How to configure and use CloudM Backup

CloudM Backup - BETA

Early Access

Table of Contents

Introduction **2**

Prerequisites **3**

Google Cloud Storage Setup **4**

Obtaining the Service Account Key File 4

Creating a Key Ring and Key 4

Creating a Bucket 5

Adding permissions to the Bucket 6

Create and assign a role in CloudM Manage **7**

Create an Archive Admin Role 7

Assign the Archive Admin Role to a user 10

Configuring Archive in CloudM Manage **12**

Adding the Archive step to an Offboarding Workflow **13**

Using Archive in CloudM Manage **14**

How to archive a user's email and drive data 15

How to restore user email and drive data to an account 16

How to abort a restoration 18

How to set the Retention Policy 19

How to use the Status screen 20

Troubleshooting **22**

The Archive step in the offboarding workflow has failed 22

A Restoration process has failed 22

File Type Conversion - Google documents **23**

Support **23**

Introduction

Whether for compliance with regulations such as GDPR, HIPAA, FOI requests or for potential future legal disputes, having a robust data retention solution is essential for modern businesses.

CloudM Archive is a new module, as part of the CloudM platform, that will migrate the Mail and/or Drive data of offboarded users to customer owned cloud storage and allow you to quickly restore the data back into your domain as required, providing you with an all-in-one solution which is simple, secure, and affordable.

Prerequisites

- Access to Google Cloud Platform (GCP) via https://console.cloud.google.com/
- A valid GCP Billing Account
- A new Customer owned GCP Project with the above Billing Account assigned to it
- A GCP Service Account created in the above Project
- Enable the **Cloud Key Management Service (KMS) API** if not already enabled
    - Search for KMS in the search field, or select **Security** > **Cryptographic Keys**
    - If presented with a screen to enable API, click **Enable**
- Google Cloud Storage
    - Please refer to our Google Cloud Storage recommendations documentation.
- CloudM Automate
- CloudM Backup (enabled by a CloudM representative)

Google Cloud Storage Setup

Prior to attempting these steps, please ensure that you have purchased and configured Cloud Storage, to meet your storage requirements, in accordance with instructions provided by Google here.

Obtaining the Service Account Key File

1. Go to https://console.cloud.google.com/
2. Ensure your project is set at the top of the screen.
3. To create the Service Account Key File, go to **IAM & Admin** > **Service Accounts** from the left menu
4. Go to any active service account (preferable) or create a new one.
5. Select **Add Key** > **Create New Key** > **JSON**
    - You will need to upload the Service Account JSON key file later when configuring the Archive feature in CloudM Manage. Keep the file confidential as it allows full access to your archive.

Creating a Key Ring and Key

1. Search for KMS in the search field, or select **Security** > **Cryptographic Keys**
2. Create a new Key Ring. The name can be set to the same as the bucket name.
3. Ensure the keyring location matches the bucket location (europe-west1 or us-central1), and remember which location you set as you will need it when configuring Archive in CloudM Manage
4. Click **Next**,
5. On the Create Key screen, use the same Key name as the Key ring name (optional),
6. Leave all the other settings as default except **Rotation Period**,
7. Set **Rotation Period** to **Never (manual rotation)** and select **Create**.
8. Copy the **Resource name** of the KMS key that you have just created (by selecting the 3 dot ellipsis under **Actions** and clicking **Copy resource name**)

- You will need the **Resource name** later to configure the Archive feature within CloudM Manage.

The key ring and key are used to encrypt the blob storage and should not be removed or deleted at any point. If they are removed or deleted, the blobs in the storage bucket will become inaccessible.

Creating a Bucket

1. From the left menu, go to **Storage** > **Browser** and select **Create Bucket** > **Set to specific region** (europe-west1 or us-central1), as set in step 3 of the Creating a Key Ring section above.
2. Name the bucket something unique and relevant.
3. Leave all settings to default except for **Advanced Settings**,
4. Under **Advanced Settings**, select **Google-managed key** in the **Encryption** section,
5. Click **Save** to create the Bucket.

Adding permissions to the Bucket

The owner is the only one with permissions to add members, and you will need someone to do this for you if you do not have the relevant permissions.

1. Go to **IAM & Admin > Service Accounts** and select the service account that you created the Service Account JSON key file on,
2. Copy the **Email** address in the **Service account details** section,
3. Go to **Storage** > **Browser** and then select the bucket you created earlier,
4. Click on the **Permissions** tab and select **Add a permission**,
5. Paste the email from step 1 in to the members field,
6. Add **Storage Admin** and **Storage Object Admin** roles and **Save**,
7. Go to **Storage** > **Settings**,
8. Copy the **Service Account** email (under the **Cloud Storage Service Account** section) and add the roles in the previous step to this email as well,
9. Click on the KMS key you created in **Security** > **Cryptographic Keys**. On the next page, where only the specified KMS Key should be listed, click on it again.
10. Click on **Permissions** > **Add Member**, in the panel on the right side of the screen.
    - Click on the **Show Info Panel** option if you cannot see the panel.
11. The **Storage Service Account** email will also need to be added here as a member,
12. Add the role **Cloud KMS CryptoKey Encrypter/Decrypter** and select **Save**.

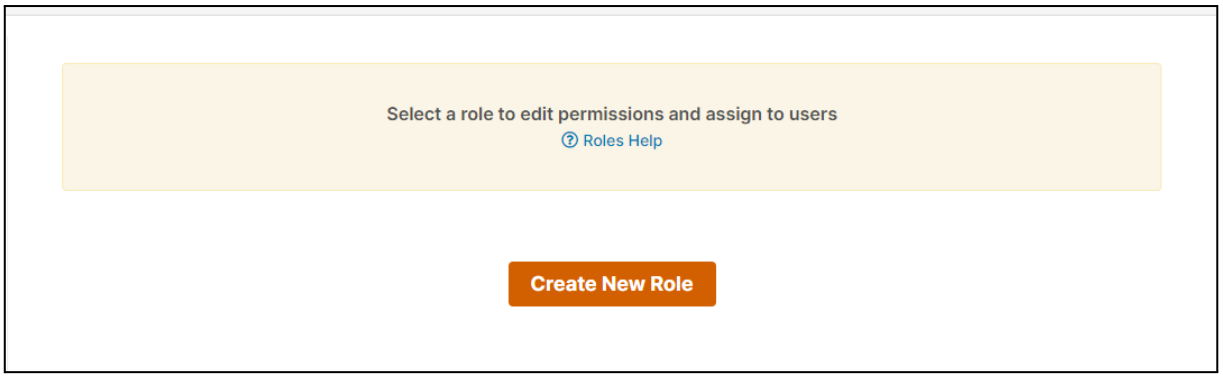
Create and assign a role in CloudM Manage

Create an Archive Admin Role

You can add the required permissions to any existing role. However, we recommend creating a new role so that you have more control over which users can view archived data and restore, if required.

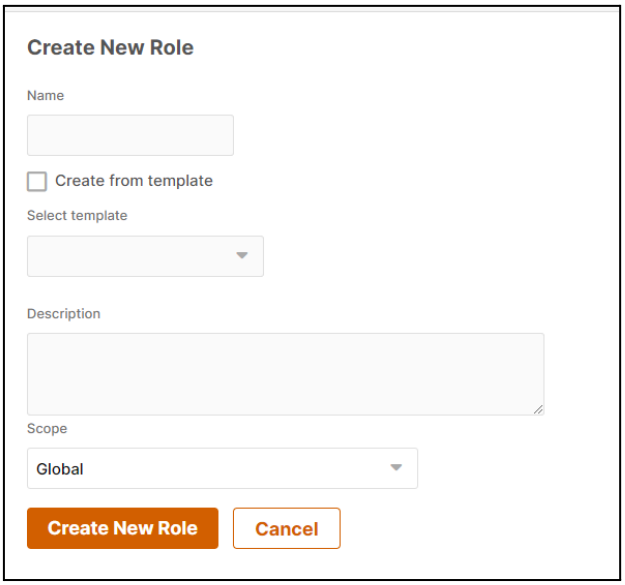
To create an Archive Admin role:

1. Sign in to CloudM Manage, using an account with permission to manage other users.
2. Select **Settings** > **Roles**.
3. Click on **Create new Role**.
    - If you cannot see the **Create new Role** option, select the **x** button at the top of the screen.

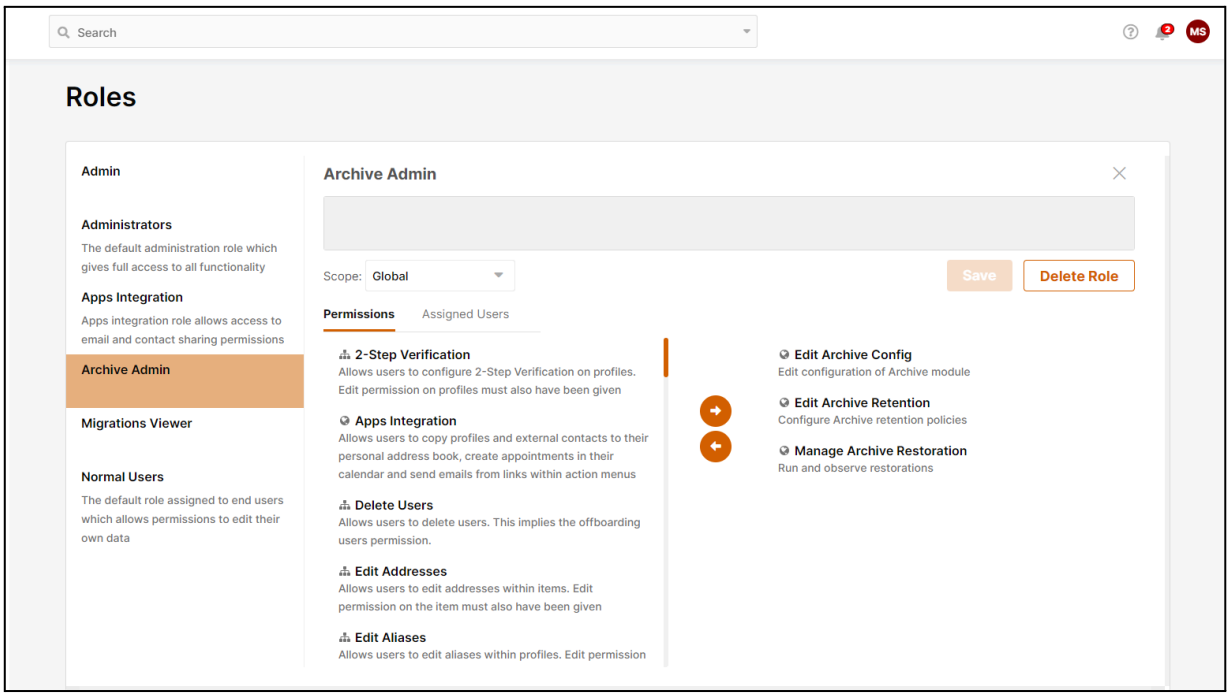


4. Set the **Name** of the new role to Archive Admin.
5. Leave the **Create from template** checkbox unticked.
6. Add a **Description** of the Archive Admin role, if required.
7. Assign the **Scope** of the new role to **Global** to apply to the whole organization.

8. Select **Create New Role**.



9. The **Archive Admin** role will now appear in the list of roles.
10. Select the role from the list.
11. On the **Permissions** tab, scroll down to each of the required permissions (Edit Archive Config and Manage Archive Restoration) in the **Unused Permissions** column (on the left) and use the right arrow to move it into the **Assigned Permissions** column (on the right).
    - The **Edit Archive Retention** permission allows assigned users to change the data retention policy for the domain. This means that they can specify the amount of time that data (Mail or Drive) will be stored before it is automatically purged (permanently deleted) from Archive.
      - You can add the permission to the Archive Admin role if you want to allow all assigned users to carry out this task, or you may want to apply this permission to a Domain / Root Administrator role to limit its usage.
    - Permissions can be applied to any other role or role template, if required, and will only be visible after the Archive option has been enabled for your domain by CloudM.

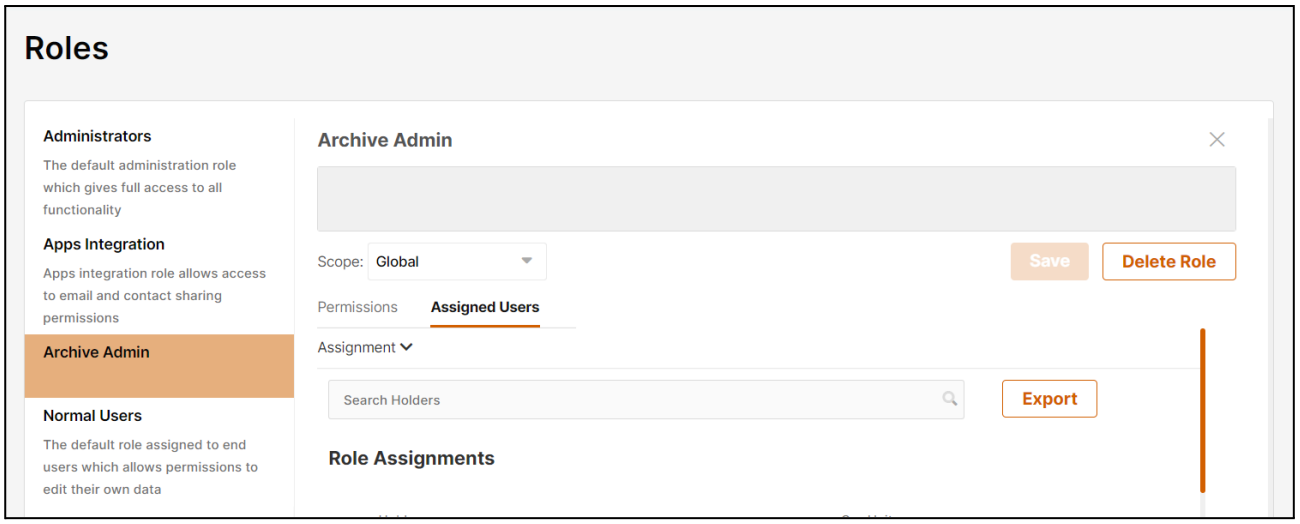


12. Select **Save** to confirm the changes.

Assign the Archive Admin Role to a user

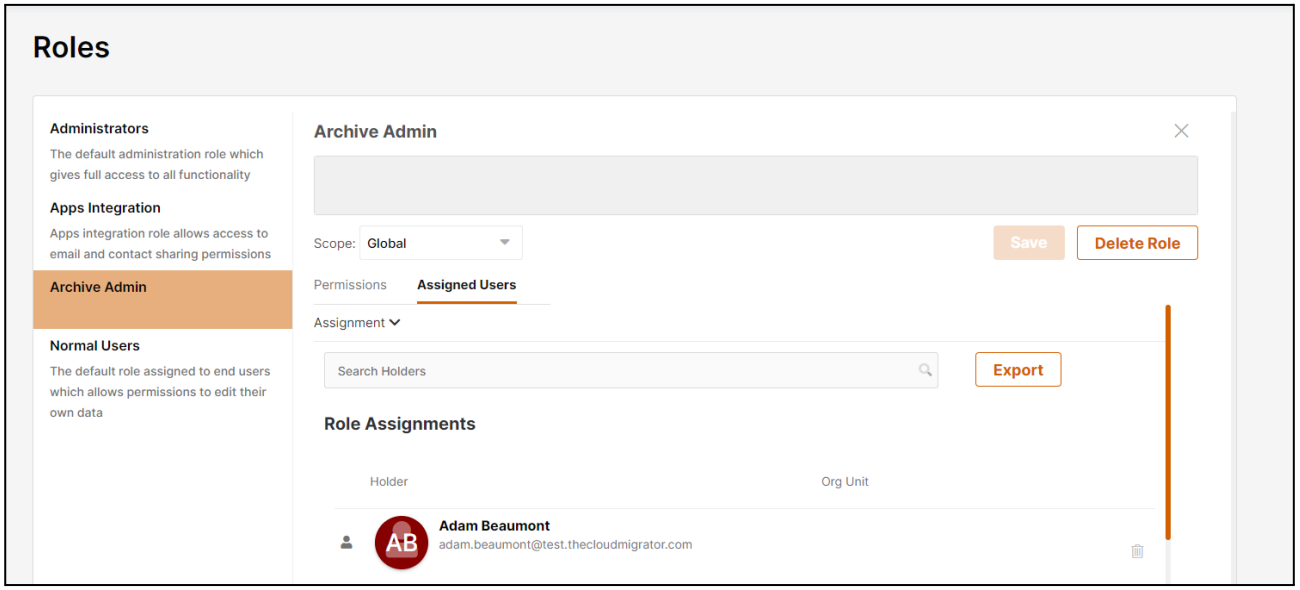
To assign the Archive Admin role to a user or users:

1. Select the role from the list,
2. On the **Assigned Users** tab, click on the downwards facing arrow next to Assignment. This will prompt the Assignment section to be displayed.
3. Click on the **Assign To** field and choose whether you are assigning the role to an Org Unit, User Profile, Group, Service Account, External Profile or External Group.
4. Click on the **Name** field to choose the name of the Holder that you want to apply the role to.
5. Set **Org Unit** to the top level Organizational Unit / domain.



6. Click on **Add**.

7. The Holder will appear in the **Role Assignments** list. This list shows all the holders that are assigned to the selected role.

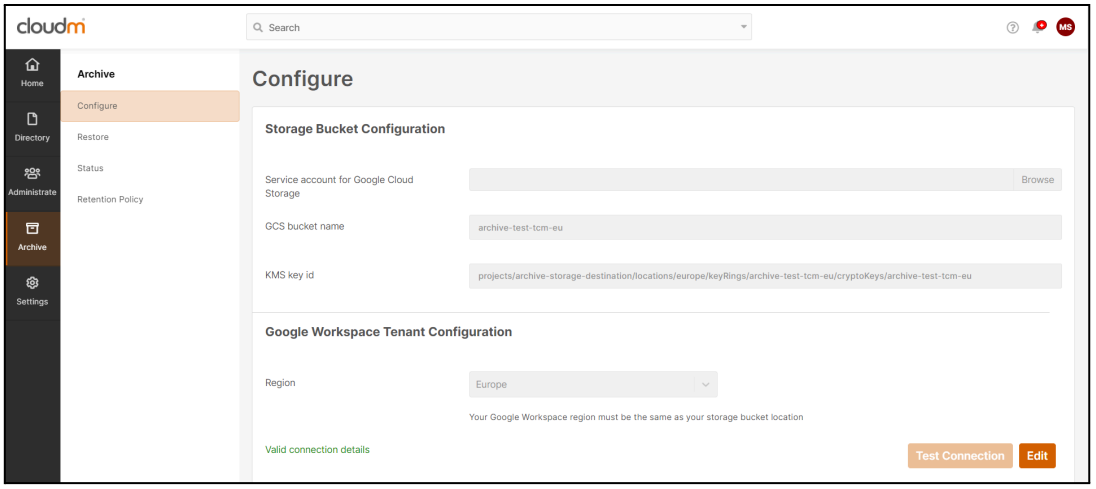


8. Once the role is assigned to a user, they will see the **Archive** option displayed in the **Functions** bar (which is persistently displayed on the left side of the screen)

Configuring Archive in CloudM Manage

Now that you have set up the required settings in the Google Cloud Platform and assigned Archive permissions in CloudM Manage, you will be able to access and configure the Archive feature in the CloudM Manage platform.

1. Sign in to CloudM Manage (using a user / admin with the required Archive permissions) and select the **Archive** option that is now visible in the Function column (on the left side of the screen)
2. In the Sub-option column, select **Configure**.

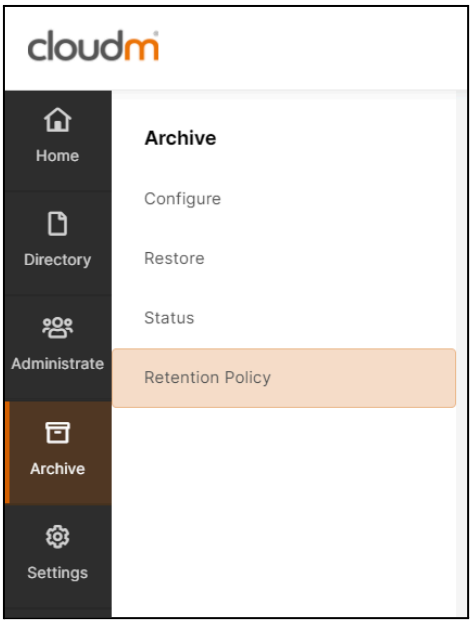


3. Upload the Service Account JSON key into the **Service Account for Google Cloud Storage** field.
4. Enter the bucket name (as created earlier) into the GCS bucket name field.
5. Paste the **Resource name** into the **KMS Key ID** field.
6. Ensure that the **Region** is set to the same region that you specified when creating the bucket.
7. Select **Test Connection** to check that the connection details are valid.
    - If the credentials entered do not match the bucket name, you will be notified of the error and should rectify before testing the connection again.
    - If the connection test continues to fail, check all steps relating to setting up Google Cloud Storage, ensuring that all permissions are enabled and credentials have been properly configured and added to CloudM Manage without error.
8. Select **Save** to confirm.

Using Archive in CloudM Manage

Now that the role has been defined and assigned to a user or users, the **Archive** button will become visible in the navigation menu. If a user is signed into CloudM Manage when the role is assigned to them, they may need to refresh their page to view the option.

Selecting the **Archive** button will prompt a list of the following options to be displayed (depending on the permissions assigned):

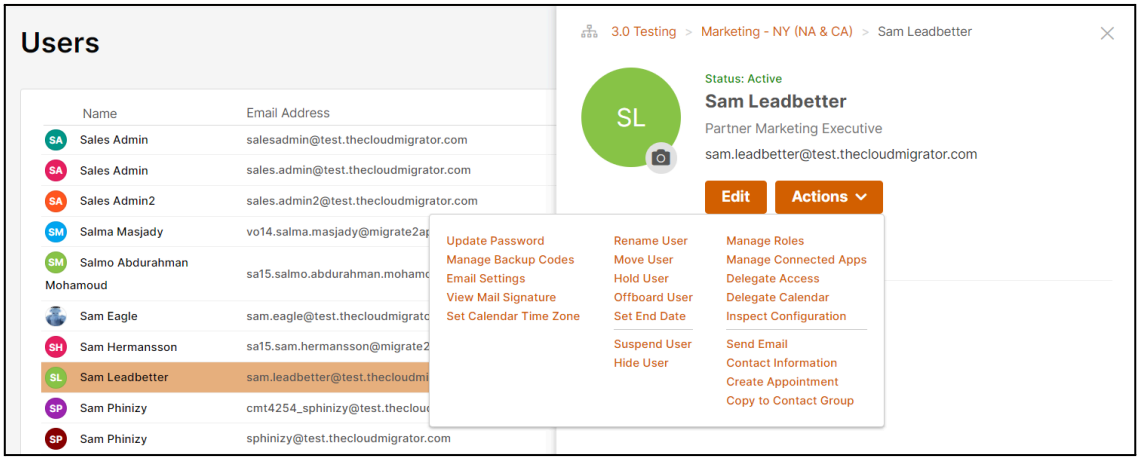


- **Configure** - You have already completed the initial configuration in the Configuring Archive in CloudM Manage section above.
    - If you need to change the storage bucket that CloudM Manage will archive to and restore from, you can select Edit and enter the updated settings.
- **Restore** - You can view all archived users and their data here.
- **Status** - You can view information on all archive and restore processes that have been attempted, including the name of the archived user, the date that the process was started, the type of data migrated, the executor of the process and the status of the process (e.g. Completed, Aborted, Failed).
- **Retention Policy** - You can set the number of days that email data and drive data will be stored in Archive before it is automatically purged (permanently deleted) from the system.

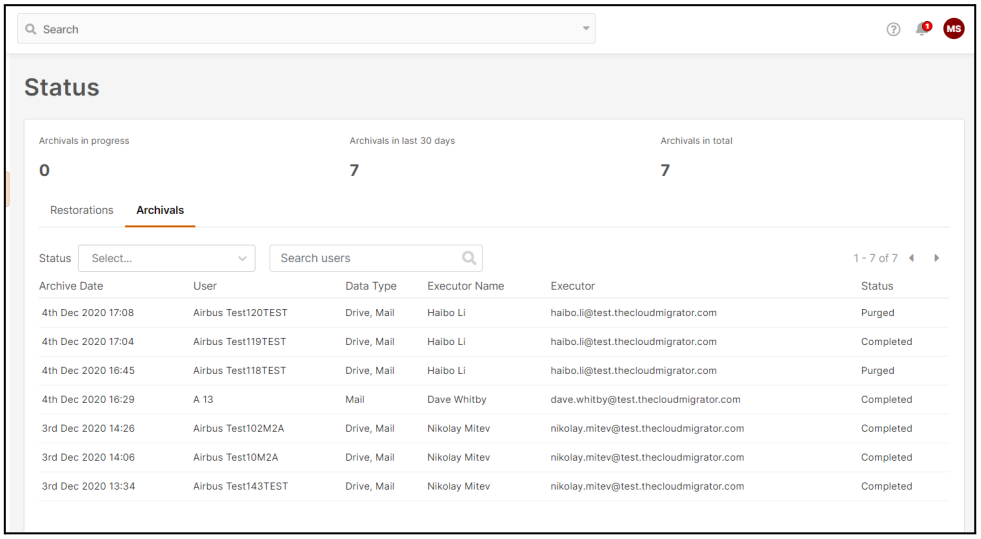
How to archive a user's email and drive data

To archive a user's email and drive data (as part of offboarding):

1. On the **Directory** > **Users** screen, search for the user that you want to offboard.
2. Once you have found them, click on the row to show their user profile.
3. Select **Actions** > **Offboard User**.



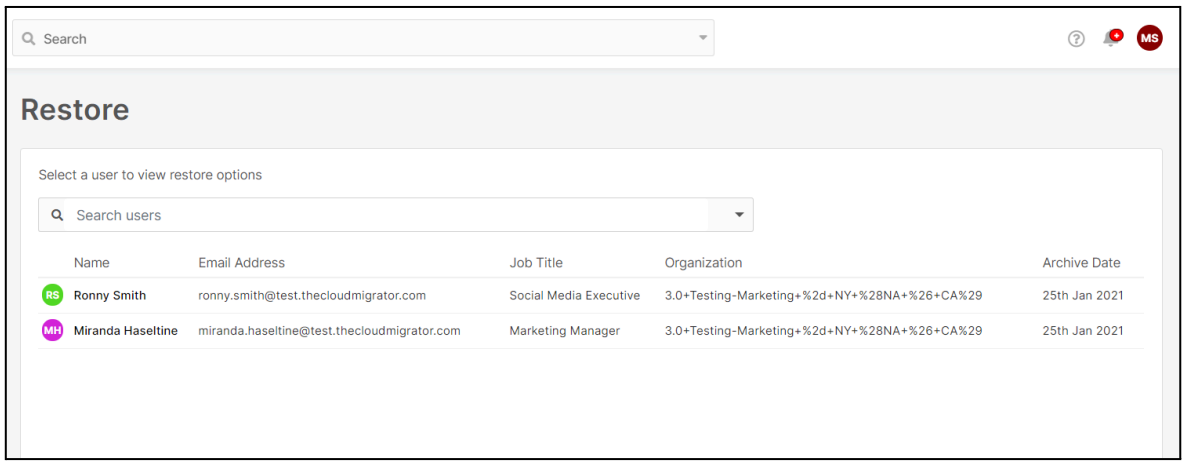
4. The user will be offboarded according to the Offboarding Policy assigned to them (either as a member of an Organizational Unit or a Smart Team).
5. Once the user has been offboarded, select **Archive** > **Status** and then select the **Archivals** tab. You will see the process listed in the table and can view whether it was successful, aborted or failed.



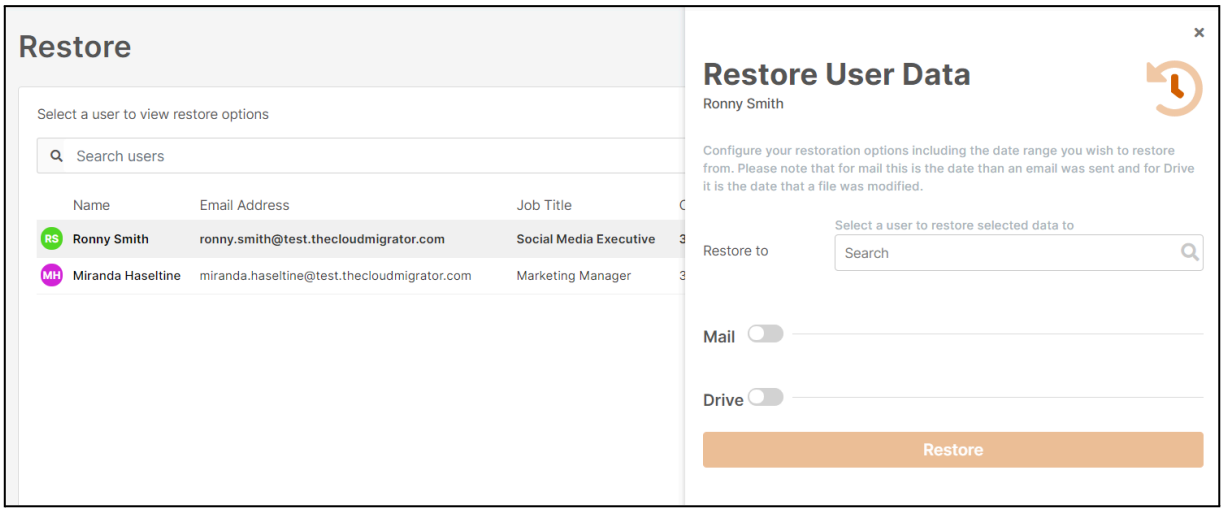
How to restore user email and drive data to an account

To restore data to a current CloudM Manage user:

1. In CloudM Manage, select **Archive** > **Restore**.
2. You will see a table of all user data currently stored in the Google Cloud Storage bucket.

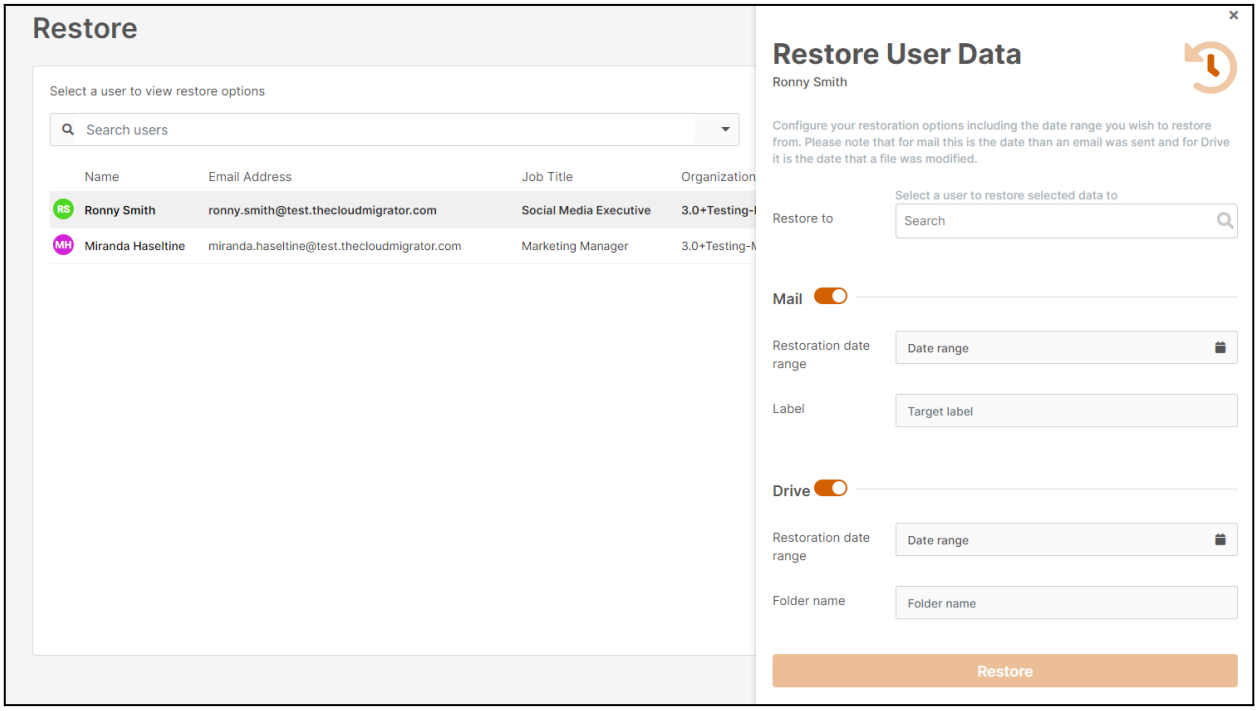


3. Select the name of a user to view the restore options for their data (displayed in a pop in side screen),



4. In the **Restore to** field, enter the name of the current CloudM Manage user that you want to send the data to. As you enter characters, the results will automatically be filtered.

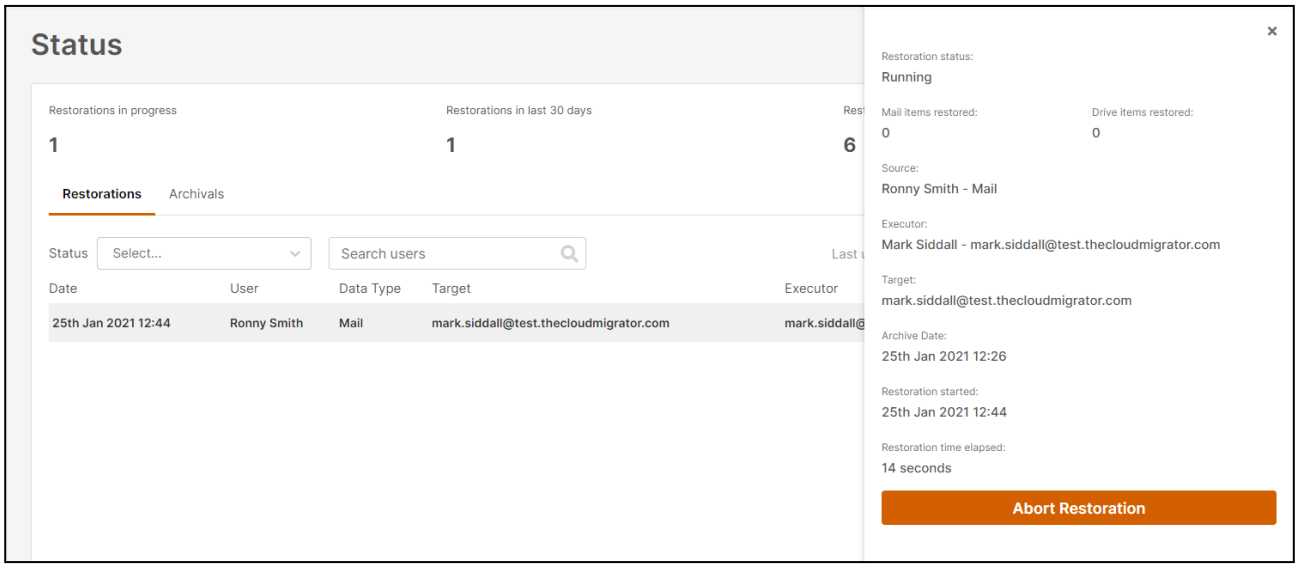
5. Select whether to restore Mail and / or Drive data by moving the pill button to enabled (colored) or disabled (grey).
    - If an option is not visible, this means that either the data wasn't archived at the point of offboarding, or the data has been purged in line with the data retention policy.



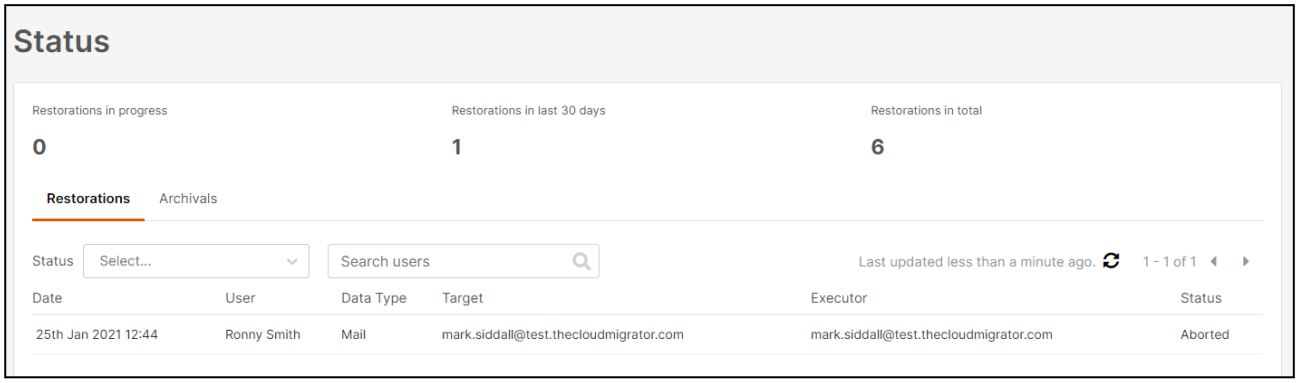
6. Select the **Restoration date range** using the pop up calendar, or leave as default to restore all data. You may only want to restore data from the past 2 or 3 months only, instead of all data, for example.
    - Under Mail, you can set a label that will be added to all restored emails, making it easier to search for them.
    - Under Drive, you can set a folder name that all documents will be restored to within the target account.
7. Once all fields are set, select the **Restore** button to start the process.
8. You can follow the progress on the **Restorations** tab in **Archive** > **Status**. The Status field will change from Running to Completed once finished.

How to abort a restoration

1. On the Restorations tab in **Archive** > **Status**, click on the row of any restoration that is currently Running.
2. Select **Abort Restoration**.



3. Select **Yes** in the Warning prompt to confirm that you want to abort the restoration.
    - Any files that have already been restored prior to this point will remain in the target account.
4. The Status will change from Running to Aborted in the table.



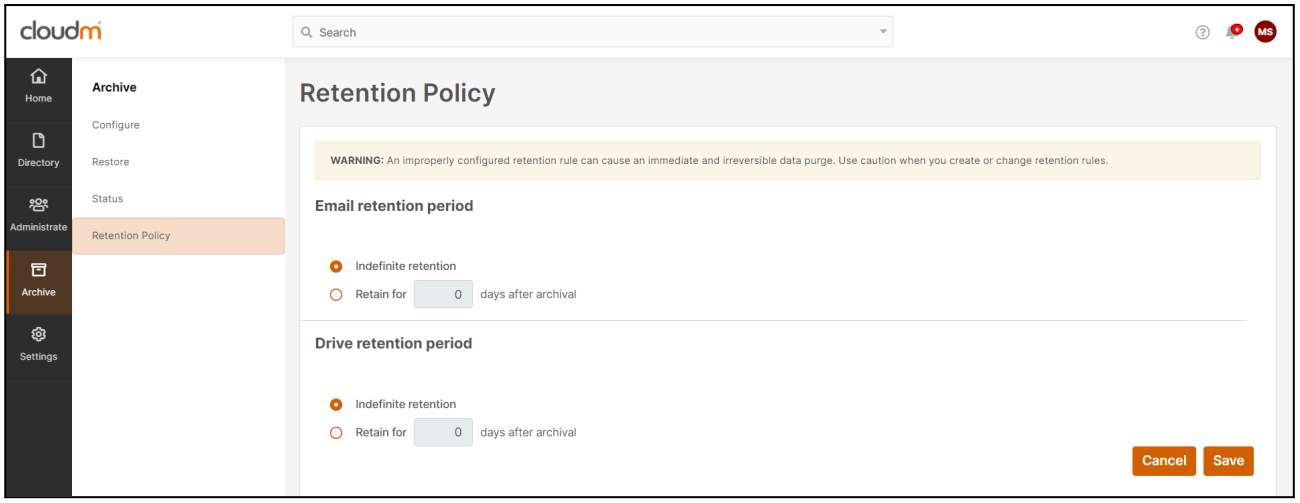
How to set the Retention Policy

Firstly, this process is potentially dangerous (as it can permanently delete all archived data if it is not configured correctly) and should only be carried out by Archive Administrators.

You can set the maximum amount of days that any data can be stored in Archive before it will be purged (permanently deleted) in line with data compliance policies (such as GDPR). You can set different values for Mail and Drive data.

To set the retention policy:

1. Sign in to CloudM Manage with a user that has been assigned the **Edit Archive Retention** permission.
2. Select **Archive** > **Retention Policy**
3. Select **Edit**



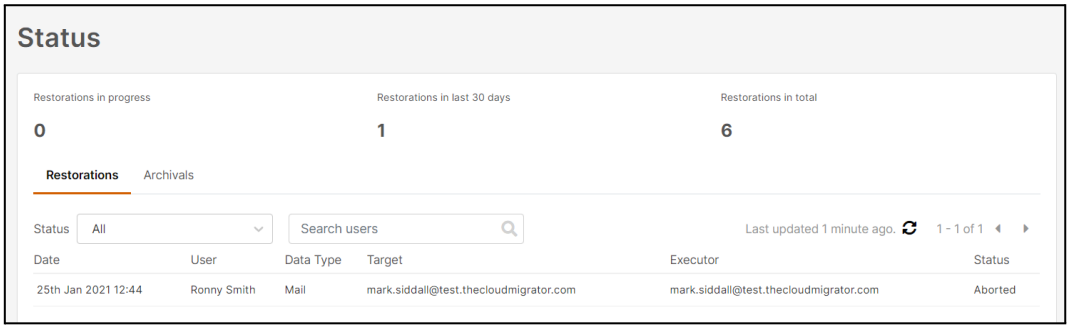
4. Edit the values for Email and Drive retention and ensure the option is selected.
    - If you do not want to set a definitive retention period, select **Indefinite Retention**.
5. Select **Save** to confirm any changes.

How to use the Status screen

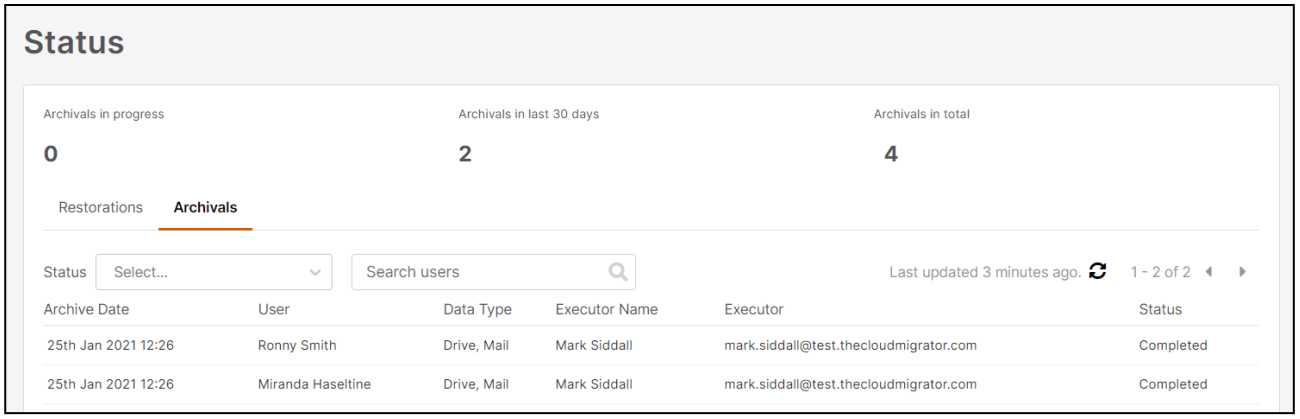
The Status screen allows you to view information about any process that has taken place via the CloudM Archive, either as data being stored (Archivals) or data being restored to CloudM Manage (Restorations). It is purely informational and you cannot use it to restore or archive any data.

To view the Status screen:

1. Sign in to CloudM Manage using an account that has Archive permissions assigned.
2. Select **Archive** > **Status**.
3. Choose whether you want to view **Archivals** or **Restorations** by selecting the relevant tab.
4. At the top of each tab, you will see an overview that displays the number of processes of the selected type currently in progress, completed in the last 30 days and completed in total.
5. Below the overview, you will see a table of all the processes of the selected type, listed from the latest to the earliest. Fields include:
    - **Restorations tab**
        - **Date** - The date that the restore process was started
        - **User** - The name of the CloudM Manage user that the data was archived from.
        - **Data Type** - The type of data (Mail, Drive or both) that was restored, as part of the process.
        - **Target** - The CloudM Manage user that the data was restored to.
        - **Executor** - The CloudM Manage user that started the restore process.
        - **Status** - The status of the process (Running, Completed, Aborting, Aborted, Failed, Purging, Purged, Purge Failed).



- **Archivals tab**
  - **Archive Date** - The date that the data was archived.
  - **User** - The name of the CloudM Manage user that the data was archived from.
  - **Data Type** - The type of data (Mail, Drive or both) that was archived, as part of the process.
  - **Executor Name** - The name of the CloudM Manage user that started the Offboarding process.
  - **Executor** - The CloudM Manage user that started the Offboarding process.
  - **Status** - The status of the process (Running, Completed, Aborting, Aborted, Failed, Purging, Purged, Purge Failed).



6. You can filter the results by either Status or by searching for a specific user.
7. Clicking on a row will prompt an informational panel to be displayed for the specific process, including the number of Mail and Drive items that have been either archived or restored.

Troubleshooting

The Archive step in the offboarding workflow has failed

If the Archive step has failed for a user, as part of the offboarding policy associated to the user:

1. Navigate to **Administrate** > **Offboarding Status**,
2. Select the **In Progress** tab,
3. If you have a lot of results displayed in the **In Progress** tab, change the **Status** filter from **All** to **Failed**,
4. You will see a table of all the offboarding processes that have failed, and at which step they failed at,
5. Click on the name of a user to prompt an informational panel to be displayed,
6. Select **Retry**,
7. If the step continues to fail, check that the configuration settings are correct in **Archive** > **Configure**, and **Test Connection**.

A Restoration process has failed

If a restoration process has failed:

1. Navigate to **Archive** > **Status**,
2. Select the **Restorations** tab,
3. If you have a lot of results displayed in the **Restorations** tab, change the **Status** filter from **All** to **Failed**,
4. You will see a table of all the restoration processes that have failed,
5. Click on the name of a user to prompt an informational panel to be displayed,
6. Select **Retry**.

File Type Conversion - Google documents

Documents that are created in Google Workspace applications will be converted to the following Microsoft Office formats when migrated:

File Type	Exported Format
Google Docs	.docx
Google Sheets	.xlsx
Google Forms	.zip (.html and .csv)
Google Slides	.pptx
Google Drawings	.pdf
Non-Google Files	No format change

Support

If you encounter any issues or errors whilst using the Backup feature, please raise a Support ticket as normal. Our dedicated Support team will process your ticket in accordance with your current Service Level Agreement (SLA).

Please note that, for the early access period, Backup articles will not be available in the Knowledge Base or in the in-software help widget.