User Guide

Google Shared Drives Backup & Recovery

GD UG-CE 25.1

Table of Contents

Third-Party Trademarks

1 Preface

1.1 About This Guide

Thank you for selecting CloudAlly for Google Shared Drives. Relax! All your Google Shared Drives data is now securely protected with easy recovery from data loss. CloudAlly comprehensively backs up your data on industry-leading AWS S3 storage. Our product's ethos is to provide feature-rich backup and recovery with security, ease of use, and flexibility woven in.

CloudAlly is cloud-native, a full cloud-to-cloud solution. No installation is required, the setup is hassle-free, backup is easy, and there are flexible recovery and export options. Read on for instructions about how to activate and manage your backups, restore your data by keyword, from any point-in-time, and at any granular/hierarchical level, export your backups to your own storage, activate summary/exception reporting, and set up MFA and other helpful features.

Questions or comments? Please contact us at support@cloudally.com or search our Knowledge Base at https://support.cloudally.com/hc/en-us.

1.2 Audience

This guide is intended for individuals who administer CloudAlly for Google Shared Drives.

1.3 What's in This Guide

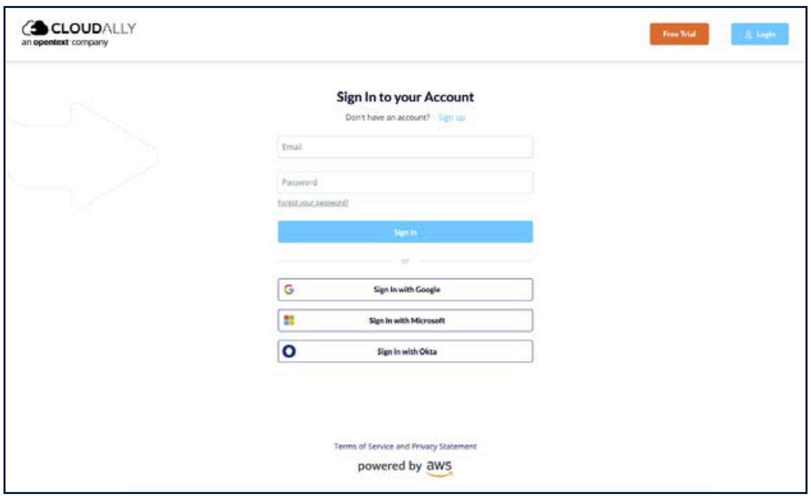
This guide is organized to help you find the information you need to manage CloudAlly for Google Shared Drives. It is divided into functional parts intended to support you as you manage your environment:

- Creating and Accessing Your Backup Account
- Backing Up Your Data
- Recovering Your Backed Up Data
- Filtering and Viewing Drill-Down Details
- Managing Your Account
- Managing Subscriptions and Payments

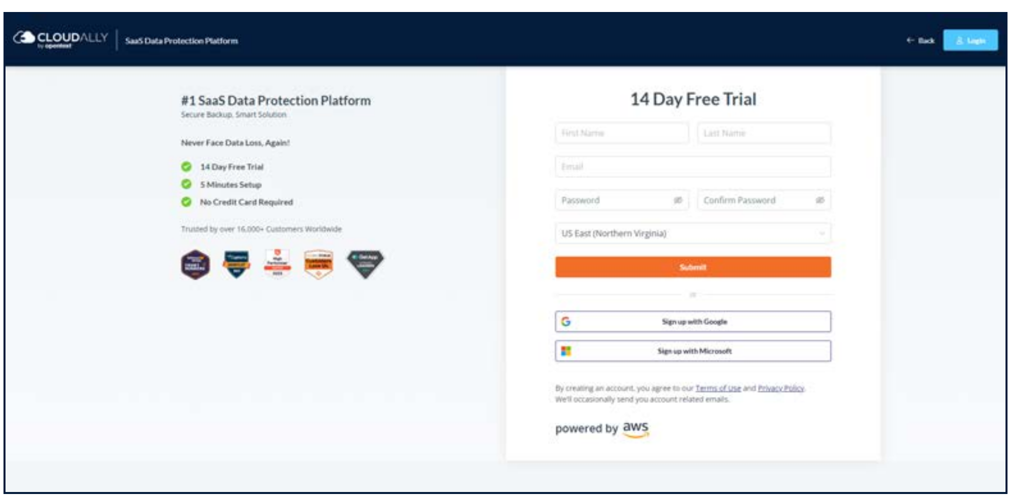
2 Creating and Accessing Your Backup Account

2.1 Sign Up/Sign In from the CloudAlly Home Page

1. In your Internet browser, open cloudally.com and click **Login**.
2. Click **Customers**. The *Sign In* page is displayed.



3. If you don't have an account yet, click **Free Trial.** The *Sign Up* page is displayed.



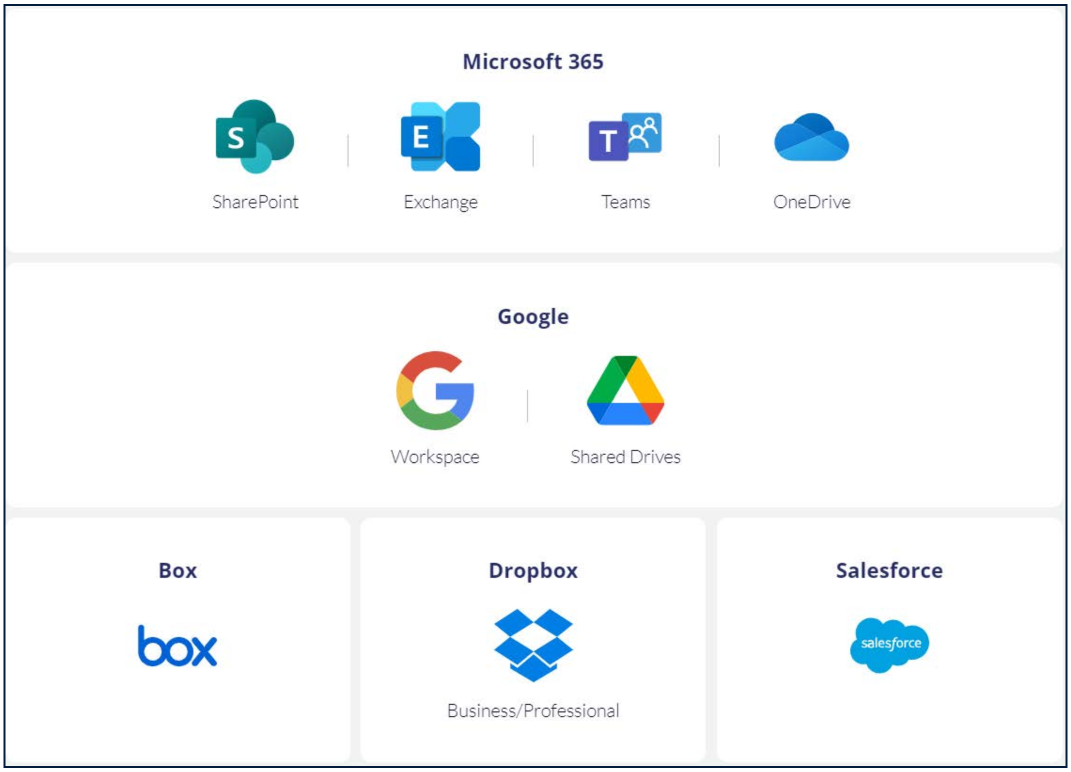
4. Complete the form, and then click Sign up.

> **Note:** CloudAlly gives you the choice of numerous AWS data centers available in the dropdown menu "Location." These include locations in Australia, Canada, EU (France, Germany, and Ireland), US, UK, South Africa, India, Japan, and Switzerland. The ability to choose from a wide range of data centers helps our customers comply with local data sovereignty laws that regulate the physical location and movement of data. In addition, we also offer a "Bring Your Own Storage" (BYOS) option on request. This allows you to backup sensitive data in your own AWS S3 buckets, S3 compatible storage service, Azure, or Google Cloud Platform. Please contact support@cloudally.com for more information.

5. Your trial account is created, and an email containing your activation link is sent to your email address. Click on the activation link contained in the email you received to activate your account. If you sign up with Google, Azure, or Okta, the activation link will not be sent to you.
6. Once your account is activated, you are redirected to the CloudAlly *login* page. Enter your email address/password and click **Sign In** to login and access your account.

> **Note:** You can also enable Two-Factor authentication to provide additional security. For more information, see Managing Your Account .

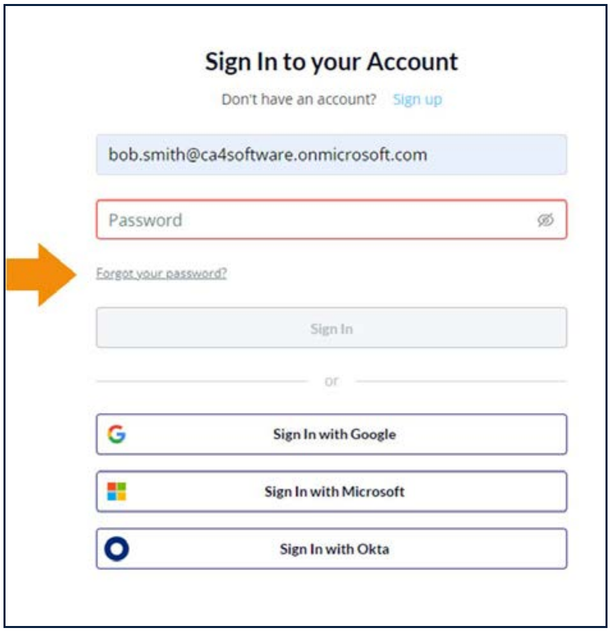
7. After you log in, you will see the following screen, enabling you to begin creating your backup tasks:



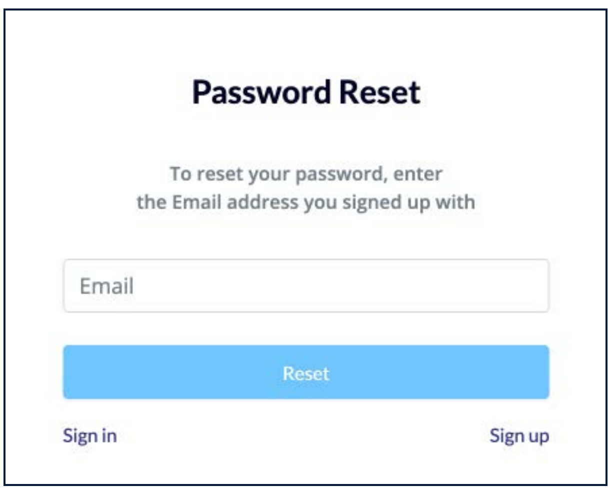
2.2 Resetting Your Password

If you do not remember your password, you can easily reset it using the **Password Reset** function.

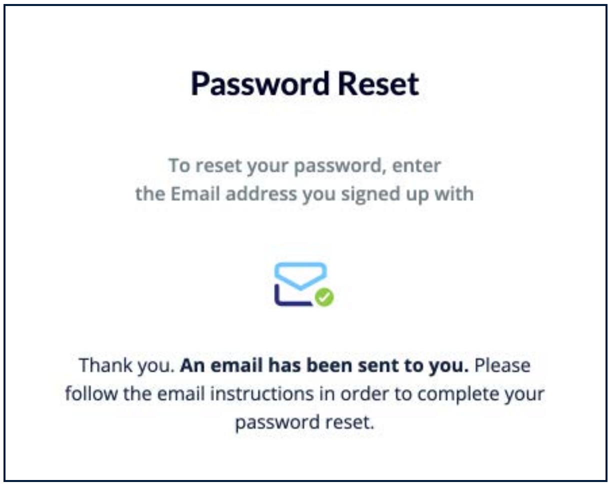
1. On the sign-in page, click **Forgot your password?** to start the process of resetting your password.



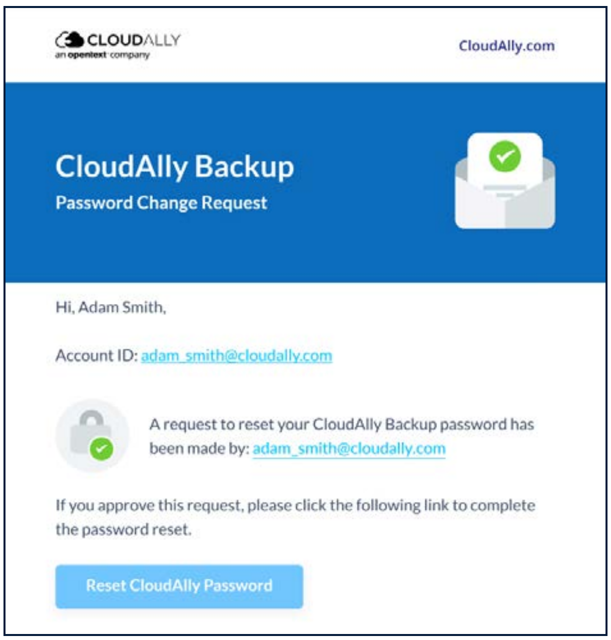
2. The *Password Reset* page will appear.



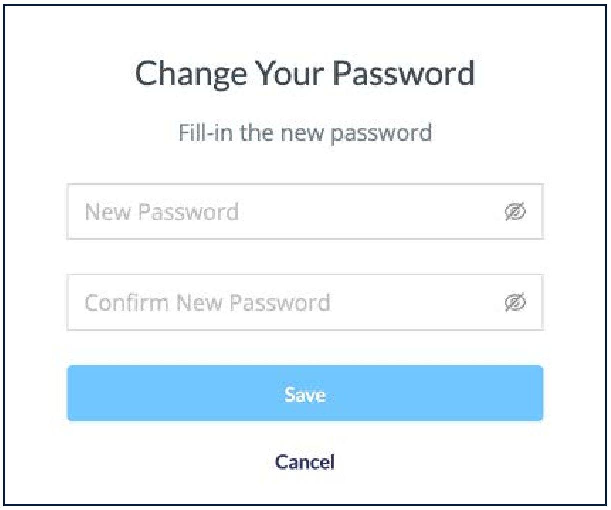
3. In the Email field, enter the email address that you used to sign up.
4. Click **Reset**, and the *Password Reset* window will appear.



The email will look as follows:



5. In the email, click **Reset CloudAlly Password** to confirm the password reset, and the *Change Your Password* window will appear.



6. Enter your new password in the **New Password** field and again in the **Confirm New Password** field, and click **Save**.

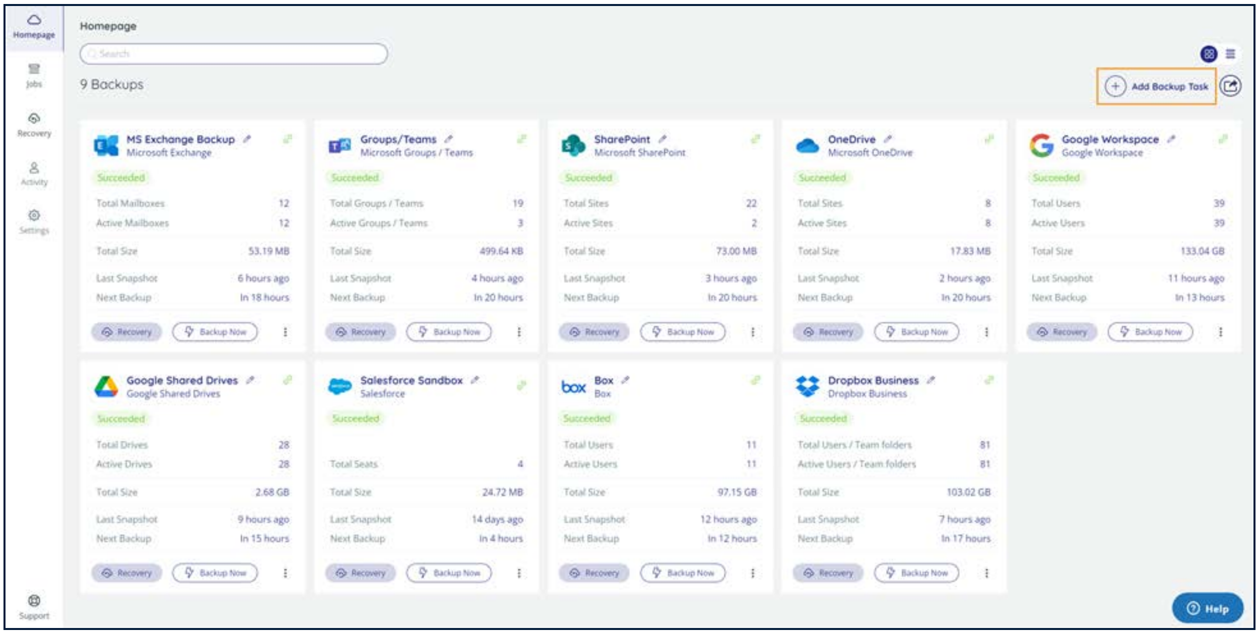
After resetting the password, you will be directed back to the *Sign In to your Account*.

3 Backing Up Your Google Shared Drives Data

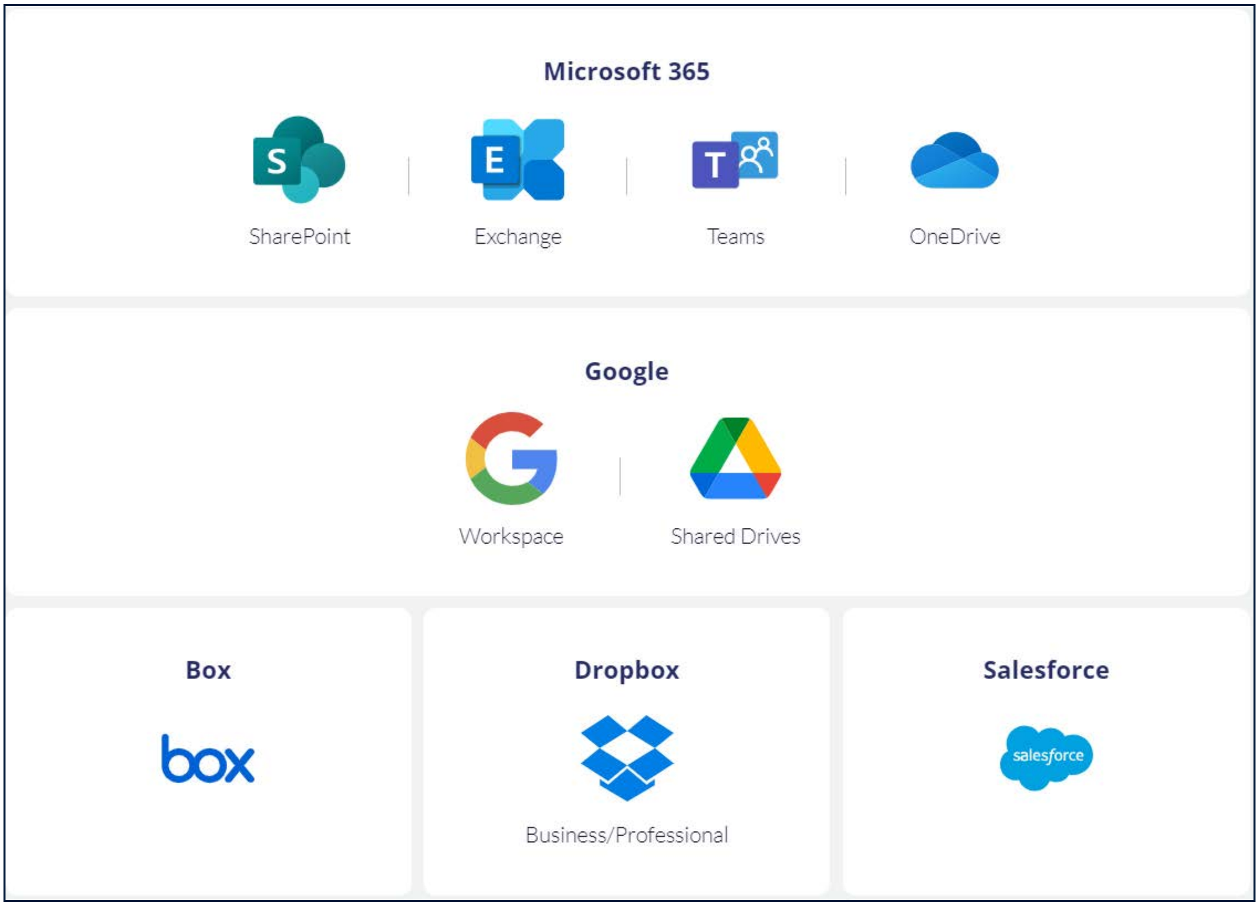
3.1 Creating a New Backup Task

To create a new backup task:

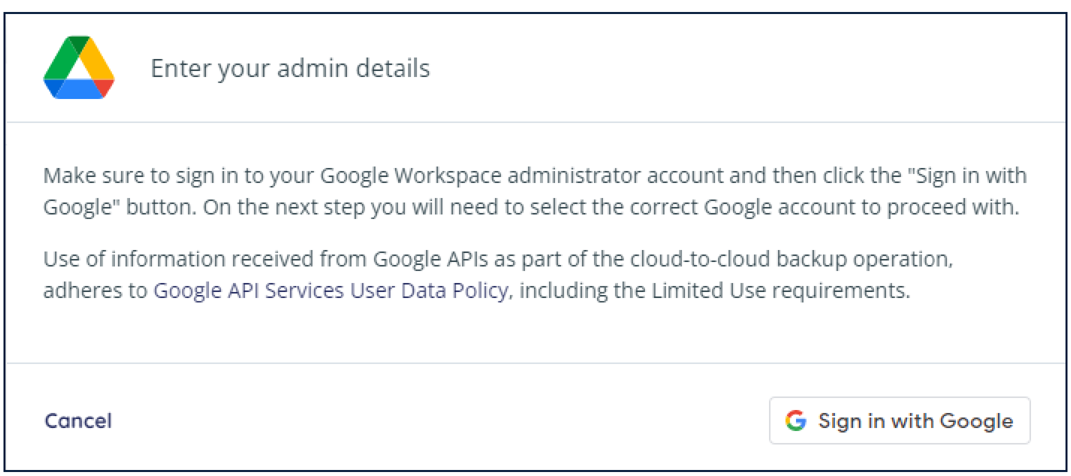
1. Sign in to your account, or if you are already signed in, click the **Homepage** option in the Navigation Panel.
2. On the Homepage, click **+ Add Backup Task**.



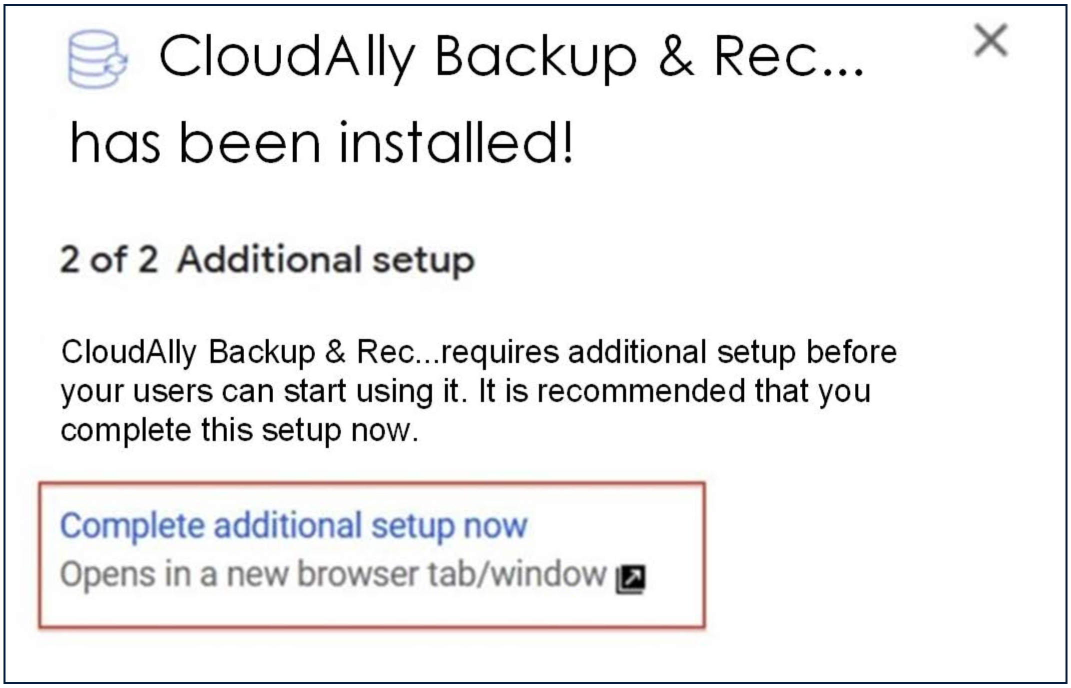
The following page is displayed:



3. Click **Google Shared Drives**. The following screen appears.

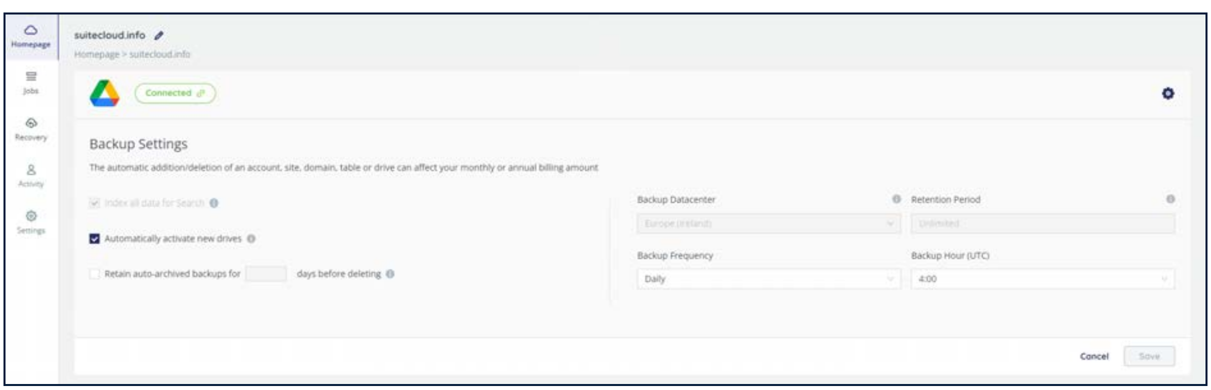


4. Click **Sign in with Google**. You will be directed to the Google Sign In page.
5. A wizard will guide you through the steps of installing the application. Enter the Google Administrator's email/phone, and then their password. Click **Confirm**.
6. On the last step, the following screen will appear. Click "Complete Additional Setup Now." This will add the Google Shared Drives backup task to CloudAlly for you.



Notes:

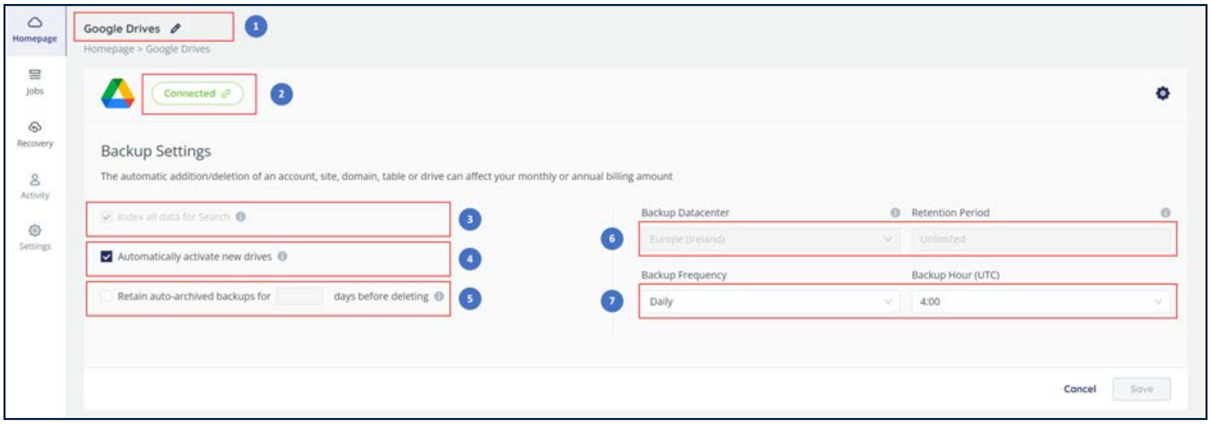
7. You will be redirected to the *Backup Settings* page, where you can adjust the settings of the backup.



On this page, you can adjust the backup settings and activate backups for the Google Shared Drives users. See the sections below for the detailed procedures.

3.2 Configuring Backup Settings

To access the configuration screen, click the gear-shaped settings icon.



1. You can change the name of the backup task by clicking the pencil icon.
2. The icon next to the Google Shared Drives logo displays whether the application was able to connect to the specified Google Shared Drives account. If the authentication token granted for the application becomes invalid (e.g., it expires due to inactivity because you put the backup task on pause for a long time), the Connected icon changes to Disconnected. To grant the application a new token, click on the icon to open the authentication dialog, and repeat the authentication process.
3. By default, the “Index all data for Search” option is selected, which enables CloudAlly to provide you with its granular search and restore functionality. In the process, your data is temporarily decrypted for a brief period of time, and then re-encrypted once the index is built. If this goes against your company policy and you would like to disable automatic indexing, please contact support@cloudally.com.
4. The Automatically activate new drives option instructs the system to detect new drives, and activate them automatically.
5. Backups are automatically archived when an entire site is deleted. The **Retain auto-archived backups** option allows you to retain them for a specified number of days, after which they will be deleted. Otherwise, the backups will be retained indefinitely.

> **Note:** The **Backup Data Center** and **Retention Period** fields are "display only," and their values can't be changed here.

6. The **Backup Data Center** field displays the Data Center location you selected when you signed up with your registration.

   The **Retention Period** field displays whether a retention period has been set up. By default, we provide unlimited retention of your daily backups for as long as you maintain your account subscription. You can override this default and specify a retention period in days, months, or years by contacting CloudAlly support. Backups older than the retention period specified will be automatically deleted.

> **Note:** Your backup storage location cannot be changed once it's been set during the account setup process. Contact CloudAlly support if you need to move backups to a different geographic region, or if you'd like more information on our "Bring Your Own Storage" (BYOS) option.

7. **Backup Frequency and Backup Hour**

   a. Click the drop-down list adjacent to the **Backup Frequency** field and select how often you would like the backups to occur. The available options include:

      i. Daily
      ii. Every 3 days
      iii. Weekly
      iv. 3 times a day

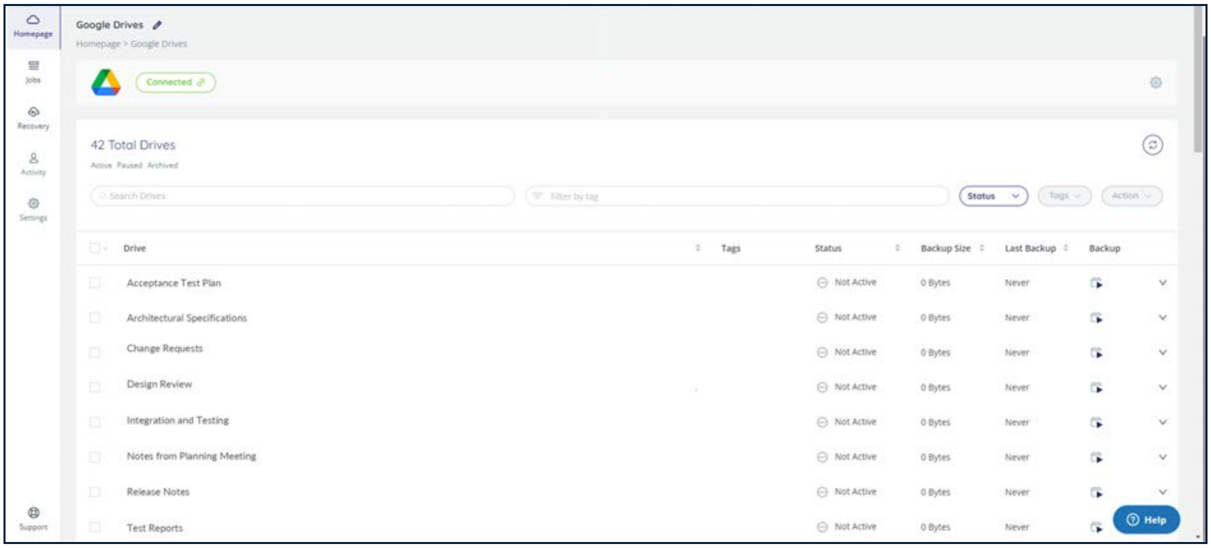
   b. Click the drop-down list adjacent to the **Backup Hour (UTC)** field and select the backup hour. Click **Save**.

> **Note:** 3x daily backups might be subject to additional charges. Please contact CloudAlly support or your sales representative if you have any questions before changing the backup frequency.

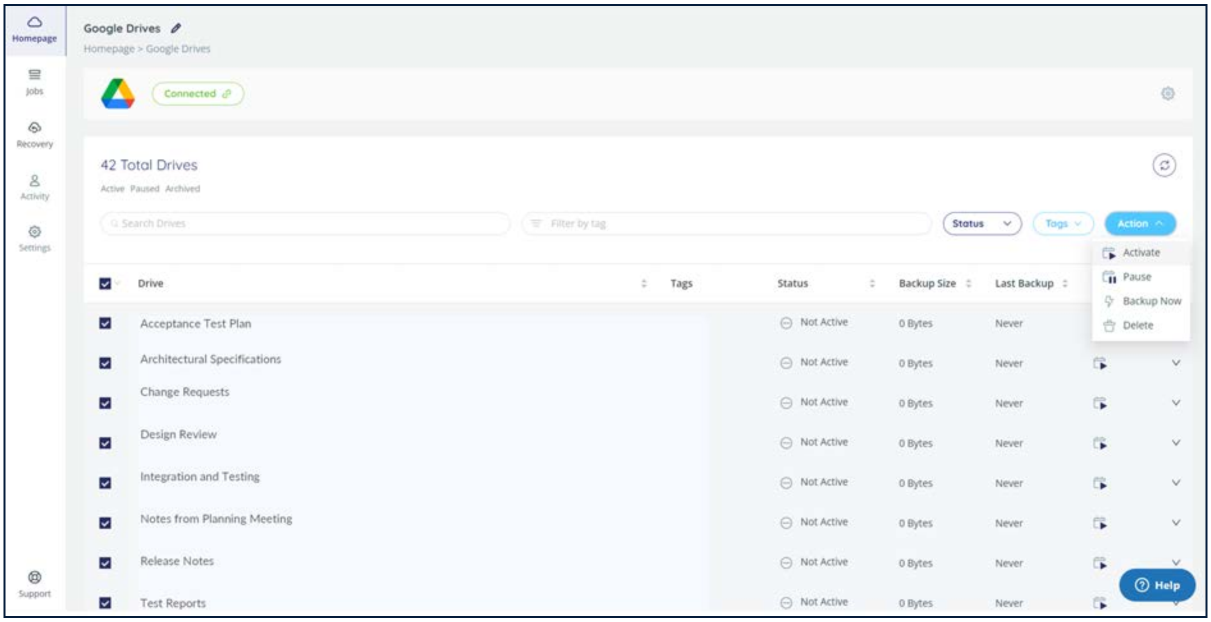
3.3 Activating Your Backups

Once you have configured your backup settings, you need to **Activate** them, in order for them to begin backing up your data.

1. Scroll down to the list of drives.

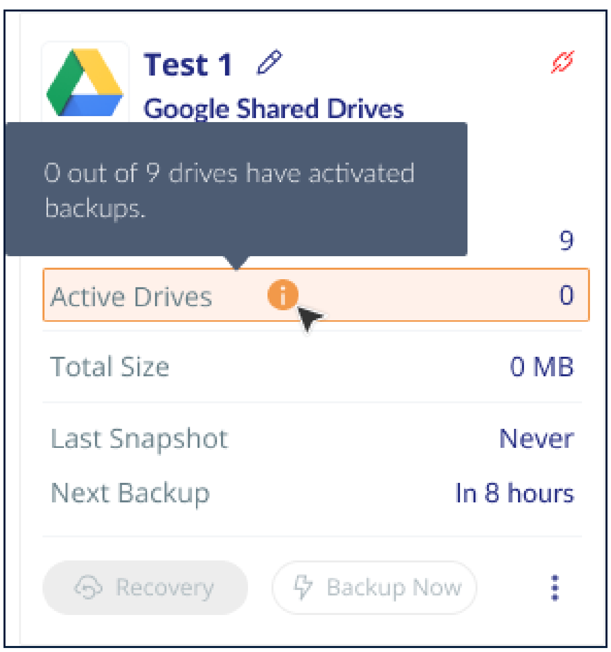


2. Select one or more drive(s).
3. Click **Action** > **Activate**. The status of your backups will now be "Scheduled." This means that they will be backed up at the time that you selected on the Configuration screen.



4. Alternatively, if you prefer to perform an immediate, on-demand backup, click **Action** > **Backup Now**.

If you forget to activate any of your backups, there will be an indicator on the Homepage that reminds you:

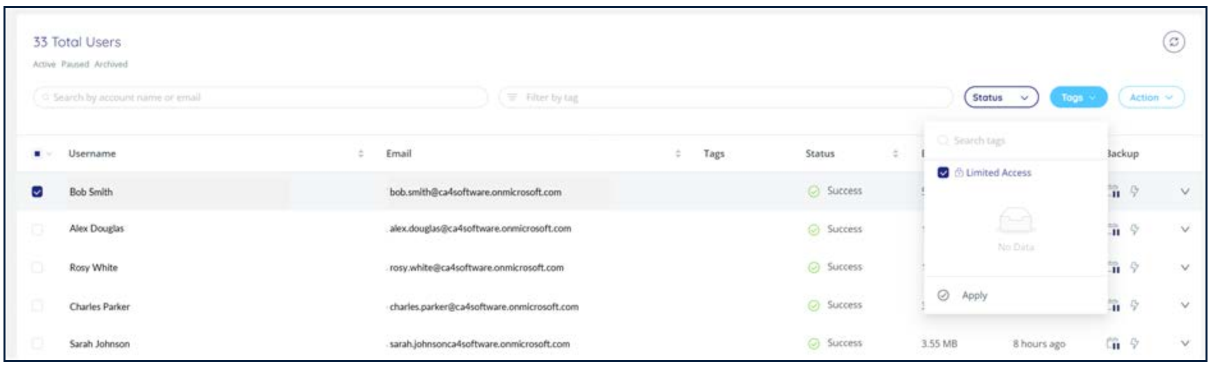


3.4 Securing Your Backups

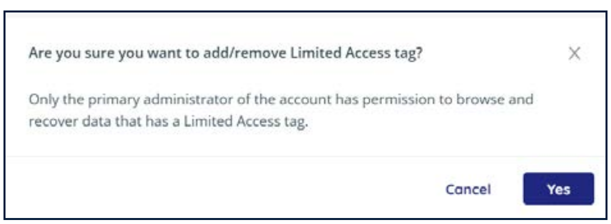
By default, all primary and secondary users can preview, browse, and recover any backed up data. This could be a security risk if sensitive information is contained in the backup snapshots.

Primary users can limit access to one or more sites, drives, accounts, or users so that only they will be able to see, restore and export this data.

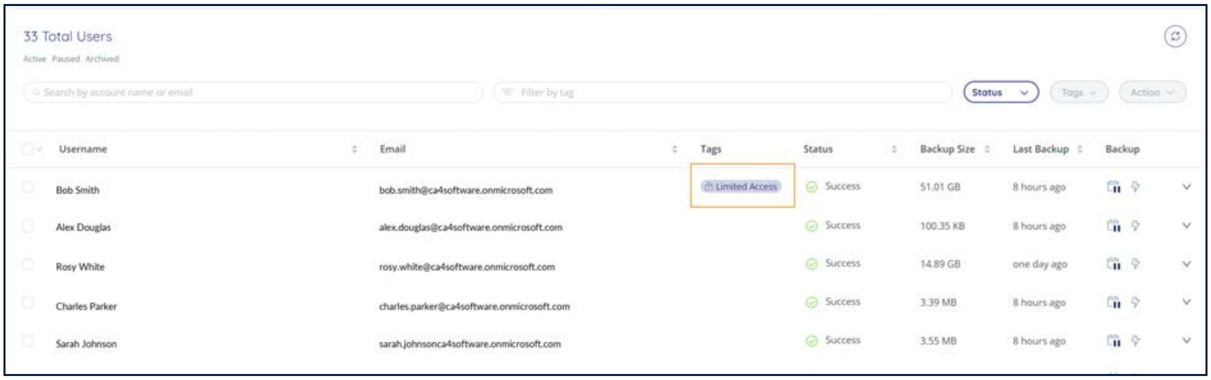
1. Primary user: From the *Homepage*, click the name of the service whose data you would like to restrict.
2. Click one or more drives.
3. Click **Tags**, and check the **Limited Access** tag.



4. Click **Apply**. You will be asked to confirm:



5. The tag will now appear in the **Tags** column as follows.



This will prevent secondary users from browsing and recovering the data.

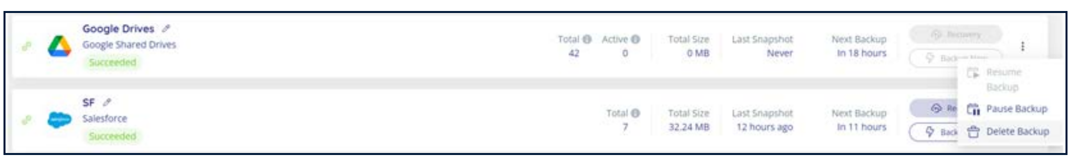
To remove the tag, the primary user should simply reverse the process - un-check the Limited Access tag, and re-apply.

3.5 Deleting a Backup

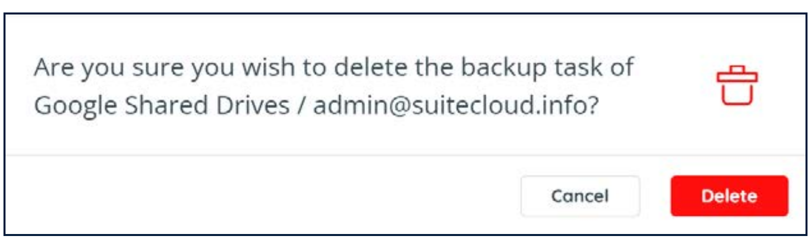
You can delete individual user backups or the entire backup service from your account if you do not want to use them further. The following sections guide you through the process of removing backup services and individual user backups.

3.5.1 Deleting a Backup Task

To remove a backup task for a service, on the *Homepage*, click Menu > **Delete Backup** adjacent to the backup task you want to remove.



The **Confirm Delete** pop-up window is displayed with a warning message.



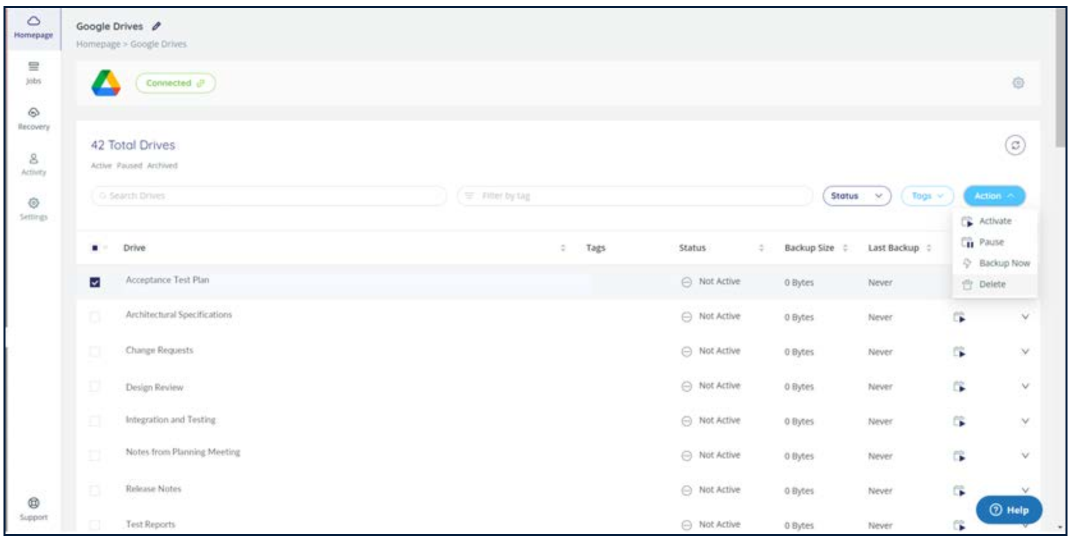
Click **Delete**. The selected backup service is removed from your account.

To prevent mistaken deletions, there is a grace period of 7 days after your backup is deleted.

3.5.2 Deleting an Individual drive

To delete an individual drive:

1. Click the backup task from which you want to delete the drive. The backup task settings page is displayed.
2. Add a check next to the drive that you want to delete. Click **Delete** in the **Actions** menu.



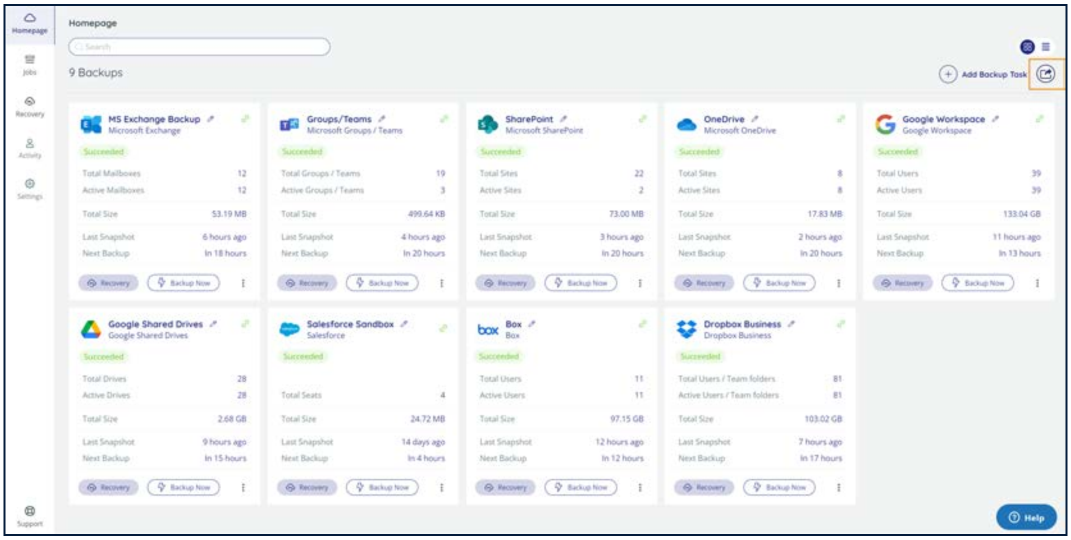
3. A pop-up window is displayed with a list of drives selected for removal. Click **Delete**. The selected drives are removed from your account.

To prevent mistaken deletions, there is a grace period of 7 days after your backup is deleted.

3.6 Usage Reports

In order to provide greater clarity to you about which drives CloudAlly is backing up, you can export a CSV file that lists all of the entities that were backed up, including the status of each entity (active, inactive, or archived).

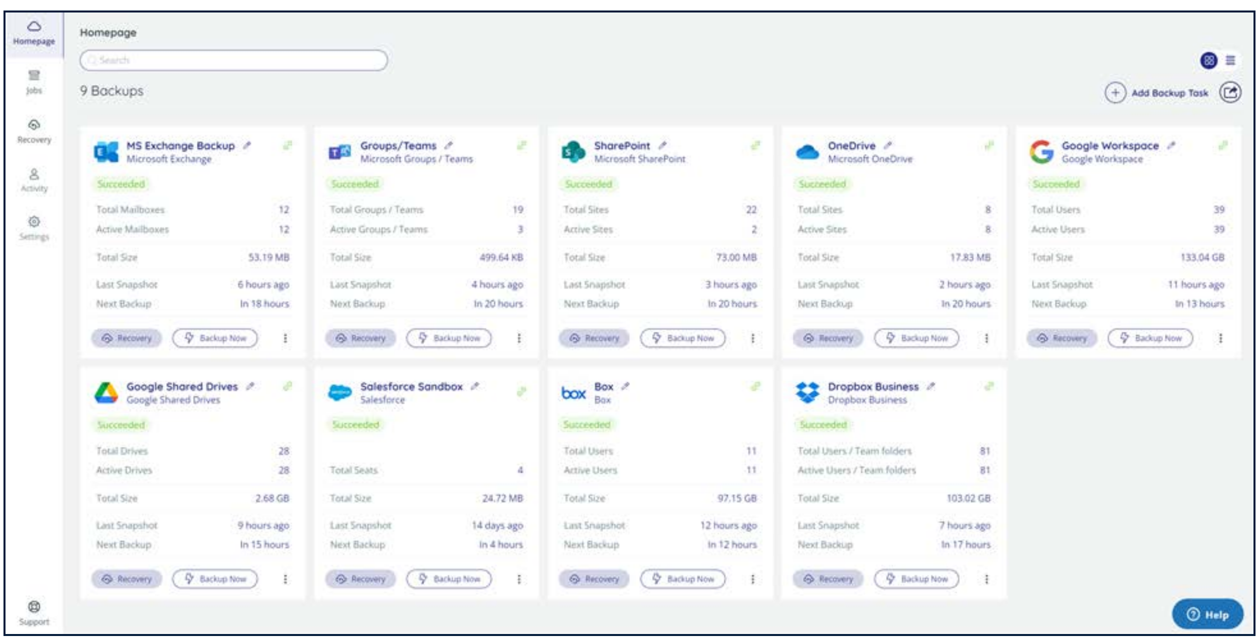
To export a usage report, click the **Export** button, next to **Add Backup Task**. The report will be sent to you via email.



3.7 Modifying the Settings of an Existing Backup

To modify an existing backup task:

1. Click the *Homepage* option from the Navigation Panel. The *Homepage* screen appears.



2. Click the Google Shared Drives icon from the list or enter a keyword in the Search field to find a specific task. The *Google Shared Drives Backup* page is displayed.
3. Click **Settings** on the top-right section of the screen to see the backup settings.

From here, it is possible to modify the fields described in Configuring Backup Settings.

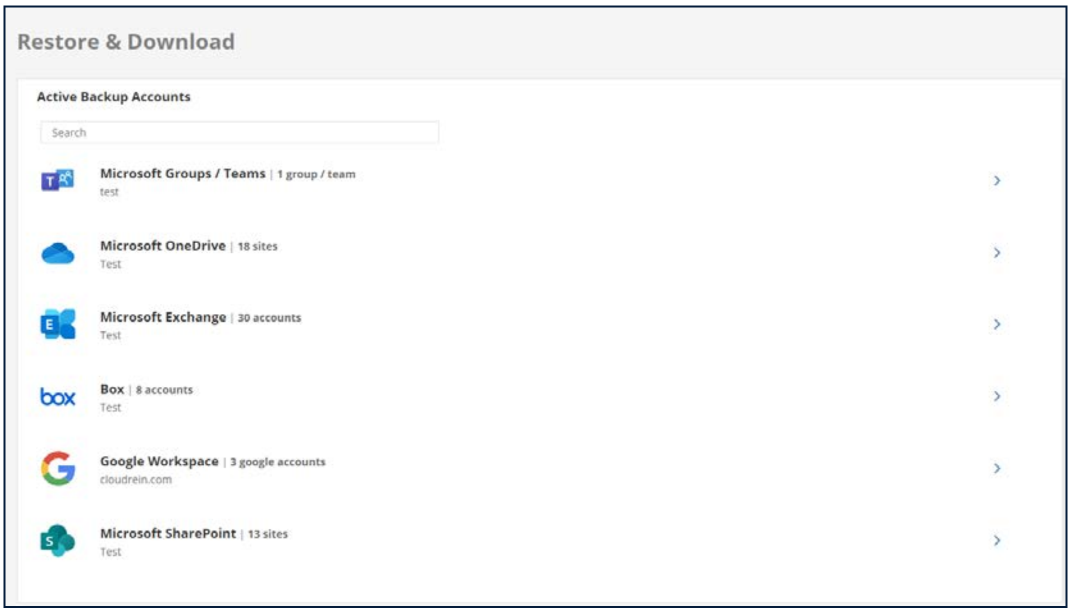
4 Recovering Your Backed Up Data

4.1 Using the Recovery Menu

The Recovery Menu provides you with options at a fine granularity for selecting which drive to restore or export.

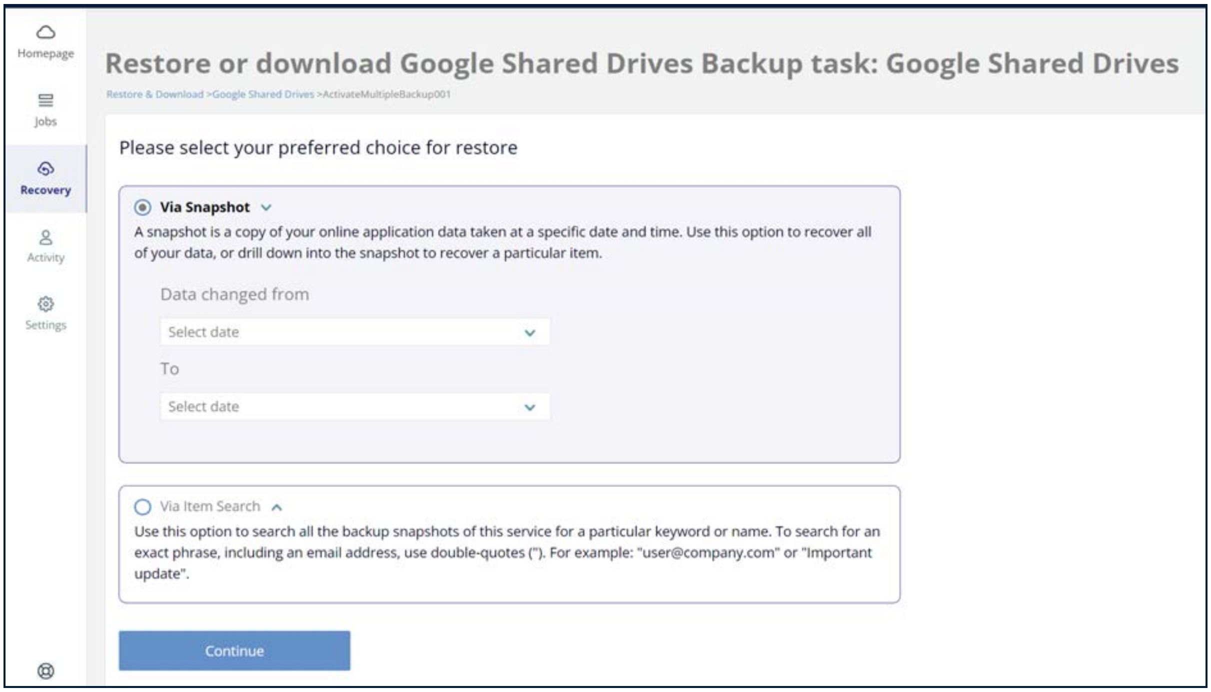
To recover your backed up data:

1. Click Recovery from the Navigation Panel. The *Restore & Download* page is displayed with all your active-backup account details.



2. Click the Google Shared Drives backup task from which you wish to recover the data.

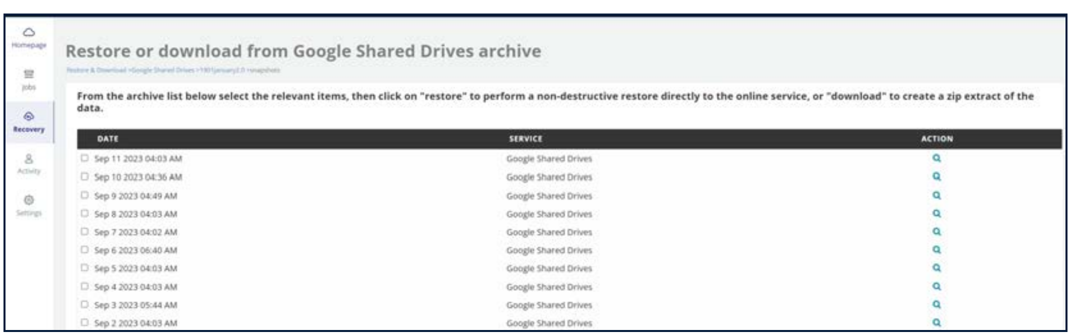
3. The *Restore or Download* Google Shared Drives page is displayed.



- Select the radio button for your preferred restore method:
  - Via Snapshot (see Via Snapshot)
  - Via Item Search (see Via Item Search)

4.1.1 Restore or Download Via Snapshot

1. Enter the date range that you would like to restore using the *Data changed from and To* fields, and press **Continue**.
2. The list of backup snapshots within that date range is displayed. Select the snapshot you want to recover.

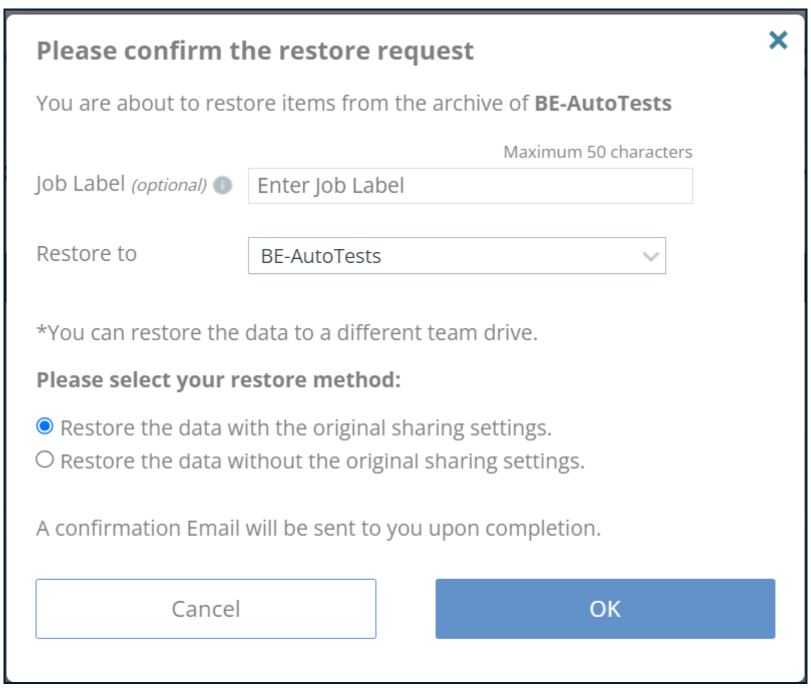


3. Alternatively, you can click the magnifying glass in the Action column to drill down into the snapshot and view the structure of the backed up data. There you can select one or more items for recovery.
4. Once you select a snapshot (if you wish to recover all the data in the backup), or one or more items (if you wish to recover only selected items), the **Restore** and **Download** buttons become available.

4.1.1.1 Restore

If you click **Restore**, the restore confirmation window appears, asking you about the following:

- You can add an optional 50-character Job Label to differentiate it from other Exports and Restores on the Jobs page.
- Do you want to restore to another folder or account? If so, provide the new location information.
- Do you want to restore the data with the original sharing settings, or without them?

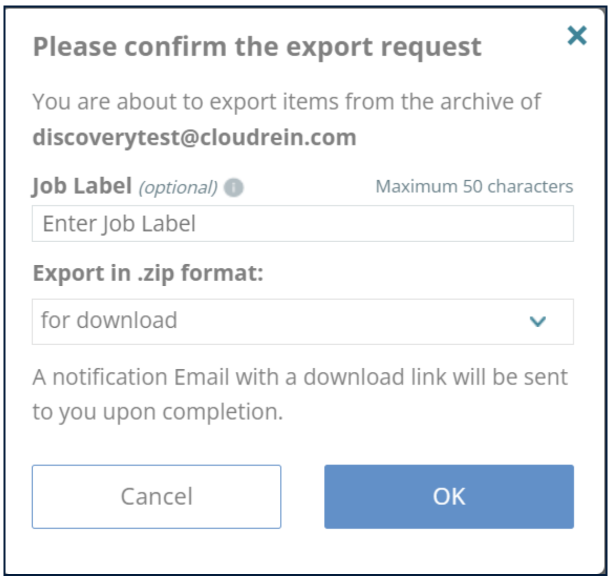


The backup data that you selected will be restored to the location that you specified. When the recovery process is complete, a summary will be sent to your email.

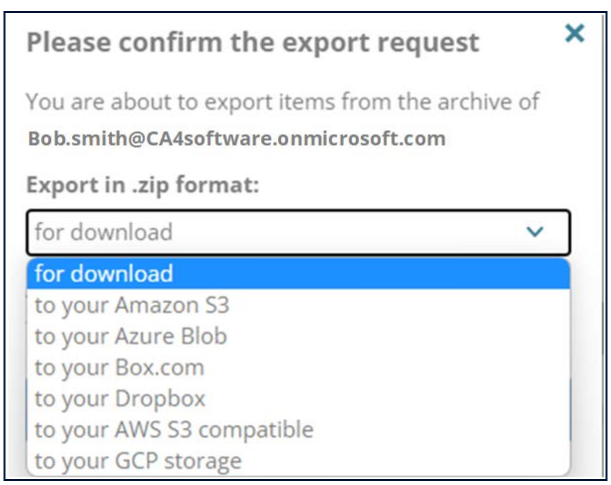
You can also check the Jobs page to see the progress of your task. See "Tracking Recovery Tasks on the Jobs Page."

4.1.1.2 Export/Download

1. If you click **Download**, the following confirmation window appears.

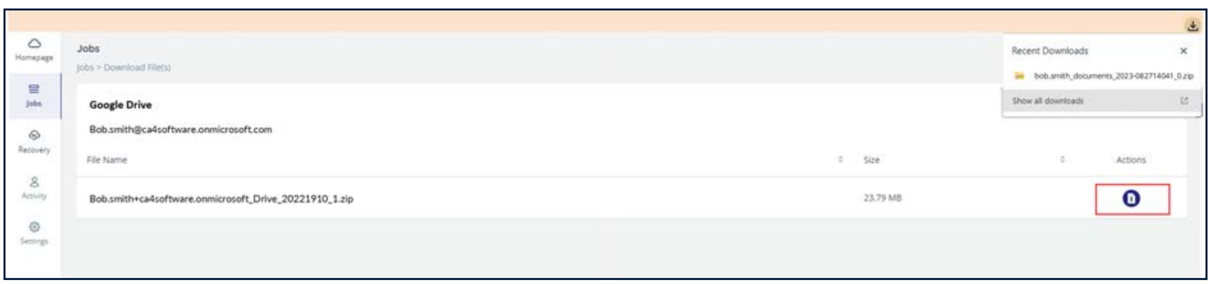


2. Click the drop-down list and select one of the following storage locations:



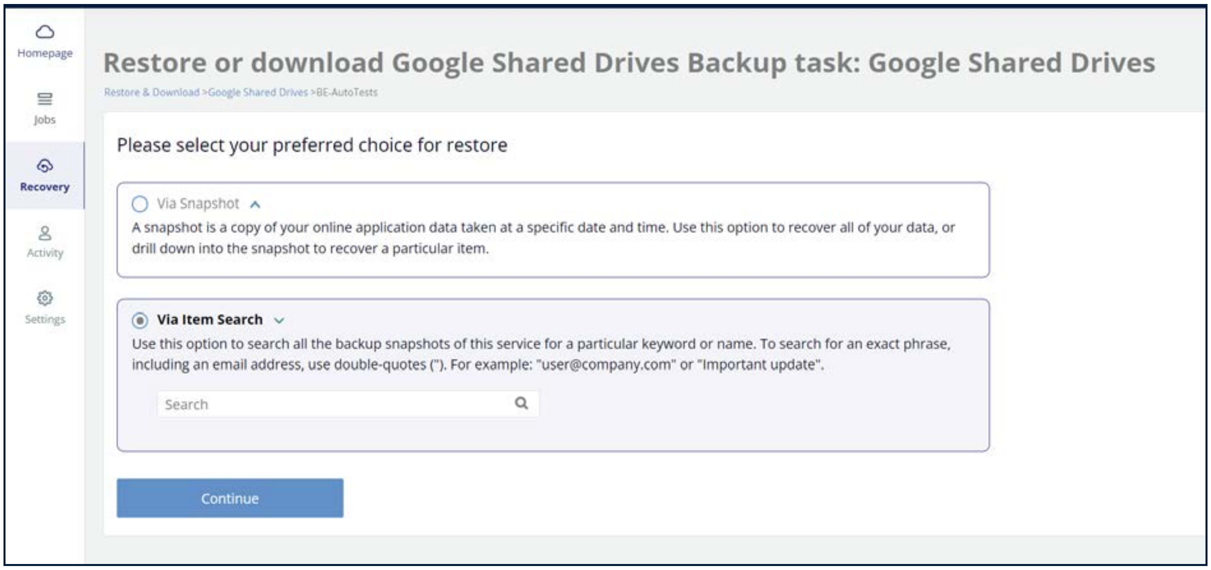
3. If you select options other than "for download," you may be asked for additional credentials and/or access tokens for the selected storage locations.
4. Click **OK**. The download instructions are sent to your registered email address. The download link is only valid for 72 hours.
5. Or, you can check the *Jobs* page. (See "Tracking Recovery Tasks on the Jobs Page.") When the task is completed, the **Download Results** button will be active.

6. Click **Download Results**, and a page will open, where you can access your backup file.



4.1.2 Restore or Download Via Item Search

1. Select **Via Item Search**, and enter a word or phrase to search on.



2. Click **Continue**. The *Restore or download* page is displayed, showing the search results with details such as . The details columns are different for different types of restored items.
3. Select items you would like to restore or download. When at least one item is selected, **Restore** and **Download** become available.
4. Follow the instructions in the Restore or Export/Download sections to complete the recovery process.

4.2 Tracking Recovery Tasks on the Jobs Page

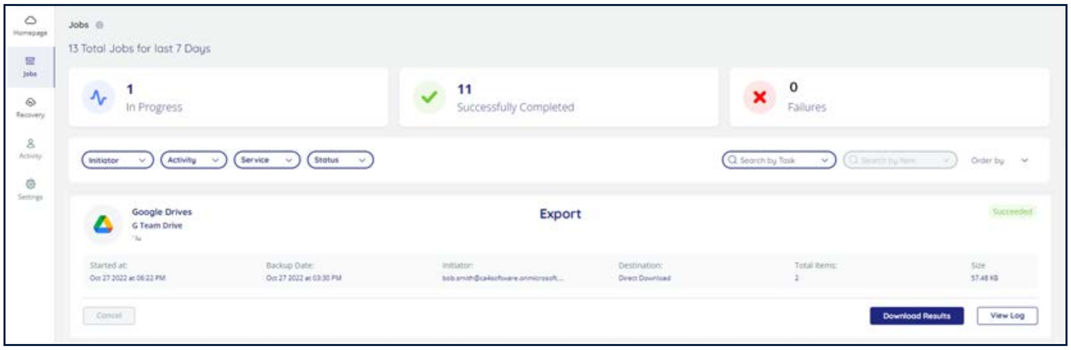
The Jobs page provides you with both high-level and drill-down views of your restore and export jobs over the last seven days.

> **Note:** To see the status of your Backups, click the name of the backup from the *Homepage*.

From the Navigation pane, click **Jobs**.

4.2.1 High-Level Summary

- The top portion of the Jobs dashboard summarizes how many of your jobs are in progress, how many have successfully completed, and how many have partially succeeded or failed over the past 7 days.



To see a list of jobs that have any of these 3 statuses, click on the status, and your results will be filtered accordingly

4.2.2 Filtering

The next section allows you to filter by numerous criteria:

- **Initiator:** Who initiated the backup / restore?
- **Activity**: Filter by restores or exports.
- **Service**: Filter by one of the following services, such as:
  - Google Workspace
  - Google Shared Drives
  - Salesforce
  - Box
  - Dropbox
  - Google Account

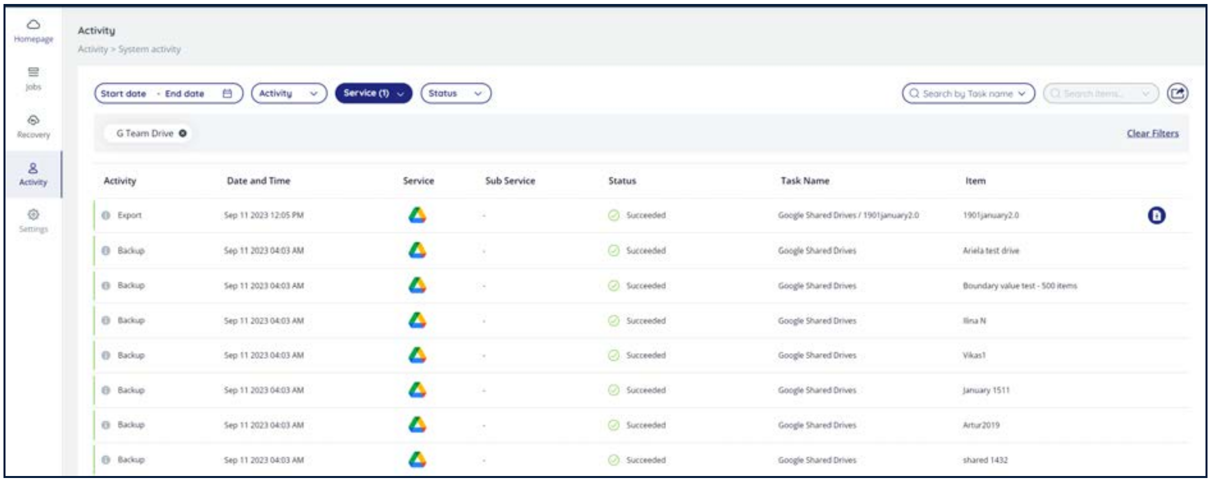
- **Status**: Filter by one of the following:
  - In progress
  - Succeeded
  - Partially succeeded
  - Failed
  - Pending
  - Canceled
- **Search by Task**: Filter by a task, such as:
  - Box
  - Dropbox
  - Google Workspace
  - Salesforce

If you choose to filter using a particular service, then you can focus on a specific item in the search bar. You can also order by:

- Latest First
- Oldest First

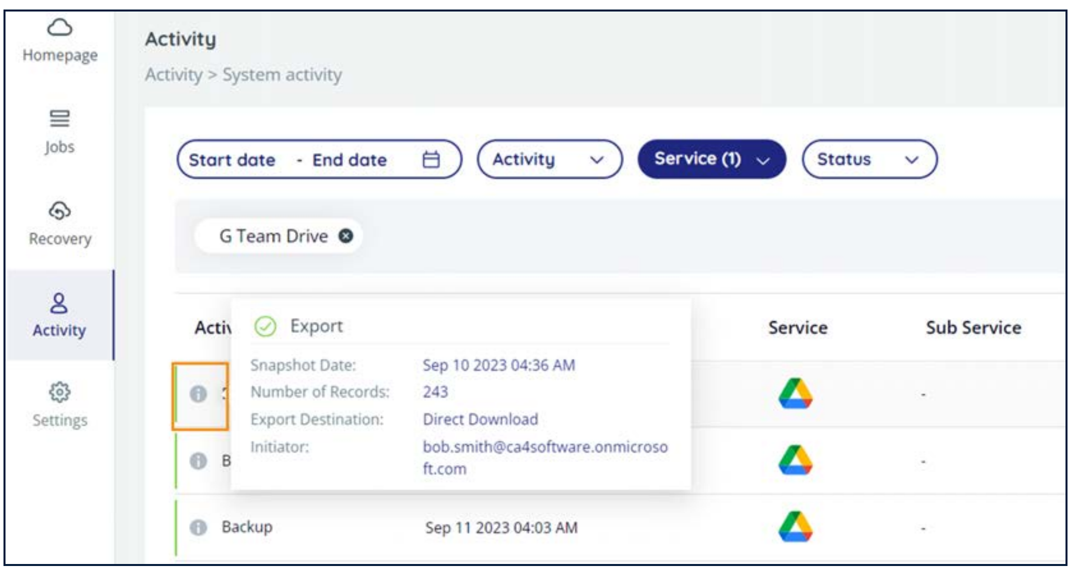
4.2.3 Description of Each Job

- The rest of the screen provides a detailed description of each individual job that you ran.
  - **Type of Job**: Export, or Restore – this appears as a large title within each job description.
  - **Name, Service**, and **Account** of the job.
  - Start date, backup date, initiator, destination, total items backed up or restored, and the size of the file(s).
- **Cancel** enables you to stop a job that is in progress.
- **Download Results** enables you to download a zip file with your recovery data.
- **View Log** redirects you to the System Activity page, which displays your account activity with details such as Activity, Date and Time, Service, Sub-Service, Status, Task Name, and Item.



This page enables you to filter and search the list of backup tasks, export the list as a CSV file, and view more details on any backup task.

The latter can be achieved by clicking the information icon in the Activity column. The Info pop-up displays the backup execution time, the size of the stored data, and the number of entities, and the summary of the backup execution.

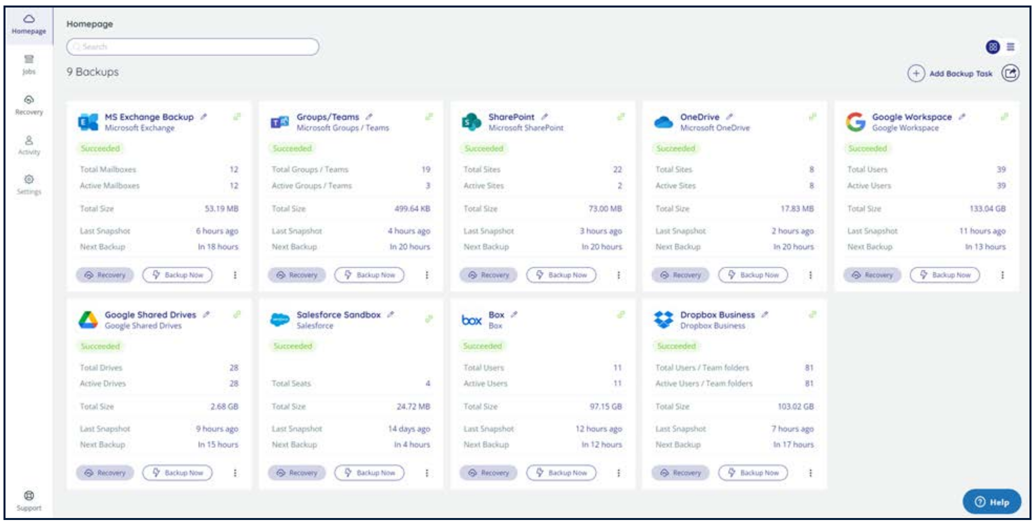


5 Filtering and Viewing Drill-Down Details

This section explains the process of finding the exact backup data you are looking for using filtering.

5.1 Filtering by drive

1. Click the *Homepage* option from the Navigation Panel. The *Homepage* screen appears.



2. Click the Google Shared Drives icon from the list or enter a keyword in the Search field to find a specific task. The *Google Shared Drives Backup* page is displayed.
3. The *Google Shared Drives Backup* page displays all the Google Shared Drives drives available for the administrator account you are using. The page displays the details such as Drive, Status, Backup Size and Last Backup date. It also provides the means to filter the drives and control the associated backup tasks.

5.1.1 Filtering Using Names or Statuses

You can filter using the following options:

- Enter a search phrase in the *Search by* field to view all the drives with the entered keyword.
- Filter by statuses such as Not Active, Scheduled, Success, In Process, Failed, Paused, Archived, or Partial.

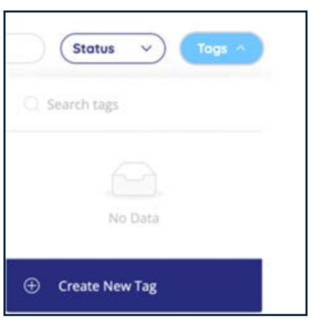
5.1.2 Filtering Using Tags

CloudAlly provides you with the means to add extra metadata to your backed up data in the form of "tags." For example, you might want to denote all drives that belong to Managers, or all those that belong to the Sales Team.

You can use tags to quickly filter your list of drives.

The **Tags** option is used to search for existing tags. By default, it is not active. To activate **Tags:**

1. Select at least one drive.
2. Click **Tags**, and the following screen appears.



3. To search your existing tags, enter a tag name in the **Search tags** field.

5.1.3 Creating a New Tag

To create a new tag:

1. Click **Create New Tag**. A pop-up appears where you can enter a new tag name.

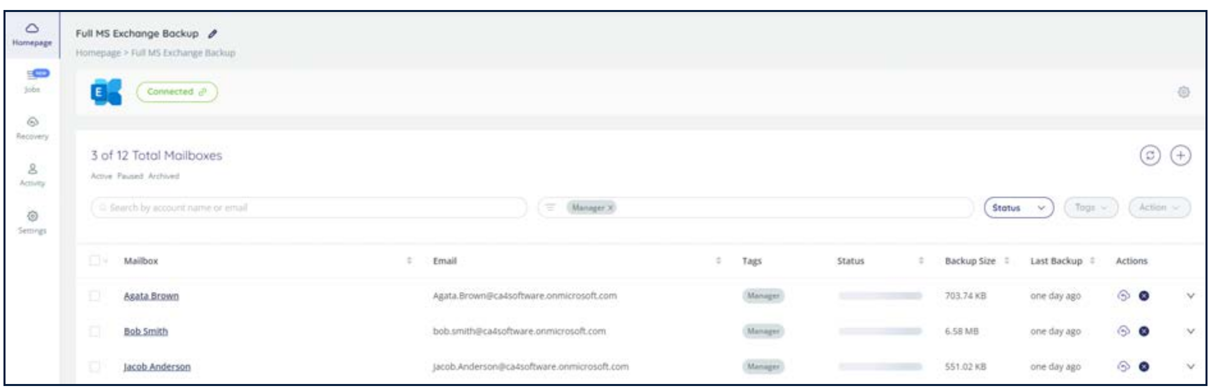
2. Enter a new tag name and click **Create.**

To apply tags to your drives:

1. Select at least one drive.
2. Click **Tag**.
3. Choose the desired tag for your drive s.
4. Click **Apply**.

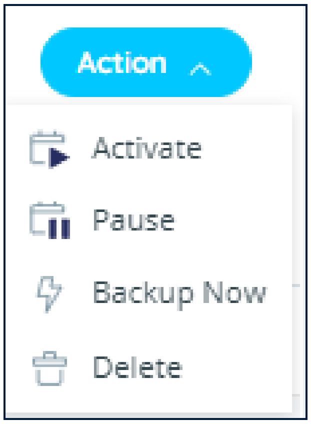
5.1.4 Filtering by Tag

In the **Filter by tag** field, enter a tag name. The accounts, teams or sites with those tags will appear.



5.1.5 Actions

To perform actions on a drive, select at least one of them on the list, and the **Action** button will be enabled. Click **Action** to see the following drop-down menu:



- **Activate** enables backup in all the selected drives.
- **Pause** halts the backup procedures on the selected drives.
- **Backup now** starts the backup immediately. The backup in this case starts as soon as a backup processing machine is available, which may take several minutes.
- **Delete** removes the backup task and backup data for the selected drives.

5.2 Viewing Backup Statistics with the Drill-down Feature

Select the desired drive, and click the downward-facing arrow at the end of the row. This option enables you to drill down to the backup history dashboard.

When you drill down, you can find a diagram describing past backups, and a brief summary of the backup outcomes.

The diagram depicts the number of items backed up each day. By hovering your mouse over a column in the diagram, you can see the number of items backed up in each service. This number includes all new and changed items, so it may be greater than the total number of items in the backup. You can select the date range of the chart with the sliders underneath it. The maximum range displayed is 30 days.

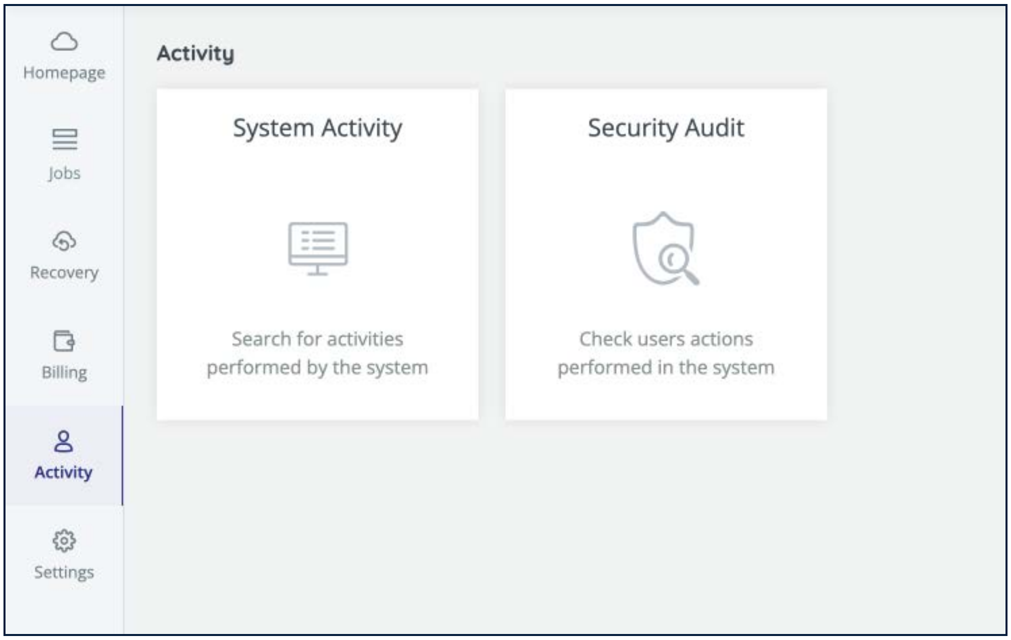
The summary tiles below the chart provide at-a-glance information about the backup: for each sub-service, they display the total number of items in the backup, the date of the last backup, and the outcome.

6 Managing Your Account

This section guides you through the processes of managing your Account activity, account settings, password, setting up two-factor authentication, and managing users.

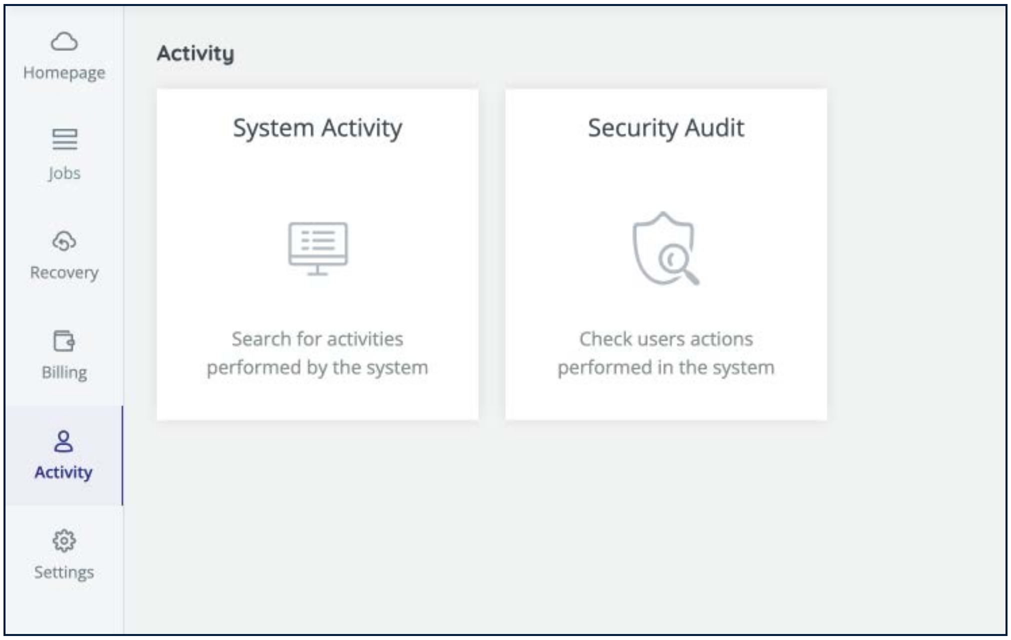
6.1 Viewing Account Activity

The Activity menu enables you to view your account activity, including System Activity and Security Audit. Click *Activity* on the navigation pane.

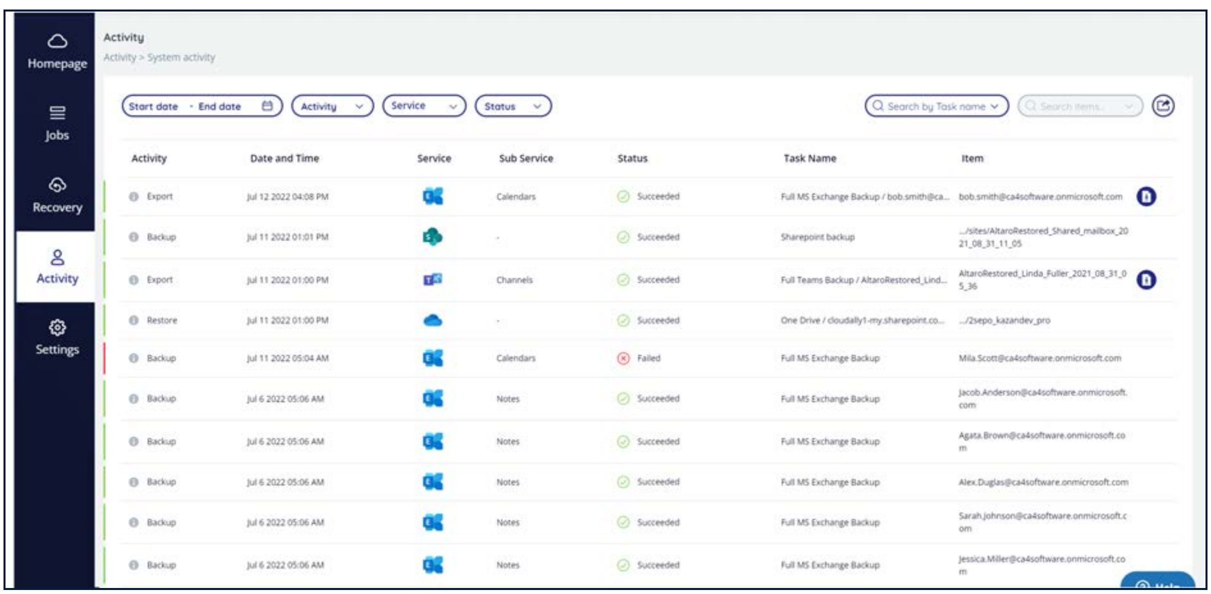


6.1.1 System Activity

Click **System Activity**.

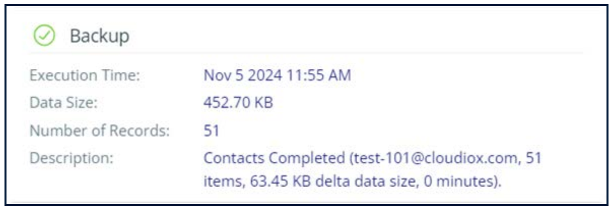


The *System Activity* page displays your account activity, with details such as Activity, Date and Time, Service, Sub-Service, Status, Task Name, and Item.

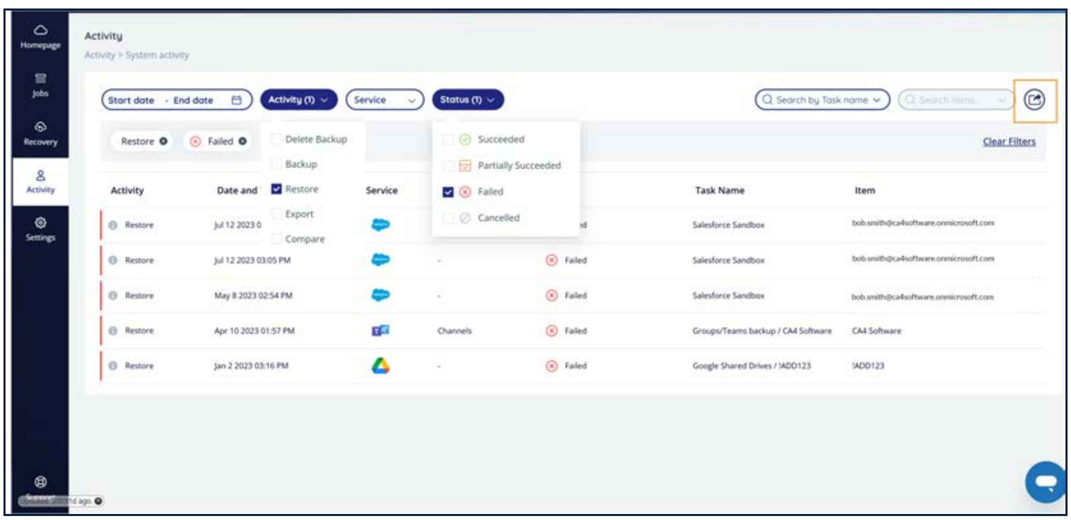


This page enables you to:

- Filter and search the list of backup tasks
- View more details on any backup task. This can be achieved by clicking the "i" (Info) icon. The Info pop-up displays the backup execution time, the size of the stored data, and the number of entities, and the summary of the backup execution.



- Export the Activity Log as a CSV file. Any filters selected on the page will also apply to the exported log file. For example, you could choose to only see Restore tasks that have failed.



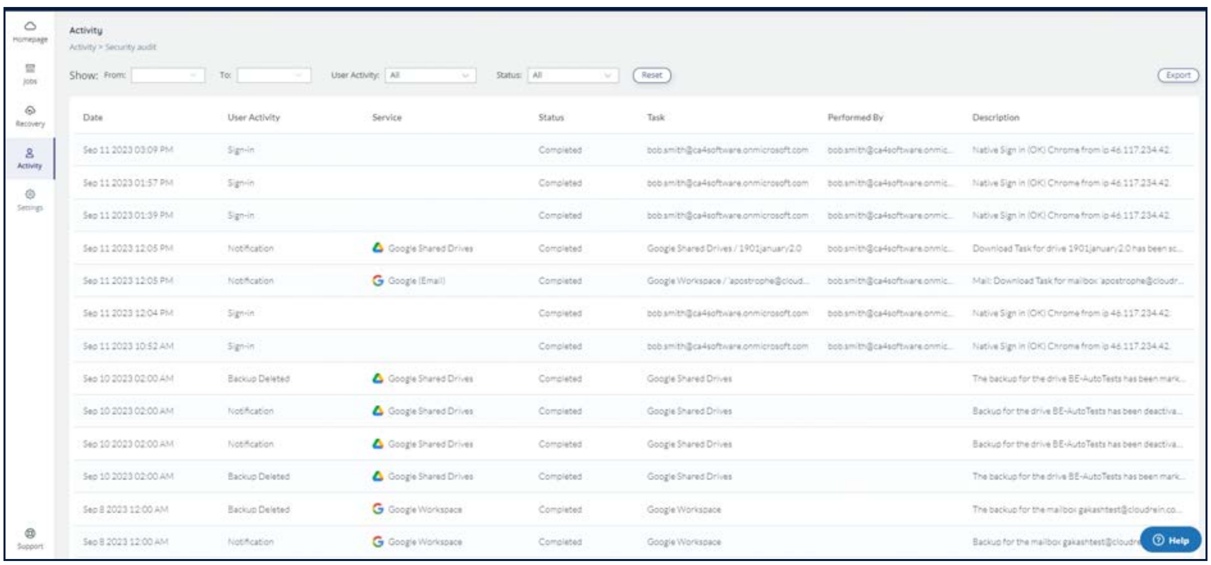
> **Note:** Administrators can grant users permission to see the *System Activity* page by clicking **Settings > User Management**, and checking "View Account Activity."

6.1.2 Security Audit

The *Security Audit* page provides information about all the security-related actions that have happened in your account. The user activity that is displayed includes:

- Backup deleted
- User deactivated
- Settings changed
- Sign-in success or failure
- Permissions changed
- Notifications.

The page includes the date of the event, the type of activity, the service involved, the status of the activity, the account performing the activity, and the description.



The Security audit table can be exported as a CSV file by clicking **Export**.

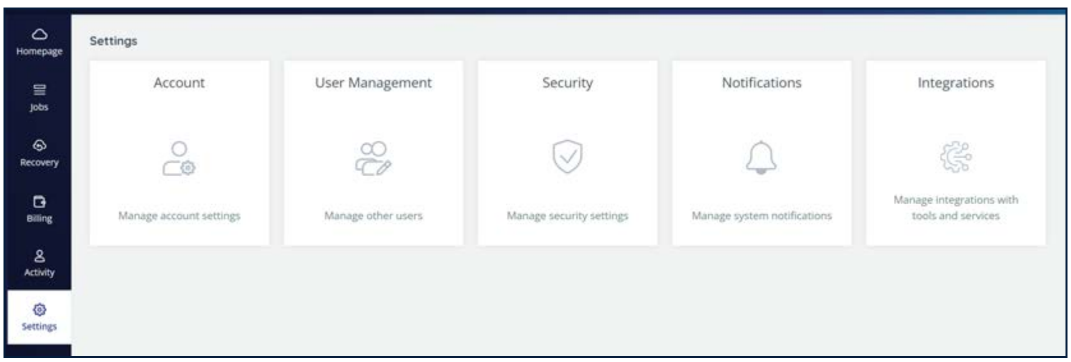
> **Note:** Administrators can grant users permission to see the *Security Audit* page by clicking **Settings > User Management**, and checking "View Security Audit Page."

6.2 Managing Your Account Settings

The *Settings* page provides you with tools to control both your account and the accounts of users whose external credentials are linked to your account. The Settings section consists of the following sub-sections:

- Account
- User Management
- Security
- Notifications
- Integrations

You can find more details on each of the *Settings* pages below.

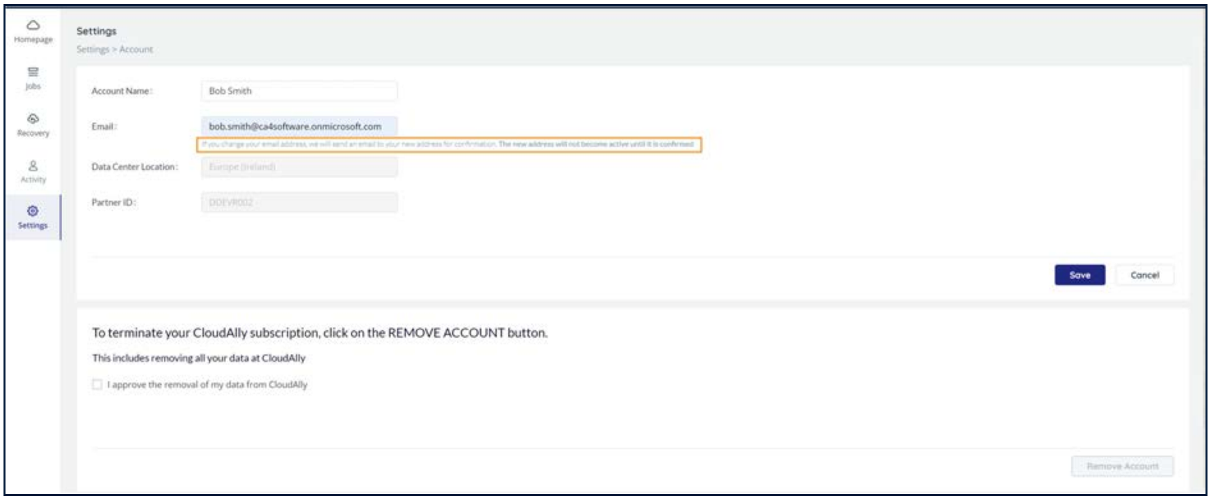


6.2.1 Account Settings

This page allows you to change the name of your account and the email address. You can only change the Data Center Location by contacting CloudAlly support. Finally, this page also allows you to terminate your account.

To update or change your account details:

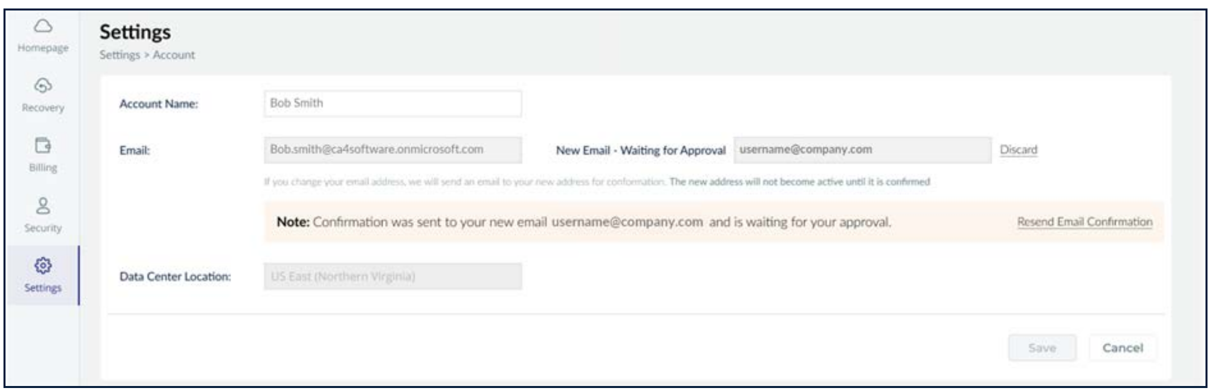
1. From the Navigation Panel, click **Settings** and then click **Account** . The *Settings > Account* page is displayed.



You can update the Account Name and/or Email.

> **Note:** If you change your email address, you will receive an email sent to your new address for confirmation. The new address will not become active until it is confirmed.

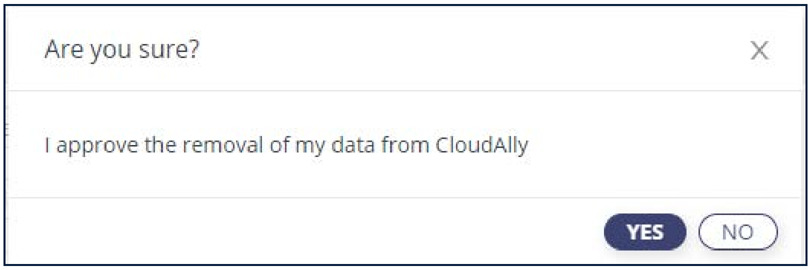
Click **SAVE**. The following screen will appear. If you did not receive the confirmation email, click **Resend Email Confirmation**



6.2.2 Canceling Your Subscription

To cancel your subscription:

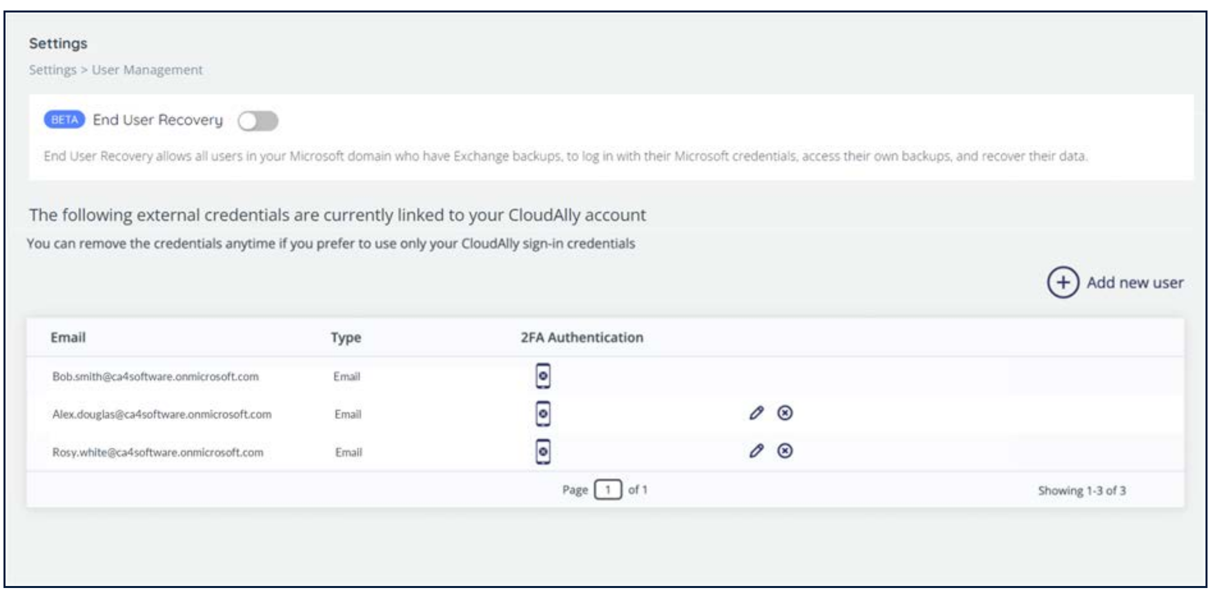
1. Check the box for "I approve the removal of my data from CloudAlly" field and click **REMOVE ACCOUNT**.
2. The *Are you sure?* pop-up window is displayed with a confirmation request.
3. Click **YES** to confirm the cancellation.



> **Note:** To prevent mistaken deletions, there is a grace period of 7 days after your account is terminated. After the grace period, if your account is not reactivated, all data from all your backups will be deleted.

6.3 User Management

The page provides tools for fine-level control of the permissions and access levels of your users.

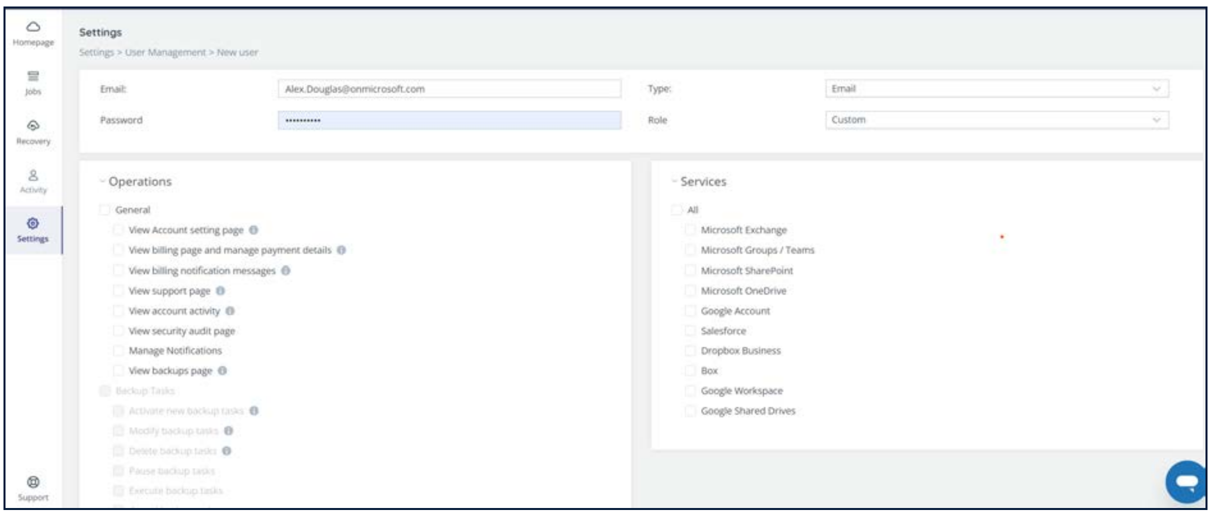


6.3.1 Adding a New User

System Administrators, both those who logged in to CloudAlly with a username and password, or with Microsoft credentials, can add new users.

Click **+ Add new user** to create a new user and start the configuration procedure for that user, or the pencil icon to edit an existing user's settings.

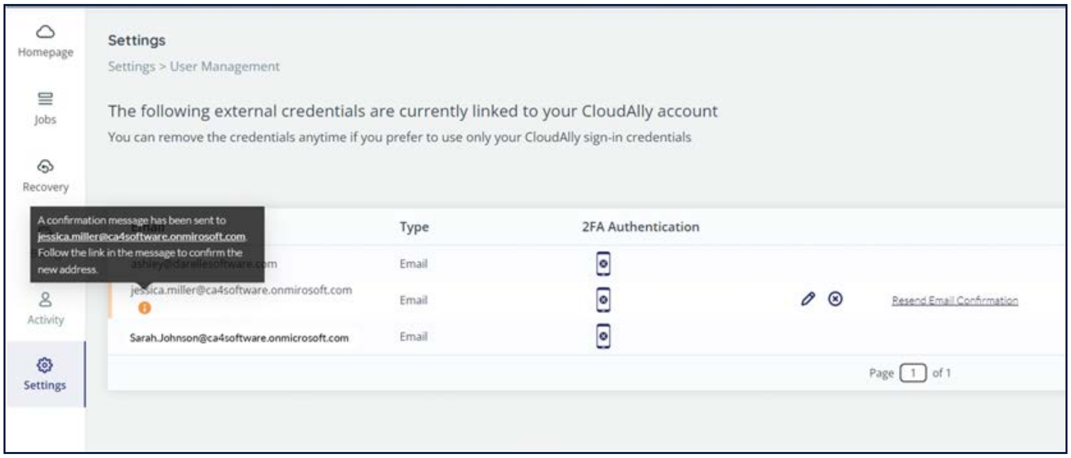
- Enter the new user's email address.
- Select the Authentication Type: Azure, Email, Google+, or Okta.
- Select the permissions role for the user. Selecting the role "Administrator" enables permissions to all services and operations. Or, you can selectively choose which permissions to grant from the list of services:



To save changes, scroll to the bottom of the page and click **SAVE**.

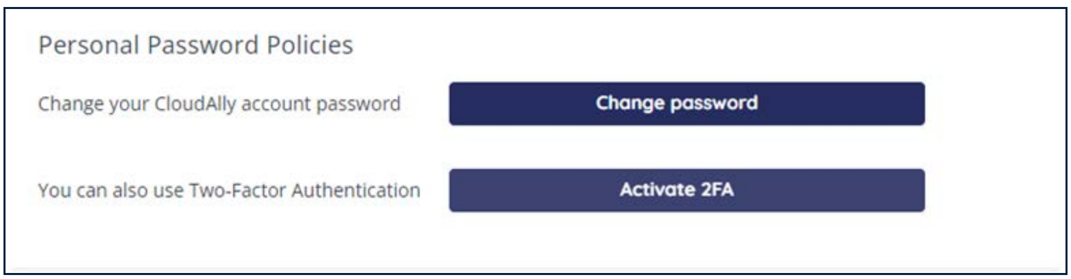
You will be returned to the Settings page. To complete the process, the user must confirm their email address using the link sent via email. This is a security measure, which ensures that the user's email address is valid.

The link is valid for 24 hours. If they did not confirm within this time period, or did not receive the confirmation email, click **Resend Email Confirmation**.



6.4 Security Settings

The *Security Settings* page enables you to:



- Update your password
- Set up two-factor authentication

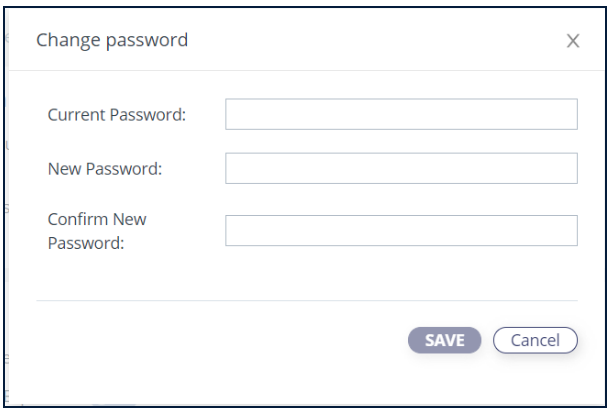
You can also enforce certain security policies for your users' accounts.

- With the **Enforce Two-Factor Authentication** option, you can make two-factor authentication mandatory for all the users in your account.
- By setting the **Password Expiration**, you can enable the password expiration option for all your users – you will be also be asked for the number of days before the users' passwords expire.

6.4.1 Changing Your Password for Credential-Based Authorization

You can change your existing account password by performing the following procedure:

1. From the **Settings** >**Security** page, in the Personal Password Policies panel, click **Change Password**.
2. The *Change password* pop-up is displayed.



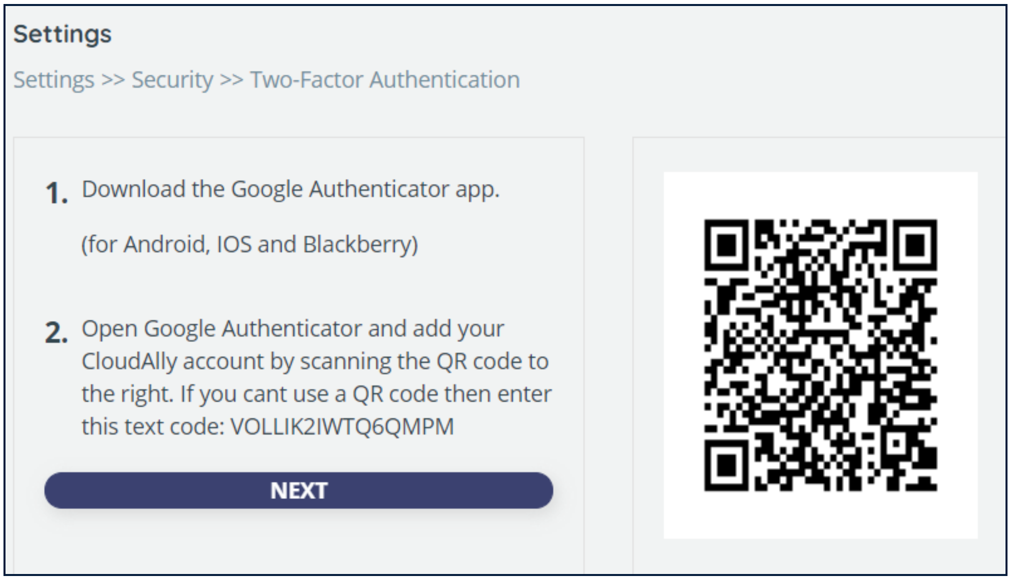
3. Enter the current password in the *Current Password* field.
4. Enter the new password in the *New Password* field.
5. Re-enter the new password in the *Confirm New Password* field.
6. Click **SAVE**. You can now use this password to access your account.

6.4.2 Two-Factor Authentication

Two-factor authentication provides additional security to your account and your backup data.

To enable two-factor authentication:

1. Click **Activate 2FA**. The Two-Factor Authentication page is displayed.



2. Download an Authenticator app, depending on your platform.
3. Open the Authenticator app and add your account by scanning the QR code provided in the web application.
4. If you cannot use a QR code, then enter the text code provided in the web application.
5. A six-digit code is generated.
6. Click **NEXT**.
7. Enter the 6-digit code that the application generated.
8. Click **ENABLE** to complete the process of activating the Two-factor authentication.

From now on, every time you sign in to your Account, you are asked to enter a 6-digit code from your authentication app, after you click **SIGN IN**. Click **VERIFY** to verify the code and access the application.

6.4.3 SAML

The Security Assertion Markup Language (SAML) is an open federation standard that allows an identity provider (IdP) to authenticate users and then pass an authentication token to another application known as a service provider (SP).

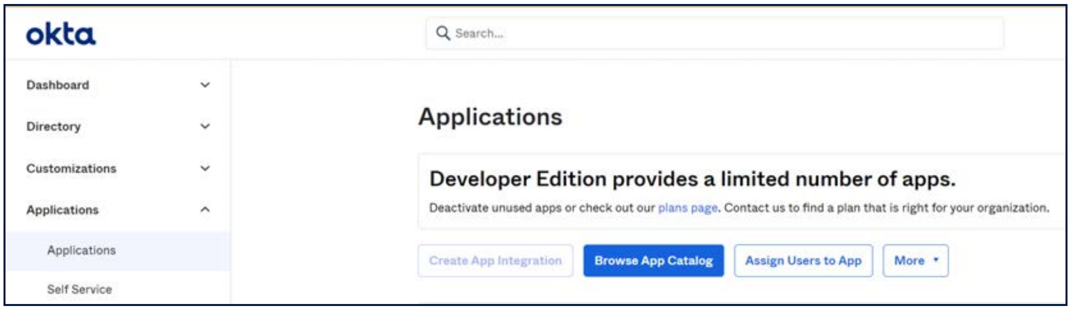
CloudAlly supports Okta as its SAML provider.

There are two steps to setting up Okta so that you can use it to log in to CloudAlly:

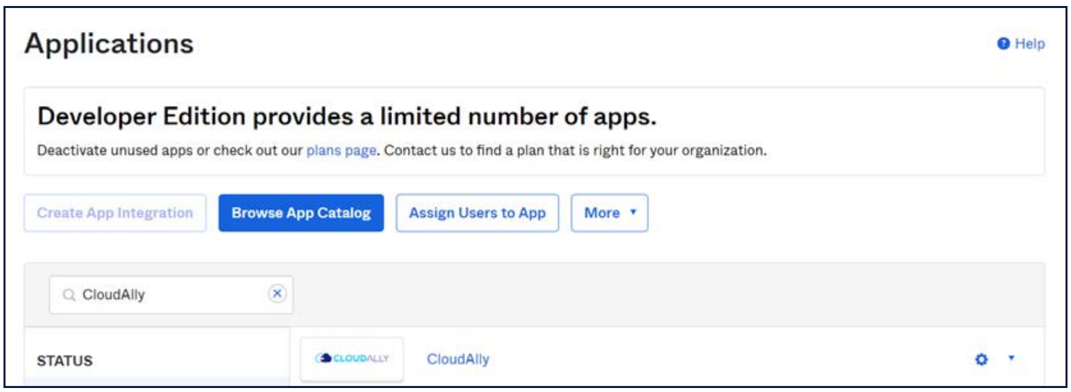
- Setting up CloudAlly in the Okta Application
- Setting up Okta in the CloudAlly application

6.4.3.1 Setting up CloudAlly in the Okta Application

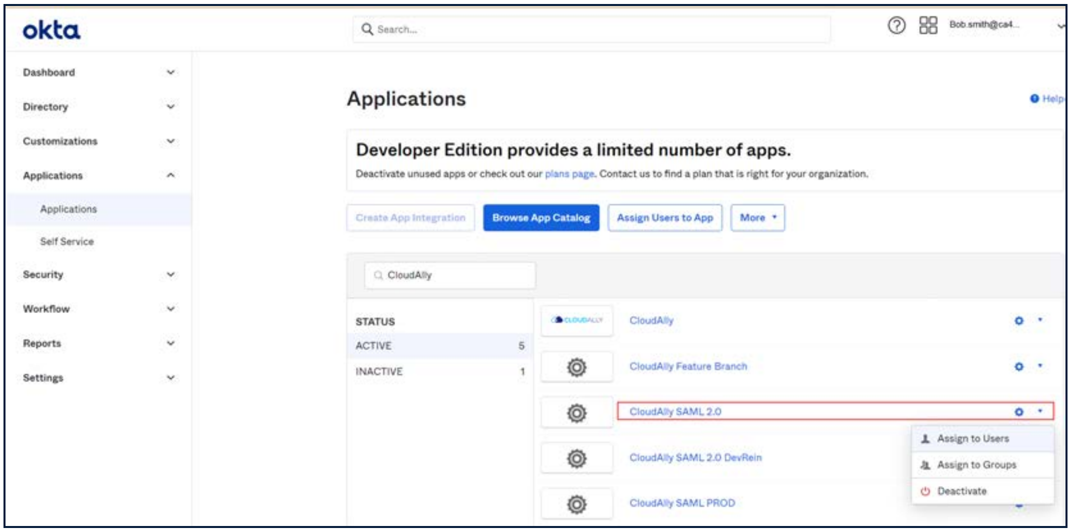
- In the Okta application, click **Applications > Applications > Browse App Catalog**.



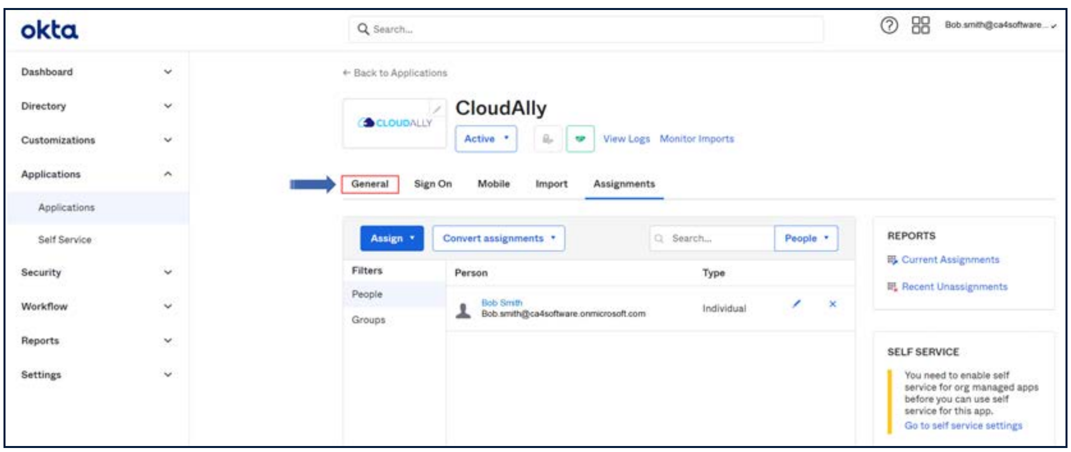
- In the search bar, enter CloudAlly.



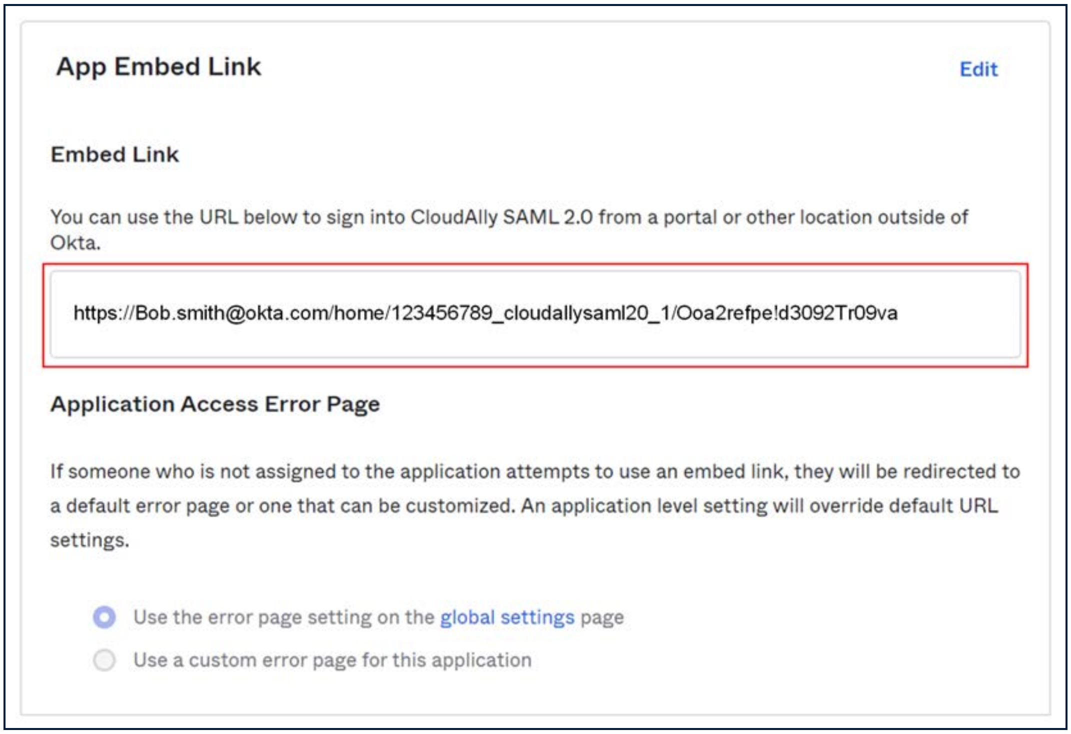
- Click the arrow next to CloudAlly SAML 2.0, and **Assign to Users** or **Assign to Groups**.



- Click CloudAlly SAML 2.0, and on the next page, click the **General** tab.

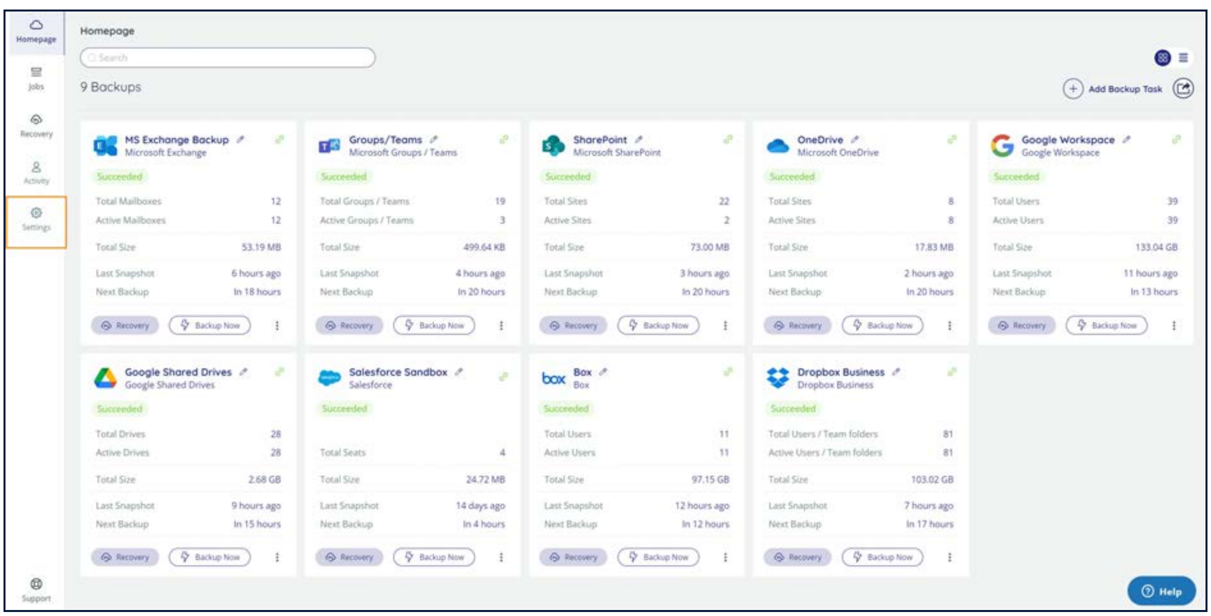


- Scroll down until you see the **App Embed Link** section. Copy the URL that is displayed - you will need this to set up Okta in the CloudAlly app.

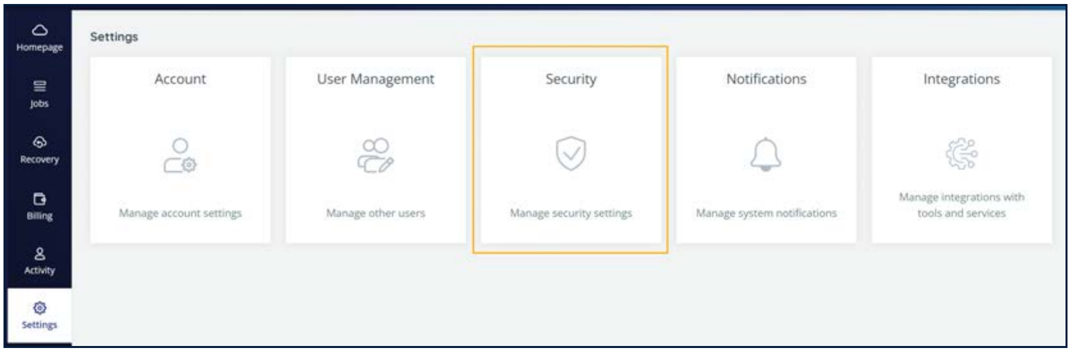


6.4.3.2 Setting Up Okta in the CloudAlly Application

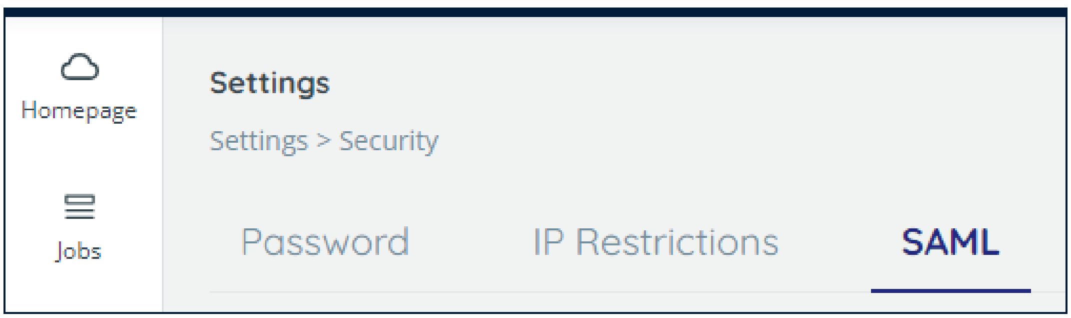
1. From the Homepage, click **Settings** in the Navigation panel.



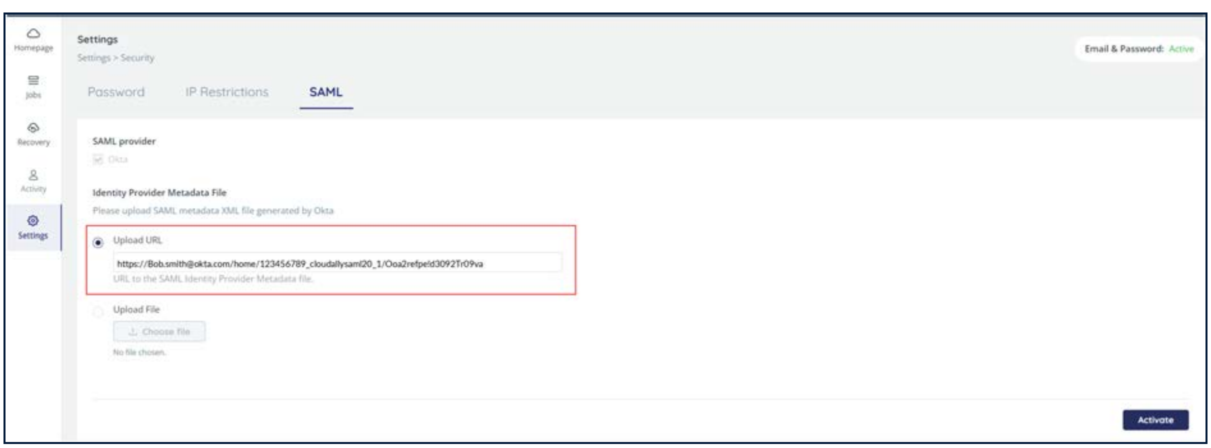
2. On the Settings page, click **Security**.



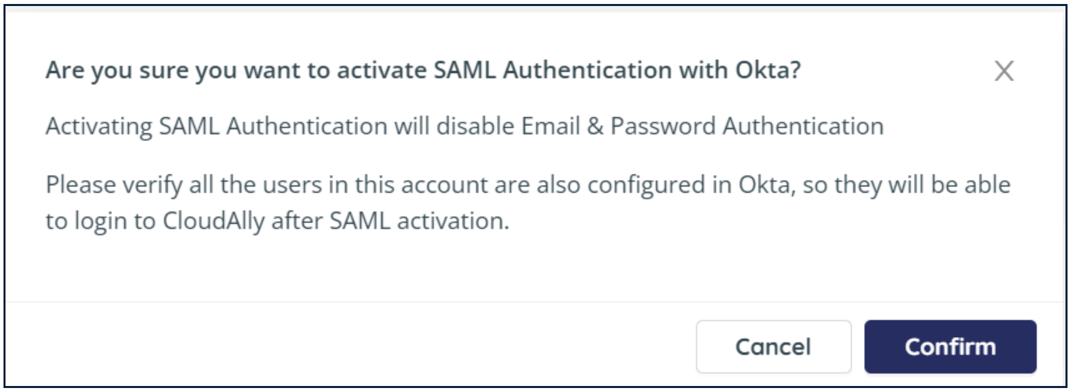
3. Click the **SAML** tab.



4. Paste the URL that you copied from the Okta site.



5. Click **Activate**.
6. Read the "Are you sure you want to activate SAML Authentication with Okta" message in the next window, and click **Confirm**.



After clicking **Confirm**, the Activate state changes from **Email & Password: Active** to **SAML: Active.**

6.4.4 IP Restrictions

Need fine-grained access control of your endpoints? You can restrict access to the Portal based on the users' IP addresses. This is especially helpful to enforce security policies and prevent unauthorized access by limiting backup/restore requests to company-approved IP addresses, such as an office IP, or a particular VPN.

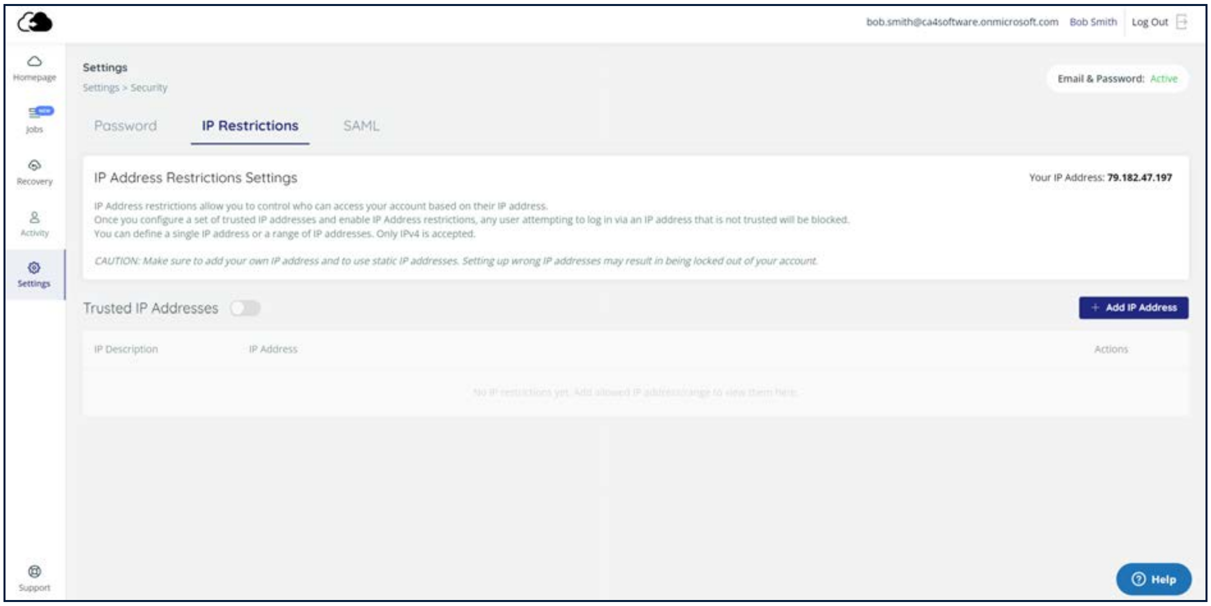
Setting Up IP Restrictions

To enable IP restrictions in your account, first create the list of trusted IP addresses.

> **IMPORTANT!**

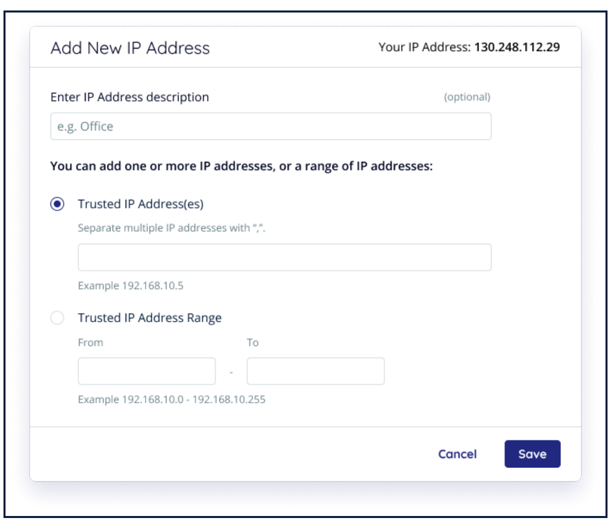
> It is strongly recommended to use this feature only if you have a static IP address, to prevent users from being locked out.

1. In the *Settings* panel, click **Security**, and then **IP Restrictions**.

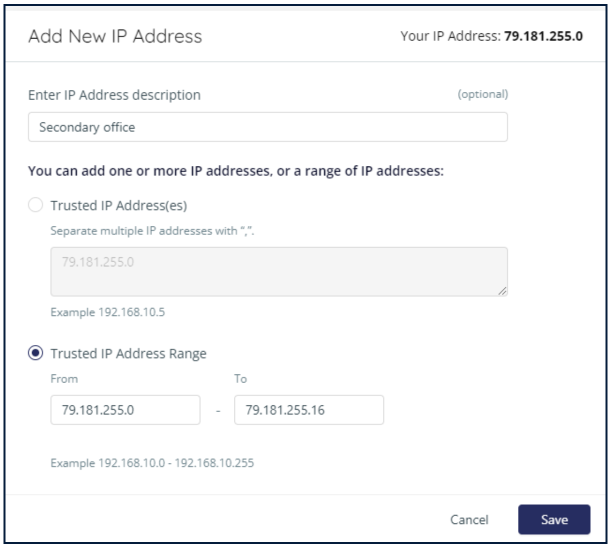


2. Click **+ Add IP Address.**
3. Enter one or more IP addresses:

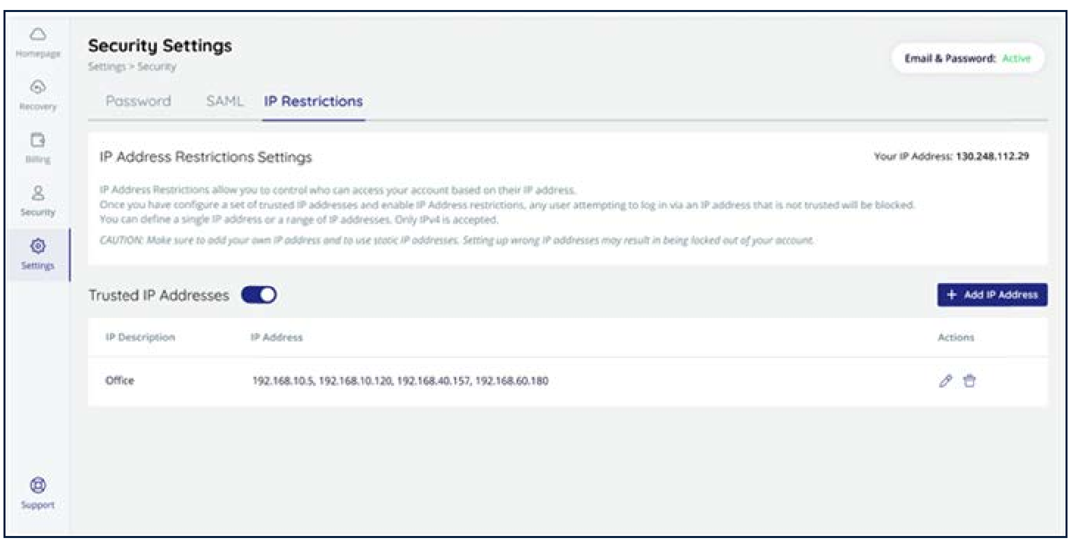
    a. Enter individual addresses separated by commas, and an optional description.



b. Or, enter a one or more ranges of contiguous addresses, and an optional description. Multiple ranges could be used to accommodate VPN and internal networks.



4. Once you enter at least one address, the **Trusted IP Addresses** toggle will be turned on. You can always return to disable IP restrictions later on.



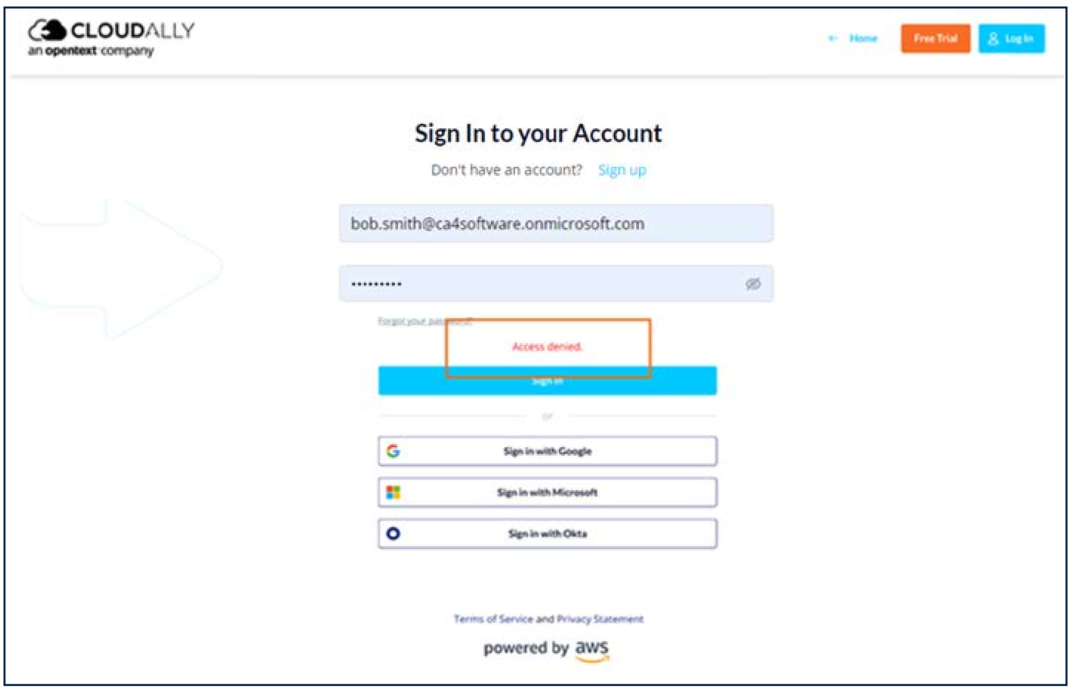
You can edit your list of addresses by clicking the pencil icon, or delete ones that you no longer want on your trusted list by clicking the trash icon.

> **Note:** If you forget to include your own IP address on the trusted list, IP restrictions cannot be enabled.

Your CloudAlly account is now protected from access by users who are not on your list.

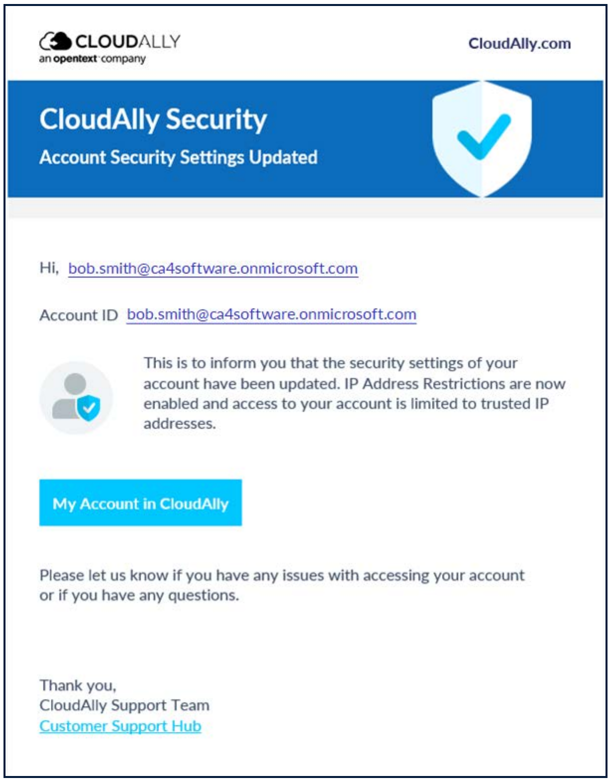
Blocking Access

If a user tries to access your CloudAlly account from an untrusted IP address, the following "access denied" error message will appear:



6.4.5 Email Notifications

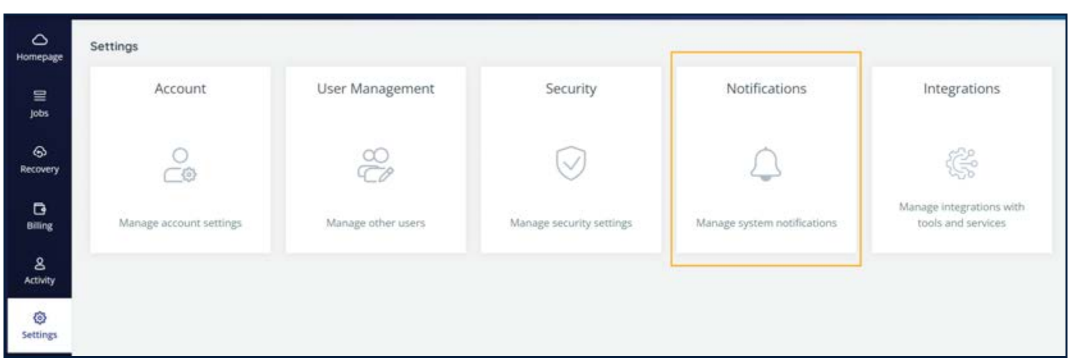
Whenever you enable or disable IP restrictions, or modify the addresses, CloudAlly will send you an email notification, letting you know what has changed.



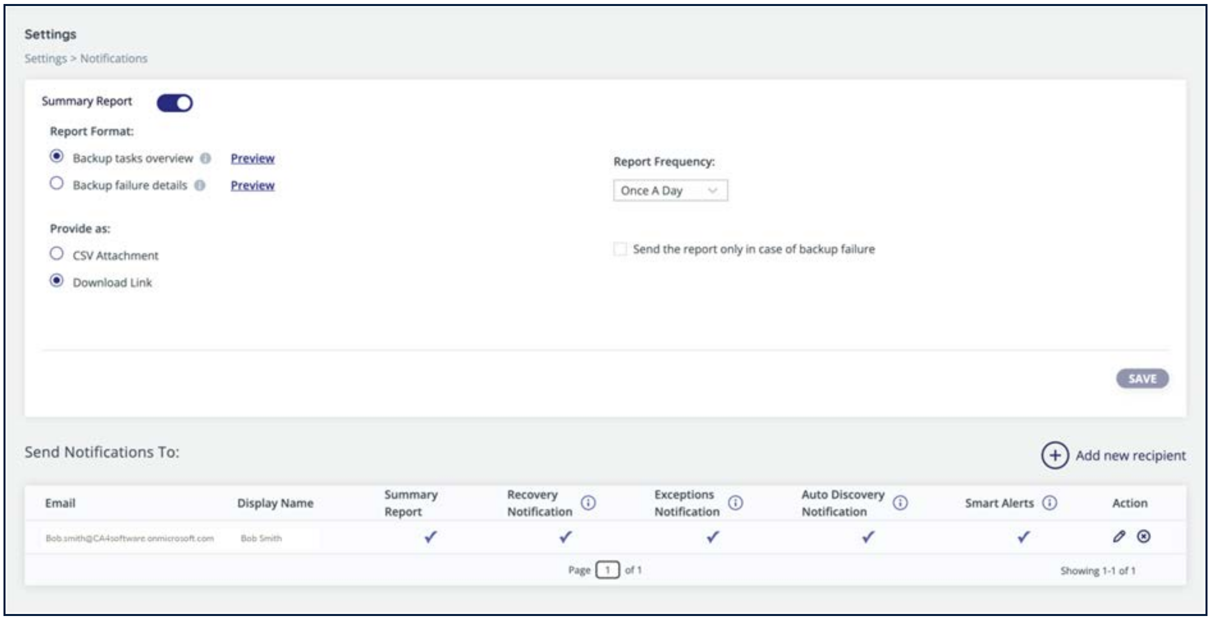
6.5 Notifications Settings

This menu option enables you to manage your system notifications.

From the Navigation Panel, click **Settings** > **Notifications**.



The following screen will appear:



The top of the screen enables you to configure the following options:

- Report Format: Backup tasks overview vs. backup failure details
- CSV Attachment vs. Download Link
- Report Frequency: daily, weekly or monthly
- Send the report only in case of backup failure

To set up a new recipient:

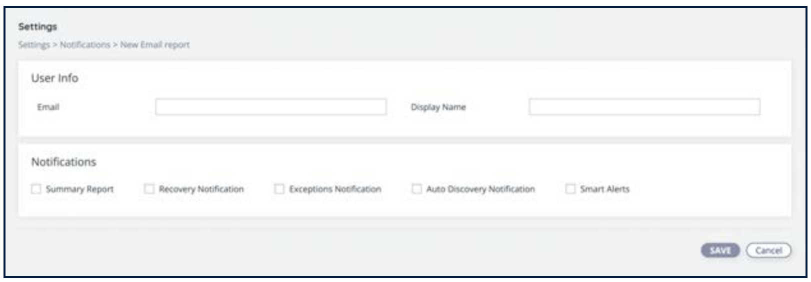
1. Click **+ Add new recipient**.
2. Enter the Email of the recipient and the Display name. The Display name is used in the report email to address the recipient.
3. Select the desired notification types:
    a. Summary Report
    b. Recovery Notification
    c. Exceptions Notification - This notification is sent both when there are backup errors and integration errors. (For integration information, see "Managing Your Account " on page 37.)

> **Note:** If no one is configured to receive Exception Notifications, then they will be sent to the Primary account user.

   d. Auto Discovery Notification

   e. Smart Alerts

4. Click **SAVE** to create the new recipient.



6.6 Integrations

The Integrations page displays all of the available integrations to external services and systems, with an option to connect either as a self-service, or by calling Support and providing additional details. The page also includes details about the REST API integration with an option to generate API tokens.

The following types of integrations may be configured on this screen:

- SIEM (Security Information and Event Management)
- RMM (Remote Monitoring and Management /PSA (Professional Services Automation)
- API - enables integrating with the CloudAlly REST API.

6.6.1 Splunk

The first available SIEM integration is with Splunk, using the Splunk HTTP Event Collector (HEC).

Versions Supported:

6.6.2 Which Events are Sent to Splunk?

You can choose to send one or more of the following to Splunk:

> **Note:** CloudAlly sends events to Splunk periodically, approximately every 10 minutes.

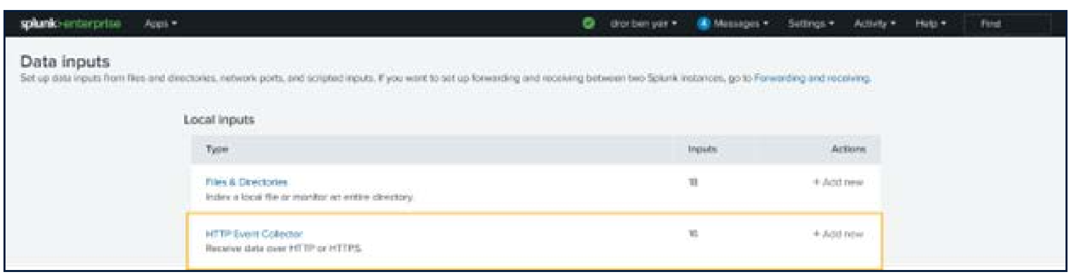
- Customers' activity events, such as backups and restores
- Customers' Security Audit logs (see " Security Audit" on page 40)

6.6.3 Pre-requisite: Setting Up Your Splunk Account

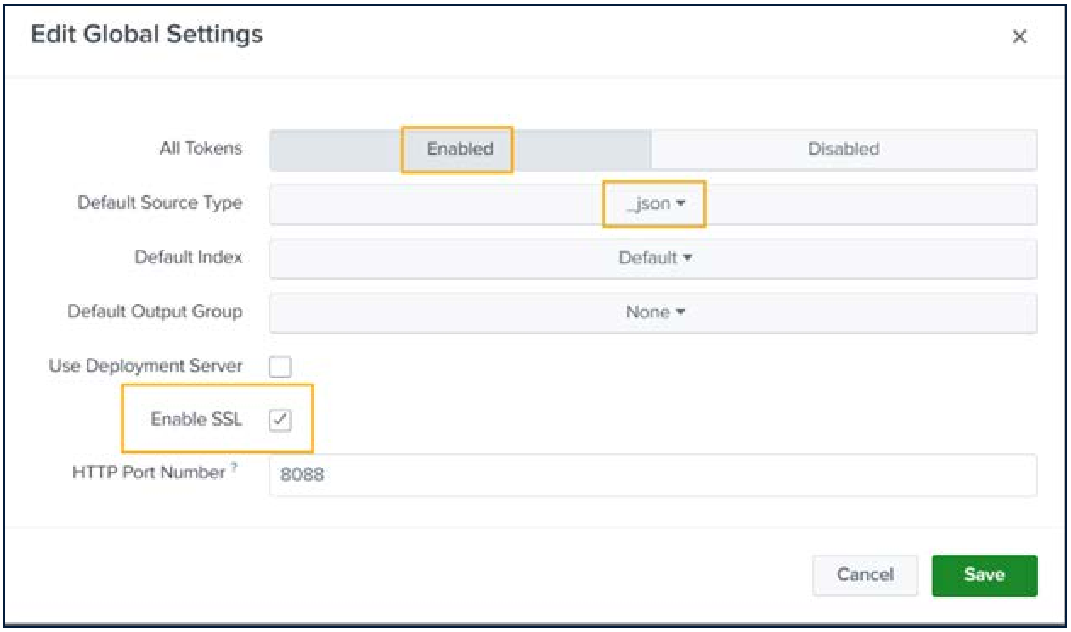
Before you can connect your backup account to Splunk, you first need to establish an account with Splunk and configure the Splunk HTTP Event Collector.

Perform the following steps in the Splunk Admin Console.

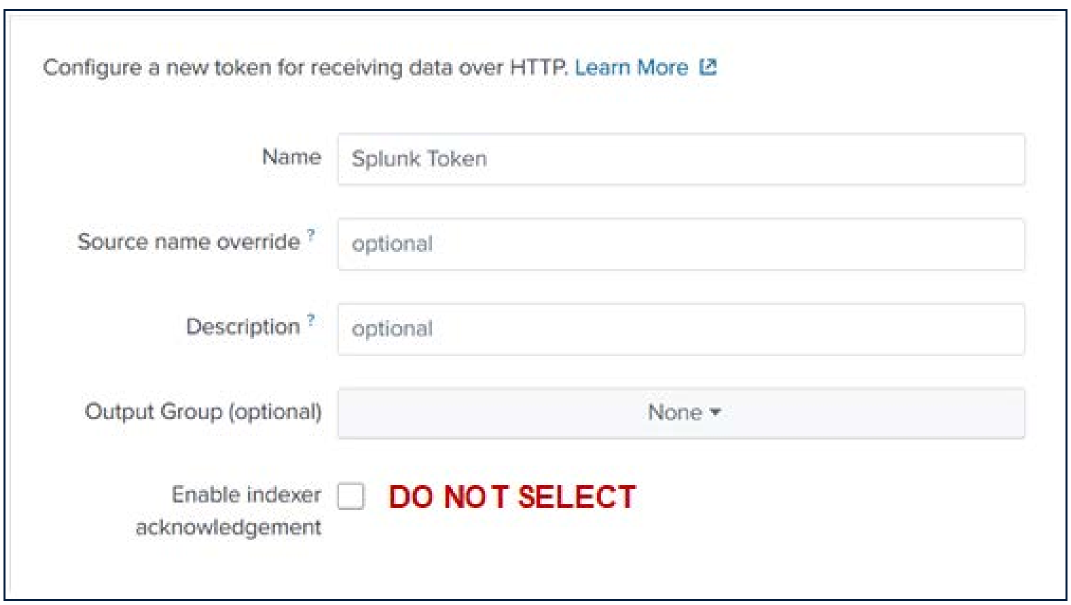
1. Navigate to **Settings>Data Inputs>HTTP Event Collector**.



2. Under the Global Settings option:
   a. Enable the HTTP Event Collector by setting All Tokens to **Enabled**.
   b. Choose **json** as default source type.
   c. Check **Enable SSL**.



3. Under the New Token option, create a new token and copy the value - it will be used in the CloudAlly Portal.



IMPORTANT NOTE: Do NOT check "Enable indexer Acknowledgment".

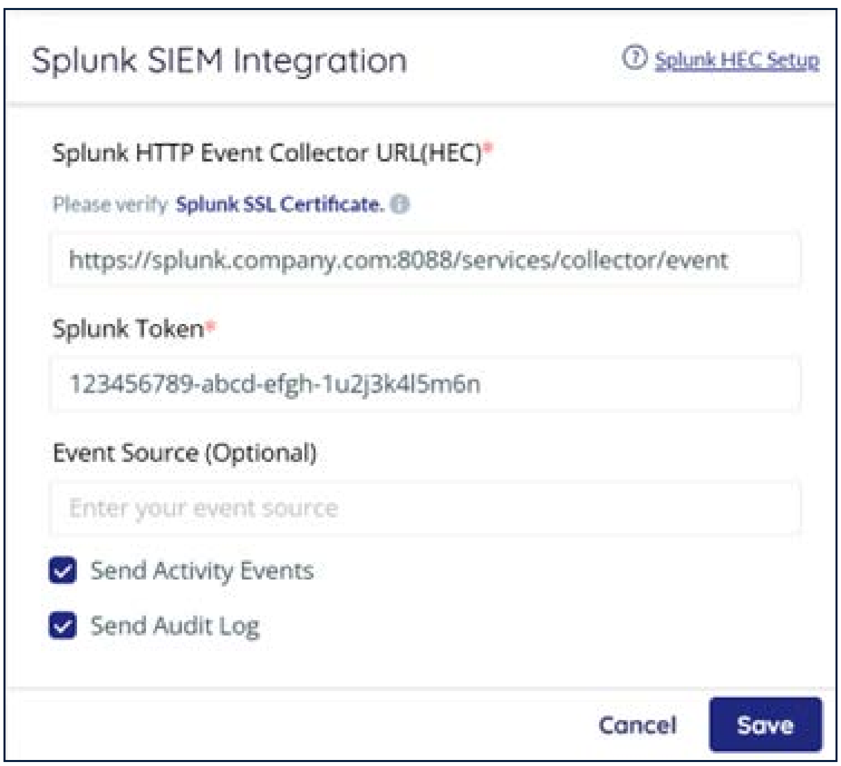
4. Find Your HEC URL.

The standard form for the HEC URL varies, depending on the Splunk software type you have. Find the standard form on this page: Set up and use HTTP Event Collector in Splunk Web.

5. Verify that you have set up an SSL certificate issued by a commonly accepted certificate authority (CA) on the Splunk HEC endpoint.

6.6.4 Setting Up Splunk in the Portal

1. From the navigation pane, click **Settings > SIEM**.
2. Click **Splunk > Connect**. Complete the fields on the following screen:
    a. Enter the Splunk HTTP Event Collector URL.
    b. Paste the token value that you copied into the Splunk Token field.
    c. Optional: Add the Event Source, which is the override value to assign to the event data.

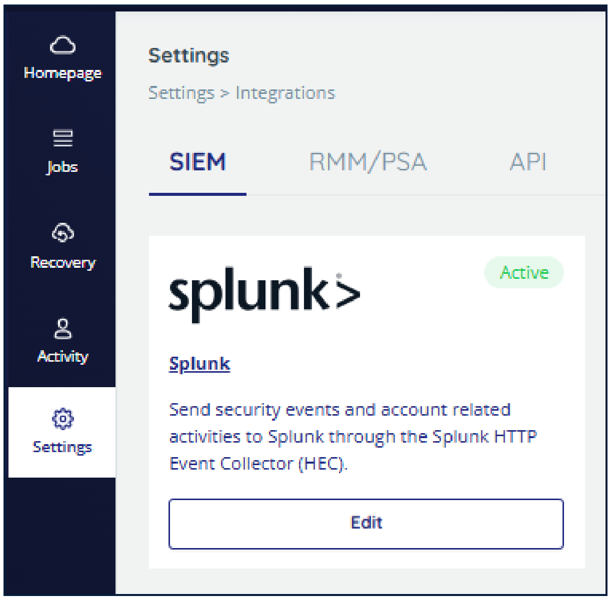


3. By default, there are 2 options at the bottom that are selected. You can de-select any that are not relevant for you:

a. Send customer activity events

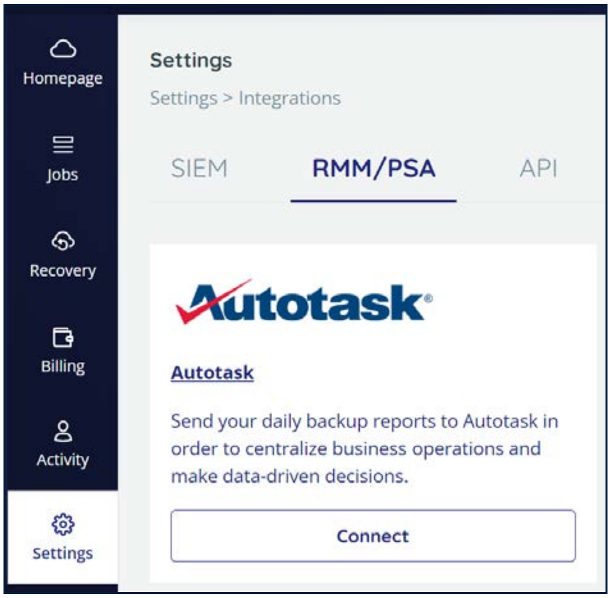
b. Send customer audit log

4. Click **Save**. The Splunk tile will now be Active.
5. To delete the integration, click **Edit > Delete**.



6.6.5 RMM/PSA

The RMM (Remote Monitoring and Management) and PSA (Professional Services Automation) page enables you to connect to Autotask.



Autotask is a PSA platform that provides complete visibility over your business with features like dashboards, sales, CRM, assets, inventory, and billing.

Once you have set up your account with [Autotask](), open a support ticket. Send us:

- Your Autotask ID
- Your Autotask ticket email service (ATES) Password
  NOTE: This password is for the ATES integration only and is separate from your Autotask log-in credentials.
- The email address you'd like your reports to be sent to.

Once the support representative has enabled Autotask, we will send any backup task failure reports to the email address provided, starting from the next backup cycle.

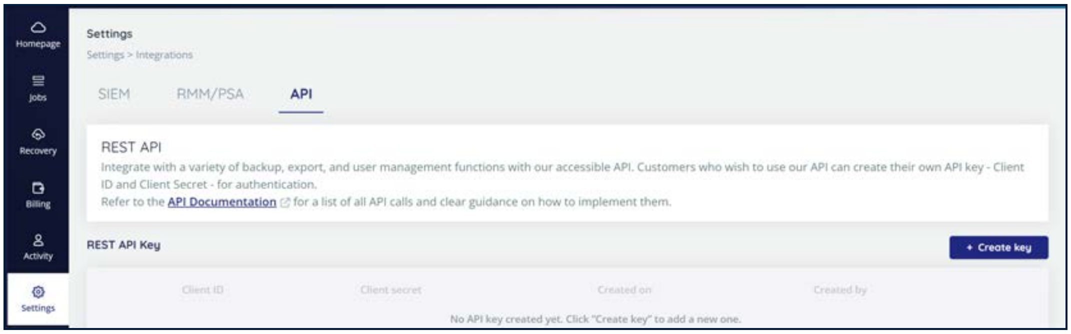
6.6.6 API

The third option on the Integrations page enables you to connect to the CloudAlly API.

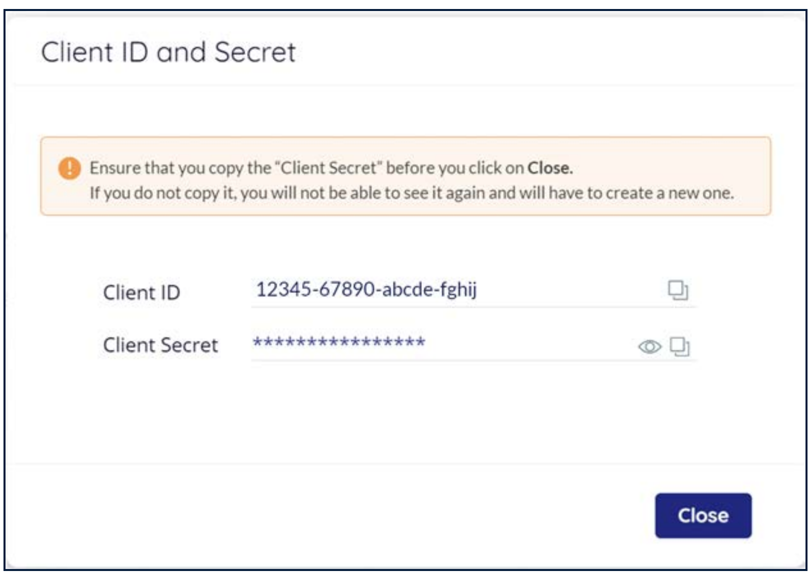
CloudAlly has a robust API, that enables you to perform billing management, backup, restore, and download management, Partner Portal management, and user management functions. It enables you to automate processes and integrate with the CloudAlly solution. The API can be used for many common business scenarios, such as exporting the data of customers who leave your company as part of the off-boarding process.

The REST API screen will be blank if you have never created an API key. If you have created one in the past, you will see it on the screen.

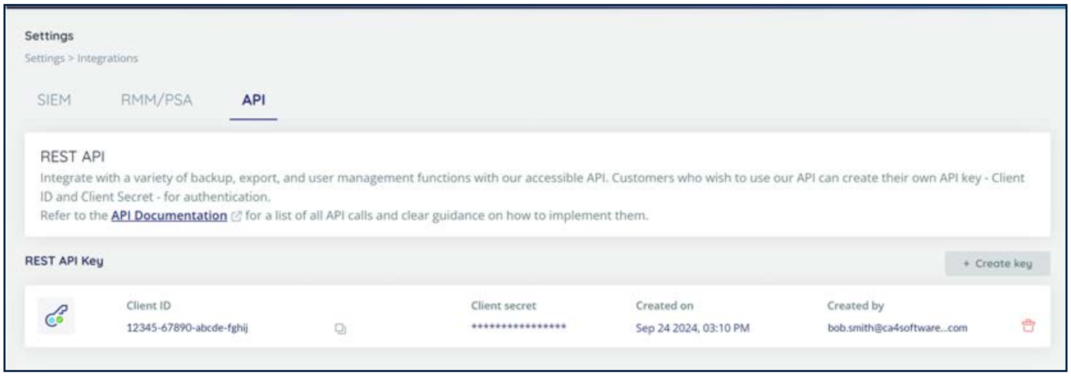
> **Note:** The Created On Date is not available for client IDs created prior to CloudAlly release 24.4.1.



The first step towards integrating with our API is generating your own Client ID and Client Secret for authentication. Click **+Create key**. The Client ID and Client Secret will be generated, so that you can copy them for use in the headers of your API calls.



> **IMPORTANT!** Ensure that you copy the "Client Secret" before you click Close. If you do not copy it, you will not be able to see it again and will have to create a new one.



If you need to delete your API key, click the trash icon.

6.6.7 Next Steps

Once you have generated an API key, the next step is to call the Authentication API using the Client ID and the Client Secret.

For each user, you need to create a unique access token and refresh token.

The complete list of CloudAlly API calls can be found here.

7 Managing Subscriptions and Payments

7.1 Subscribing to CloudAlly

Once the trial period has ended, you need to subscribe to CloudAlly to access and manage your backups, otherwise your backed up data will be deleted.

To subscribe to a plan:

1. Click the **Subscribe** link displayed in your account. Alternatively, you can click the **Billing** option of the Navigation Panel.

The *Review Billing* page is displayed with the option to select either **MONTHLY** or **ANNUAL** billing options.

> **Note:** You can subscribe before the end of the trial period, and the payment period will start after the trial period is over.

2. Click **MONTHLY** or **ANNUAL**, depending on your preference.

You are redirected to the *Payment Details* page. Fill in the billing and credit card details to finish the subscription process. Refer to Payment Details for more information.

7.1.1 Monthly Subscriptions

When you subscribe to a monthly plan, the credit card that you registered in the *Billing > Payment Details* page will be charged the amount that you owe.

CloudAlly's billing is handled by a PCI-compliant payment processor.

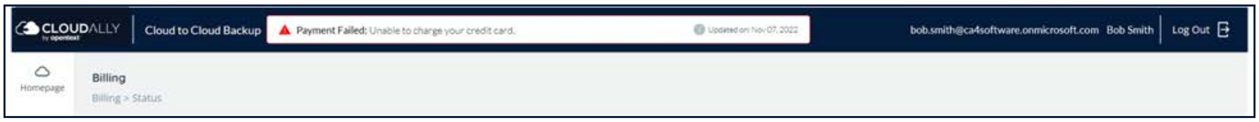
To finalize your subscription, enter your credit card details and general billing information, and then click **Subscribe**.

The initial payment will be charged at the end of your 2-week trial period.

A receipt will be emailed to you each month after you are charged.

If CloudAlly is unable to charge your credit card (e.g., because it has expired), you will be notified by email. Additionally, a message will appear in the application that you need to go to the *Billing Status* page so you can review your billing details, and then update your credit card information if necessary.

> **Note:** The billing status is usually updated within a few minutes after the payment is complete. If the status has not updated after 24 hours, please contact support@cloudally.com.



> **Note:** The monthly payments are processed automatically once you provide the required information in the Payment Details section, and it has been verified that your credit card is valid. To disable automatic payment processing, please contact CloudAlly support. Instead, you will start receiving monthly invoices for the payments.

7.1.2 Annual Subscriptions

When you subscribe to an annual plan, you will receive a confirmation message that your request has been submitted, and then CloudAlly support will send you an email, asking that you confirm your annual subscription request.

Once you have confirmed, CloudAlly will email an invoice to you, payable in 30 days by credit card, PayPal, or bank transfer.

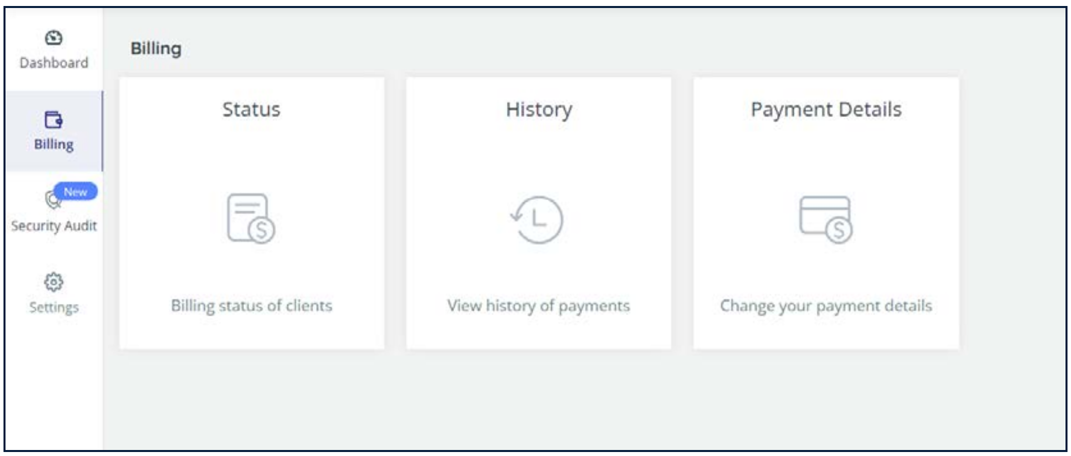
After the initial payment, CloudAlly will send you an invoice 30 days before your payment is due, in 11 months. You will also be reminded that your annual subscription is due online:

> **Note:** The billing status is usually updated within a few minutes after the payment is complete. If the status has not updated after 24 hours, please contact support@cloudally.com.

Should you fail to make your annual payment, you will be reminded with a message like this:

After you finalize your subscription, the *Billing > Payment Details* page displays additional billing management options and provides a brief summary of the payment information for the current period and the next payment date.

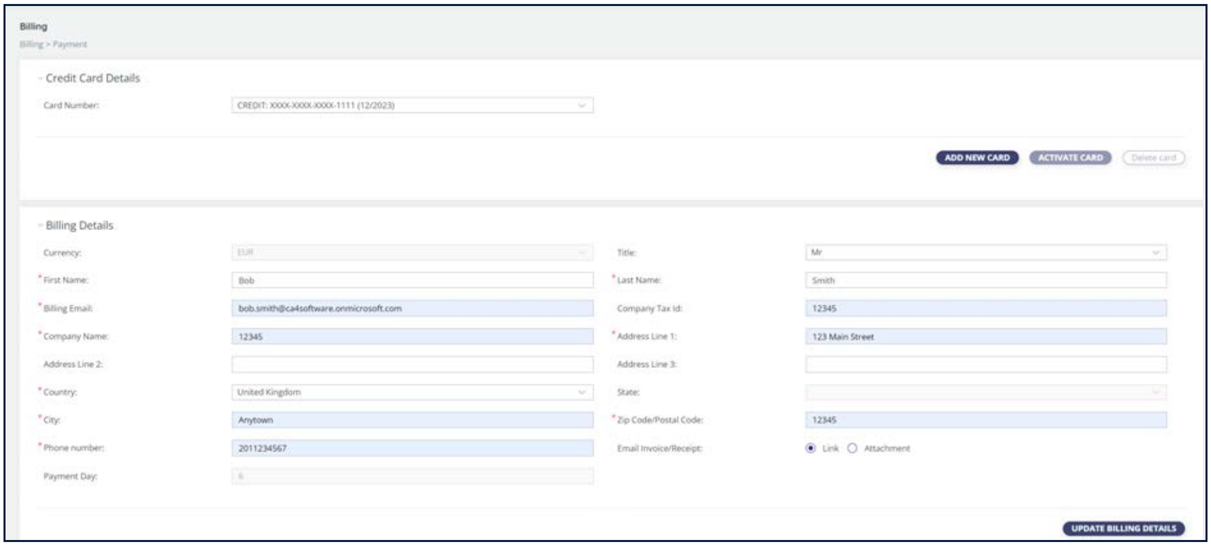
7.2 Payment Details



The *Payment Details* page contains the information used for billing.

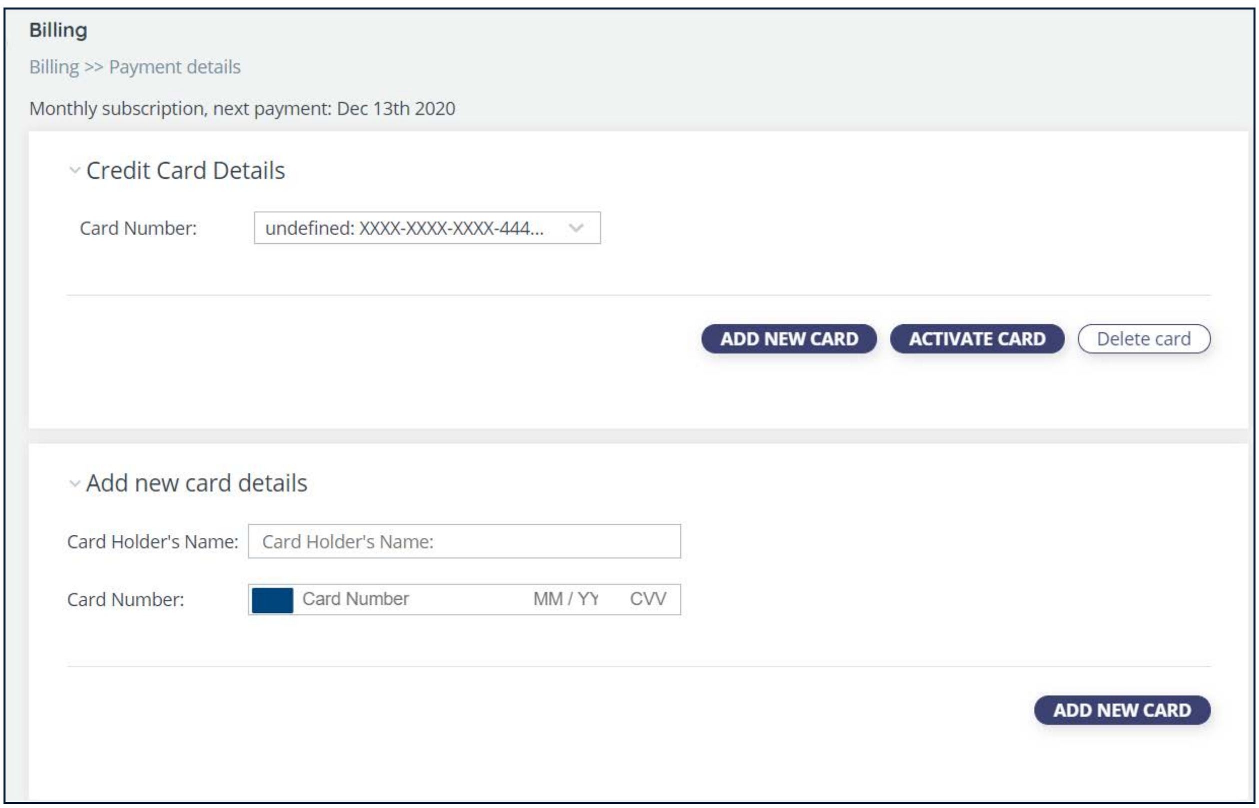
7.2.1 Monthly Subscriptions

If you have chosen a monthly payment plan, you can update your credit card and billing details here:



7.2.1.1 Add New Card

The **ADD NEW CARD** option enables you to define your card information for a monthly subscription payment.



To create a new payment method:

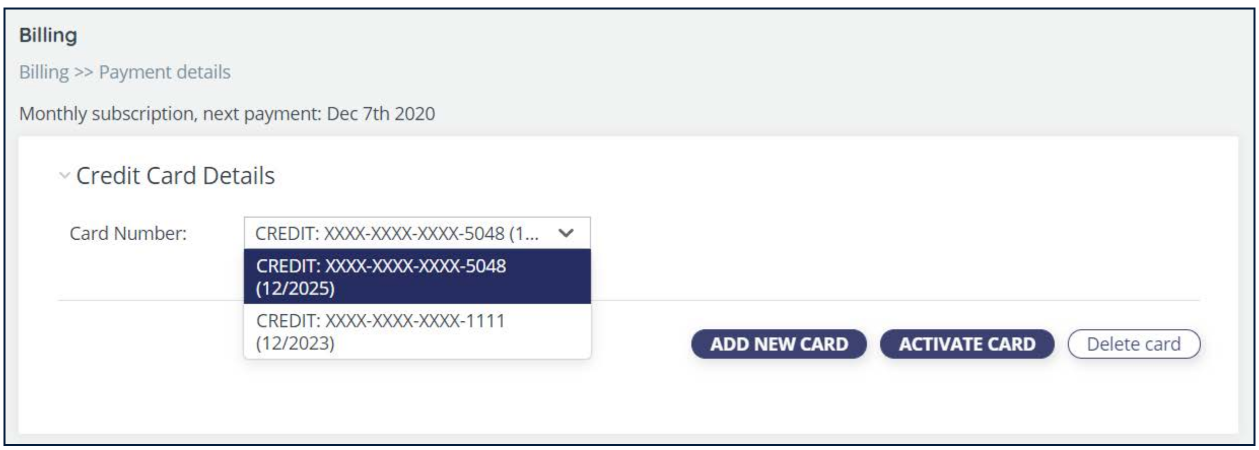
1. Click **ADD NEW CARD.**
2. Enter the card details such as Card Number, CVV, Card holder's name, and card expiry date.
3. Click **ADD NEW CARD**.

The new card information is saved and activated, and you can use this card.

7.2.1.2 Change Payment Method

To change your existing payment method:

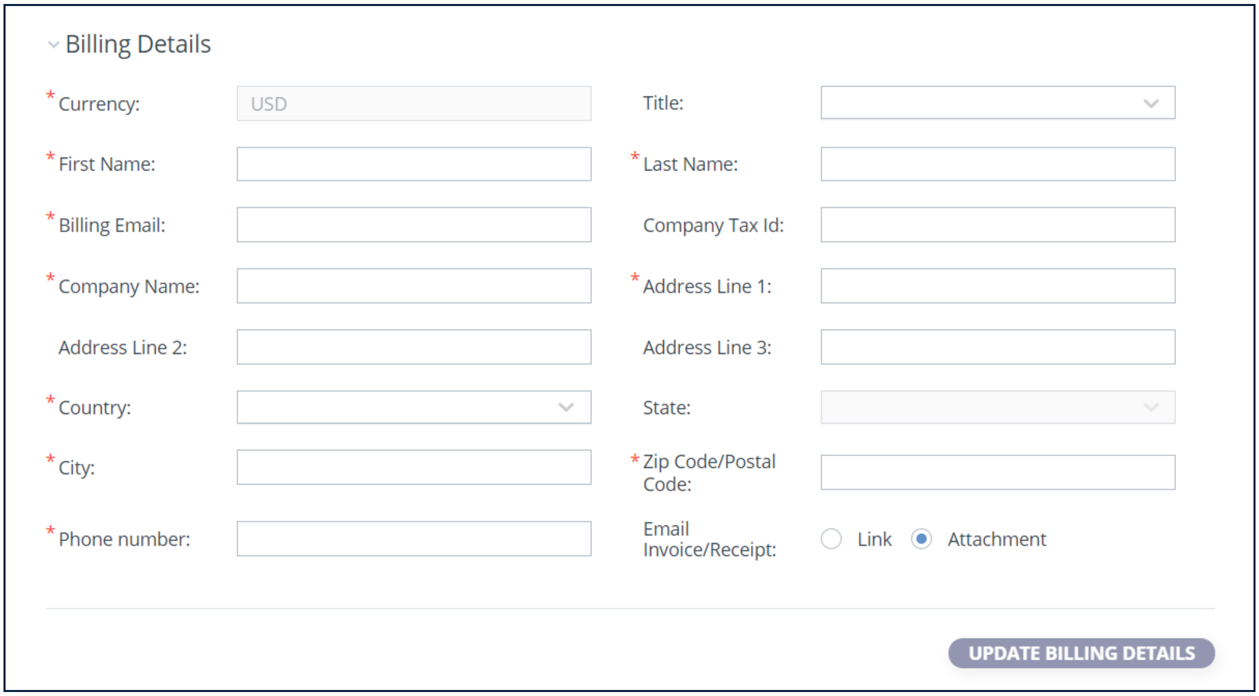
1. Click the drop-down list and select the payment method from the Cards Number drop-down list.
2. Click the payment method from the list (the screen shot below depicts choosing a different credit card).
3. Click **ACTIVATE CARD** to set the selected card as the preferred payment method.



The details section displays billing information such as Currency, Title, Name, and Billing email.

4. Below, there are more fields in the Billing details section. The Company Tax ID field indicates your company tax ID. (This is mandatory for Israeli companies.)

> **Note:** Due to Value-added tax (VAT), Israeli companies must include their Tax ID. Therefore, the Company Tax ID field is mandatory for Israel, and if this field is not completed, our company will not be able to provide you with backup services.



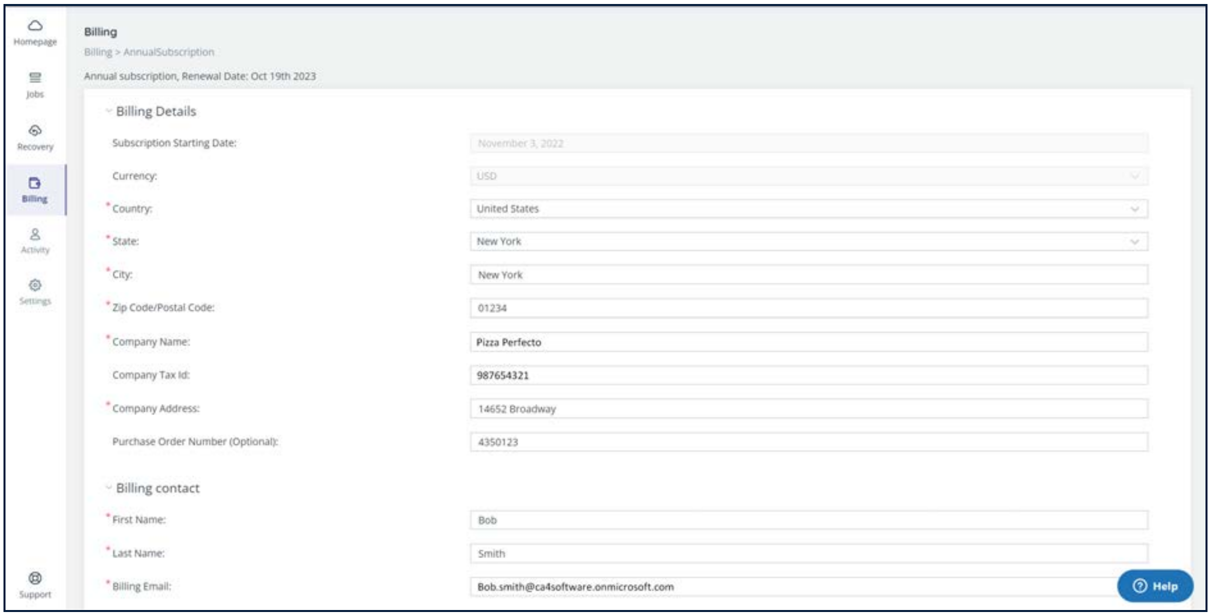
5. Update the required fields. The fields marked with the * symbol are mandatory.
6. Click **UPDATE BILLING DETAILS**.
7. The updates are saved.

You can choose whether you want to receive the Invoices or Receipts as a link or as an attachment to the email.

> **Note:** You can change the billing currency by contacting CloudAlly support.

7.2.2 Annual Subscriptions

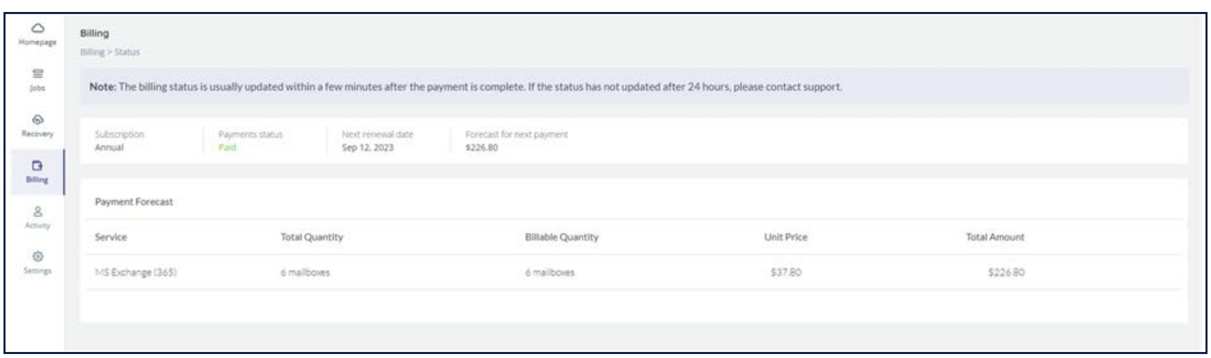
If you have chosen an annual payment plan, you can update your billing details here. When you are done, click **SAVE**.



7.3 Billing Status

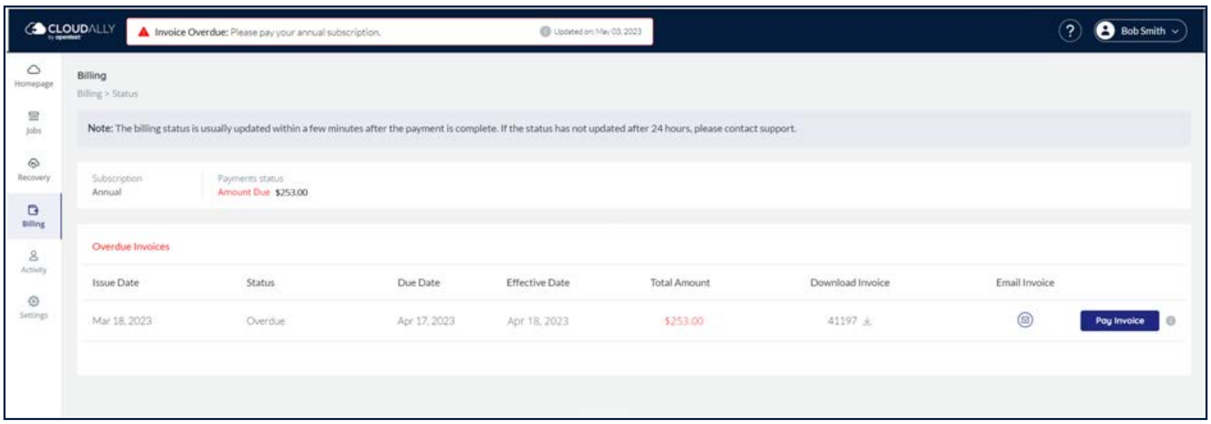
Annual Subscription

When you have paid your annual subscription, this page displays the next payment forecast for the upcoming payment date. The details include Service type and backup name, Quantity, Unit Price, and the Total Amount.

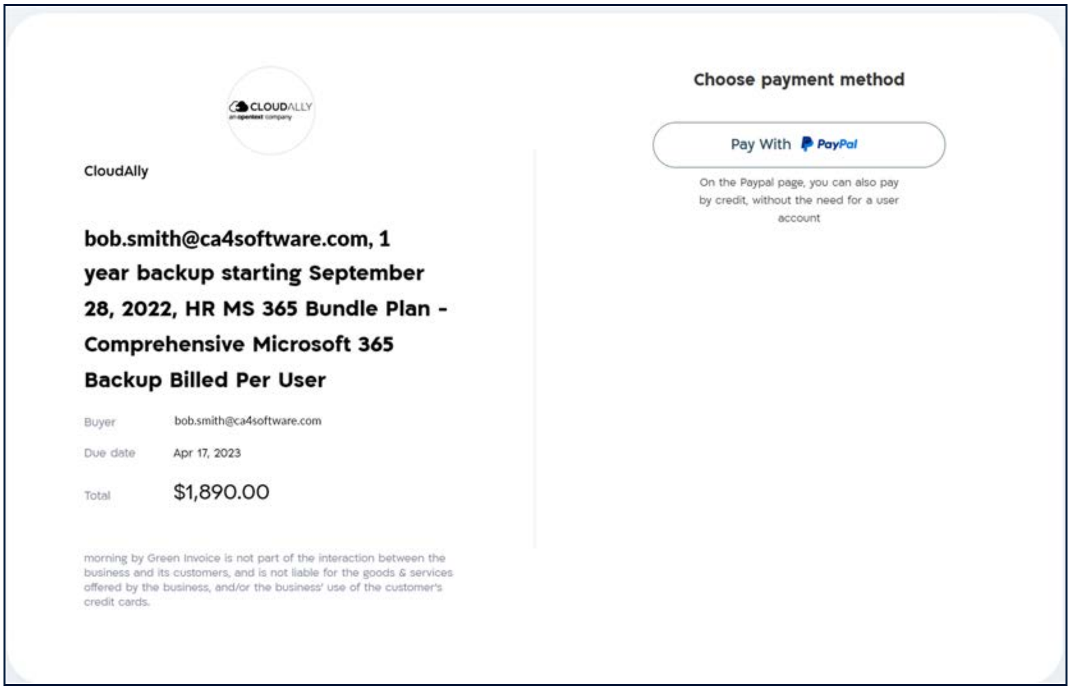


When your subscription amount becomes due, the Billing Status page displays the following information:

- **Issue date** - the date the invoice was issued
- **Status** - Paid, Due or Overdue
- **Due Date** - the date by which the invoice must be paid.
- **Effective Date** - the date the subscription period begins.
- **Total Amount** - amount owed.
- **Download Invoice** - Click this to download a PDF copy of your invoice.
- **Email Invoice** - Click this to send an invoice to your email address.
- **Pay Invoice** - Click this to directly pay the amount owed online.

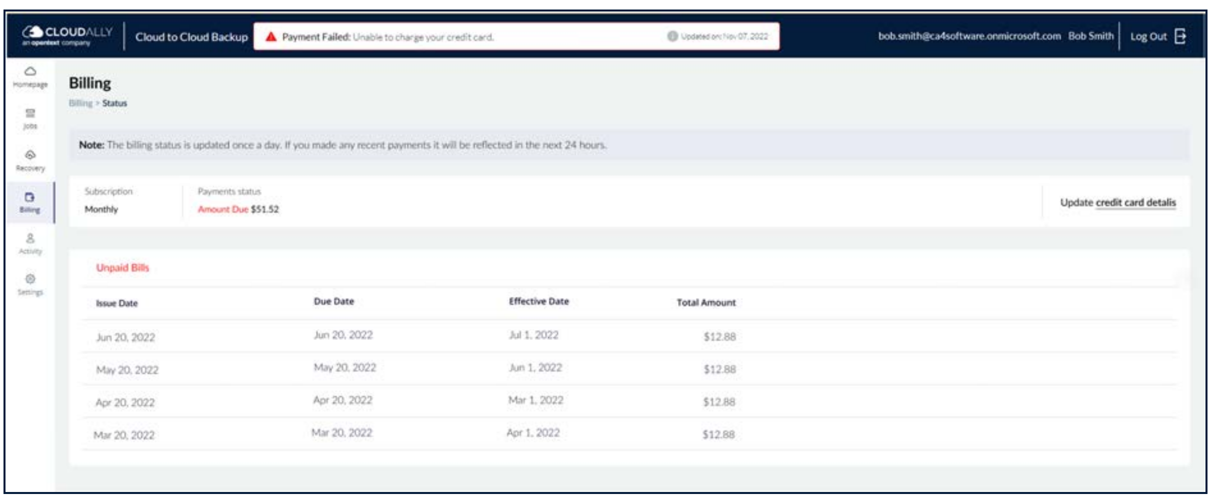


You can click **Pay Invoice**, and you will be directed to the following screen, where you can pay your invoice via PayPal or by credit card:



Monthly

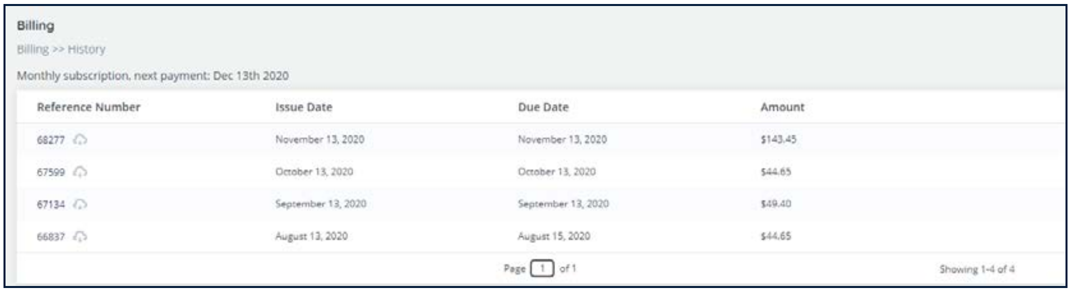
Similarly, if there was a problem with your monthly subscription payment, the status will look as follows:



From here, click **Update credit card details** and provide the new information.

7.4 History

This page displays the history of payments.



Reference Number	Issue Date	Due Date	Amount
68277	November 13, 2020	November 13, 2020	$143.45
67599	October 13, 2020	October 13, 2020	$44.65
67134	September 13, 2020	September 13, 2020	$49.40
66837	August 13, 2020	August 15, 2020	$44.65

By clicking on the reference number, you can download the receipt, which provides details about the number of backed-up accounts or the amount of stored data, and the total amount paid. It also displays the payment method used.

An example of a receipt is displayed below.

CLOUDALLY

To: pizza-perfecto.com – PPV001

Pizza Perfecto Ltd
18 Mozarella Lane
United Kingdom ID 307 123 08

CloudAlly Ltd.

Tax ID: 514596667
12 Harimon st., Gan Hayyim 4491000,
Israel
www.cloudally.com
accounting@cloudally.com

Invoice / Receipt 51646

Certified Copy

26 Apr 2021

Invoice / Receipt for admin@pizza-perfecto.com, 1 year backup starting April 22, 2021, GBP

QTY	Description	Price	Total
70	Dropbox 696.56 GB	16.25 GBP	1,137.50 GBP
		Subtotal	1,137.50 GBP
		VAT 0%	0.00 GBP
		Total payable	**1,137.50 GBP**

Payments Details

Type	Description	Date	Amount
PayPal	Account 12345678 / Transaction # 987654321	26 April 2021	1,137.50 GBP
		Total	**1,137,50 GBP**

Invoice / Receipt for Proforma Invoice 11392
Paid with PayPal
Merchant Account: KQMTW2PHR5CUG

Signature: CloudAlly Ltd
c.n 514596667

Secured Electronic Signature
Digital Document Signed by **Green Invoice**

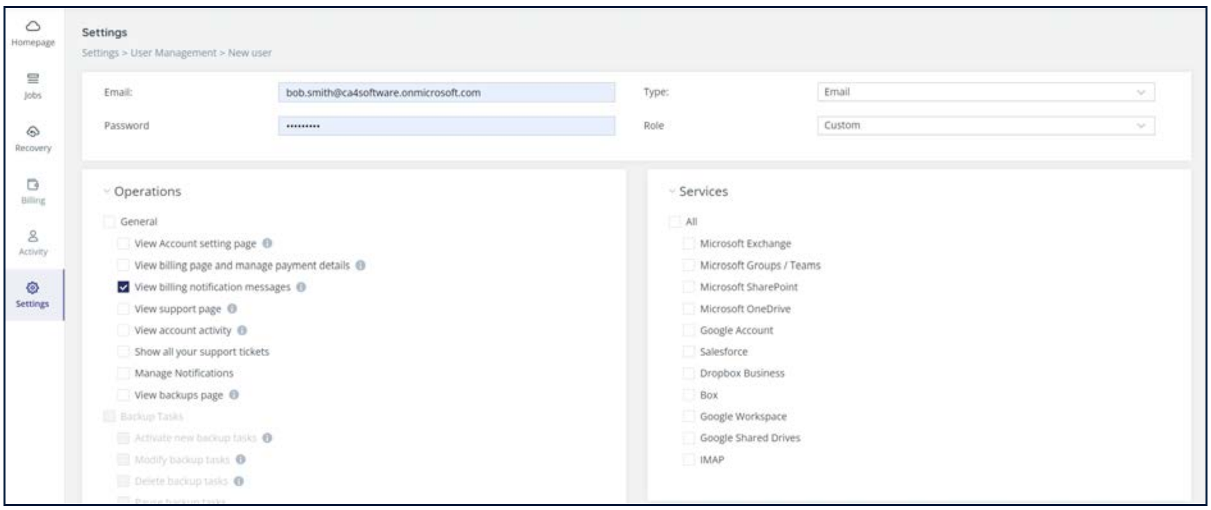
Created 26/04/2021 16:29 | Invoice / Receipt 51646 | page 1 of 1

7.5 Billing Notification Messages

Administrators can define whether individual users will see the Billing Notification Messages on their screens (e.g., Payment Due, Payment Overdue, Payment Failed).

To turn notifications on or off:

1. From the Navigation Panel, click **Settings > User Management**.
2. For an existing user, click the pencil icon next to the user's name.
   For a new user, the notification options will appear when you define the new user's details.
3. Click **View billing notification messages** on or off.



8 Helpful Resources

8.1 About CloudAlly

Founded in 2011 as one of the world's first cloud-to-cloud backup services for Google Apps and Salesforce, CloudAlly led the industry with the first commercially available Microsoft cloud backup in Q1 2014. ISO 27001 and HIPAA certified CloudAlly adheres to industry-standard best practices for information security management, including EU-GDPR compliance.

8.2 Knowledge Base

Search through articles in our Knowledge Base at https://support.cloudally.com to find answers to the most common user questions.

8.3 Support

Support - If you have any question or need further help, do not hesitate to contact us via email at support@cloudally.com. or visit our customer support hub: https://support.cloudally.com

8.4 Privacy

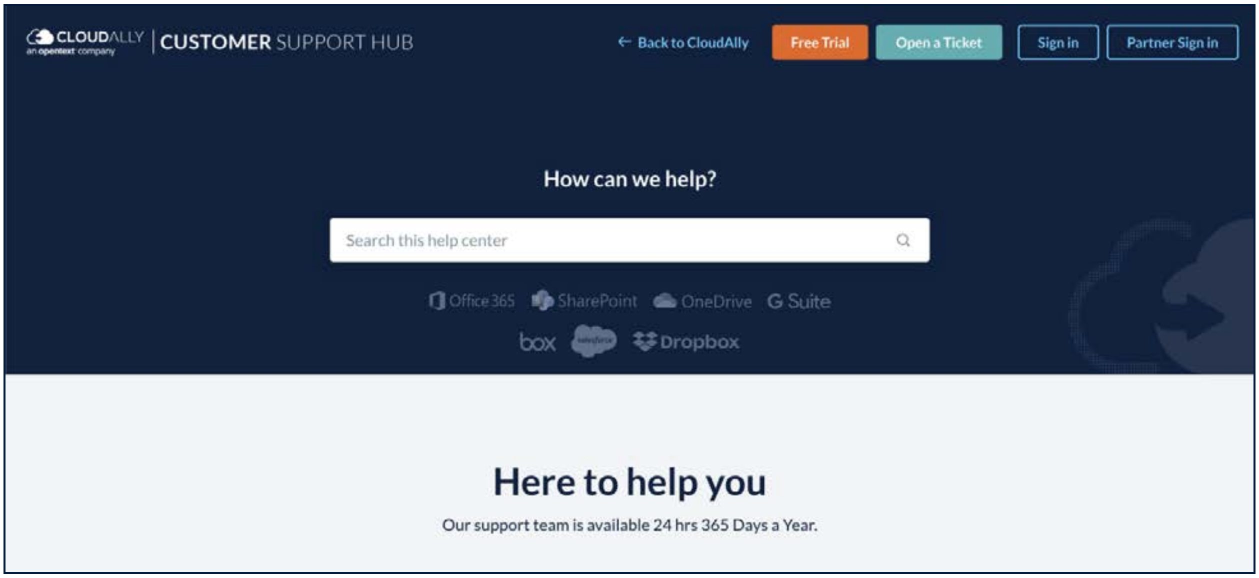
CloudAlly takes privacy seriously. Read our Privacy Policy at https://www.cloudally.com/privacy-policy

8.5 Security

CloudAlly provides a secure online backup solution with internationally recognized accreditation for information security management. Read how we protect your data at https://www.cloudally.com/resources/secure-saas-backup/

9 Support Pages

The Support option at the bottom of the Navigation Panel redirects you to our support hub. In the support hub, you can find articles covering some of the most common questions and providing instructions.



CloudAlly provides multi-channel support options:

Phone Numbers:

USA: +1 (424) 304-1959

AU: +61 2 8599 2233

UK: +44 114 303 2758

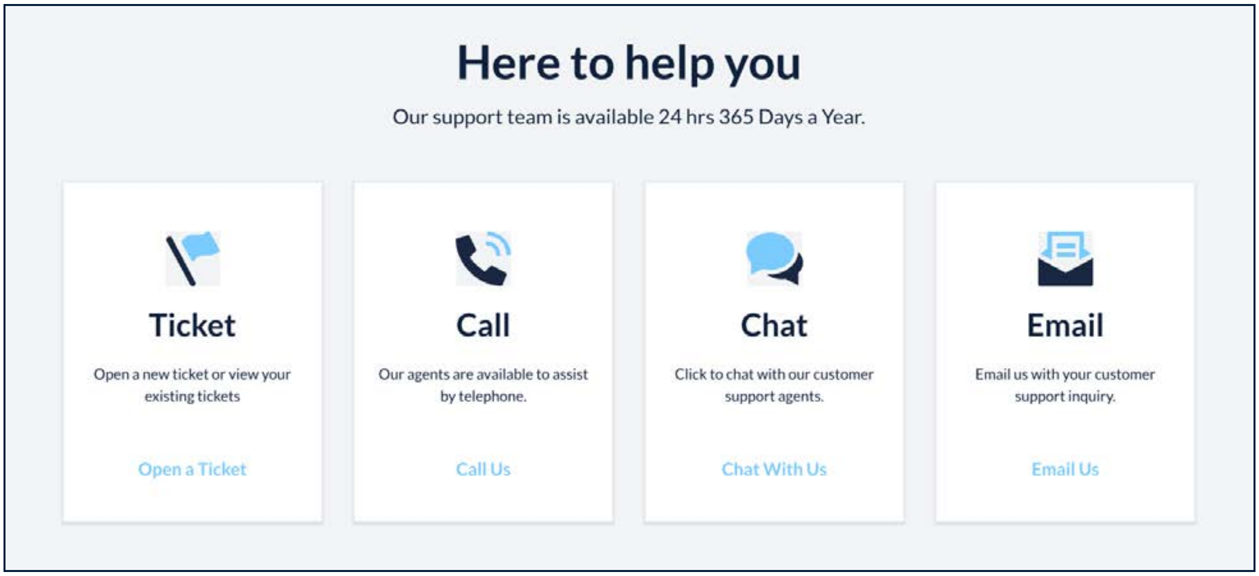
Email Addresses:

General Inquiries: Info@cloudally.com

Customer Support: Support@cloudally.com

Sales: Sales@cloudally.com

Open a ticket and the support team will contact you to help you with any question or problem.



Browse the articles, instructions, and tutorials in the Help Topics section. These materials are especially useful for new users as they explain the settings and procedures of backup activation, management, and recovery.