels of backup objects.

Container	**Class**				
Object type	Announcement	Classwork	People	Grade	Drive
Content	announcements	classwork of the following types: assignment, short answer, multiple choice, and material	students and teachers	students	owners folders and files

Note the following:

- When you hover the mouse over an item with sub-level items, you can click that item and continue to select sub-level items as you needed.
- When you select a parent-level item, all sub-level items will also be selected. If you only want to recover some of the sub-level items, you can return to the parent-level item and deselect it.

8. Based on the object type you want to recover, refer to the following sections to proceed.

Announcement

Follow the steps below to recover data:

1. You can choose one of the following methods:

- To restore items, select the checkboxes next to the items, and click **Restore** above the table.
- To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.

2. Refer to the instructions below to configure settings for restore or export.
   - After you click **Restore**, the **Restore** pane appears on the right. Refer to the following instructions to configure settings:
     a. The restore method is **Restore the data to its original location**, and the related drive files will be restored together.
     b. Refer to the information below to select a content-level conflict resolution:
        - **Skip** – Existing data in the destination will remain unchanged.
        - **Append** – All announcements included will be recovered as new announcements. This option has the best performance but may result in duplicate announcements if they already exist.
     c. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

        > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

     d. If necessary, enter your comments in the **Description** field for this restore job.
     e. Click **Next** to have an overview of the restore settings.
     f. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.
   - After you click **Export**, the **Export** pop-up window appears, and the data will be exported as the **ZIP** format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.
3. After the restore or export job is finished, you can navigate to **Job monitor** to view job details and download job reports. For details, see Monitor Jobs and Download Job Reports.

Classwork

Follow the steps below to recover data:

1. You can choose one of the following methods:
   - To restore items, select the checkboxes next to the items, and click **Restore** above the table.
   - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
2. Refer to the instructions below to configure settings for restore or export.
   - After you click **Restore**, the **Restore** pane appears on the right. Refer to the following instructions to configure settings:
     a. The restore method is **Restore the data to its original location**, and the related drive files will be restored together.
     b. Refer to the information below to select a content-level conflict resolution:
        - **Skip** – Existing data in the destination will remain unchanged.
        - **Append** – All classwork included will be recovered as new classwork. This option has the best performance but may result in duplicate classwork if they already exist.
     c. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

> **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

d. If necessary, enter your comments in the **Description** field for this restore job.

e. Click **Next** to have an overview of the restore settings.

f. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

- After you click **Export**, the **Export** pop-up window appears, and the data will be exported as the **ZIP** format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.

3. After the restore or export job is finished, you can navigate to **Job monitor** to view job details and download job reports. For details, see Monitor Jobs and Download Job Reports.

People

Follow the steps below to recover data:

1. You can choose one of the following methods:
   - To restore items, select the checkboxes next to the items, and click **Restore** above the table.
   - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
2. Refer to the instructions below to configure settings for restore or export.
   - After you click **Restore**, the **Restore** pane appears on the right. Refer to the following instructions to configure settings:
     a. The restore method is **Restore the data to its original location**, and the related drive files will be restored together.
     b. The content-level conflict resolution is **Skip**. After the restore, existing data in the destination will remain unchanged.
     c. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

     > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

     d. If necessary, enter your comments in the **Description** field for this restore job.
     e. Click **Next** to have an overview of the restore settings.
     f. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.
   - After you click **Export**, the **Export** pop-up window appears, and the data will be exported as the **ZIP** format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.
3. After the restore or export job is finished, you can navigate to **Job monitor** to view job details and download job reports. For details, see Monitor Jobs and Download Job Reports.

Grade

Follow the steps below to recover data:

1. To export backup data, select the checkboxes next to the items, and click **Export** above the table.

2. After you click **Export**, the **Export** pop-up window appears, and the data will be exported as the **ZIP** format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.
3. After the export job is finished, you can navigate to **Job monitor** to view job details and download job reports. For details, see Monitor Jobs and Download Job Reports.

Drive

Follow the steps below to recover data:

1. You can choose one of the following methods:
   - To restore items, select the checkboxes next to the items, and click **Restore** above the table.
   - To export backup data of items, select the checkboxes next to the items, and click **Export** above the table.
2. Refer to the instructions below to configure settings for restore or export.
   - After you click **Restore**, the **Restore** pane appears on the right. Refer to the following instructions to configure settings:
     a. The selected items will be restored to a new folder in the class owner's drive. If necessary, you can change the default folder name in the **Restore to a new folder in the class owner's drive** field.

     > **Note:** If this folder name conflicts with another folder name in the destination, this folder name will be appended with "**_1**".

     b. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

     > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

     c. If necessary, enter your comments in the **Description** field for this restore job.
     d. Click **Next** to have an overview of the restore settings.
     e. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.
   - After you click **Export**, the **Export** pop-up window appears, and the data will be exported as the **ZIP** format. Click **Export** to start the export job. After the export job is finished, to get the exported data, see Download Data of Export Jobs.
3. After the restore or export job is finished, you can navigate to **Job monitor** to view job details and download job reports. For details, see Monitor Jobs and Download Job Reports.

Bulk Restore for Classes

About this task

As a user in the **Administrators** group, if you want to add a large number of classes to a restore queue for performing a bulk restore, refer to the steps below:

Procedure

1. Click **Restore** () on the left navigation.
2. On the **Restore** page, select the **Calendar mode** tab.

> **Note:** On the **Restore** page, select the **Google Classroom** tab if your organization also has other modules.

3. By default, only the successful backup jobs are displayed on the calendar. If you also want to check backup jobs with exceptions, select the **Include jobs with partial backup data** option.
4. Each recovery point on the calendar represents the start time of a backup job. By default, the calendar displays the current month's page. You can click components on the calendar to find the month page which lists your desired recovery points.
5. Click a recovery point, and you are directed to the table listing classes in the backup scope.

> **Note:** By default, the scope contains historical backup data. If you want to recover contents that were just backed up by the selected backup job, select the **Include data from this backup only** option.

6. Select the classes that you want to add to a restore queue, and then click **Add to restore queue**. You can use the search box on the upper-right corner to search for classes. If you want to import classes via uploading a CSV file, click the **Restore queue** () icon and see Bulk Import Classes for more details. The classes in the restore queue will be labeled as **Added to queue**, and the number shown on the **Restore queue** icon indicates the total classes in the queue.

   Note the following:

   - The restore queue has a maximum limit of 100 classes.
   - If you want to upload a CSV file to bulk import classes, the file size cannot exceed 10 MB.

7. Click the **Restore queue** () icon. The **Restore queue** panel appears.
8. In the **Restore queue** panel, manage classes in the queue.

   - **Remove** – If you want to remove classes from the restore queue, you can click the **Remove** () button to remove a single class, or you can select multiple classes and click **Remove** at top of the panel.
   - **Bulk import** – You can also use this function to add multiple classes by uploading a CSV file. For details, refer to Bulk Import Classes.

9. In the **Restore queue** panel, select classes and click **Restore**. The **Restore** panel appears. Refer to the following instructions to configure restore settings.
   a. The restore method is **Restore the data to its original location**.

   > **Note:** Restoring each class will restore the announcements, classwork, people, and related drive files.

   b. The content-level conflict resolution is **Skip**. After the restoration, existing data in the destination will remain unchanged.
   c. If you want to restore backup data stored on the Azure archive storage tier, select the **Automatically rehydrate if backup data is in Azure archive storage tier** checkbox.

   > **Note:** This setting is only for the Microsoft Azure Blob custom storage location in a BYOS (Bring your own storage) subscription. For IBM default storage, the restore job will automatically rehydrate data.

   d. If necessary, enter your comments in the **Description** field for this restore job.

e. Click **Next** to have an overview of the restore settings.

f. Click **Restore** to start the restore job. If you want to go back to edit restore settings, click **Back**.

Bulk Import Classes

About this task

The **Bulk import** function is only available to users in the **Administrators** group. After clicking **Bulk import** in the **Restore queue** panel, the **Bulk import** panel appears. In the **Bulk import** panel, you can do the following:

Procedure

1. Click **Download CSV template**.
2. Configure the downloaded CSV template to add the classes to be included in the restore queue. Note the following:
   - The restore queue has a maximum limit of 100 objects.
   - The CSV file size cannot exceed 10 MB.
   - Ensure the added objects' backup data are covered by the selected recovery point.
3. Click **Upload** and select the configured CSV file.
4. Click **Import**.
5. The system will check objects imported via uploading a CSV file. In the **Restore queue** panel, an error message will be displayed under each invalid object. You can click **Remove all invalid objects** to clear them.

Data Management

This function is only available for organizations that have the Google Workspace module in their IBM® Storage Protect for Cloud Google Workspace subscription. If an organization wants to disable the **Data management** function, the administrator can reach out to the IBM representative.

If your organization wants to avoid accidental data loss, navigate to **Settings** > **General** and enable the **Approval process for data deletion**. With this feature enabled, data deletion requests and email notifications will be sent to the administrators when requesters are about to delete data in **Manually delete backup data** or **Data subject access requests**. To process with the data deletion requests, administrators can access the IBM® Storage Protect for Cloud Google Workspace interface and click the **My tasks** ( ) button on the upper-right corner of the interface. Note that the requests that are not approved within 7 days will be removed from the task list. For details, refer to Approve or Reject Data Deletion Requests.

Data Subject Access Requests

IBM® Storage Protect for Cloud Google Workspace offers a GDPR compliance tool that identifies and deletes all user-generated backups, including those from the following services:

- **Google Workspace** – Gmail, Calendar, Contacts, Drive, Chat, and shared drives
- **Vault** – Gmail (Vault), Drive (Vault), and shared drives (Vault)

The backup data stored on the backend is immutable to users. Administrators can enable data availability for data subject access requests by their organization's GDPR policy.

To discover and delete backup data, complete the steps below:

1. In the **Data management** section, click **Data subject access requests**.
2. Click **Discover & Delete**.
3. If your organization uses multiple modules, select a module from **Google Workspace**, **Vault**, and **Google Directory**.
4. Under the Google Workspace or Vault module, select the **User services** or **Shared drives** tab. Under the Google Directory module, only the **Users** tab is displayed.
5. Refer to the following instructions to search for users or shared drives backup data to delete.
   - Under the **User services or Users** tab, follow the steps below:
     a. In the search box, enter keywords of the username, and then select the desired user's email address from the drop-down list. You can repeat this step to add multiple users.
     b. There is a table listing the selected users' backup data grouped in service types. To delete data of one or multiple service types, select the service types, and then click **Delete** above the table.
   - Under the **Shared drives** tab, follow the steps below:
     a. In the search box, enter keywords of the shared drive name, and then select the desired shared drives from the drop-down list. You can repeat this step to add multiple shared drives.
     b. The table displays backup data for the selected shared drives within the **Shared drives** option. Select the **Shared drives** option, and then click **Delete** above the table.
6. If your organization has enabled the **Approval process for data deletion** in **Settings** > **General** and there are multiple users in the Administrator group, the **Delete data** confirmation window appears as below. To submit a deletion request for approval, enter your comment and click **Submit**. Data deletion requests and email notifications will be sent to the administrators. Once the requests are approved, the deletion jobs will start to delete data.
7. You can export a list of recovery points to view the object backup history. Select the service types and click **Export recovery point**. A ZIP file will be automatically saved to the download location of your browser on the local computer.

You can click **View the right-to-be-forgotten requests** to navigate to the **Job monitor** page to view deletion jobs in response to the right-to-be-forgotten requests.

Manually Delete Backup Data

IBM® Storage Protect for Cloud Google Workspace allows the removal of Drive and Gmail backup data for specific users, as well as the deletion of backups for specific shared drives, to prevent future restores. To search for users or shared drives for removing the relevant backup data at the item level, navigate to **Data management** > **Manually delete backup data**.

About this task

> **Note:** The data deletion actions will be recorded in **System auditor**.

Procedure

On the **Manually delete backup data** page, refer to the following instructions to delete backup data:

1. If your organization has enabled Vault data protection, select a tab from **Google Workspace** and **Vault**.
2. Select the **User services** or **Shared drives data type** .
3. Refer to the following instructions to search for users or shared drives.
   - Under the **User services** tab, follow the steps below:
     a. To search for a user, enter keywords of the username in the **Delete data for user** field and select the desired user's email address from the drop-down list.
     b. Click the **Gmail** tab to delete the user's Gmail backup data, or click the **Drive** tab to delete the user's Drive backup data.
     If your organization has enabled Vault data protection, you can click the **Gmail** or **Drive** tab in the **Google Workspace** section, and click the **Gmail(Vault)** or **Drive (Vault)** tab in the **Vault** section.
     c. To search for the user's item-level backup data to be deleted, configure the following search conditions:
        - Under the **Gmail** or **Gmail (Vault)** tab, you can configure **Backup time range**, **Label name**, **Subject**, **Date sent**, **Sent from**, **Sent to**, and **Sent cc** conditions to search for backup data of the user's emails.
        - Under the **Drive** or **Drive (Vault)** tab, you can configure **Backup time range**, **Folder name**, **File name**, **Label name**, **Created date**, **Modified by**, and **File size** conditions to search for backup data of the user's files.
   - Under the **Shared drives** tab, follow the steps below:
     a. To search for a shared drive, enter keywords of the shared drive name in the **Delete data from your shared drives** field and select the desired shared drive from the drop-down list.
     b. You can configure **Backup time range**, **Folder name**, **File name**, **Label name**, **Created date**, **Modified by**, and **File size** conditions to search for item-level backup data.
4. Click **Search** to search for backup data based on your configured search conditions. If you want to reset the search conditions, click **Reset**.
5. In the search results table, find and select the items that you want to delete. If you want to modify the search conditions, click the more filters () button to expand the search panel and configure the search conditions.
6. If you want to archive information of the data deletion, before you delete backup data of the selected items, you can click **Export deletion information** to export an Excel file that contains information of the selected items.
7. To delete one or multiple items, select items in the search results table, and then click **Delete** above the table.

8. Refer to the instructions below based on your organization scenarios:
    - If your organization has enabled the **Approval process for data deletion** and there are multiple users in the Administrator group, the **Delete data** confirmation window appears as below. To submit a deletion request for approval, enter your comment and click **Submit**. Data deletion requests and email notifications will be sent to the administrators. Once the requests are approved, the deletion jobs will start to delete data.
    - If your organization hasn't enabled the **Approval process for data deletion**, or if your organization has enabled the approval process but there is only one user in the Administrator group, the **Delete data** confirmation window appears. To confirm the deletion, select **I understand that the selected backup data will be permanently deleted.** option and click **OK**. A notification message appears on the page to show if the job has successfully started.
9. Once the job starts, you can monitor the deletion job process and view the job report in **Job monitor**. For more information, see Monitor Jobs and Download Job Reports.

Approve or Reject Data Deletion Requests

Once a requester submits a data deletion request in **Manually delete backup data** or **Data subject access requests**, the deletion request and notification email will be sent to the administrators for approval. Administrators can refer to the instructions below to process requests:

1. On the IBM® Storage Protect for Cloud Google Workspace interface, click the **My tasks** ( ) button on the upper-right corner of the interface.
2. The **My tasks** page appears with the requests pending your approval. Note that the requests that are not approved within 7 days will be removed from the task list.
3. To approve or reject requests, refer to the instructions below:
    - To process a single request, you can click the Actions (•••) button in the row of the task, and then click **Approve** or **Reject** from the drop-down menu.
    - To approve or reject multiple requests in a batch, select the requests, and then click **Approve** or **Reject** above the task list.

Configure Job Status Notification Settings

To better monitor job statuses in IBM® Storage Protect for Cloud Google Workspace, you can configure **Notification settings** to define which job statuses will trigger email notifications and specify recipients who will receive the emails.

Before you begin

> **Note:** If you are a customer managed of a service provider and your account manager has configured the job notification profiles in the IBM® Storage Protect for Cloud Partnerss platform, you will not be able to edit the **Notification settings**. If you are a managed service provider, refer to the Manage Job Notification Profiles section in IBM® Storage Protect for Cloud Partners User Guide for guidance.

Procedure

Follow the steps below to configure **Notification settings**:

1. Click **Settings** () on the left navigation and click **Notification** from the drop-down menu.
2. On the **Notification** page, you can create, edit, or delete notification profiles:
   - **Create** – To create a notification profile, click **Create** on the top menu.
   - **Edit** – To edit a profile, you can select the profile and click **Edit** on the top menu, or you can also click the more actions (•••) button and click **Edit** from the drop-down menu.
   - **Delete** – To delete profiles, select the profiles that you want to delete, and click **Delete** on the top menu. To delete one profile, you can also click that profile's more actions (•••) button and click **Delete** from the drop-down menu.
3. When you create or edit a profile, refer to the instructions below to configure the profile settings:
   - **Profile name** – Enter a name for this profile.
   - **Description** – If necessary, you can enter your comments in the **Description** field for this profile.
   - **Type** – Follow the instructions below to configure notification profile settings of a specific type:
     - **Job** – Select the **Job** option and configure the following settings:
       - **Send email notifications to the following email addresses** – To specify recipients who will receive the notification emails for all jobs of specific statuses, enter email addresses in this text box.
       - **Send the email notifications for the jobs in the following statuses** – To specify the job statuses which will trigger the job notification emails, select the checkbox next to **Finished**, **Finished with exception**, or **Failed**.
       - **Customize the notification for the restore and export jobs** – If you want to send notification emails to recipients who manage the export and restore jobs, turn on this toggle to configure the specific recipients and job statuses.
         Click **Save** at the bottom of the pane to apply the configured settings.
     - **Unusual activities notification** – Select the **Unusual activities** option and configure the following settings:
       - **Send email notifications to the following email addresses** – To specify recipients who will receive the notification emails for the detection of specific unusual activities, enter email addresses in this text box.
       - **Send the email notifications for the jobs in the following statuses** – To send notification emails to notify recipients about the potential ransomware attack or unusual activities detected in IBM® Storage Protect for Cloud Google Workspace, select the corresponding options.

Click **Save** at the bottom of the pane to apply the configured settings.

Configure Self-service Settings for Recovery Portal

This function is only available for organizations that have the Google Workspace module in their IBM® Storage Protect for Cloud Google Workspace subscription.

Procedure

To manage users' access and actions in Recovery Portal, follow the steps below:

1. Click **Settings** () on the left navigation, and then click **Self-service** in the drop-down menu.
2. On the **Self-service** page, you can configure the following.
   - Once a user submits a request from the Recovery Portal, a notification email will be sent to the Tenant Owner by default. If you want to update the recipients who will receive user requests from the Recovery Portal, click **Help desk settings** and enter email addresses. Then, click **Save** to save your changes. The updates will take effect immediately.
   - By default, all users added to your tenant in IBM® Storage Protect for Cloud can access the Recovery Portal to restore and export backup data. If you want to change users' permissions in the Recovery Portal, click the **Access Settings** tab and refer to the steps in "Manage Access" on page 90.

Manage Access

Follow the steps below to manage users' access in Recovery Portal.

Procedure

1. On the **Self-service** page, click **Access setting** . The **Access settings** pane appears, listing users synchronized from your tenant in IBM® Storage Protect for Cloud.
2. To synchronize the latest user information from your tenant in IBM® Storage Protect for Cloud, click the Sync () button.
3. You can use the search box to search for specific users. You can also click **Filters** and configure the **Role** filter to filter users with the **Standard user**, **Application administrator**, or **Service administrator** role.
4. In the **Access settings** pane, the colorful icons in the **Services** column represent the users who have been granted with permissions.
5. The **Manage access** pane appears on the right of the page. Refer to the instructions below to configure the settings.
   a. Turn on the toggles of the services this user can access.
   b. Select the actions this user can take.
   c. Click **Apply**. The updates will take effect immediately.

Monitor Jobs and Download Job Reports

On the **Dashboard** page, you can view backup points of the protected services. To view reports of jobs supported in IBM® Storage Protect for Cloud Google Workspace, click the **Job monitor** () on the left navigation.

Procedure

On the **Job monitor** page, follow the instructions below to search for jobs and view details:

1. You can use the search box and configure filter conditions to search for jobs.
   - In the search box, you can enter keywords of job operators, job IDs, or descriptions to search for jobs.
   - To configure filter conditions, click **Filters**. In the **Filters** pane, you can configure the following filters: **Type**, **Job type**, **Data source**, **Status**, and **Time range**. Then, click **Apply** to apply the filters.
2. If you want to customize columns to be displayed in the table, click **Columns**.
3. Clicking a job ID will open the **Job details** pane.
4. You can get job reports on both the **Job monitor** page and the **Job details** pane. To generate and download a job report, follow the steps below:
   a. Click the more actions (•••) button.
   b. Click **Generate report** from the drop-down menu.
   c. Select a type for the report you want to generate, **Simple report** or **Detailed report**.
      - Simple report includes the exceptions and skipped items.
      - Detailed report includes the successful top-level objects and the exceptions or skipped items.
   d. Click **Generate** to start generating the job report.
   e. After the job report is successfully generated, the notification (●) icon will be displayed on the more (•••) actions button. To download the report, click the more actions (•••) button and click **Download report** from the drop-down menu.

> **Note:** In the **Details** sheet of the job report, you can click the link in the **Error Code** column to open the Troubleshooting Guide and search the error code to check the solution.

> **Note:** Note the following:
>
> - If you want to generate a report of the other type, click the more actions (•••) button and click **Regenerate report** from the drop-down menu. Then, select the other type to generate a new report.
> - For an object has exceptions to be backed up in consecutive backup jobs, the **Failed Attempts** column in job reports would show the number of failed attempts for backing up the object in consecutive backup jobs, and the **Attempts per Job** column would show the maximum limit of attempts for backing up the object in each job.
> - If there are exceptions in a restore job and you want to rerun a restore for these exceptions only, click the more actions (•••) button and click the **Rerun** from the drop-down menu.

Download Data of Export Jobs

To download data of export jobs, click **Job monitor** () tab on the left pane. The **Job monitor** page will appear.

Find the export job that contains the data you want to download. After the job is finished,, click the more actions (•••) button and click **Download content** from the drop-down menu. Note that the exported data of a job will be available for download within 7 days after the export job is finished. By default, the export capacity limit for your tenant is 100 GB per month.

> **Note:** In the following cases, the exported data will be separated into multiple files. Then, you. You can click the **Download** ( ) button next to each file to download it.
>
> - The file size of the exported data exceeds the maximum limit of download.
> - The export job was performed via the calendar mode and multiple users / shared drives / classes were included in the export job.

The exported data will be downloaded as a .zip file protected with a password. Only the user who performed the export job or the recipients of notification emails on export and restore jobs can follow the steps below to get the password and download content.

1. Click the more actions (•••) button and click **Download content** from the drop-down menu.
2. The **Download content** panel appears with the following steps:
    a. Click the **Copy** ( ) button to copy the password to your clipboard.
    b. Click **Download** to download the ZIP file.

View Reports

To view reports provided in IBM® Storage Protect for Cloud Google Workspace, refer to the following sections.

Storage Consumption

For the organization who is using the BYOS (Bring your own storage) subscription, IBM® Storage Protect for Cloud Google Workspace supports the **Storage consumption** report. The report provides an overview of storage consumption by different service types, the history and trends of storage usage, and utilization information of containers. If you want to add this report, you can contact IBM Software Support for help.

To view the **Storage consumption** reports, click **Report** () ton the left navigation, and click **Storage consumption** in the drop-down menu. On the **Storage consumption** page, you can view reports under **Dashboard**, **Usage**, and **Utilization** tabs. When you view reports under each tab, you can click **Download report** to export the report.

Note the following:

- Only users in the Administrator group can view the reports.
- The system will refresh the reports every seven days.
- For the organization with the Multi-Geo function enabled, the reports can only display data of the current data region.

Unusual Activities Analysis

This function is only available for organizations that have the Google Workspace module in their IBM® Storage Protect for Cloud Google Workspace subscription.

The Unusual activities analysis report shows the unusual activities detected in your backup data of drives and shared drives. This report requires the drives / shared drives to have at least 12 days of incremental backups with changes. The unusual activities analysis report can detect up to 1000 drives / shared drives.

Based on the unusual activities detected in the backup data, IBM® Storage Protect for Cloud Google Workspace will help you analyze whether there are suspicious drives / shared drives under potential ranwomware attack. You can also select suspicious drives / shared drives and recover them to a safe state.

You can configure notification for unusual activities detected in the report. For details, refer to "Configure Job Status Notification Settings" on page 88.

In the **Unusual activities analysis** report, both the **Drive** and **Shared drive** tabs contain the **Dashboard** and **Details** sections. Follow the instructions below to use the report:

- **Dashboard** – On the Dashboard, there is an overview of the unusual activities tracked over the last 30 days. In the **Unusual activities trends** section, you can customize the Time range (UTC) filter to view the trends in different periods, and you can hover the mouse over the line chart to view details of files that are **Under potential ransomware attack / With unusual activities.**
- **Details** – To open the **Details** page, you can choose one of the following methods:
  On the **Details** page, you can take the following actions:
  - Click the **Details** tab.
  - Click the arrow (→) button in the **Unusual activities trends** section under **Dashboard**.
  - Click **Suspicious drives** / **Suspicious shared drives** under **Dashboard**.
  - Click a point **With unusual activities** on the line chart

  On the **Details** page, you can take the following actions:
  - Customize the **Time range (UTC)** filter to view details in different periods.
  - To view details of a suspicious drive / shared drive, click the link in the **Drive** / **Shared drive** column.

On the **View details** page, you can customize the **Time range (UTC)** filter and hover the mouse over the line chart to view details of unusual activities detected in the drive / shared drive. You can click a point on the chart to open the details pane of that day. In the details pane, after clicking the more actions (•••) button, you can do the following:

- Click **Download list** to download the report on that day for further investigation.
- Click **Go to restore** to restore your files to a healthy state.
- Click **Download report** to export the unusual activities report as an Excel file.
- Select items in the **Drive** / **Shared drive** column, and click **Restore** to restore files to a healthy state.

Audit User Activities in System Auditor

To view user activities in IBM® Storage Protect for Cloud Google Workspace, click **System auditor** () on the left navigation.

On the **System auditor** page, you can perform the following actions to view user activities:

- If you want to customize columns to be displayed in the table, click **Columns**.
- Click **Filters**, and then select an option in the **Operation type**, **Type**, **Data source** or **Time range** filter.
- In the search box, enter keywords of usernames to search for user activities.
- Click the **View** link in the **Details** column to open the **View details** pane.
- To export the **System auditor** report to an Excel file, click **Export**. In the **Export** pop-up window, click the calendar () button to select a time range for the data you want to export, and click **Export**.

View Subscription Information

To view the subscription information, click **Subscription** on the left navigation. The **Subscription** section provides reports under the **Dashboard** and **Usage** tabs.

> **Note:** The subscription information is only visible for an enterprise subscription of IBM® Storage Protect for Cloud Google Workspace.

Under the **Dashboard** tab, you can view the information on the following panes:

- **Subscription utilization** shows the basic information of your subscription, the subscription expiration date, and the number and percentage of the following:
  - Purchased, assigned, and available user seats
  - Purchased, consumed, and available objects

    > **Note:** The object-based subscription type is only for the **Google Classroom** module

- **Top subscription consumers** shows the ranking of the major consumers (Google Workspace editions) of your subscription.

  > **Note:** If a subscription type cannot be detected due to API limitations, the placeholder will be **Unknown subscription type**.

- **Usage history** displays a line chart reflecting the history of assigned user seats or consumed objects. To view additional information on usage history, click the arrow (→) button to navigate to the **Usage** tab

Under the **Usage** tab, the **Usage history and trends** pane displays a line chart reflecting the history and trends of assigned user seats or consumed objects, and you can hover the mouse over a point on the line chart to view the details. To download a copy of the usage report, click **Download report**. The **Average growth rate** and **Largest spike** panes are also under the **Usage** tab.

View Notification Center

You can click the **Notification Center** () button on the top bar to view notifications of your subscription.

Troubleshooting

This troubleshooting guide is aimed at addressing unexpected issues and errors that you may encounter when using IBM® Storage Protect for Cloud Google Workspace.

ArchivedUser

Issue:

The archived user failed in the job with the following error code:

- **ArchivedUser**

Solution:

Due to the Google API limitations, IBM® Storage Protect for Cloud Google Workspace cannot support Google users with the **Archived** or **Suspended** status. If you want to include these Google users in the protection scope of IBM® Storage Protect for Cloud Google Workspace, you can change the status of these Google users and purchase more user seats in the subscription of IBM® Storage Protect for Cloud Google Workspace.

B-ClassNotExist

Issue:

The class failed in backup with the following error code:

- **B-ClassNotExist**

Solution:

From when the class was deleted from the Google tenant, there is no scan job for the corresponding scan profile to update the objects in the container. Go to IBM® Storage Protect for Cloud > **Auto discovery** and run the scan profile, or wait for the next scan job to be completed if the scan profile has enabled daily-scan.

B-GoogleAPI404NotFound

Issue:

The file failed in backup with the following error code:

- **B-GoogleAPI404NotFound**

Solution:

The path of the file can be displayed in the job report. Manually download the file to check whether it is a damaged file. Usually, the size of a damaged file is below 1 KB. A file may have been damaged during the creation process. If it is confirmed that the file is damaged, you can ask the file owner to try deleting the file to not affect the backup job status.

B-GoogleAPIRiskFile

Issue:

The file skipped in backup with the following error code:

- **B-GoogleAPIRiskFile**

Solution:

The Drive and Shared Drive services do not support backing up virus-contaminated files.

B-GoogleAPIServiceError

Issue:

The file failed in backup with the following error code:

- **B-GoogleAPIServiceError**

Solution:

The path of the file can be displayed in the job report. Manually download the file to check whether it is a damaged file. Usually, the size of a damaged file is below 1 KB. A file may have been damaged during the creation process. If it is confirmed that the file is damaged, you can ask the file owner to try deleting the file to not affect the backup job status.

B-NoDownloadPermission

Issue:

A file skipped in backup with the following error code:

- **B-NoDownloadPermission**

Solution:

Check whether the current Google user has permission to download the file.

B-SDNoMember

Issue:

The shared drive skipped in backup with the following error code:

- **B-SDNoMember**

Details:

The user credentials of the service account or account pool users may have been updated.

Solution:

Go to https://admin.google.com/ and navigate to **Apps** > **Google Workspace** > **Settings for Drive and Docs** > **Manage shared drives**. Add members and ensure there is at least one member who has the **Manager** permission to the shared drive.

B-SDNotExist

Issue:

The shared drive failed in backup with the following error code:

- **B-SDNotExist**

Details:

The user credentials of the service account or account pool users may have been updated.

Solution:

From when the shared drive was deleted from the Google tenant, there is no scan job for the corresponding scan profile to update the objects in the container. Go to IBM® Storage Protect for Cloud > **Auto discovery** and run the scan profile, or wait for the next scan job to be completed if the scan profile has enabled daily-scan.

B-UserNotExist

Issue:

A user failed in backup with the following error code:

- **B-UserNotExist**

Solution:

From when the user was deleted from the Google tenant, there is no scan job for the corresponding scan profile to update the objects in the container. Go to IBM® Storage Protect for Cloud > **Auto discovery** and run the scan profile, or wait for the next scan job to be completed if the scan profile has enabled daily-scan

GoogleAPIFailedPrecondition

Issue:

A job failed with the following error code:

- **GoogleAPIFailedPrecondition**

Solution:

A Failed precondition error occurs when calling the Google API.

GoogleAPIQuota

Issue:

The job failed with the following error code:

- **GoogleAPIQuota**

Solution:

This is a temporary error caused by the Google API quota. You can try to configure a custom Google app to avoid this error.

R-ChangeSubscription

Issue:

The restore failed with the following error code:

- **R-ChangeSubscription**

Solution:

The restore job failed due to the Google API exception. For example, after the Calendar service has been backed up, modify the user's email and run the scan profile again. Then, perform the backup job and restore the default calendar using the previous email.

R-GoogleAPIAbortedError

Issue:

The job failed in restore with the following error code:

- **R-GoogleAPIAbortedError**

Solution:

This exception is usually caused by a concurrency conflict. If multiple jobs calling the Google API at the same time to create the same object, the Google API may return the Aborted Error.

R-GoogleAPIAlreadyExistsError

Issue:

The job failed in restore with the following error code:

- **R-GoogleAPIAlreadyExistsError**

Solution:

If multiple jobs calling the Google API at the same time to create the same object, the Google API may return the Already Exists Error.

R-GoogleAPIFailedValueExceedsLimit

Issue:

The job failed in restore with the following error code:

- **R-GoogleAPIFailedValueExceedsLimit**

Solution:

When calling the Google API to create an object but the provided value exceeds the maximum limit, the API may return the Field Value Exceeds Limit Error.

R-GoogleAPIInvalidArgument

Issue:

The job failed in restore with the following error code:

- **R-GoogleAPIInvalidArgument**

Solution:

When calling the Google API to create an object but a field in the request body is invalid, the API may return the Invalid Argument Error.

R-SDNoAvailableMember

Issue:

The shared drive failed in restore with the following error code:

- **R-SDNoAvailableMember**

Solution:

Go to https://admin.google.com/ and navigate to **Apps** > **Google Workspace** > **Settings for Drive and Docs** > **Manage shared drives**. Add members and ensure there is at least one member who has the **Contributor** permission to the shared drive.

R-SDNoManagerPermission

Issue:

The shared drive failed in restore with the following error code:

- **R-SDNoManagerPermission**

Solution:

Go to https://admin.google.com/ and navigate to **Apps** > **Google Workspace** > **Settings for Drive and Docs** > **Manage shared drives**. Add members and ensure there is at least one member who has the **Manager** permission to the shared drive.

R-SDNotFound

Issue:

The shared drive failed in restore with the following error code:

- **R-SDNotFound**

Solution:

From when the shared drive was deleted from the Google tenant, there is no scan job for the corresponding scan profile to update the objects in the container. Go to IBM® Storage Protect for Cloud > **Auto discovery** and run the scan profile, or wait for the next scan job to be completed if the scan profile has enabled daily-scan.

RetrieveUsersInfoError

Issue:

The job failed with the following error code:

- **RetrieveUsersInfoError**

Solution:

Unable to obtain user information through the Google API. Connecting a Google tenant requires an account with the **Users** > **Read**, **Groups** > **Read**, and **License Management** > **License Read** privileges in the same tenant. Please check if the account used for connecting your Google tenant has the required permissions.

SharedWithMeError

Issue:

The folder/file failed in restore/export with the following error code:

- **SharedWithMeError**

Solution:

The shared objects can be restored/exported only when they have been backed up by the owner. Check whether the owner's **My Drive** has been successfully backed up.

SharedWithMeFileError

Issue:

The file failed in export/restore with the following error code:

- **SharedWithMeFileError**

Solution:

The shared objects can be exported/restored only when they have been backed up by the owner. Check whether the owner's **My Drive** has been successfully backed up.

SharedWithMeFolderError

Issue:

The folder failed in export/restore with the following error code:

- **SharedWithMeFolderError**

Solution:

The shared objects can be exported/restored only when they have been backed up by the owner. Check whether the owner's **My Drive** has been successfully backed up.

SuspendedUser

Issue:

The suspended user failed in the job with the following error code:

- **SuspendedUser**

Solution:

Due to the Google API limitations, IBM® Storage Protect for Cloud Google Workspace cannot support Google users with the **Archived** or **Suspended** status. If you want to include these Google users in the protection scope of IBM® Storage Protect for Cloud Google Workspace, you can change the status of these Google users and purchase more user seats in the subscription of IBM® Storage Protect for Cloud Google Workspace.

UnauthorizedClient

Issue:

The job failed with the following error code:

- **UnauthorizedClient**

Solution:

Unable to obtain user data through the Google API. This problem is usually caused by uncompleted authorization. Go to the Google Admin console as a Super Admin, then check if Data Access and User Access have been successfully authorized.

Submit Feedback

IBM® Storage Protect for Cloud provides a platform to collect feedback where you can submit suggestions for features from your experience.

To submit your feedback, click Help & Resources () on the left navigation, and then click **Submit feedback** from the drop-down menu. You will be redirected to the **Submit feedback** pane in IBM® Storage Protect for Cloud. Complete the form in the **Submit feedback** pane by referring to instructions in the Submit Feedback section in the IBM® Storage Protect for Cloud user guide.

Support Lists

The following table details the support lists included in this document.

Appendix	Description
“Gmail Data Types” on page 105	Lists the Gmail data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.
“Drive Data Types” on page 106	Lists the Drive data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.
“Calendar Data Types” on page 108	Lists the Calendar data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.
“Contacts Data Types” on page 111	Lists the Contacts data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.
“Shared Drive Data Types” on page 111	Lists the Shared drive data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.
“Classroom Data Types” on page 114	Lists the Classroom data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.

Gmail Data Types

The table below lists data types that are supported or unsupported for Gmail restore in IBM® Storage Protect for Cloud Google Workspace.

Data Types		Support Status	Comments
User	User’s primary email	Supported	If you select backup data of the emails displaying a Calendar event above the mail content and choose to **Restore the data to another location**, the restored emails in the destination will not show the Calendar event above the mail content.
Label	Inbox	Supported	
	Starred	Supported	The stars will be restored in the default style. The styles of the stars cannot be kept due to Google API limitations. You can manually change the star styles after the restore.
	Snoozed	Partially Supported	In user or mail level restore, the snoozed emails will be restored to the **All Mail** label, but the original **Snoozed** status cannot be kept.
	Important	Supported	
	Sent	Supported	
	Drafts	Supported	If you select backup data of emails in **Drafts** and choose to **Restore the data to another location**, after the restore, the emails in the destination are no longer drafts and cannot be edited.
	All Mail	Unsupported	
	Spam	Supported	Supports backup and restore when the **Spam** label is selected in **Backup Settings**.

Data Types		Support Status	Comments
	Trash	Supported	Supports backup and restore when the **Trash** label is selected in **Backup Settings**.
	Updates	Supported	
	Forums	Supported	
	Promotions	Supported	
	Social	Supported	
	Custom labels	Supported	Does not support restoring labels whose names contain the character "/."
	Personal	Supported	To find emails with this category in Gmail, enter **personal** in the search box and click **category:personal** in the drop-down list.
	Unread	Supported	To find emails with this label in Gmail, enter **unread** in the search box and click **label:unread** in the drop-down list.
	Scheduled	Unsupported	
	Archive	Supported	
Mail	Muted email	Partially Supported	The muted emails will be restored to the **All Mail** label, but their original **Muted** label cannot be kept.
	Attached files	Supported	For files that are larger than 25 MB and attached to emails via Drive links, after the restore, the links still work only when the files remain in Drive.
			The attachments in the emails sent from external users are unsupported due to Google API limitations.
	Files inserted with Drive link	Supported	After the restore, the links still work only when the files remain in Drive.
Task		Unsupported	
Keep		Unsupported	
Add-ons		Unsupported	
Gmail Settings		Unsupported	
Chat		Unsupported	

Drive Data Types

The table below lists data types that are supported or unsupported for Drive recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types		Support Status	Comments
User's drive	Priority	Unsupported	
	Recent	Unsupported	
	Starred	Unsupported	
	Trash	Supported	Supports backup and restore when the `Trash` folder is selected in **Backup Settings**.
	Computer	Unsupported	
Folder	Owner	Supported	
	Description	Supported	

Data Types		Support Status	Comments
	Created time	Unsupported	After the restore, the folder's created time will be updated to the restored time.
	Modified	Partially Supported	Does not support restoring the last modifying user.
	Opened	Unsupported	
	Share with people and groups	Supported	
	Get link	Partially Supported	If the original folder has been deleted, after the restore, the original shared link will be unavailable. The resolution is getting a new shared link to the restored folder.
			If you removed the target audience with who a folder was shared with, after the restore job is **Finished**, the target audience would be restored as a group, but this security change cannot be reported in job details due to Google API limitations.
	Color	Supported	
	Added to Starred/ Removed from Starred	Supported	
File (includes documents, images, audio, and videos)	Share with people and groups	Supported	
	Get link	Partially Supported	If the original file has been deleted, after the restore, the original shared link will be unavailable. The resolution is getting a new shared link of the restored file.
			If you removed the target audience with whom a file was shared with, after the restore job is **Finished**, the target audience would be restored as a group, but this security change cannot be reported in job details due to Google API limitations.
	Added to Starred/ Removed from Starred	Supported	
	Description	Supported	
	Owner	Supported	
	Labels	Supported	
	Created time	Unsupported	After the restore, the folder's created time will be updated to the restored time.
	Modified	Partially Supported	Does not support restoring the last modifying user.
	Opened	Unsupported	
	Version History	Unsupported	

Data Types		Support Status	Comments
File (includes documents, images, audios, and videos)	Google Docs	Supported	The format of comments and replies cannot be kept in the restored file. For Google Docs, Google Sheets, and Google Slides, the add-ons cannot be kept after the restore due to Google API limitations. You can manually insert add-ons after the restore.
	Google Sheets		
	Google Slides		
	Google Vids	Supported	
	Google Forms	Unsupported	
	Google Drawings	Unsupported	
	Google My Maps	Unsupported	
	Google Sites	Unsupported	
	Google App Scripts	Supported	
	Google Jamboards'	Unsupported	
	Shortcuts	Unsupported	
	Shortcuts of third-party apps	Unsupported	
	Files identified as malware or spam	Unsupported	
	Files which the current user has no permission to download or export	Unsupported	

Calendar Data Types

The table below lists data types that are supported or unsupported for Calendar recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types		Support Status	Comments
Calendar	Birthdays	Unsupported	
	Reminders	Unsupported	
	Tasks	Unsupported	
	Other calendars	Unsupported	
	Subscribe to calendar	Unsupported	
	Custom calendars	Supported	
	Hide from calendar list	Partially supported	The hidden calendar can be backed up but will be shown in the list after the restore.
	Calendar settings	Supported	
	Access permissions	Supported	Does not support backup and restore for the **Show calendar info in other Google apps, limited by access permissions** option due to Google API limitations.

Data Types		Support Status	Comments
	Share with specific people	Supported	
	Event notifications	Supported	If you set the content-level conflict resolution to **Merge**, after the restore, the notification settings will be replaced with the backup data.
	All-day event notifications	Unsupported	
	Other notifications	Supported	
	Integrate calendar	Unsupported	
	Auto-accept invitations	Unsupported	
Event types	Event	Supported	If an event was backed up in Calendar A before you move the event to Calendar B, and then you select the backup data to restore Calendar A to its original location, after the restore, the event will be moved from the Calendar B to Calendar A.
			If a calendar is restored to another location, the events on the destination calendar will not be associated with the original calendar.
	Focus time	Unsupported	
	Out of office	Unsupported	
	Working location	Unsupported	
	Task	Unsupported	
	Appointment slots	Unsupported	
	Recurring	Partially supported	“Notes for Events Restore” on page 110
Event details	Title	Supported	
	Event time	Supported	
	Time zone	Supported	
	Settings for repeat	Supported	
	Join with Google Meet	Unsupported	
	Join by phone	Unsupported	
	Location	Supported	
	notification	Supported	If you set the content-level conflict resolution to **Merge**, after the restore, the notification settings will be replaced with the backup data.
	color	Supported	

Data Types		Support Status	Comments
	Description	Supported	
	Linked attachments	Supported	Only Drive files are supported. After the restore, the links still work only when the files remain in Drive.
	Guest permissions	Supported	
	Rooms	Supported	
	Guest	Supported	"Notes for Events Restore" on page 110

Notes for Events Restore

Due to Google API limitations, you may encounter the following cases when you restore calendars with events.

Guest Cases

- After the restore, the replies of guests in groups cannot be kept.
- After the restore, the non-Google external users cannot view the restored events in their calendars.
- A guest's response to an event is **Yes, in a meeting room** or **Yes, joining virtually**. After the restore, the response status will be updated to **Yes**.
- You select the backup data of a guest in an event to **Restore the data to another location**. After the restore, the other guests of the event will not be restored in the destination event.
- An event was deleted from the organizer's calendar. You select a guest's backup data to **Restore the data to its original location**. After the restore, only the selected guest can view the restored event.
- An event was deleted from a guest's calendar. You select this guest's backup data to **Restore the data to its original location**. After the restore, the organizer's updates on the event can be synced to the restored event, but the guest's reply to the event cannot be synced to the organizer's calendar.
- A guest has the **Modify event** permission to an existing event in the calendar. You select the guest's backup data to **Restore the data to its original location** with the **Merge** conflict resolution. After the restore, the backup data will not be merged with the existing event.

Recurring Event Cases

- Backed up a calendar with recurring events. The deletion of a recurring event was applied to **This event** or **All events** on the calendar. You select the calendar backup data (contains the recurring events) to **Restore the data to its original location**. After the restore, the deleted events will not be restored to the calendar.
- The updates (any update except for the time) of a recurring event were applied to **This event** or **This and following events**. The updated events haven't been backed up. You perform a restore job to **Restore the data to its original location** with the **Merge** conflict resolution. After the restore, the updated events will not be merged with the backup data.
- The updates (any update except for the time) of a recurring event were applied to **This and following events**, and then the updated events have been backed up. Delete the following events, and then select the backup data to **Restore the data to its original location**. After the restore, the restored events will not be associated with the original recurring event.
- A recurring event was updated (any update except for the time) multiple times and the edits were applied to **This and following events**. Perform a restore job for an updated event to **Restore the data to another location**. After the restore, the restored event cannot keep the guests' original response statuses in the destination.

Contacts Data Types

The table below lists data types that are supported or unsupported for Contacts recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types		Support Status	Comments
Label	Custom labels	Supported	
	Starred	Supported	
	My contacts	Supported	
	Other contacts	Partially Supported	The items in **Other contacts** will be restored to **Contacts**.
			Only supports restoring the following properties: **Name**, **Email**, and **Phone number**.
Contact	All properties of contacts	Supported	

Note: If you perform a job to restore a created contact whose address is the Gmail address of an existing user, note the following issue:
When you edit the details of the restored contact, you will see multiple addresses and locations. This issue is due to Google will automatically add directory profile information to a contact that is directly created with an existing Gmail address.

Shared Drive Data Types

The table below lists data types that are supported or unsupported for Shared Drive recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types		Support Status	Comments
Shared drive	members	Supported	
	Shared drive settings	Supported	
	Trash	Supported	Supports backup and restore when the `Trash` folder is selected in **Backup Settings**.
	theme	Unsupported	
	Hidden	Unsupported	
Folder	Creator	Unsupported	
	Description	Supported	
	Created time	Unsupported	After the restore, the folder's created time will be updated to the restored time.
	Modified	Partially Supported	Does not support restoring the last modifying user.
	Opened	Unsupported	
	Share with people and groups	Supported	

Data Types		Support Status	Comments
	Get link	Partially Supported	If the original folder has been deleted, after the restore, the original shared link will be unavailable. The resolution is getting a new shared link to the restored folder.
			If you removed the target audience with whom a folder was shared with after the restore job is **Finished**, the target audience would be restored as a group, but this security change cannot be reported in job details due to Google API limitations.
	Color	Unsupported	
	Added to Starred/ Removed from Starred	Unsupported	
File (includes documents, images, audio, and videos)	Share with people and groups	Supported	
	Get link	Partially Supported	If the original file has been deleted, after the restore, the original shared link will be unavailable. The resolution is getting a new shared link of the restored file.
			If you removed the target audience with whom a file was shared with after the restore job is **Finished**, the target audience would be restored as a group, but this security change cannot be reported in job details due to Google API limitation.
	Added to Starred/ Removed from Starred	Unsupported	
	Description	Supported	
	Labels	Supported	
	Creator	Unsupported	
	Created time	Unsupported	After the restore, the folder's created time will be updated to the restored time.
	Modified	Partially Supported	Does not support restoring the last modifying user.
	Opened	Unsupported	
	Version History	Unsupported	
	Google Docs	Supported	The format of comments and replies cannot be kept in the restored file. For Google Docs, Google Sheets, and Google Slides, the add-ons cannot be kept after the restore due to Google API limitations. You can manually insert add-ons after the restore.
	Google Sheets		
	Google Slides		
	Google Forms	Unsupported	
	Google Drawings	Unsupported	
	Google My Maps	Unsupported	
	Google Sites	Unsupported	

Data Types		Support Status	Comments
	Google App Scripts	Supported	
	Google Jamboards	Unsupported	
	Shortcuts	Unsupported	
	Files identified as malware or spam	Unsupported	

Chat Data Types

The table below lists data types that are supported or unsupported for Chat recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types			Support Status	Comments
Spaces			Supported	
Direct Messages			Supported	Message Requests are unsupported.
Chat	Format	Bold	Supported	
		Italic	Supported	
		Underline	Unsupported	
		Text Color	Unsupported	
		Strikethrough	Supported	
		Link	Supported	
		Bulleted List	Supported	
		@user	Supported	
		@space	Supported	
		Picture	Supported	
	Send By		Supported	The Google Chat API does not support retrieving the name information of external users. The placeholder will be **Unknown user**.
	Emoji		Partially Supported	Custom emojis are unsupported.
	Gif			
	Voice message recording			
	Video message recording			
	Video Meeting		Unsupported	
	Call ended/Call missed message		Unsupported	
	Calendar Event		Unsupported	
	Tasks		Unsupported	
	Edit Message/Edit Reply/Edit Quote in Reply Message		Unsupported	
	Deleted Message		Unsupported	

Data Types			Support Status	Comments
	App Message		Partially Supported	The Google Chat API does not support retrieving the name information of apps. The placeholder will be **Unknown app**.
	Link	Message link	Supported	
		Drive file link	Supported	
		Copy link to the space	Supported	
	Reply in thread		Partially Supported	The message texts will be backed up, but the original format cannot be kept.
	Quote in Reply		Supported	
	Files	Links to the files in Google Drive	Supported	
		Links to the folders in Google Drive	Supported	
		Files uploaded in Google Chat	Supported	
		Policy violation type	Unsupported	
	Reaction		Supported	
	Star		Unsupported	
	Mark as Unread		Unsupported	
	Active threads		Partially Supported	The message texts will be backed up, but the original format cannot be kept.

Classroom Data Types

The table below lists data types that are supported or unsupported for Classroom recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types			Support Status	Comments
Class	Status	Active	Supported	
		Archive	Supported	The restored classes will be in the Active status.
		Deleted	Unsupported	
	Class Details	Class name	Supported	
		Class description	Supported	
		Section	Supported	
		Room	Supported	
		Subject	Unsupported	

Data Types			Support Status	Comments
		Customize appearance	Unsupported	
	General	Invite Codes	Unsupported	
		Stream	Unsupported	
		Classwork on the Stream	Unsupported	
		Show deleted items	Unsupported	
		Guardian summaries	Supported	
		Meet link settings	Unsupported	
	Grading	Overall grade calculation	Unsupported	
		Show overall grade to students	Unsupported	
		Grade categories	Unsupported	
Announcement	Status		Supported	
	Text		Partially Supported	Format cannot be kept in the restored contents.
	Creator		Supported	The restored Creator content will be appended with a suffix. If using the default service app, the suffix is **via IBM® Storage Protect for Cloud**. If using a custom Google app, the suffix depends on the project's **OAuth consent screen** value. Without this value, the suffix will be displayed as **via Unknown**.
	Assigned to		Supported	
	Created time		Unsupported	
	Updated time		Unsupported	
	Scheduled time		Supported	
	Attached files		Partially Supported	Support backup and restore for the files in the `Classroom` (default name) folder of the class owners' / students' My Drive. The other attached files cannot be backed up, and they will be unavailable after the restore if the original files have been deleted.
	Comments		Unsupported	
Classwork	Common properties	Title	Supported	
		Instructions	Partially Supported	Format cannot be kept in the restored contents.

Data Types			Support Status	Comments
		Creator	Supported	The restored Creator content will be appended with a suffix. If using the default service app, the suffix is **via IBM® Storage Protect for Cloud**. If using a custom Google app, the suffix depends on the project's **OAuth consent screen** value. Without this value, the suffix will be displayed as **via Unknown**.
		Status	Supported	
		Assigned to	Supported	
		Created time	Unsupported	
		Updated time	Unsupported	
		Scheduled time	Supported	
		Due date	Supported	
		Grade category	Unsupported	
		Points	Supported	
		Topic	Supported	
		Rubric	Unsupported	
		Classwork comments	Unsupported	
		Private comments	Unsupported	
		Attached files	Partially Supported	Support backup and restore for the files in the `Classroom` (default name) folder of the class owners' / students' My Drive. The other attached files cannot be backed up, and they will be unavailable after the restore if the original files have been deleted.
Classwork	Assignment	Student work	Unsupported	
		Permission of attached files	Supported	
	Quiz assignment	Quiz form	Unsupported	
		Grade importing setting	Unsupported	
	Question	Short answer	Supported	
		Multiple choice	Supported	
		Students can reply to each other	Unsupported	
		Students can edit the answer	Supported	
		Students can see class summary	Unsupported	

Data Types			Support Status	Comments
		Students’ answer	Unsupported	
	Material	Attached files	Partially Supported	Support backup and restore for the files in the `Classroom` (default name) folder of the class owners' / students' My Drive. The other attached files cannot be backed up, and they will be unavailable after the restore if the original files have been deleted.
	Associated app	Google Calendar	Unsupported	
		Google Drive folder	Supported	
People	Teacher		Supported	
	Student		Supported	
	Mute/Unmute students		Unsupported	
	People in the Invited status		Unsupported	
Drive	Folder	Properties	Supported	
		Permissions	Unsupported	
	File	Properties	Supported	
		Content	Supported	
		Permissions	Unsupported	

Support Lists

The following table details the support lists included in this document.

Appendix	Description
“Gmail Data Types” on page 105	Lists the Gmail data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.
“Drive Data Types” on page 106	Lists the Drive data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.
“Calendar Data Types” on page 108	Lists the Calendar data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.
“Contacts Data Types” on page 111	Lists the Contacts data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.
“Shared Drive Data Types” on page 111	Lists the Shared drive data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.
“Classroom Data Types” on page 114	Lists the Classroom data types that are supported or unsupported in IBM® Storage Protect for Cloud Google Workspace.

Gmail Data Types

The table below lists data types that are supported or unsupported for Gmail restore in IBM® Storage Protect for Cloud Google Workspace.

Data Types		Support Status	Comments
User	User’s primary email	Supported	If you select backup data of the emails displaying a Calendar event above the mail content and choose to **Restore the data to another location**, the restored emails in the destination will not show the Calendar event above the mail content.
Label	Inbox	Supported	
	Starred	Supported	The stars will be restored in the default style. The styles of the stars cannot be kept due to Google API limitations. You can manually change the star styles after the restore.
	Snoozed	Partially Supported	In user or mail level restore, the snoozed emails will be restored to the **All Mail** label, but the original **Snoozed** status cannot be kept.
	Important	Supported	
	Sent	Supported	
	Drafts	Supported	If you select backup data of emails in **Drafts** and choose to **Restore the data to another location**, after the restore, the emails in the destination are no longer drafts and cannot be edited.
	All Mail	Unsupported	
	Spam	Supported	Supports backup and restore when the **Spam** label is selected in **Backup Settings**.

Data Types		Support Status	Comments
	Trash	Supported	Supports backup and restore when the **Trash** label is selected in **Backup Settings**.
	Updates	Supported	
	Forums	Supported	
	Promotions	Supported	
	Social	Supported	
	Custom labels	Supported	Does not support restoring labels whose names contain the character "**/**."
	Personal	Supported	To find emails with this category in Gmail, enter **personal** in the search box and click **category:personal** in the drop-down list.
	Unread	Supported	To find emails with this label in Gmail, enter **unread** in the search box and click **label:unread** in the drop-down list.
	Scheduled	Unsupported	
	Archive	Supported	
Mail	Muted email	Partially Supported	The muted emails will be restored to the **All Mail** label, but their original **Muted** label cannot be kept.
	Attached files	Supported	For files that are larger than 25 MB and attached to emails via Drive links, after the restore, the links still work only when the files remain in Drive.
			The attachments in the emails sent from external users are unsupported due to Google API limitations.
	Files inserted with Drive link	Supported	After the restore, the links still work only when the files remain in Drive.
Task		Unsupported	
Keep		Unsupported	
Add-ons		Unsupported	
Gmail Settings		Unsupported	
Chat		Unsupported	

Drive Data Types

The table below lists data types that are supported or unsupported for Drive recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types		Support Status	Comments
User's drive	Priority	Unsupported	
	Recent	Unsupported	
	Starred	Unsupported	
	Trash	Supported	Supports backup and restore when the `Trash` folder is selected in **Backup Settings**.
	Computer	Unsupported	
Folder	Owner	Supported	
	Description	Supported	

Data Types		Support Status	Comments
	Created time	Unsupported	After the restore, the folder's created time will be updated to the restored time.
	Modified	Partially Supported	Does not support restoring the last modifying user.
	Opened	Unsupported	
	Share with people and groups	Supported	
	Get link	Partially Supported	If the original folder has been deleted, after the restore, the original shared link will be unavailable. The resolution is getting a new shared link to the restored folder.
			If you removed the target audience with who a folder was shared with, after the restore job is **Finished**, the target audience would be restored as a group, but this security change cannot be reported in job details due to Google API limitations.
	Color	Supported	
	Added to Starred/ Removed from Starred	Supported	
File (includes documents, images, audio, and videos)	Share with people and groups	Supported	
	Get link	Partially Supported	If the original file has been deleted, after the restore, the original shared link will be unavailable. The resolution is getting a new shared link of the restored file.
			If you removed the target audience with whom a file was shared with, after the restore job is **Finished**, the target audience would be restored as a group, but this security change cannot be reported in job details due to Google API limitations.
	Added to Starred/ Removed from Starred	Supported	
	Description	Supported	
	Owner	Supported	
	Labels	Supported	
	Created time	Unsupported	After the restore, the folder's created time will be updated to the restored time.
	Modified	Partially Supported	Does not support restoring the last modifying user.
	Opened	Unsupported	
	Version History	Unsupported	

Data Types		Support Status	Comments
File (includes documents, images, audios, and videos)	Google Docs	Supported	The format of comments and replies cannot be kept in the restored file. For Google Docs, Google Sheets, and Google Slides, the add-ons cannot be kept after the restore due to Google API limitations. You can manually insert add-ons after the restore.
	Google Sheets		
	Google Slides		
	Google Vids	Supported	
	Google Forms	Unsupported	
	Google Drawings	Unsupported	
	Google My Maps	Unsupported	
	Google Sites	Unsupported	
	Google App Scripts	Supported	
	Google Jamboards'	Unsupported	
	Shortcuts	Unsupported	
	Shortcuts of third-party apps	Unsupported	
	Files identified as malware or spam	Unsupported	
	Files which the current user has no permission to download or export	Unsupported	

Calendar Data Types

The table below lists data types that are supported or unsupported for Calendar recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types		Support Status	Comments
Calendar	Birthdays	Unsupported	
	Reminders	Unsupported	
	Tasks	Unsupported	
	Other calendars	Unsupported	
	Subscribe to calendar	Unsupported	
	Custom calendars	Supported	
	Hide from calendar list	Partially supported	The hidden calendar can be backed up but will be shown in the list after the restore.
	Calendar settings	Supported	
	Access permissions	Supported	Does not support backup and restore for the **Show calendar info in other Google apps, limited by access permissions** option due to Google API limitations.

Data Types		Support Status	Comments
	Share with specific people	Supported	
	Event notifications	Supported	If you set the content-level conflict resolution to **Merge**, after the restore, the notification settings will be replaced with the backup data.
	All-day event notifications	Unsupported	
	Other notifications	Supported	
	Integrate calendar	Unsupported	
	Auto-accept invitations	Unsupported	
Event types	Event	Supported	If an event was backed up in Calendar A before you move the event to Calendar B, and then you select the backup data to restore Calendar A to its original location, after the restore, the event will be moved from the Calendar B to Calendar A.
			If a calendar is restored to another location, the events on the destination calendar will not be associated with the original calendar.
	Focus time	Unsupported	
	Out of office	Unsupported	
	Working location	Unsupported	
	Task	Unsupported	
	Appointment slots	Unsupported	
	Recurring	Partially supported	“Notes for Events Restore” on page 110
Event details	Title	Supported	
	Event time	Supported	
	Time zone	Supported	
	Settings for repeat	Supported	
	Join with Google Meet	Unsupported	
	Join by phone	Unsupported	
	Location	Supported	
	notification	Supported	If you set the content-level conflict resolution to **Merge**, after the restore, the notification settings will be replaced with the backup data.
	color	Supported	

Data Types		Support Status	Comments
	Description	Supported	
	Linked attachments	Supported	Only Drive files are supported. After the restore, the links still work only when the files remain in Drive.
	Guest permissions	Supported	
	Rooms	Supported	
	Guest	Supported	"Notes for Events Restore" on page 110

Notes for Events Restore

Due to Google API limitations, you may encounter the following cases when you restore calendars with events.

Guest Cases

- After the restore, the replies of guests in groups cannot be kept.
- After the restore, the non-Google external users cannot view the restored events in their calendars.
- A guest's response to an event is **Yes, in a meeting room** or **Yes, joining virtually**. After the restore, the response status will be updated to **Yes**.
- You select the backup data of a guest in an event to **Restore the data to another location**. After the restore, the other guests of the event will not be restored in the destination event.
- An event was deleted from the organizer's calendar. You select a guest's backup data to **Restore the data to its original location**. After the restore, only the selected guest can view the restored event.
- An event was deleted from a guest's calendar. You select this guest's backup data to **Restore the data to its original location**. After the restore, the organizer's updates on the event can be synced to the restored event, but the guest's reply to the event cannot be synced to the organizer's calendar.
- A guest has the **Modify event** permission to an existing event in the calendar. You select the guest's backup data to **Restore the data to its original location** with the **Merge** conflict resolution. After the restore, the backup data will not be merged with the existing event.

Recurring Event Cases

- Backed up a calendar with recurring events. The deletion of a recurring event was applied to **This event** or **All events** on the calendar. You select the calendar backup data (contains the recurring events) to **Restore the data to its original location**. After the restore, the deleted events will not be restored to the calendar.
- The updates (any update except for the time) of a recurring event were applied to **This event** or **This and following events**. The updated events haven't been backed up. You perform a restore job to **Restore the data to its original location** with the **Merge** conflict resolution. After the restore, the updated events will not be merged with the backup data.
- The updates (any update except for the time) of a recurring event were applied to **This and following events**, and then the updated events have been backed up. Delete the following events, and then select the backup data to **Restore the data to its original location**. After the restore, the restored events will not be associated with the original recurring event.
- A recurring event was updated (any update except for the time) multiple times and the edits were applied to **This and following events**. Perform a restore job for an updated event to **Restore the data to another location**. After the restore, the restored event cannot keep the guests' original response statuses in the destination.

Contacts Data Types

The table below lists data types that are supported or unsupported for Contacts recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types		Support Status	Comments
Label	Custom labels	Supported	
	Starred	Supported	
	My contacts	Supported	
	Other contacts	Partially Supported	The items in **Other contacts** will be restored to **Contacts**.
			Only supports restoring the following properties: **Name**, **Email**, and **Phone number**.
Contact	All properties of contacts	Supported	

Note: If you perform a job to restore a created contact whose address is the Gmail address of an existing user, note the following issue:
When you edit the details of the restored contact, you will see multiple addresses and locations. This issue is due to Google will automatically add directory profile information to a contact that is directly created with an existing Gmail address.

Shared Drive Data Types

The table below lists data types that are supported or unsupported for Shared Drive recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types		Support Status	Comments
Shared drive	members	Supported	
	Shared drive settings	Supported	
	Trash	Supported	Supports backup and restore when the `Trash` folder is selected in **Backup Settings**.
	theme	Unsupported	
	Hidden	Unsupported	
Folder	Creator	Unsupported	
	Description	Supported	
	Created time	Unsupported	After the restore, the folder's created time will be updated to the restored time.
	Modified	Partially Supported	Does not support restoring the last modifying user.
	Opened	Unsupported	
	Share with people and groups	Supported	

Data Types		Support Status	Comments
	Get link	Partially Supported	If the original folder has been deleted, after the restore, the original shared link will be unavailable. The resolution is getting a new shared link to the restored folder.
			If you removed the target audience with whom a folder was shared with after the restore job is **Finished**, the target audience would be restored as a group, but this security change cannot be reported in job details due to Google API limitations.
	Color	Unsupported	
	Added to Starred/ Removed from Starred	Unsupported	
File (includes documents, images, audio, and videos)	Share with people and groups	Supported	
	Get link	Partially Supported	If the original file has been deleted, after the restore, the original shared link will be unavailable. The resolution is getting a new shared link of the restored file.
			If you removed the target audience with whom a file was shared with after the restore job is **Finished**, the target audience would be restored as a group, but this security change cannot be reported in job details due to Google API limitation.
	Added to Starred/ Removed from Starred	Unsupported	
	Description	Supported	
	Labels	Supported	
	Creator	Unsupported	
	Created time	Unsupported	After the restore, the folder's created time will be updated to the restored time.
	Modified	Partially Supported	Does not support restoring the last modifying user.
	Opened	Unsupported	
	Version History	Unsupported	
	Google Docs	Supported	The format of comments and replies cannot be kept in the restored file. For Google Docs, Google Sheets, and Google Slides, the add-ons cannot be kept after the restore due to Google API limitations. You can manually insert add-ons after the restore.
	Google Sheets		
	Google Slides		
	Google Forms	Unsupported	
	Google Drawings	Unsupported	
	Google My Maps	Unsupported	
	Google Sites	Unsupported	

Data Types		Support Status	Comments
	Google App Scripts	Supported	
	Google Jamboards	Unsupported	
	Shortcuts	Unsupported	
	Files identified as malware or spam	Unsupported	

Classroom Data Types

The table below lists data types that are supported or unsupported for Classroom recovery in IBM® Storage Protect for Cloud Google Workspace.

Data Types			Support Status	Comments
Class	Status	Active	Supported	
		Archive	Supported	The restored classes will be in the Active status.
		Deleted	Unsupported	
	Class Details	Class name	Supported	
		Class description	Supported	
		Section	Supported	
		Room	Supported	
		Subject	Unsupported	
		Customize appearance	Unsupported	
	General	Invite Codes	Unsupported	
		Stream	Unsupported	
		Classwork on the Stream	Unsupported	
		Show deleted items	Unsupported	
		Guardian summaries	Supported	
		Meet link settings	Unsupported	
	Grading	Overall grade calculation	Unsupported	
		Show overall grade to students	Unsupported	
		Grade categories	Unsupported	
Announcement	Status		Supported	
	Text		Partially Supported	Format cannot be kept in the restored contents.

Data Types			Support Status	Comments
	Creator		Supported	The restored Creator content will be appended with a suffix. If using the default service app, the suffix is **via IBM® Storage Protect for Cloud**. If using a custom Google app, the suffix depends on the project's **OAuth consent screen** value. Without this value, the suffix will be displayed as **via Unknown**.
	Assigned to		Supported	
	Created time		Unsupported	
	Updated time		Unsupported	
	Scheduled time		Supported	
	Attached files		Partially Supported	Support backup and restore for the files in the `Classroom` (default name) folder of the class owners' / students' My Drive. The other attached files cannot be backed up, and they will be unavailable after the restore if the original files have been deleted.
	Comments		Unsupported	
Classwork	Common properties	Title	Supported	
		Instructions	Partially Supported	Format cannot be kept in the restored contents.
		Creator	Supported	The restored Creator content will be appended with a suffix. If using the default service app, the suffix is **via IBM® Storage Protect for Cloud**. If using a custom Google app, the suffix depends on the project's **OAuth consent screen** value. Without this value, the suffix will be displayed as **via Unknown**.
		Status	Supported	
		Assigned to	Supported	
		Created time	Unsupported	
		Updated time	Unsupported	
		Scheduled time	Supported	
		Due date	Supported	
		Grade category	Unsupported	

Data Types			Support Status	Comments
		Points	Supported	
		Topic	Supported	
		Rubric	Unsupported	
		Classwork comments	Unsupported	
		Private comments	Unsupported	
		Attached files	Partially Supported	Support backup and restore for the files in the `Classroom` (default name) folder of the class owners' / students' My Drive. The other attached files cannot be backed up, and they will be unavailable after the restore if the original files have been deleted.
Classwork	Assignment	Student work	Unsupported	
		Permission of attached files	Supported	
	Quiz assignment	Quiz form	Unsupported	
		Grade importing setting	Unsupported	
	Question	Short answer	Supported	
		Multiple choice	Supported	
		Students can reply to each other	Unsupported	
		Students can edit the answer	Supported	
		Students can see class summary	Unsupported	
		Students’ answer	Unsupported	
	Material	Attached files	Partially Supported	Support backup and restore for the files in the `Classroom` (default name) folder of the class owners' / students' My Drive. The other attached files cannot be backed up, and they will be unavailable after the restore if the original files have been deleted.
	Associated app	Google Calendar	Unsupported	
		Google Drive folder	Supported	
People	Teacher		Supported	
	Student		Supported	
	Mute/Unmute students		Unsupported	
	People in the Invited status		Unsupported	
Drive	Folder	Properties	Supported	
		Permissions	Unsupported	
	File	Properties	Supported	

Data Types			Support Status	Comments
		Content	Supported	
		Permissions	Unsupported	

Notices

This information was developed for products and services offered in the US. This material might be available from IBM® in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM® representative for information on the products and services currently available in your area. Any reference to an IBM® product, program, or service is not intended to state or imply that only that IBM® product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM® intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM® product, program, or service.

IBM® may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM® Intellectual Property Department in your country or send inquiries, in writing, to:
Intellectual Property Licensing
Legal and Intellectual Property Law
IBM® Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM® may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM® websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM® product and use of those websites is at your own risk.

IBM® may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:
IBM® Director of Licensing
IBM® Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM® under terms of the IBM® Customer Agreement, IBM® International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM® products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM® has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM® products. Questions on the capabilities of non-IBM® products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM®, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM®, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM® shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM® Corp. Sample Programs. © Copyright IBM® Corp. _enter the year or years_.

Trademarks

IBM®, the IBM® logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM® or other companies. A current list of IBM® trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe™ is a registered trademark of Adobe™ Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open™, LTO™, and Ultrium™ are trademarks of HP, IBM® Corp. and Quantum in the U.S. and other countries.

Intel™ and Itanium™ are trademarks or registered trademarks of Intel™ Corporation or its subsidiaries in the United States and other countries.

The registered trademark Linux® is used pursuant to a sublicense from the Linux® Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft™, Windows™, and Windows NT™ are trademarks of Microsoft™ Corporation in the United States, other countries, or both.

Java™ and all Java™-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Red Hat®, OpenShift®, Ansible®, and Ceph® are trademarks or registered trademarks of Red Hat®, Inc. or its subsidiaries in the United States and other countries.

UNIX® is a registered trademark of The Open Group in the United States and other countries.

VMware, VMware vCenter Server™, and VMware vSphere™ are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM® website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM®.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM®.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.
IBM® reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM®, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM® MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM® Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM®’s Privacy Policy at http://www.ibm.com/privacy and IBM®’s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM® Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.