cloudally
NEVER FACE DATA LOSS

User Guide

Microsoft 365 Backup & Recovery

Microsoft 365

MS 365 CE 24.4.1

Table of Contents

Third-Party Trademarks

1 Preface

1.1 About this Guide

Thank you for selecting CloudAlly for Microsoft 365. Relax! All your Microsoft 365 data is now securely protected with easy recovery from data loss. CloudAlly comprehensively backs up your Microsoft 365 Exchange, OneDrive, SharePoint, OneNote, Teams & Groups 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 Microsoft 365.

1.3 What's in this Guide

This guide is organized to help you find the information you need to manage CloudAlly for Microsoft 365. It is divided into functional parts intended to support you as you manage your environment:

- Creating and Accessing Your Backup Account
- Backing Up Your MS 365 Data
- Recovering Your Backed Up Data
- Compliance
- Filtering and Viewing Drill-Down Details

- Managing Your Account
- Managing Subscriptions and Payments

2 Creating and Accessing Your Backup Account

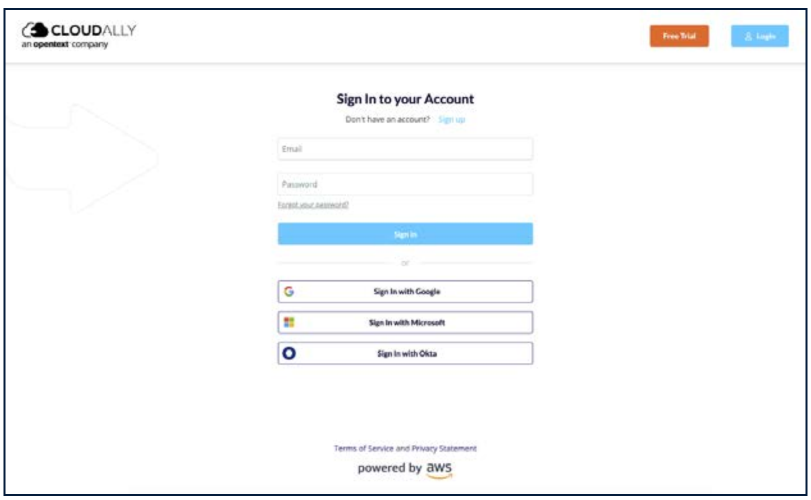
2.1 Prerequisites

To administer the backup for the Microsoft 365 environment, the following is required:

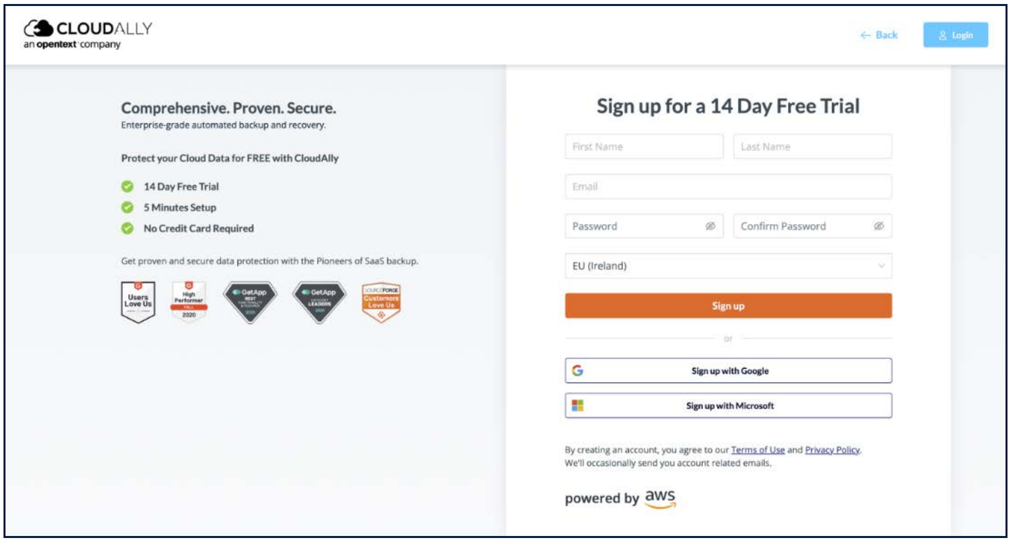
- Microsoft license
- Global Administrator account in Microsoft Office - online version

2.2 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 **Sign Up.** The *Sign Up* page is displayed.



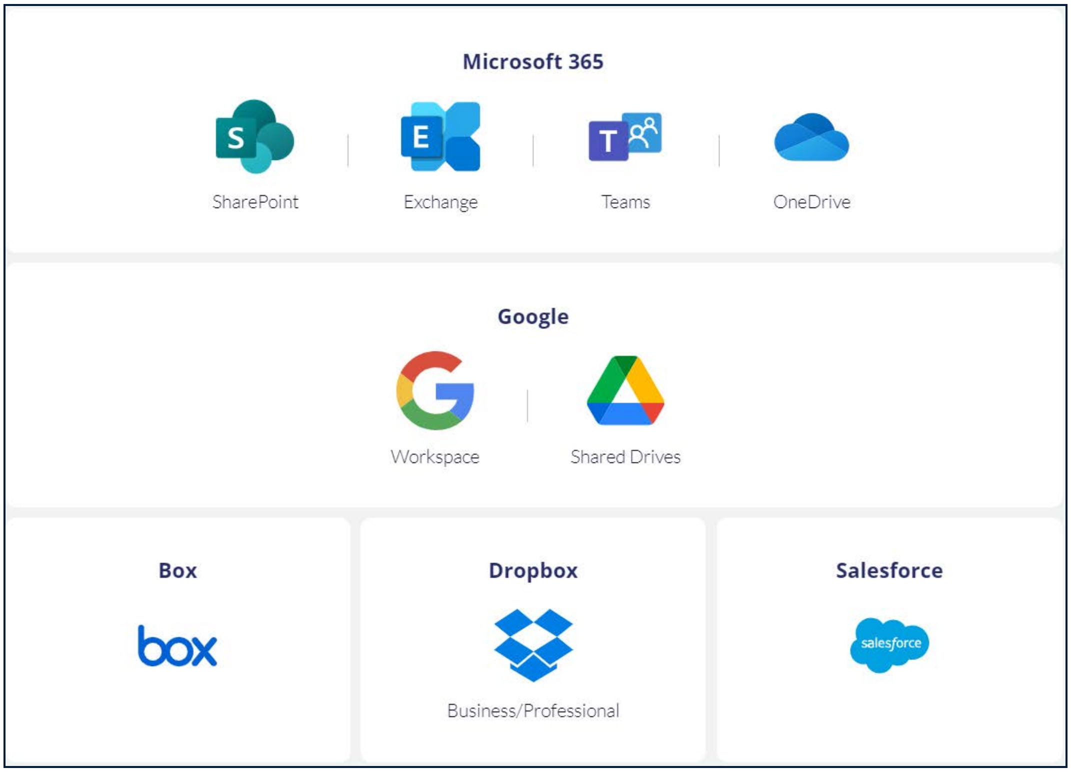
4. Complete the form, and then click Sign up. You can log in using a username and password, with your Google credentials, or with your Microsoft credentials.

> **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, and Japan. 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 .

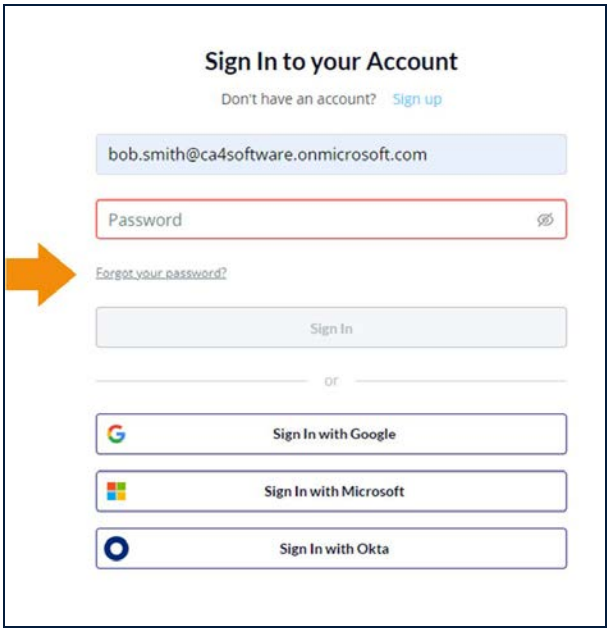
7. After you log in, you will see the following screen, enabling you to begin creating your backup tasks:



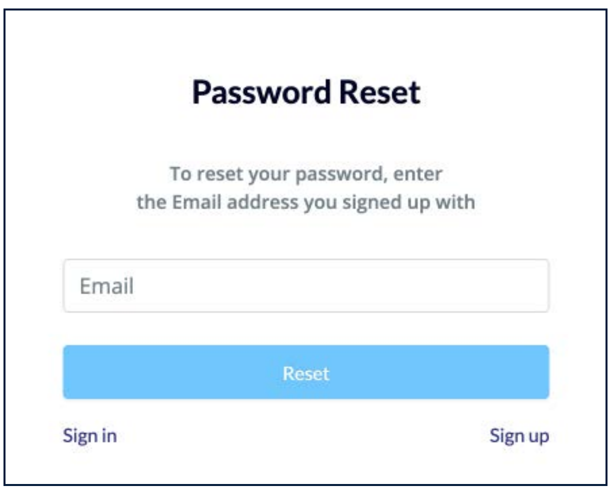
2.3 Resetting Your Password

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

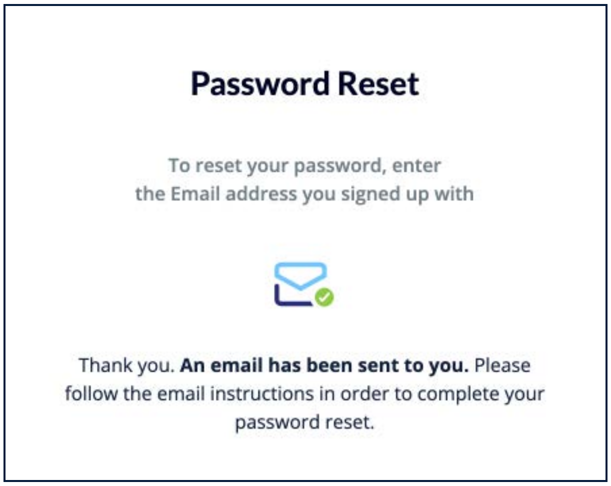
1. On the sign-in page, click **Forgot your password?** to start the process of resetting your password.



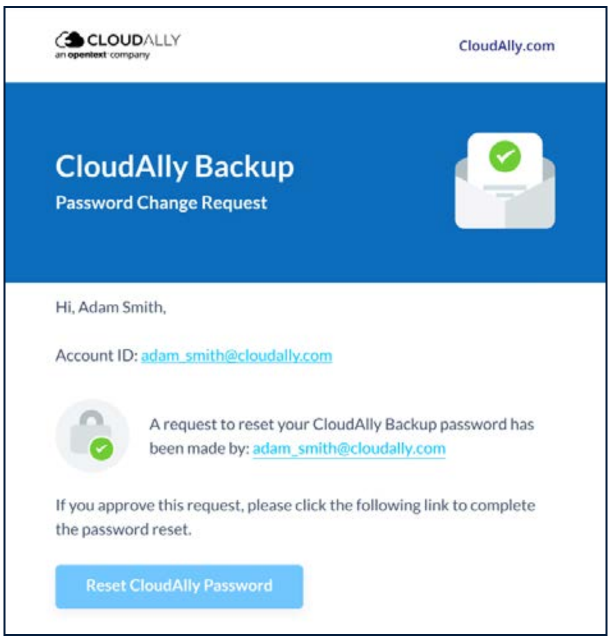
2. The *Password Reset* page will appear.



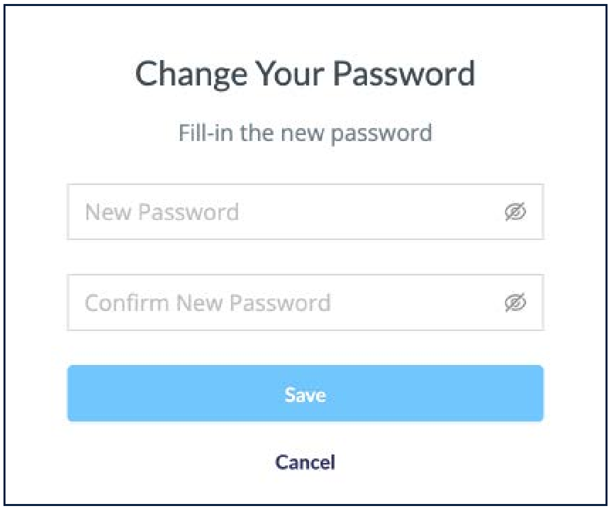
3. In the Email field, enter the email address that you used to sign up.
4. Click **Reset**, and the *Password Reset* window will appear.



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 Microsoft 365 Data

Microsoft 365 lacks the daily backup and archiving process necessary for you to restore data after it has been manually or automatically removed from the recycle bin. CloudAlly's automated daily backup of your Microsoft 365 data ensures that you can both quickly recover data from any point in time as well as export your archives for local storage.

CloudAlly's Microsoft 365 service backs up data from:

- Mail, Calendar, Contacts, Tasks and Notes (Microsoft Exchange)

> **Note:** CloudAlly does not back up Exchange Online Archive by default. If you would like your Online Archive to be backed up, contact Support.

- Conversations, Sites, Calendars and Channels (Microsoft Teams and Groups)
- All of your sites, files, and libraries (Microsoft OneDrive and Microsoft SharePoint)

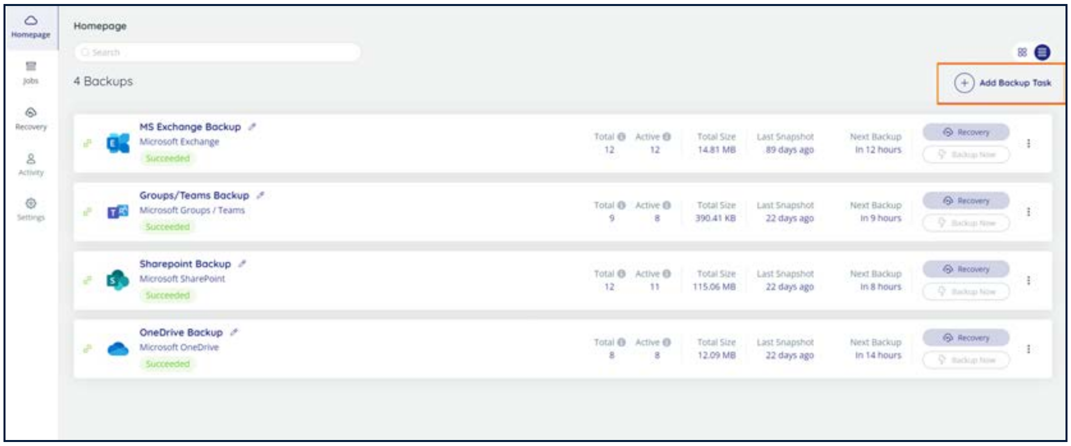
With a few simple clicks, you can activate backups for all or selected users.

3.1 Microsoft 365 Exchange

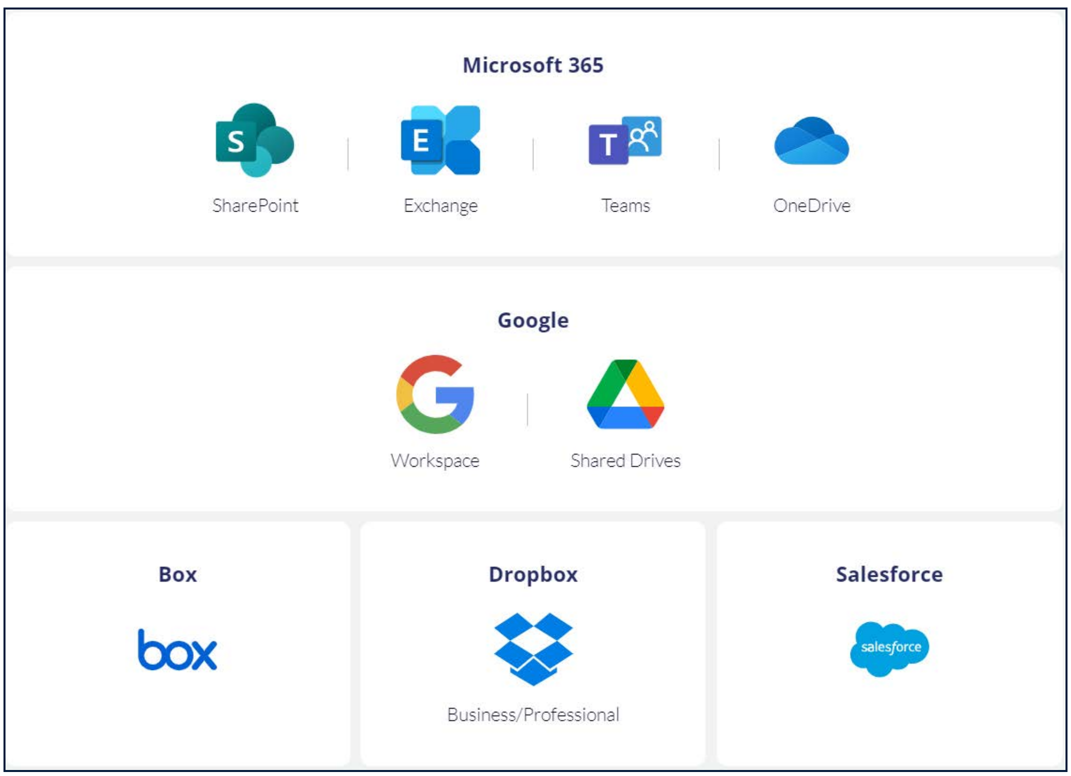
3.1.1 Creating a New Backup Task

To create a new backup task:

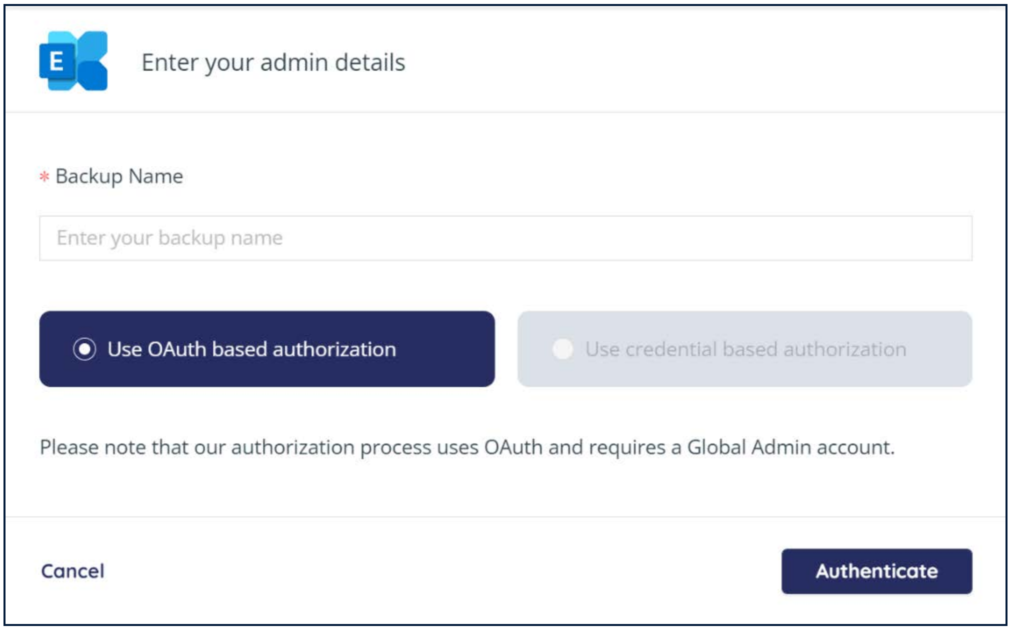
1. Sign in to your account, or if you are already signed in, click the **Homepage** option in the Navigation Panel.
2. On the Homepage, click **+ Add Backup Task**.



The following page is displayed:



3. Click the name of the service you would like to back up, in this case: Microsoft Exchange.



1. Fill in the name of the backup task. This name is used in the notifications and reports, and it can be changed later.
2. You will see the OAuth based authorization Click **Authenticate** to start the process of granting the access token. You will be redirected to the *Microsoft sign-in* page. Enter Global Admin credentials to sign in to your Microsoft account.

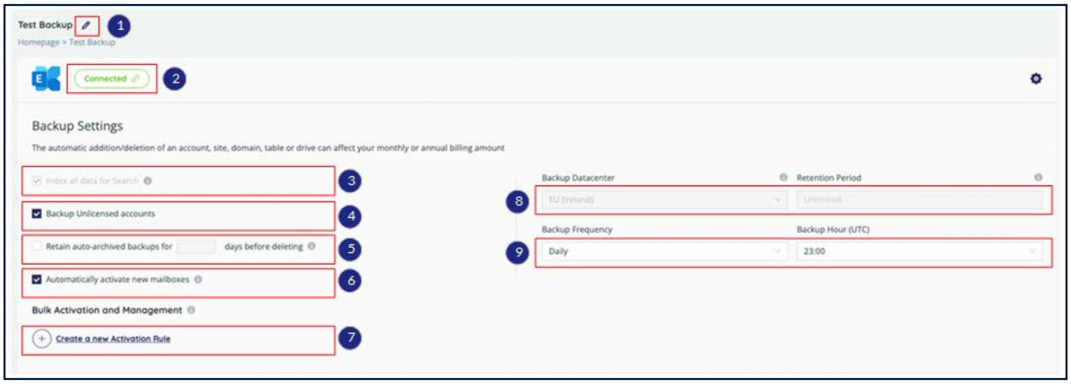
IMPORTANT!

The user that you enter **must** have Global Admin permissions.

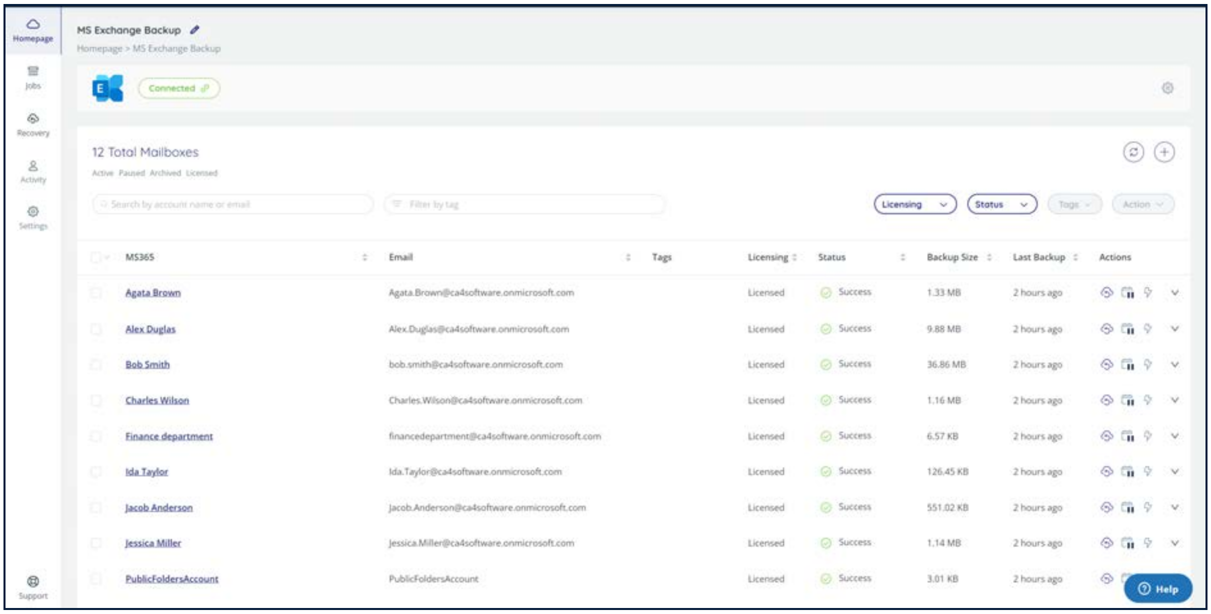
Note: "Use credential-based authorization" is not active by default, and we don't recommend it. If you would like to use this, contact Support.

3.1.2 Configuring a Backup Task: Microsoft Exchange

This set of options enables you to select the backup settings for the account, team or site. Click the gear-shaped settings icon.



1. You can change the name of the backup task by clicking the pencil icon.
2. The Connected / Disconnected icon indicates whether the application was able to connect to the specified Microsoft 365 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 the Disconnected icon. 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.
4. In the Microsoft Exchange system, accounts can have a Microsoft “Unlicensed” status (not to be confused with “Unlicensed CloudAlly product”). These can be the external accounts invited by users with an active license, accounts automatically generated for shared file storage, etc. Check the Backup Task page to see which accounts are MS licensed and unlicensed.



> **Note:** "Unlicensed" accounts have limited permissions, and we don't advise using "Unlicensed" administrator accounts.

5. Backups are automatically archived when an entire account is deleted. The **Retain auto-archived backups** option allows you to retain them for a specified number of days, after which they will be automatically deleted. Otherwise, the backups will be retained indefinitely.
6. The **Automatically activate new mailboxes** option instructs the system to detect new mailboxes, and begin backing them up automatically.
7. Create a new activation rule - see explanation below.

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

8. The **Backup Datacenter** field displays the Datacenter location you selected when you signed up with your registration.
9. 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 submitting a support ticket. Backups older than the retention period specified will be automatically deleted.

> **Note:** Your backup storage data center cannot be changed once it's been set during the account setup process. Contact 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.

10. **Backup Frequency and Backup Hour**

    a. Click the drop-down list of 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 of the **Backup Hour (UTC)** field and select the backup hour. Click **Save**.

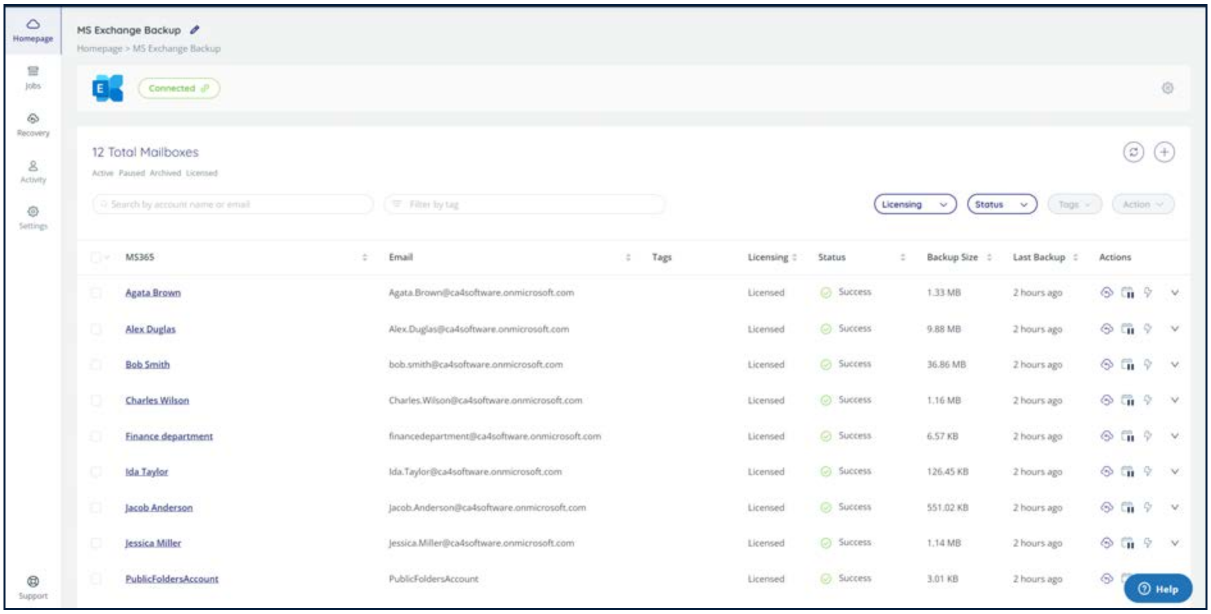
> **Note:** 3x daily backups might be subject to additional charges. Please contact Support or your sales representative if you have any questions before changing the backup frequency.

3.1.3 Activating Your Backups

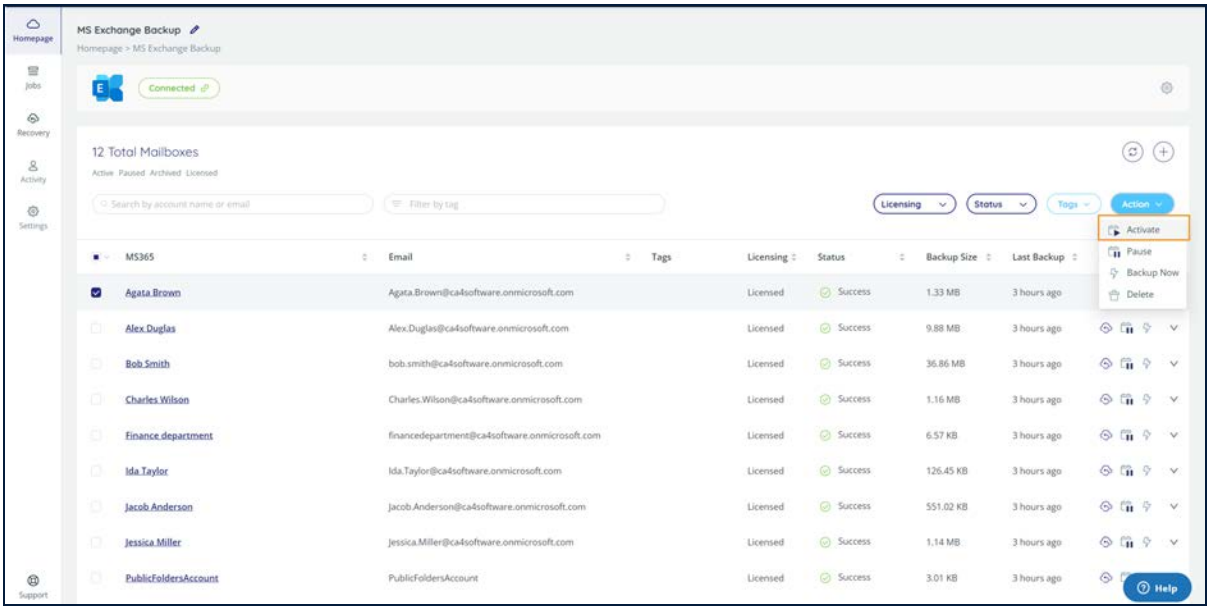
Once you have configured your backup settings, you need to **Activate** them, in order for them to begin backing up your data.

1. Navigate to the list of account, team or sites following the Backup Settings section.

> **Note:** The screens below are from Microsoft 365 Exchange, but the functionality is identical for all of the Microsoft 365 applications.

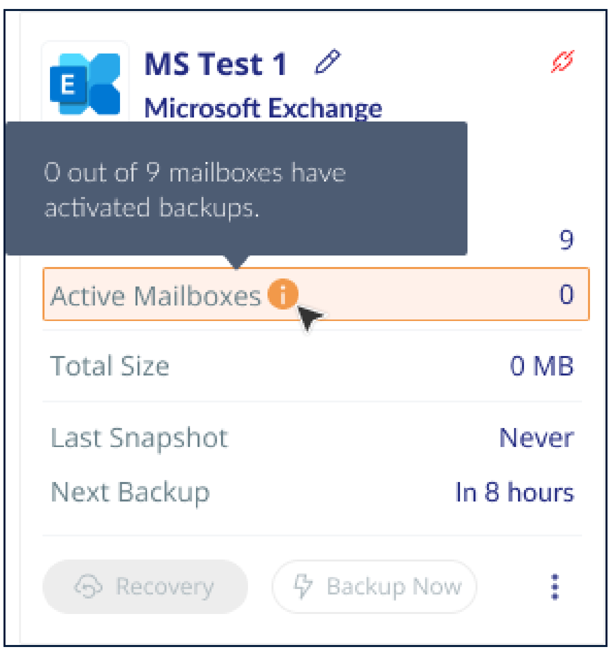


2. Select one or more account, team or site(s).
3. Click **Action** > **Activate**. The status of your backups will now be "Scheduled." This means that they will be backed up at the time that you selected on the *Configuration* screen.



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:

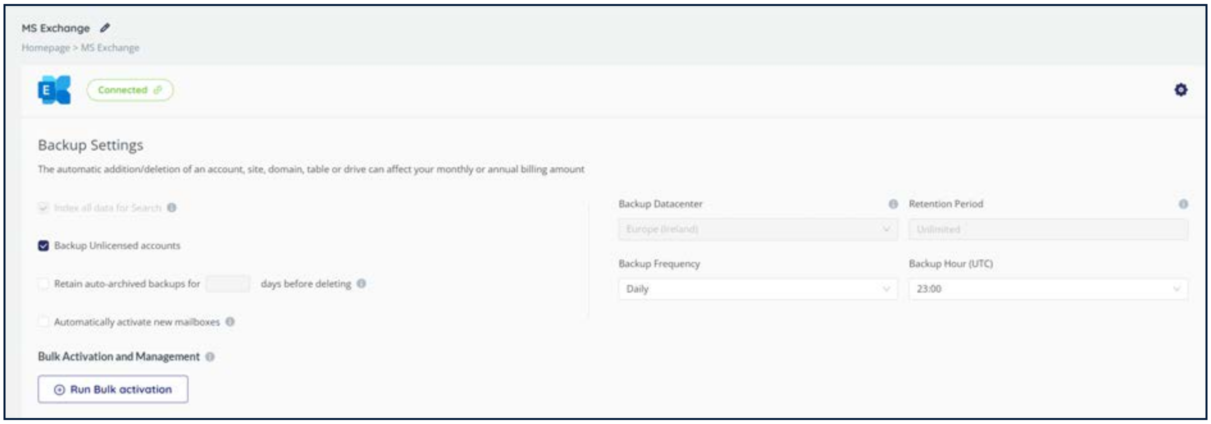


3.1.4 Bulk Activation and Management

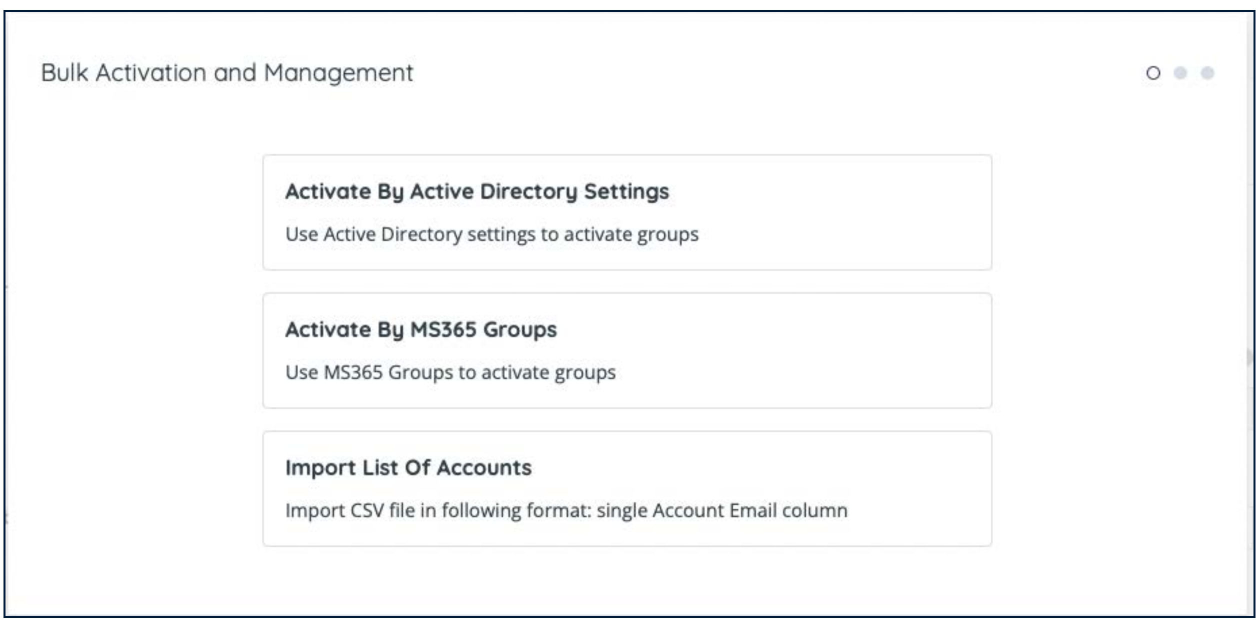
Want to save time and effort when setting up large numbers of Microsoft 365 backups?

CloudAlly's Bulk Activation feature enables you to activate the backups of all members of Microsoft Groups with a single click. When users are added or removed from the group, their backups will respond accordingly.

To create a new Activation Rule, from the *Backup Settings* screen, click **+Run Bulk Activation**.

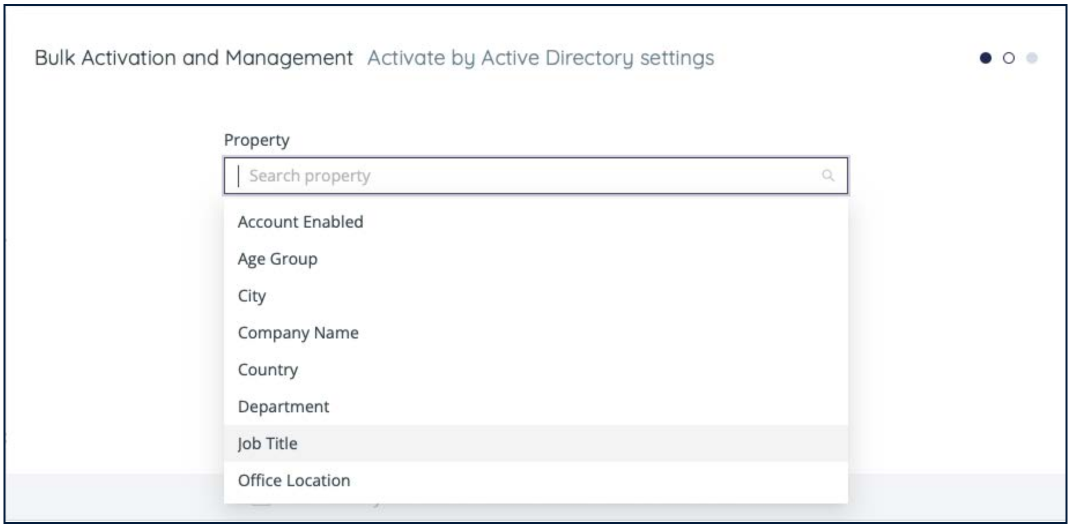


The following *Bulk Activation and Management* screen appears:

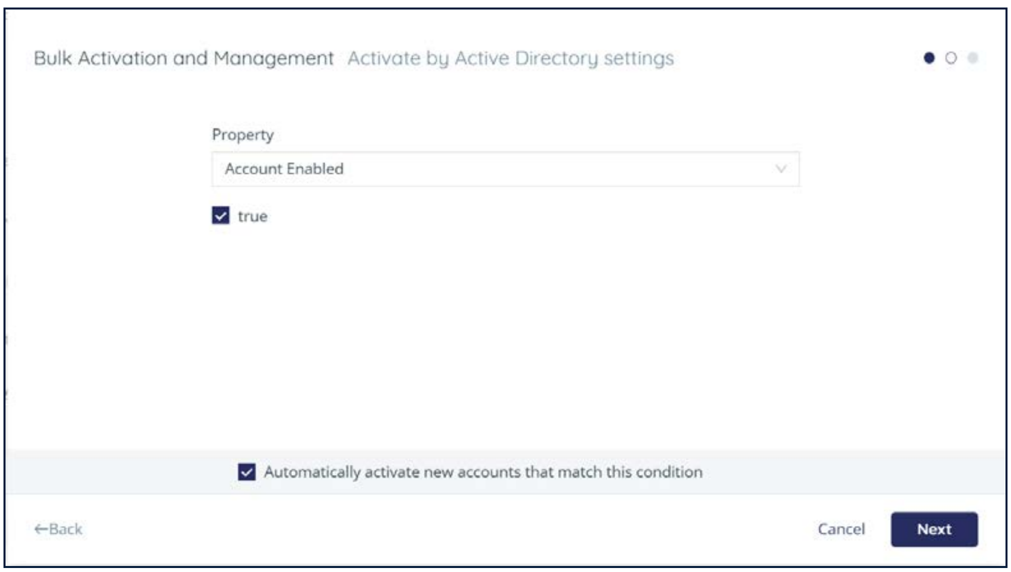


3.1.4.1 Activate by Active Directory Settings

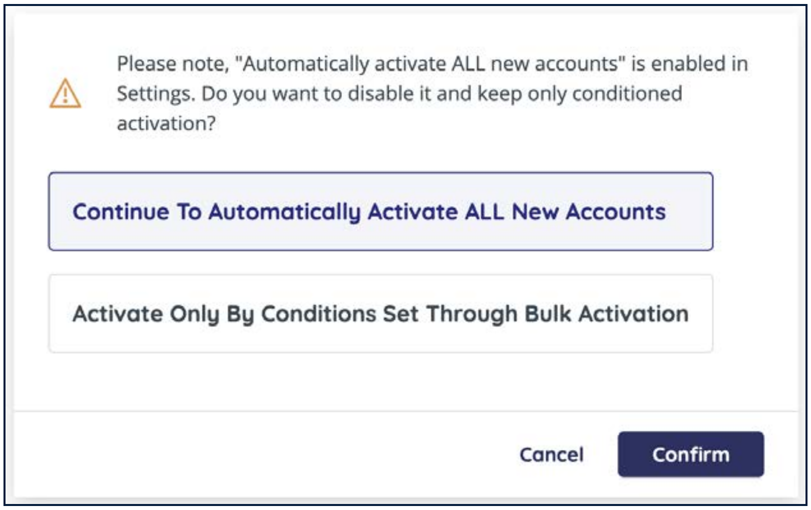
If you choose to activate by directory settings, the following screen appears next. Select the property that will be the basis for your new Activation Rule.



If you want to create a conditional activation rule, click **Automatically activate new accounts that match this condition,** and then click **Next**.



The following pop up will appear.

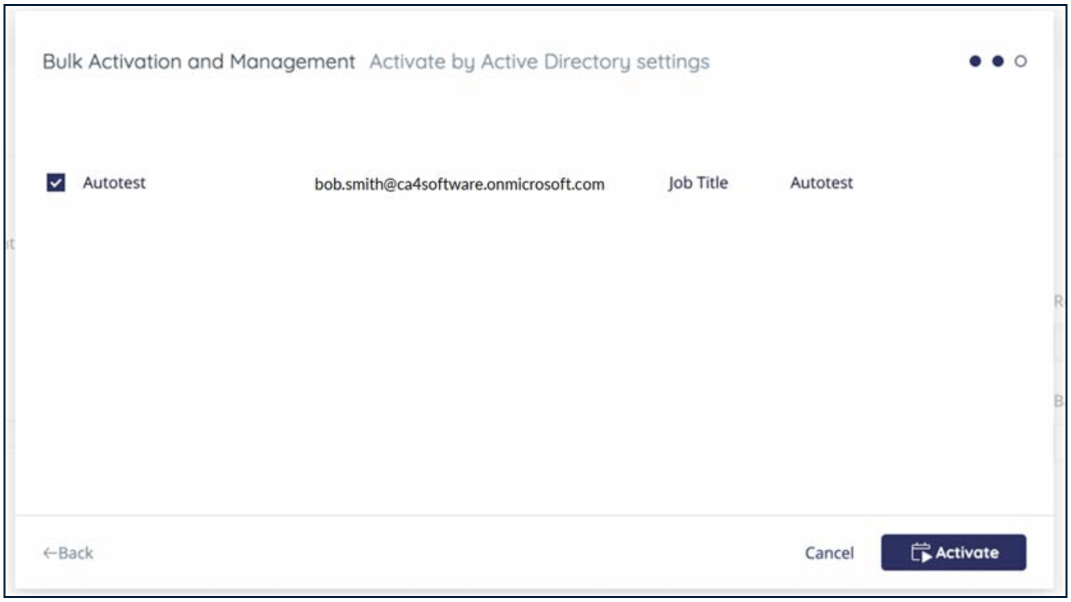


The pop up includes two available options for activation:

- Continue To Automatically Activate ALL New Accounts
- Activate Only By Conditions Set Through Bulk Activation

New accounts matching the selected Property will be automatically detected and activated in the backup system. This does not affect the already existing accounts.

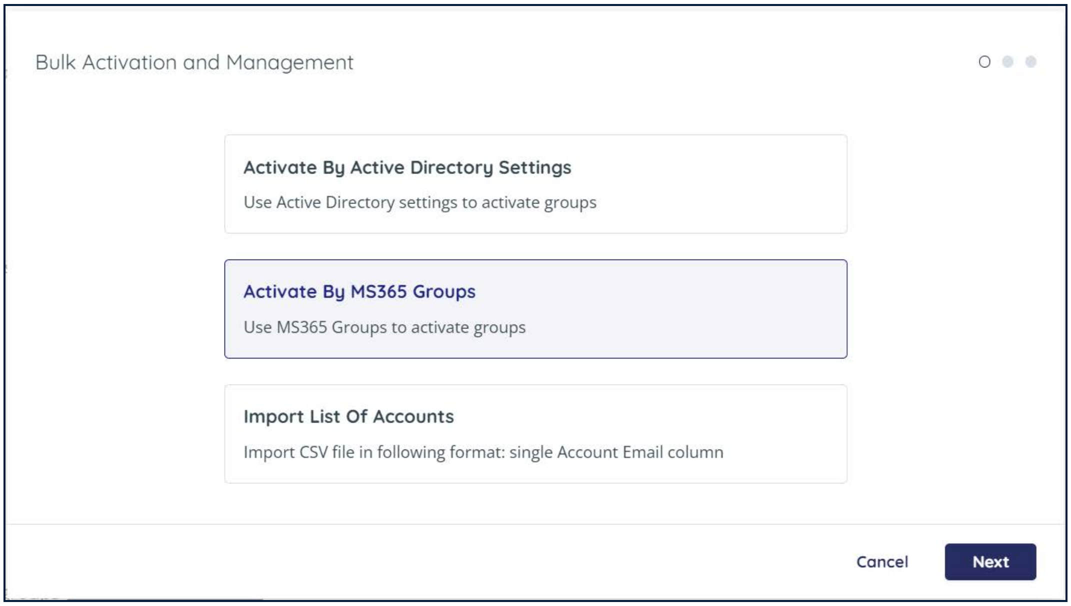
- Click **Next** once you have selected the desired Property and its values. The list of accounts matching the selected Property is displayed. Review the list of accounts that will be activated. You can clear the check boxes next to an account to exclude it from the activation process.



- Click **Activate**. The selected accounts are activated, and if you have selected the **Automatically activate new accounts that match this condition** check box, the conditional activation rule is created.

3.1.4.2 Activate by MS365 Groups

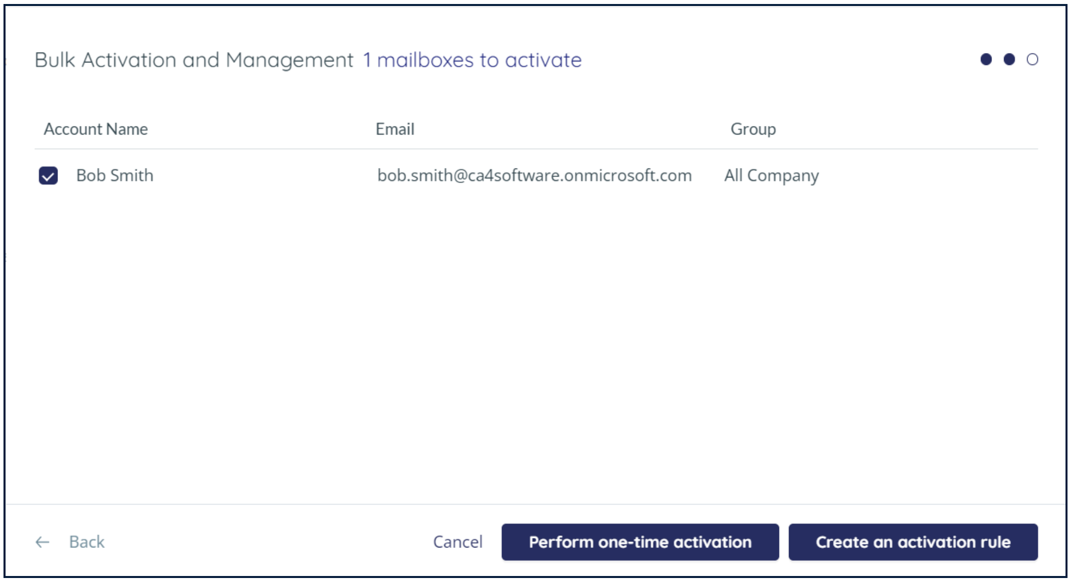
If you choose to activate by Microsoft 365 Groups, the following screen appears next.



Select the group(s) you would like to back up:

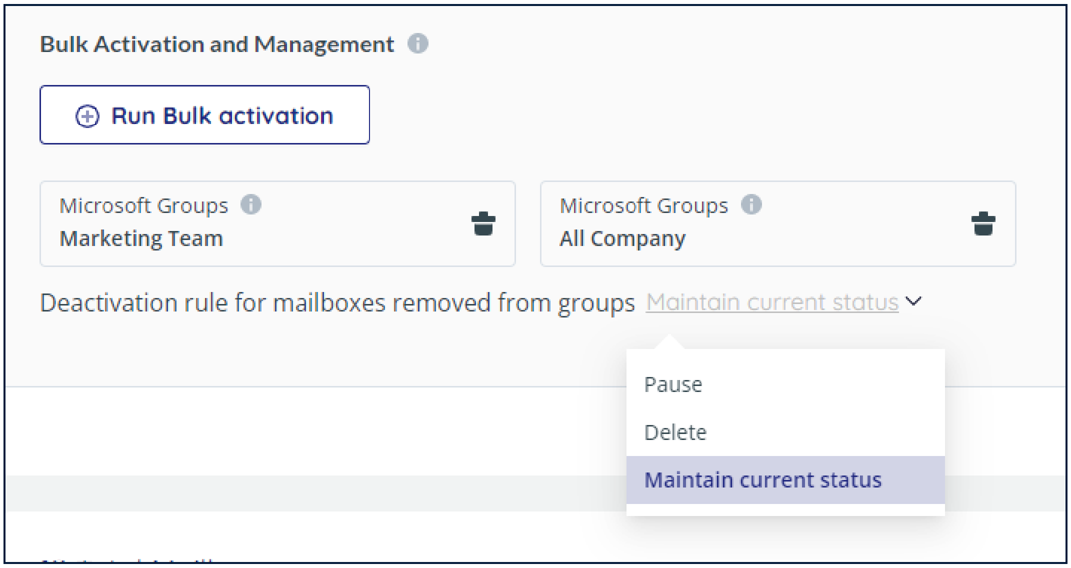
> **Note:** Activation by Microsoft Groups works for already-existing mailboxes.

Select one or more groups, and click **Next**.



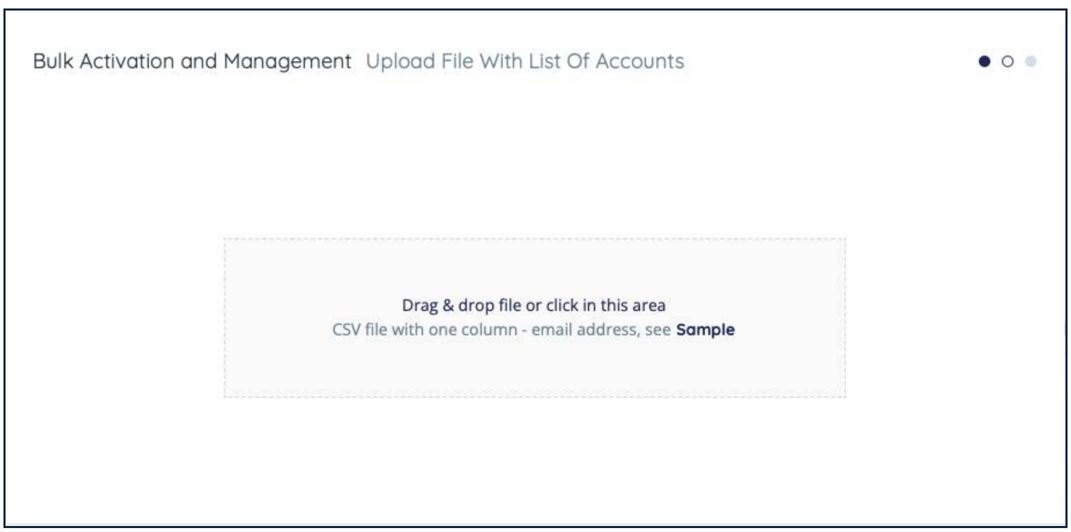
You have the option of a **one-time activation**, which will only run once, or **Create an activation rule**, which will run automatically. It checks daily to see changes to each group, and will back up mailboxes that are added to groups.

You can also configure a deactivation rule. There are three options: maintaining the current status, pausing backups or deleting backups.



3.1.4.3 Import a List of Accounts

If you choose to **Import a List of Accounts**, you will be prompted to upload a CSV file with a single column titled "Account Email."



3.1.5 Backing Up a Public Folder

In order to back up a Public Folder, the Admin account must have a mail Microsoft 365 Exchange license and needs to have read/write permissions for the Public Folder.

To back up a Public Folder:

1. From the Exchange Admin Center, click **Public Folders**.
2. Select the Public Folder that you want to back up and click '...' to select Root Permissions.
3. Verify that the Admin account used for the CloudAlly backups has read/write access to the Public Folder. If not, click '+' to add the Admin account.

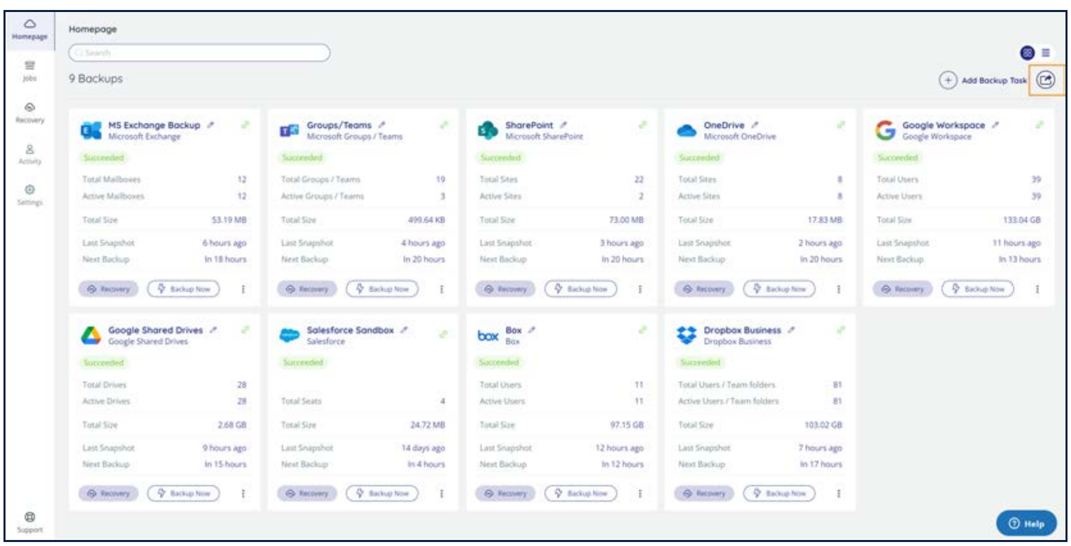
Public Folders data will be available for recovery under the PublicFoldersAccount record, listed among other backed up Exchange users.

The restore process for a Public Folder creates a sub-folder. Add the generated restore folder as a new Public Folder in order to allow access to the restored data.

Follow the normal Microsoft 365 Exchange Online procedures to create a public folder, using the CloudAlly restored sub-folder as the path, as well as any additional sub-folders that are included in the restore.

3.1.6 Usage Reports

In order to provide greater clarity about what CloudAlly is backing up, you can export a CSV file that lists all of the entities - mailboxes, teams and sites - that were backed up, including the status of each entity (active, inactive, or archived). And for Microsoft Exchange mailboxes, the file will list whether each one is licensed or unlicensed. To export a usage report, click the **Export** button. The report will be sent to the user via email.

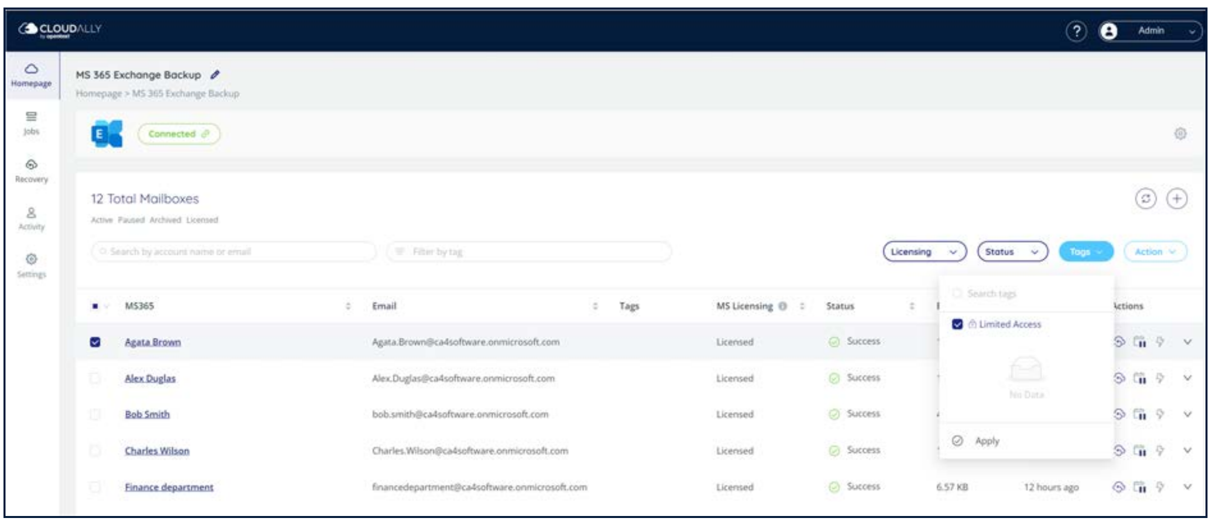


3.2 Securing Your Backups

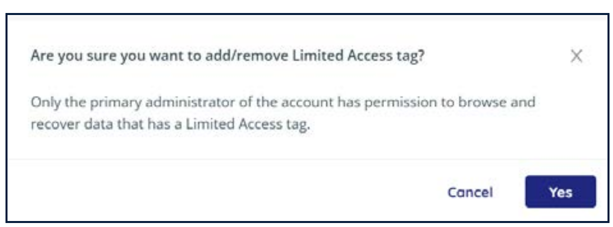
By default, all primary and secondary users can preview, browse, and recover any backed up data. This could be a security risk if sensitive information is contained in the backup snapshots.

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.

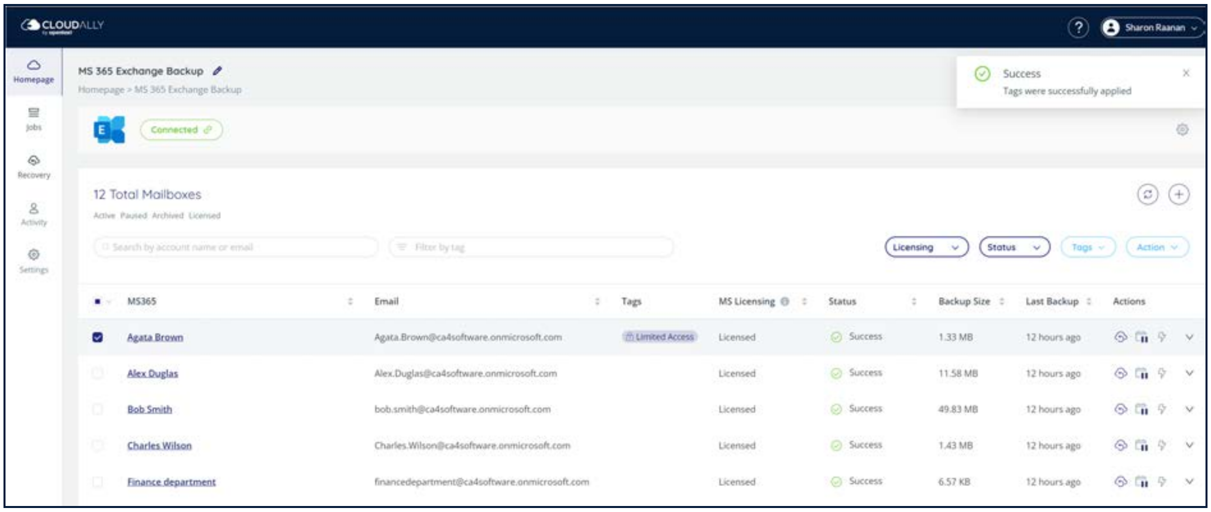
1. Primary user: From the *Homepage*, click the name of the service whose data you would like to restrict.
2. Click one or more account, team or sites.
3. Click **Tags**, and check the **Limited Access** tag.



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.

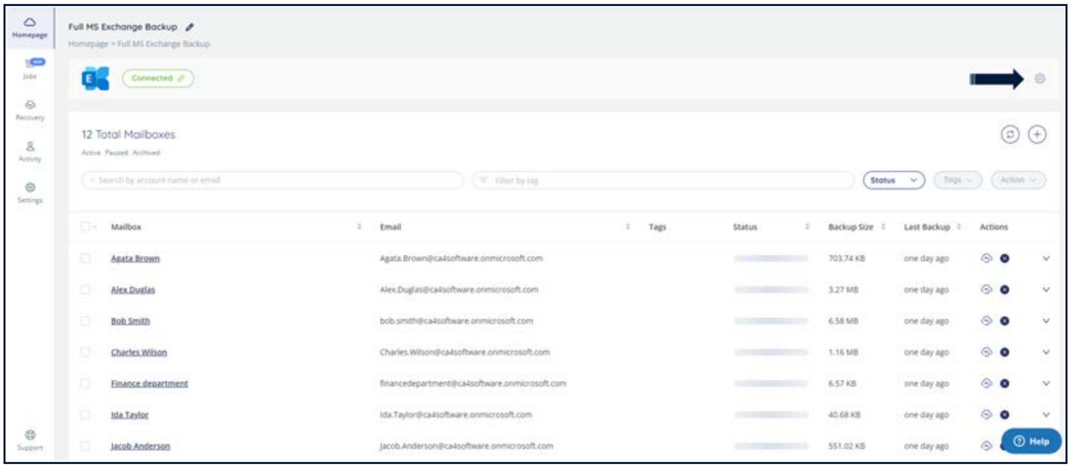
To remove the tag, the primary user should simply reverse the process - un-check the Limited Access tag, and re-apply.

3.2.1 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.

6. Click the particular Microsoft 365 icon from the list or enter a keyword in the Search field to find a specific task. The *Microsoft 365 Backup* page is displayed.
7. Click the gear-shaped **Settings** icon.



From here, it is possible to modify the fields described in ["Configuring a Backup Task: Microsoft Exchange."]()

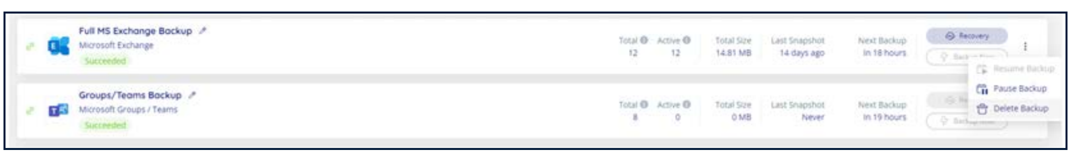
3.2.2 Removing a Backup

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.

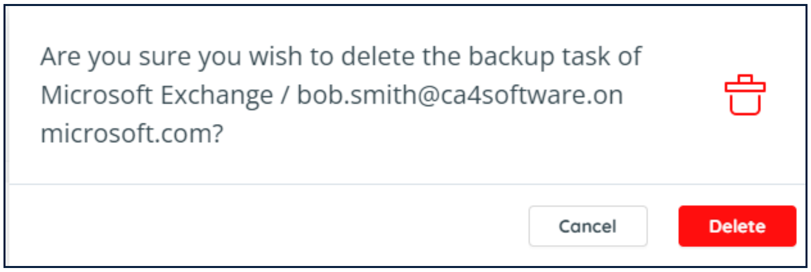
3.2.2.1 Removing an Entire Backup Service

To remove an entire backup service, click the **Delete Backup** icon of the backup service you want to remove.

Microsoft 365 Exchange



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

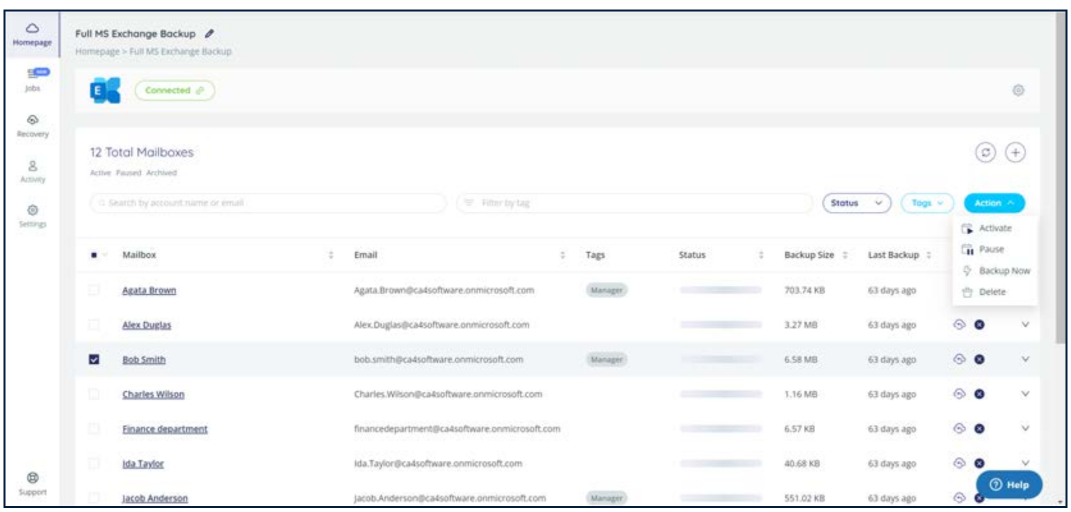


Click **Delete**. The selected backup service is removed from your account.

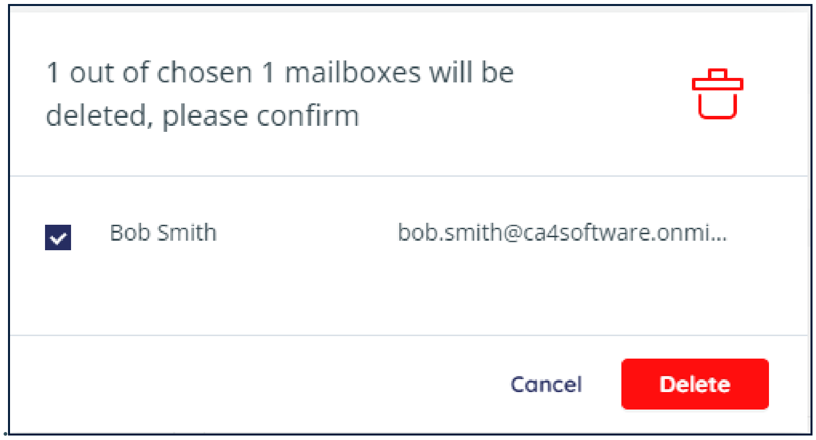
To prevent mistaken deletions, there is a grace period of 7 days, during which your data is still maintained and you can cancel the operation.

3.2.2.2 Removing an Individual Account, Team or Site

1. Click the backup service from which you want to remove the account, team or site. The backup task settings page is displayed.
2. Add a check next to the item that you want to remove. Click **Delete** in the **Actions** menu.



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



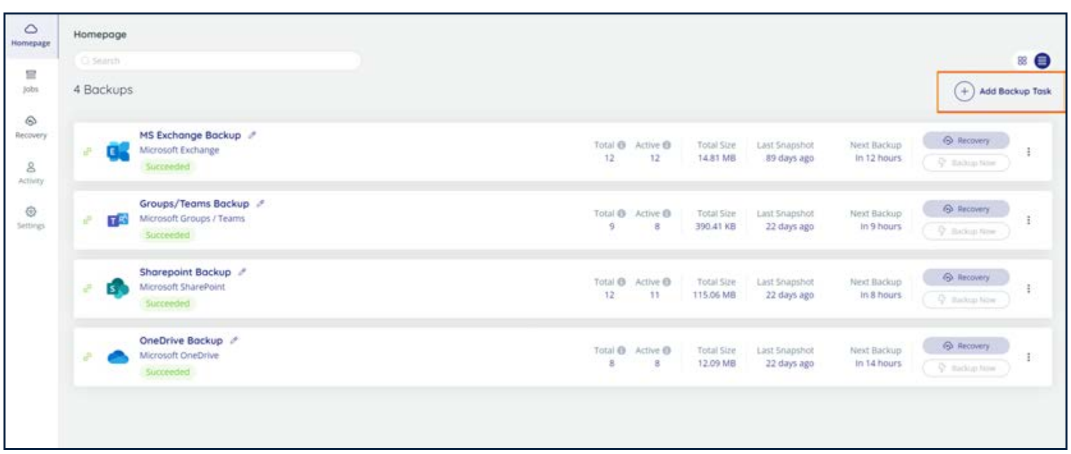
To prevent mistaken deletions, there is a grace period of 7 days, during which your data is still maintained and you can cancel the operation.

3.3 Microsoft 365 OneDrive

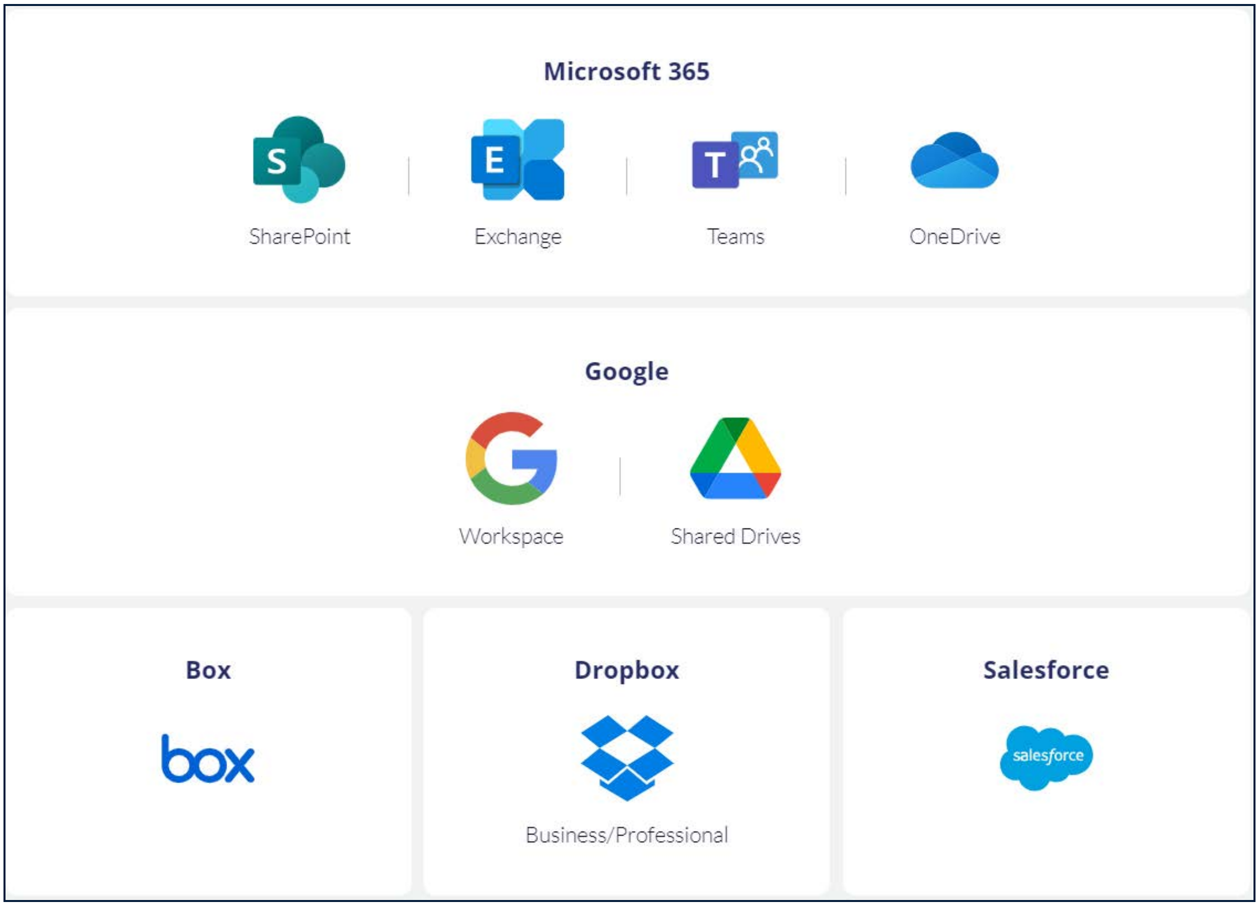
3.3.1 Adding a OneDrive Backup Task

To create a new backup task:

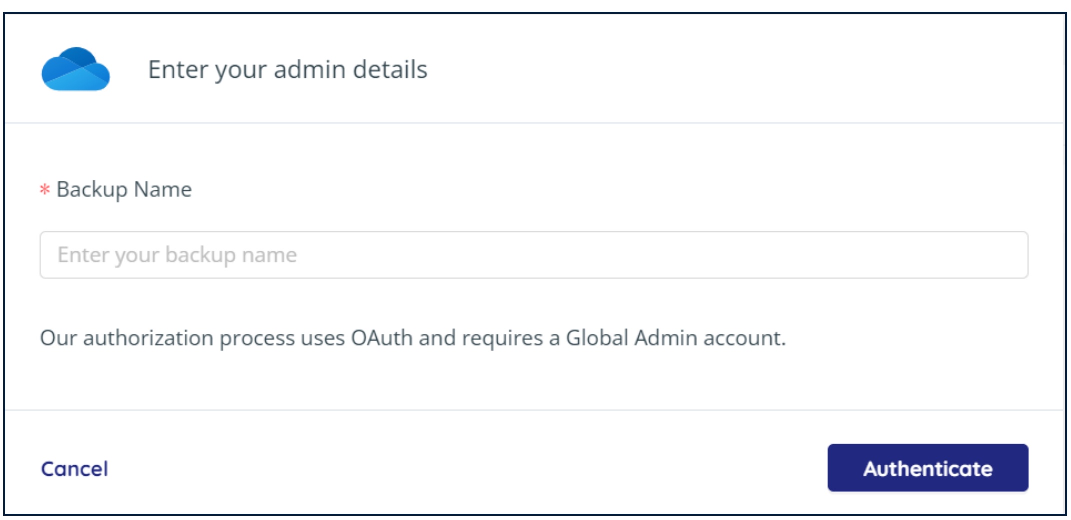
1. Sign in to your account, or if you are already signed in, click the **Homepage** option in the Navigation Panel.
2. On the Homepage, click **+ Add Backup Task**.



The following page is displayed:



4. Click **OneDrive**.

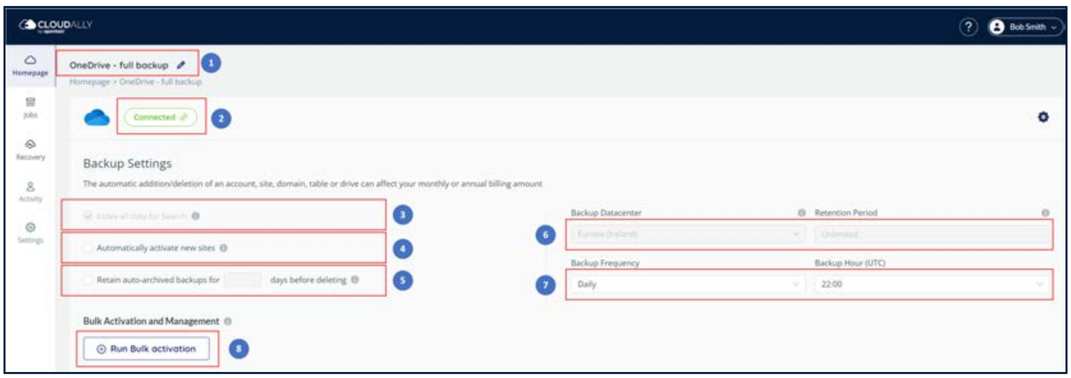


5. Fill in the name of the backup task. This name is used in the notifications and reports, and it can be changed later.

6. Click **Authenticate** to start the process of granting the access token. You will be redirected to the *Microsoft sign-in* page. Enter Global Admin credentials to sign in to your Microsoft account.

> **IMPORTANT!**
>
> The user that you enter **must** have Global Admin permissions.

3.3.2 Configuring a OneDrive Backup Task



1. You can change the name of the backup task by clicking the pencil icon.
2. The Connected / Disconnected icons indicate whether the application was able to connect to the specified Microsoft 365 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 the Disconnected icon. 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 sites** option instructs the system to detect new teams and groups, 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 submitting a support ticket. 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 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 of the **Backup Frequency** field and select how often you would like the backups to occur. The available options include:

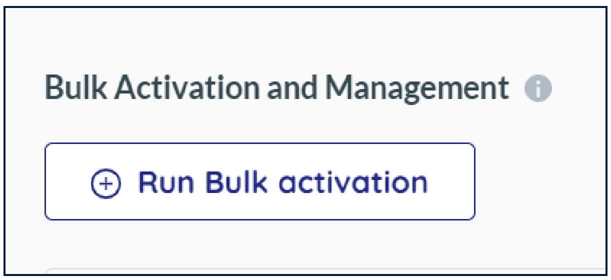
      i. Daily
      ii. Every 3 days
      iii. Weekly
      iv. 3 times a day.

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

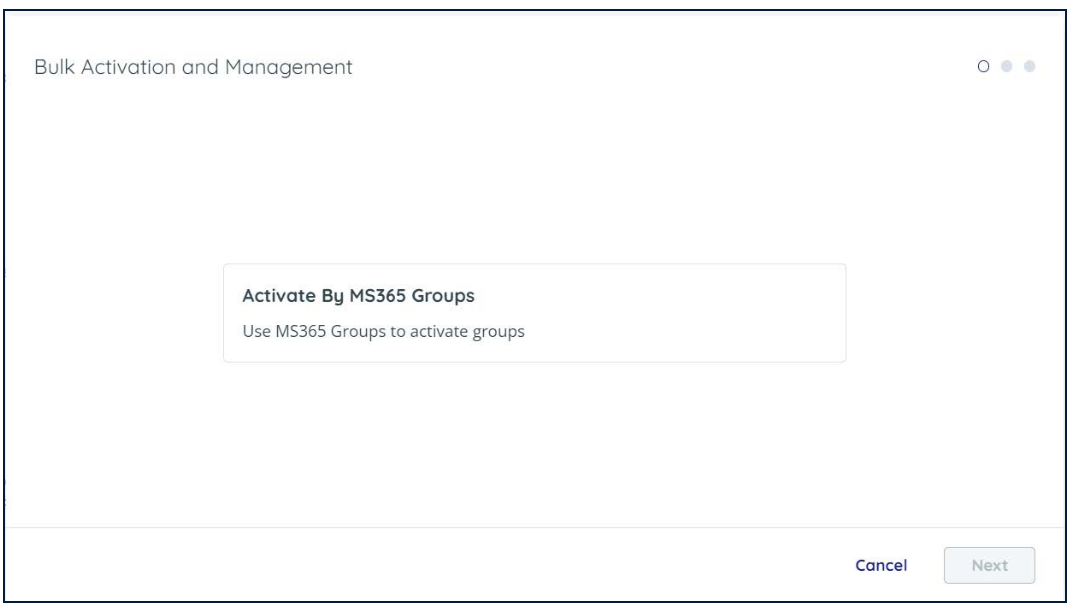
> **Note:** 3x daily backups might be subject to additional charges. Please contact Support or your sales representative if you have any questions before changing the backup frequency.

3.3.3 Bulk Activation and Management

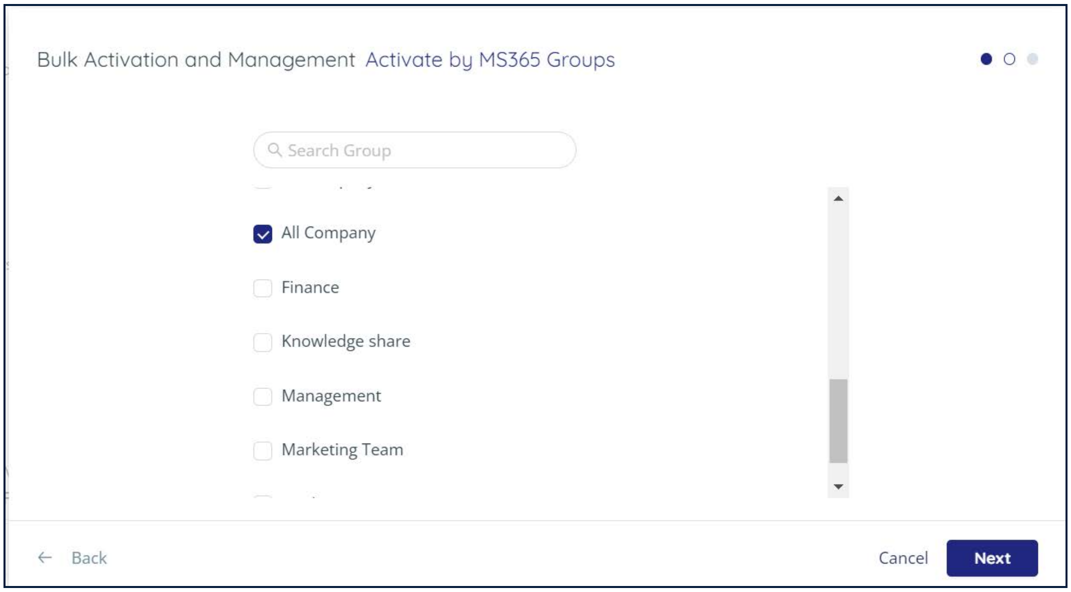
To create a bulk activation rule, click **+Run Bulk Activation**.



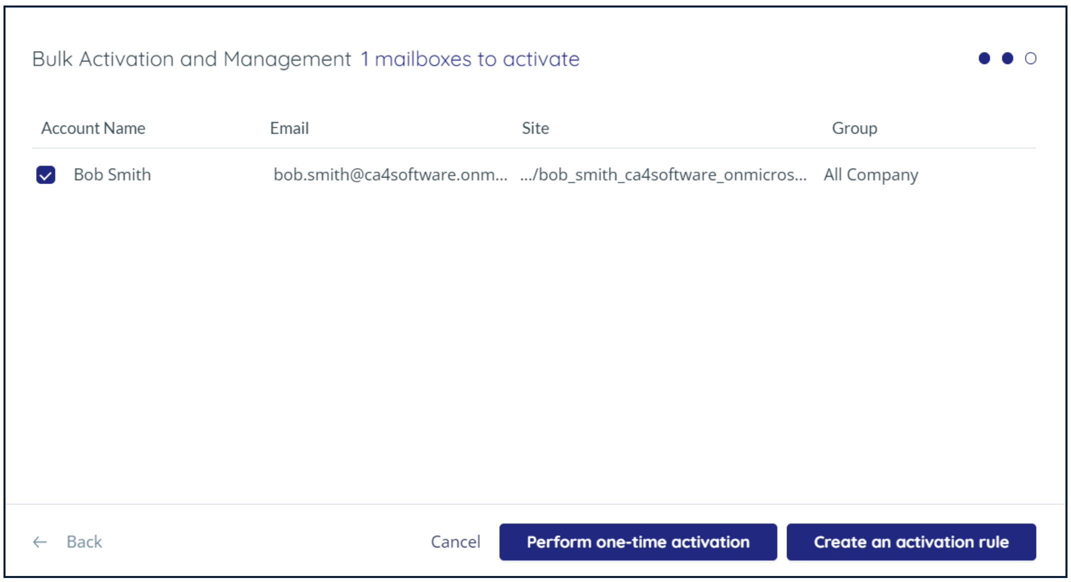
Click **Activate by MS365 Groups**, and then click **Next**.



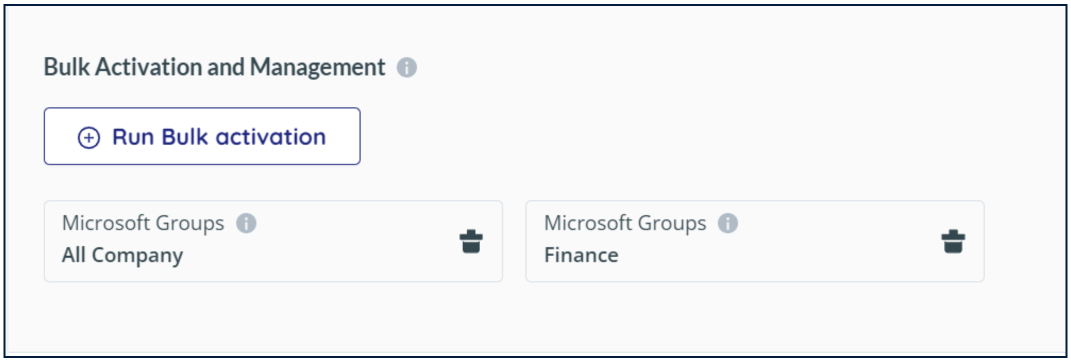
Choose one or more groups that you would like to activate:



You have the option of a **one-time activation**, which will only run once, or **Create an activation rule**, which will run automatically. It checks daily to see changes to each group, and will back up sites that belong to users that have been added to groups.



The OneDrive settings screen will display the group activation rules that you enabled.



3.3.4 Activating a Backup Task

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

For instructions, see "Activating Your Backups."

3.3.5 Modifying the Settings of an Existing Backup

See instructions in "Modifying the Settings of an Existing Backup."

3.3.6 Removing a Backup

See instructions in "Removing a Backup."

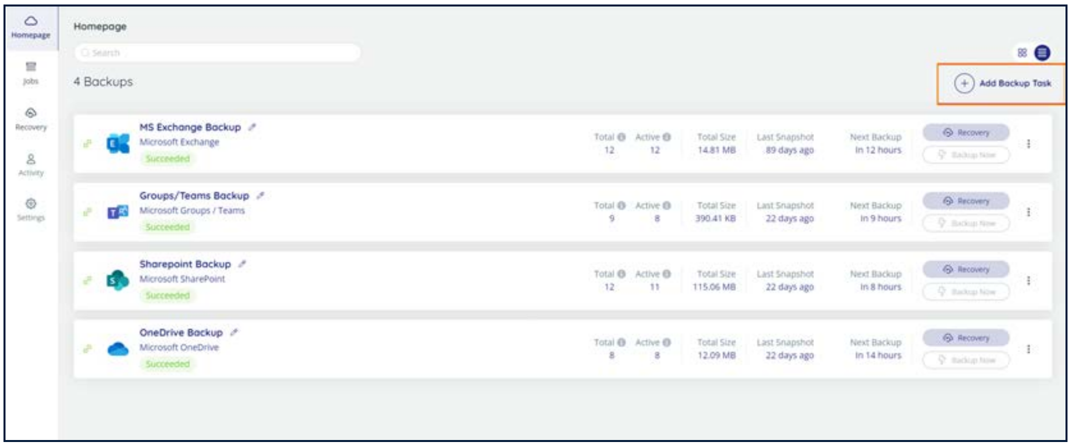
3.4 Microsoft 365 SharePoint

3.4.1 Adding a Microsoft 365 SharePoint Backup Task

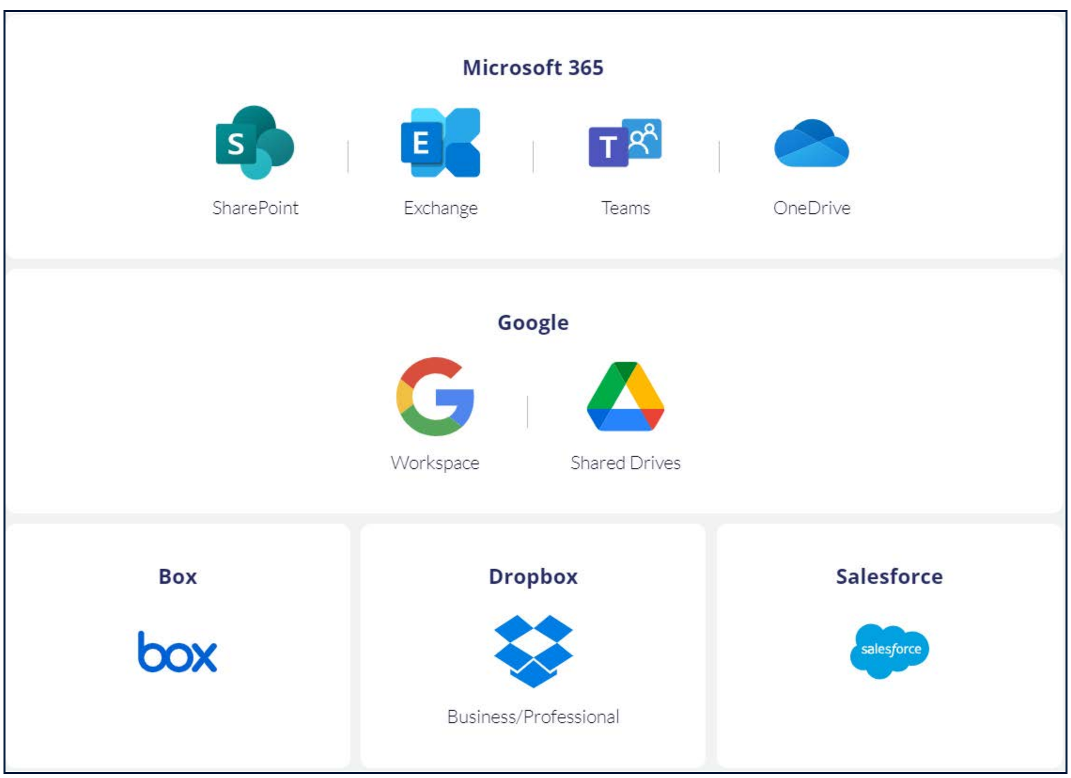
> **Note:** In order to back up all data, CloudAlly assigns the backup user to be the site collection administrator. If CloudAlly is unable to do so (for example, because the user doesn't have proper permissions), then the user needs to be added manually.

To create a new backup task:

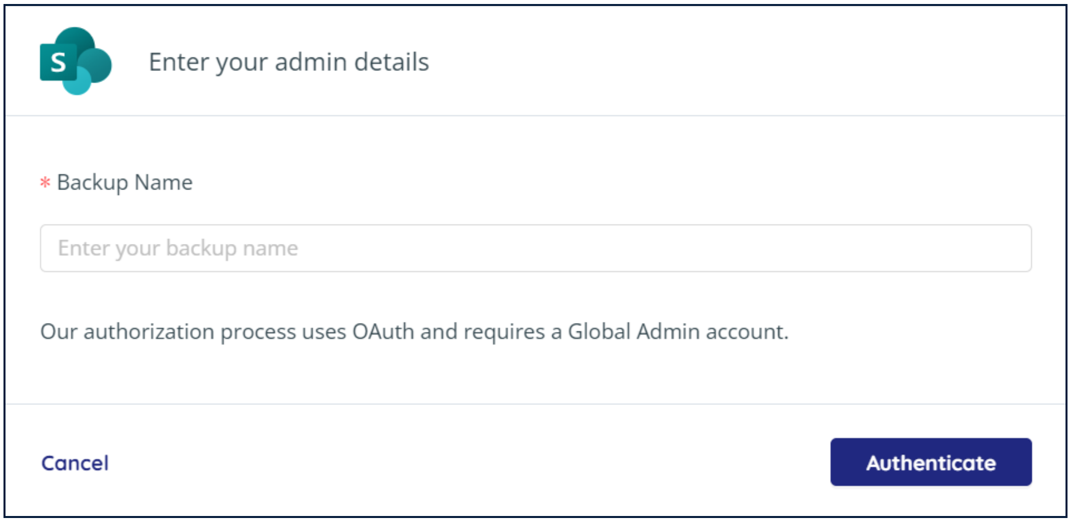
1. Sign in to your Account, or if you are already signed in, click the **Homepage** option in the Navigation Panel.
2. On the Homepage, click **+ Add Backup Task**.



The following page is displayed:



8. Click the name of the service you would like to back up.



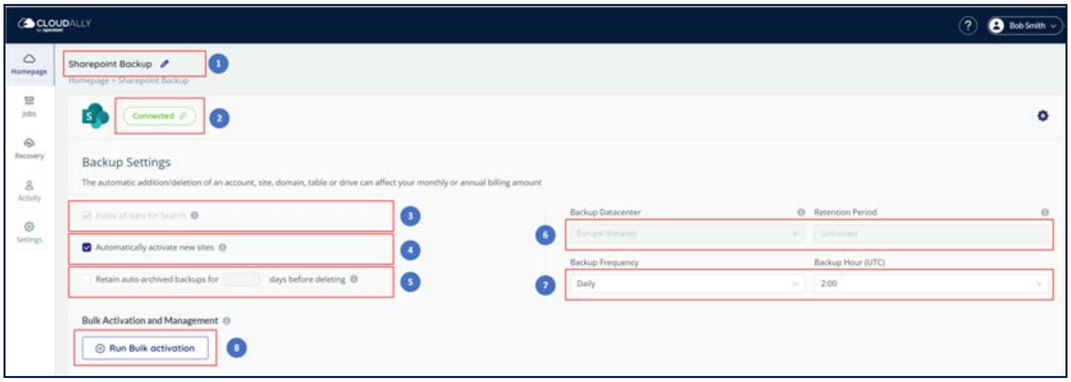
9. Fill in the name of the backup task. This name is used in the notifications and reports, and it can be changed later.

10. Click **Authenticate** to start the process of granting the access token. You will be redirected to the *Microsoft sign-in* page. Enter Global Admin credentials to sign in to your Microsoft account.

> **IMPORTANT!**
>
> The user that you enter **must** have Global Admin permissions.

3.4.2 Configuring a Microsoft 365 SharePoint Task

This set of options enables you to select the backup settings for the account, team or site. Click the gear-shaped Settings icon.



1. You can change the name of the backup task by clicking the pencil icon.
2. The Connected / Disconnected icon indicates whether the application was able to connect to the specified Microsoft 365 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 the Disconnected icon. 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 sites** option instructs the system to detect new sites, 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 Datacenter** and **Retention Period** fields are "display only," and their values can't be changed here.

6. The **Backup Datacenter** field displays the Datacenter 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 submitting a support ticket. Backups older than the retention period specified will be automatically deleted.

> **Note:** Your backup storage datacenter cannot be changed once it's been set during the account setup process. Contact CloudAlly 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 of the **Backup Frequency** field and select how often you would like the backups to occur. The available options include:

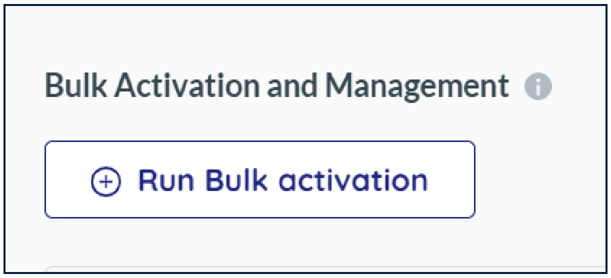
      i. Daily
      ii. Every 3 days
      iii. Weekly
      iv. 3 times a day. Note: 3x daily backups might be subject to additional charges. Please contact Support or your sales representative if you have any questions before changing the backup frequency.

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

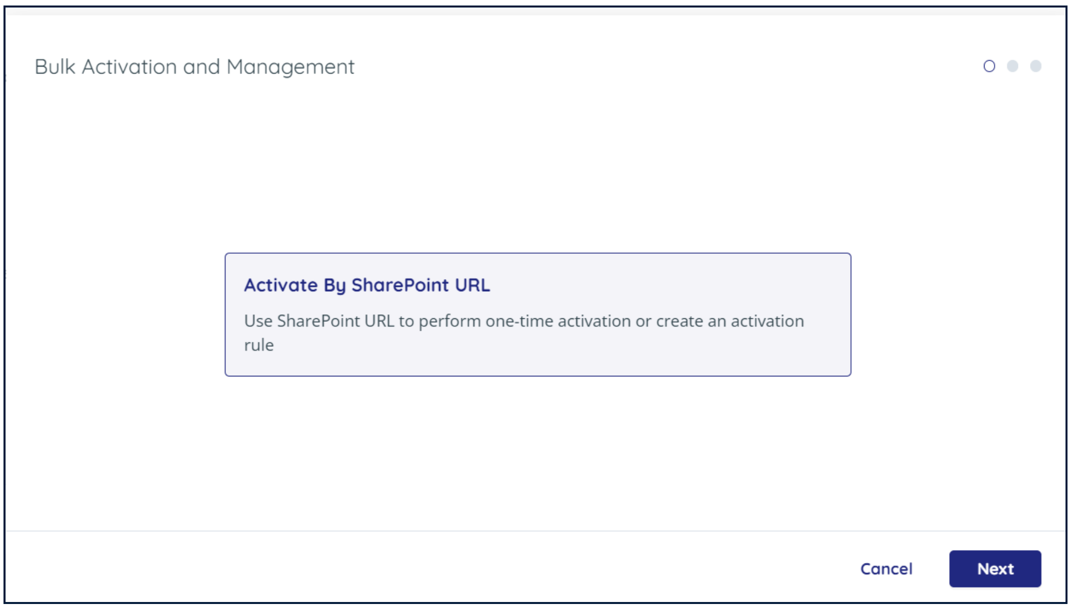
8. Bulk Activation - see below.

3.4.3 Bulk Activation and Management

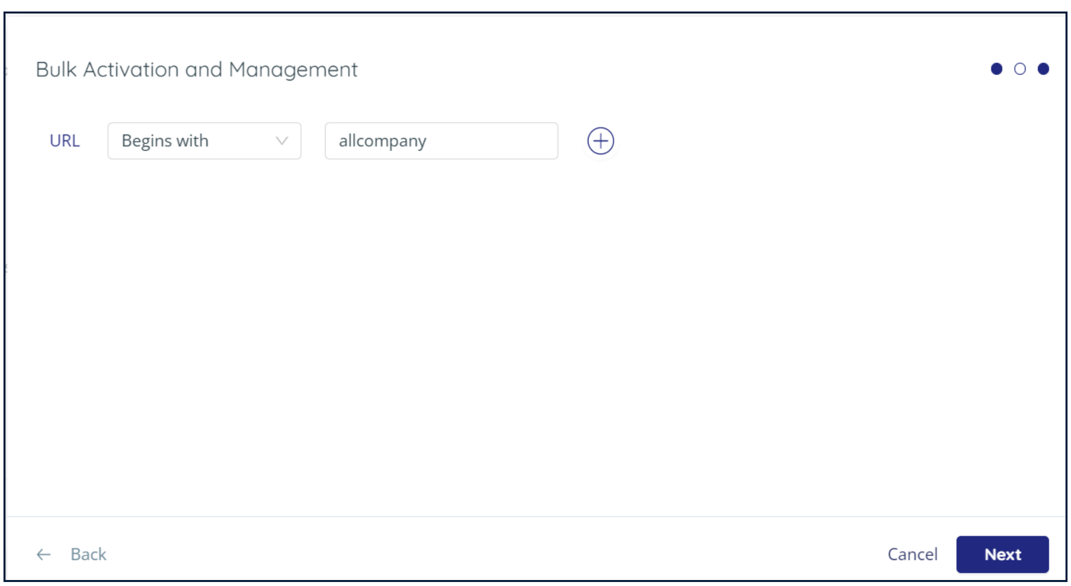
To create a bulk activation rule, click **+Run Bulk Activation**.



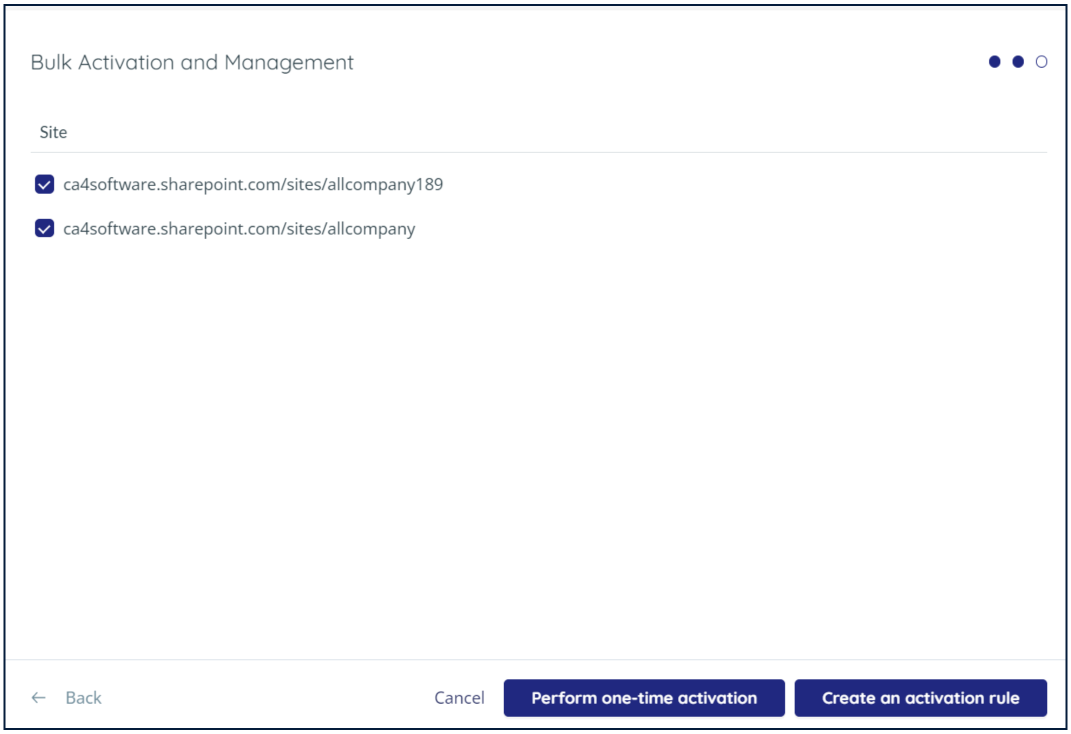
Click **Activate by SharePoint URL**, and then click **Next**.



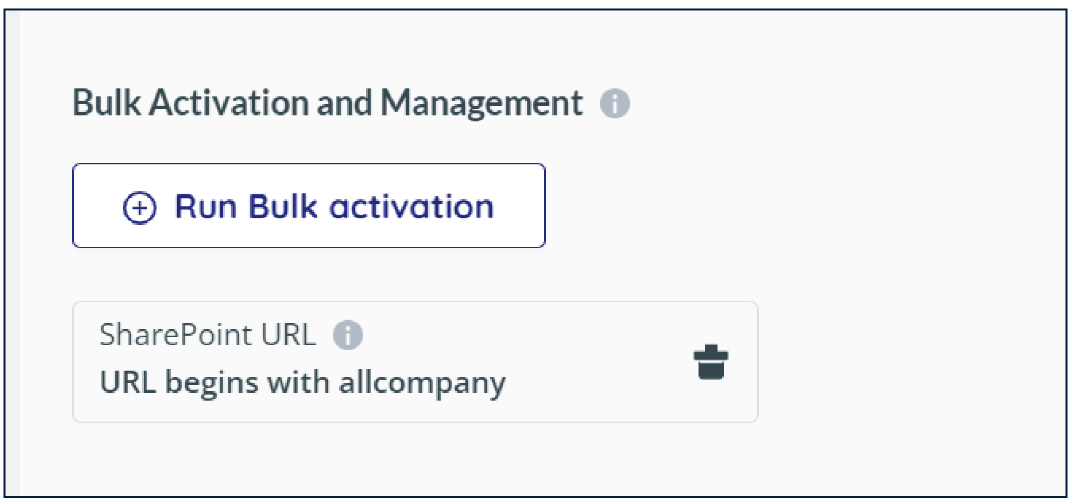
Choose a filter to locate which SharePoint URLs you would like to back up, and click **Next**.



You have the option of a **one-time activation**, which will only run once, or **Create an activation rule**, which will run automatically. It checks daily to see if there are new SharePoint sites that match the conditions set in the activation rules (for example, "begins with X, " "ends with Y"), and then backs up these sites.



The SharePoint settings screen will display the activation rules that you enabled.



3.4.4 Activating a Backup Task

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

For instructions, see "Activating Your Backups."

3.4.5 Modifying the Settings of an Existing Backup

See instructions in "Modifying the Settings of an Existing Backup."

3.4.6 Removing a Backup

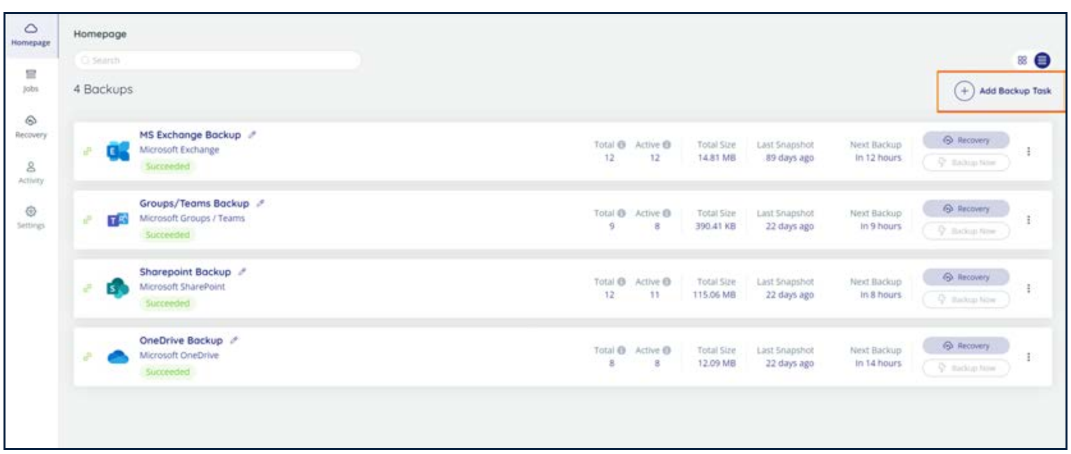
See instructions in "Removing a Backup."

3.5 Microsoft 365 Teams & Groups

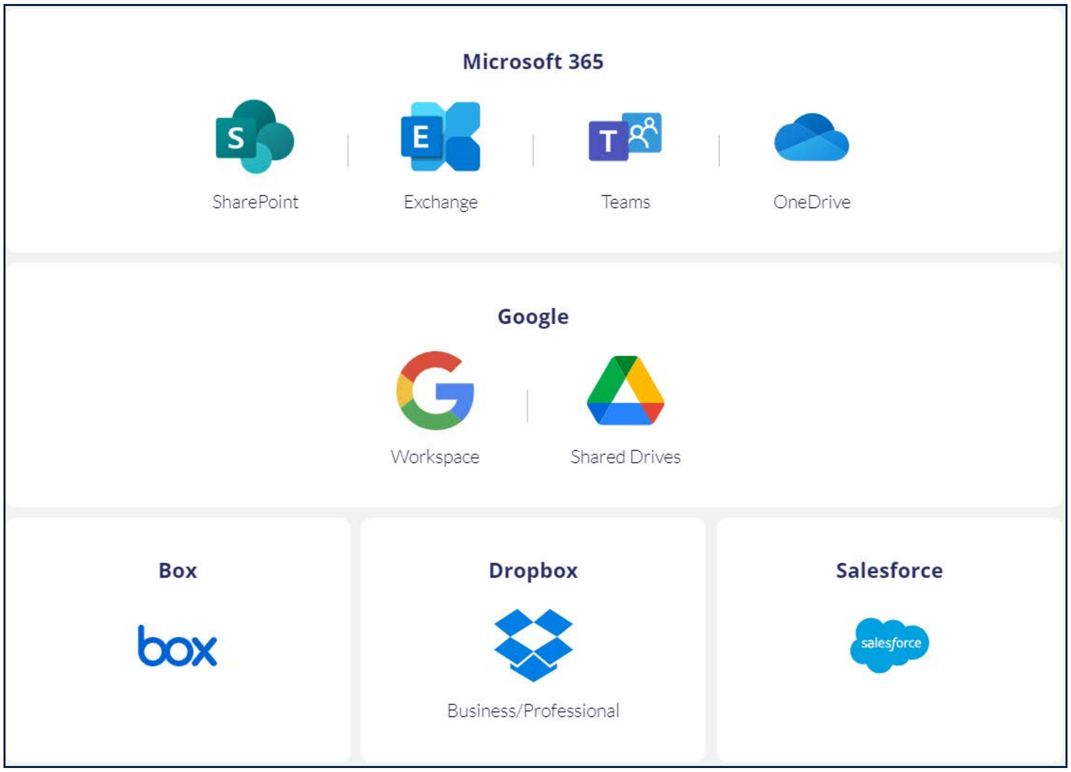
3.5.1 Adding a Microsoft 365 Teams & Groups Backup Task

To create a new backup task:

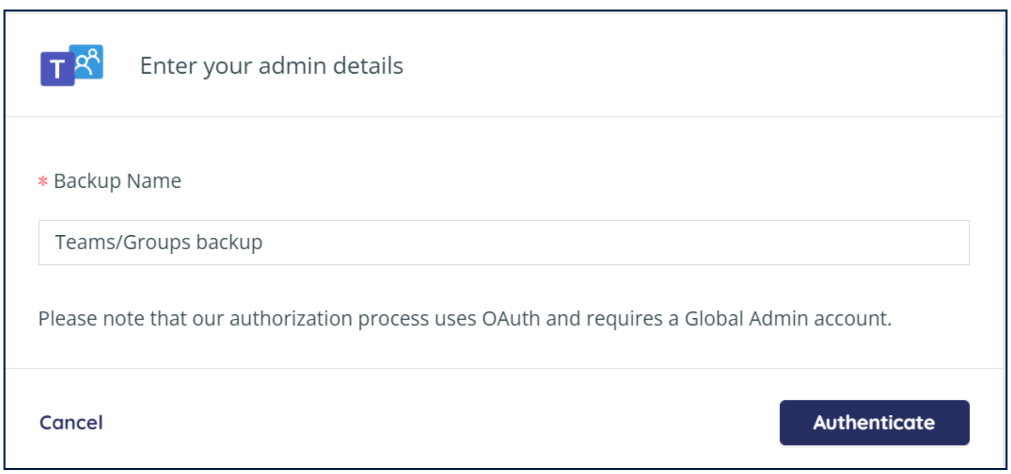
1. Sign in to your Account, or if you are already signed in, click the **Homepage** option in the Navigation Panel.
2. On the *Homepage*, click **+ Add Backup Task**.



The following page is displayed:



3. Click the name of the service you would like to back up.



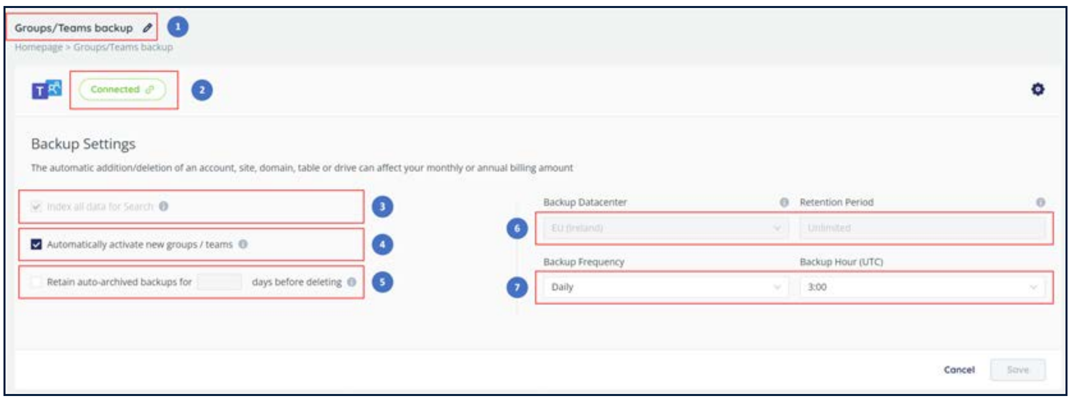
1. Fill in the name of the backup task. This name is used in the notifications and reports, and it can be changed later.

2. You will see the OAuth based authorization Click **Authenticate** to start the process of granting the access token. You will be redirected to the *Microsoft sign-in* page. Enter Global Admin credentials to sign in to your Microsoft account.

> **IMPORTANT!**
>
> The user that you enter **must** have Global Admin permissions, as well as a Microsoft 365 Teams license.

3.5.2 Configuring a Microsoft 365 Teams & Groups Backup Task

This set of options enables you to select the backup settings for the account, team or site. Click the gear-shaped Settings icon.



1. You can change the name of the backup task by clicking the pencil icon.
2. The Connected/ Disconected icon indicates whether the application was able to connect to the specified Microsoft 365 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 the Disconnected icon. 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 groups/teams** option instructs the system to detect new teams and groups, and activate them automatically.
5. Backups are automatically archived when an entire team or group 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 Datacenter** and **Retention Period** fields are "display only," and their values can't be changed here.

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

> **Note:** Your backup storage datacenter cannot be changed once it's been set during the account setup process. Contact 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.

   a. 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 submitting a support ticket. Backups older than the retention period specified will be automatically deleted.

7. **Backup Frequency and Backup Hour**

   a. Click the drop-down list of 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 of the **Backup Hour (UTC)** field and select the backup hour. Click **Save**.

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

3.5.3 Activating a Backup Task

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

For instructions, see "Activating Your Backups."

3.5.4 Modifying the Settings of an Existing Backup

See instructions in "Modifying the Settings of an Existing Backup."

3.5.5 Removing a Backup

See instructions in "Removing a Backup."

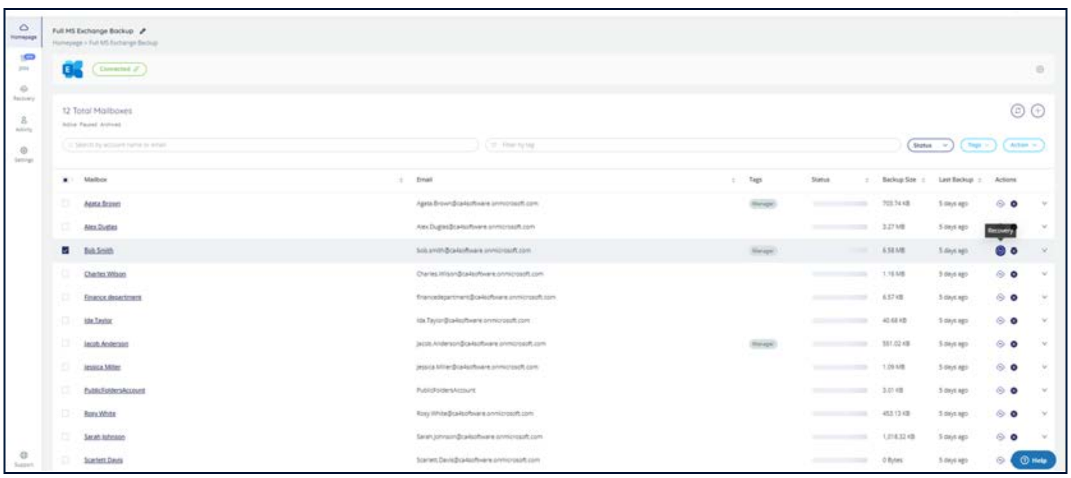
4 Recovering Your Backed Up Data

4.1 Microsoft 365 Exchange: Performing a Full Mailbox Recovery

1. There are two ways to perform a one-click full mailbox recovery:

   a. From the Homepage, on the Microsoft 365 backup that you would like to restore or export, click **Recovery.**

   b. OR: From the Homepage, click the backup you would like to restore. Locate the user account you want to restore, and click the **Recovery** icon in the **Actions** column.



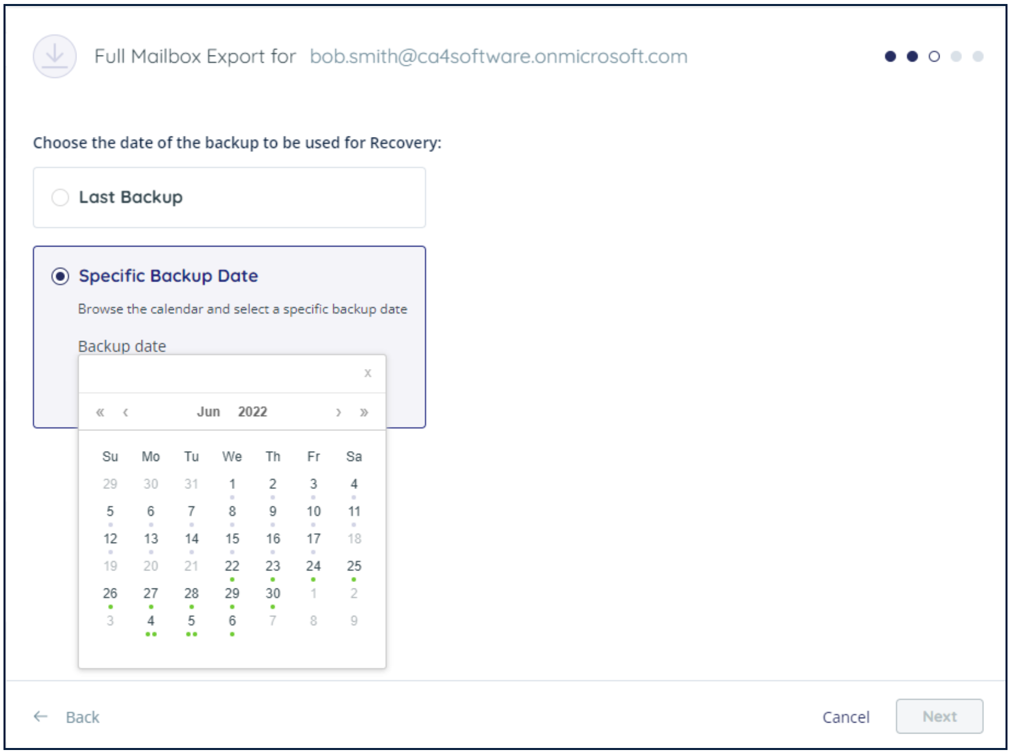
3. Click **Full Mailbox Recovery**.

The subsections below explain about the two options: Export or Restore.

4.1.1 Exporting Your Backed Up Data

1. Click **Export** to download a .zip file of your backed up data.

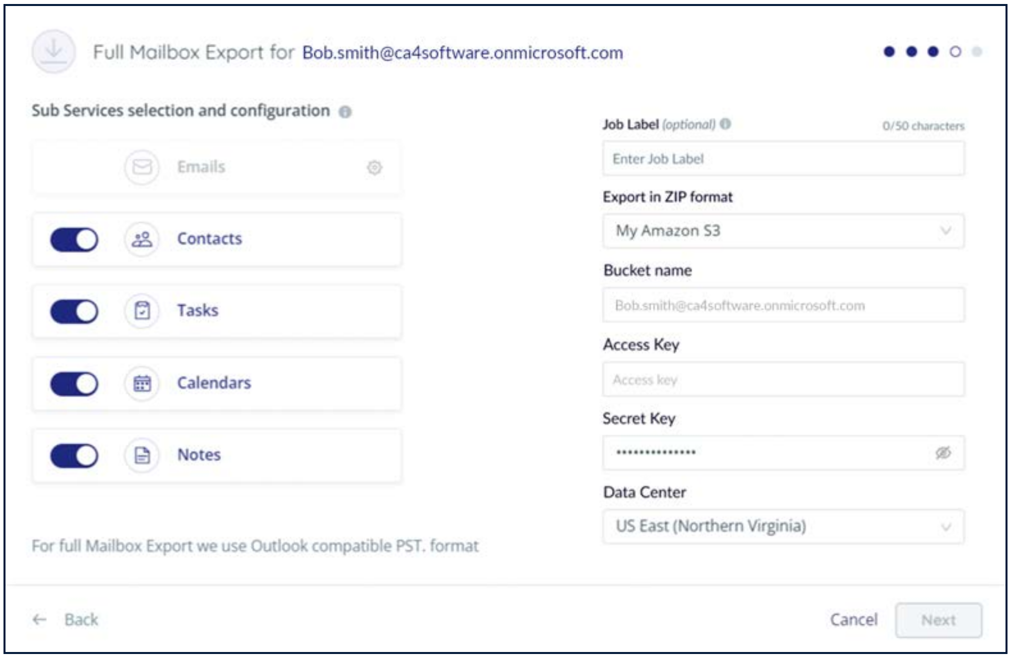
2. Choose the backup you want to export.
    a. First option: restore the **Last Backup**.
    b. Second option: click **Specific Backup Date** and select a backup date from the calendar with a backup status indication. Once you click a particular date, a card will open, indicating whether the backup was successful, partially successful, or if it failed.



Legend: Meaning of Calendar Dots

Dot Color	Meaning
Green	Successful backup
Orange	Partially successful backup
Two dots	Multiple backups on that date

3. Select which sub-services to export.
    a. The default is all sub-services.
    b. Click a toggle to the "off" position to remove individual sub-services.

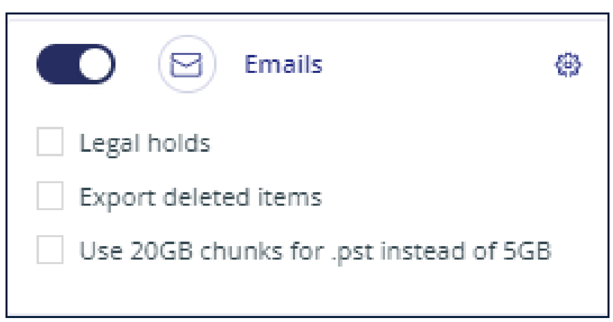


4. Click the gear-shaped settings icon. The following options are available:

    a. **Legal holds**: Choose this option if you want to export all legal / litigation holds placed on this mailbox using Microsoft's Exchange Online Archive (EOA) service.

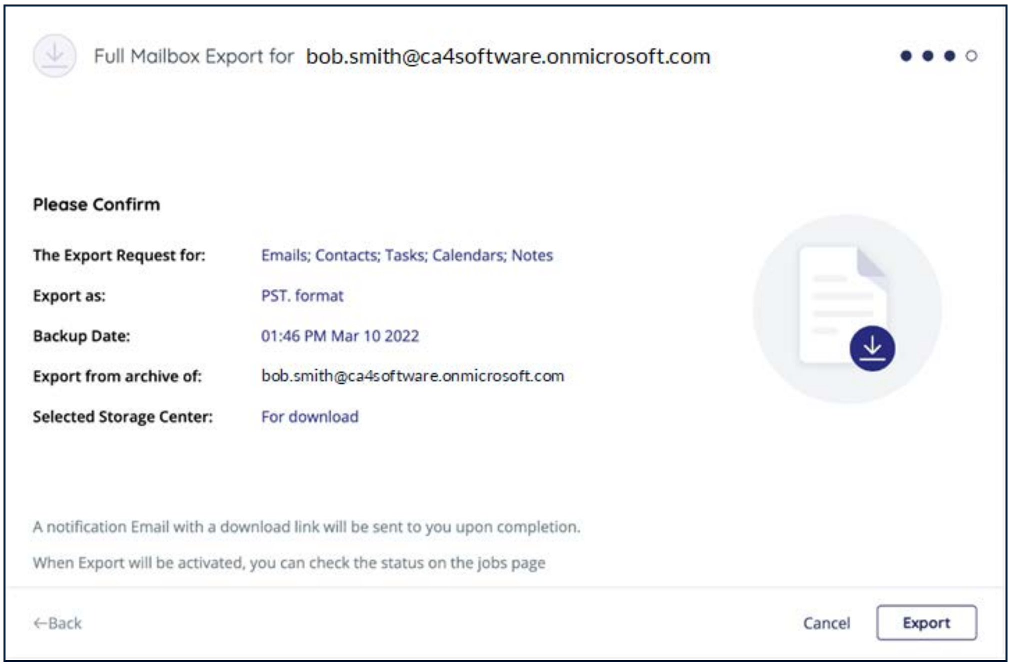
    b. **Export deleted items**: recover items that were deleted in the past, even those that are no longer in the Deleted or Recoverable Items folders.

    c. **Use 20 GB chunks for .pst**: By default, we download data in 5 GB files. But if your backed up data is large, you can choose to download in 20 GB chunks instead.



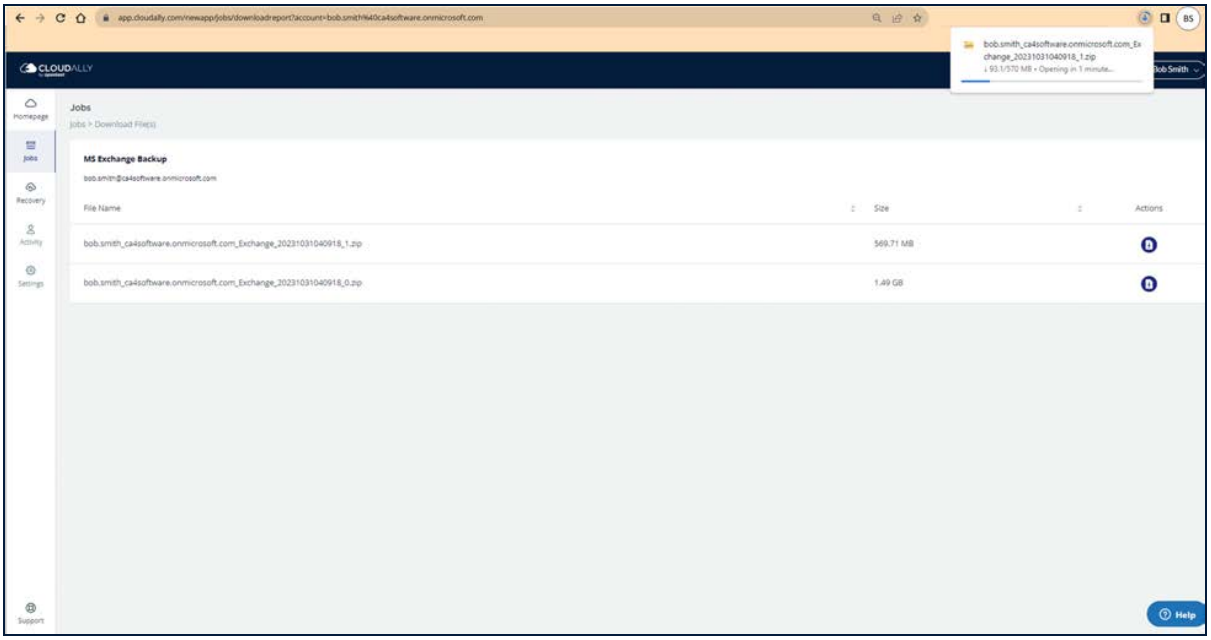
5. Add an optional Job Label to describe this specific job. It will appear on the Jobs page so you can distinguish between your different exports.

6. Select the export ZIP destination, such as direct download, Amazon S3, Azure Blob, Box, Dropbox, AWS S3 Compatible (if you are bringing your own storage) or Google Cloud Platform. Depending on which option you choose, there will be other data to complete (e.g., Bucket Name, Access Key and Secret Key for Amazon S3).
7. Review the information on the confirmation screen. If the information is correct, click **Export** to begin the recovery task. (If the information is not correct, click **Cancel**.)



8. Check the *Jobs* page to track the progress of your job. See "Tracking Recovery Tasks on the Jobs Page" on page 93 for details.
9. When the export is complete, click **Download Results**.

A new page will open which will enable you to download your data file.



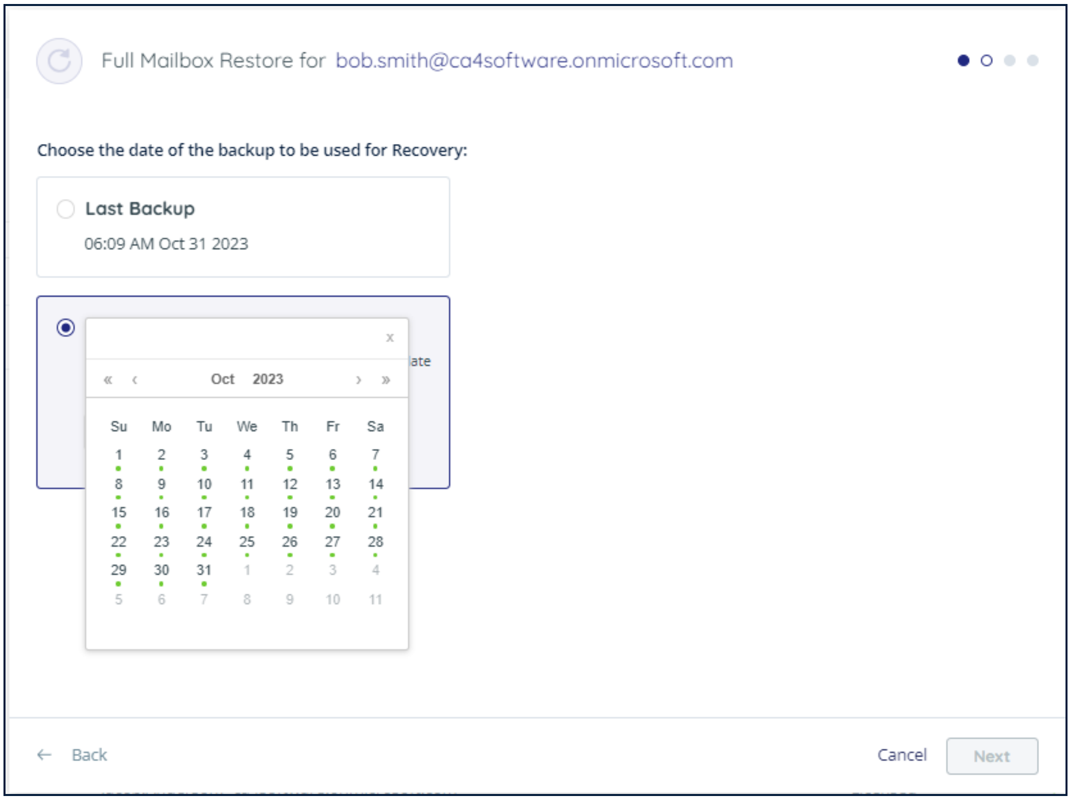
4.1.2 Restoring Your Backed Up Data

1. Click **Restore** to recover your backed up data and store it either in its original location or a different one.

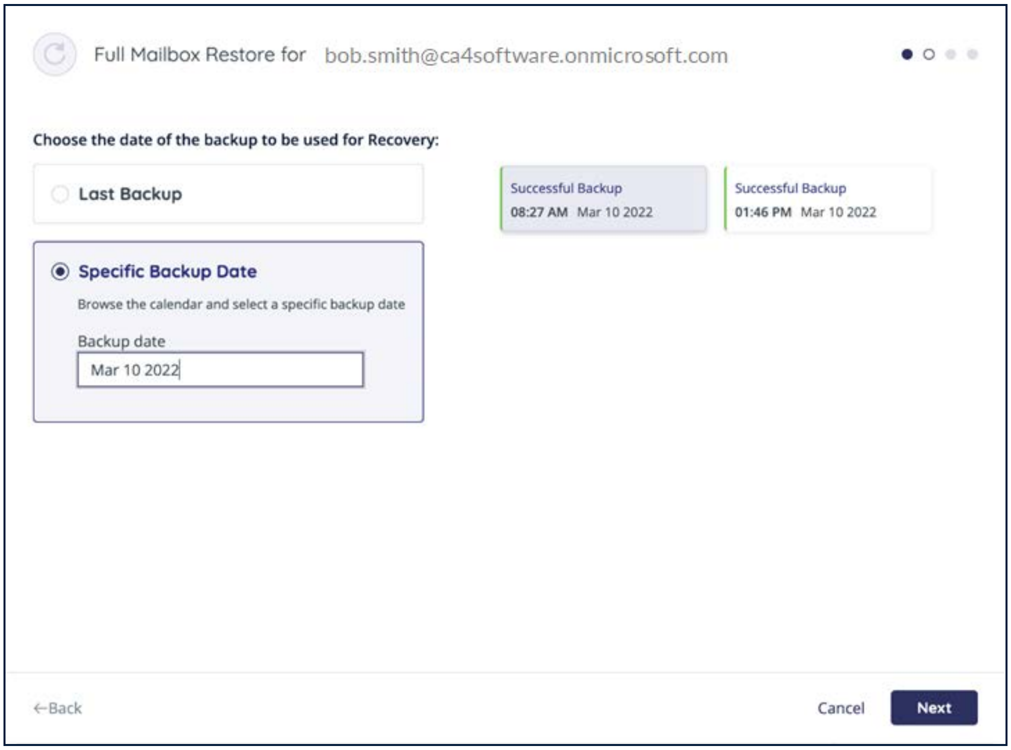
10. Choose the backup you want to restore.

    a. First option: restore the **Last Backup**.

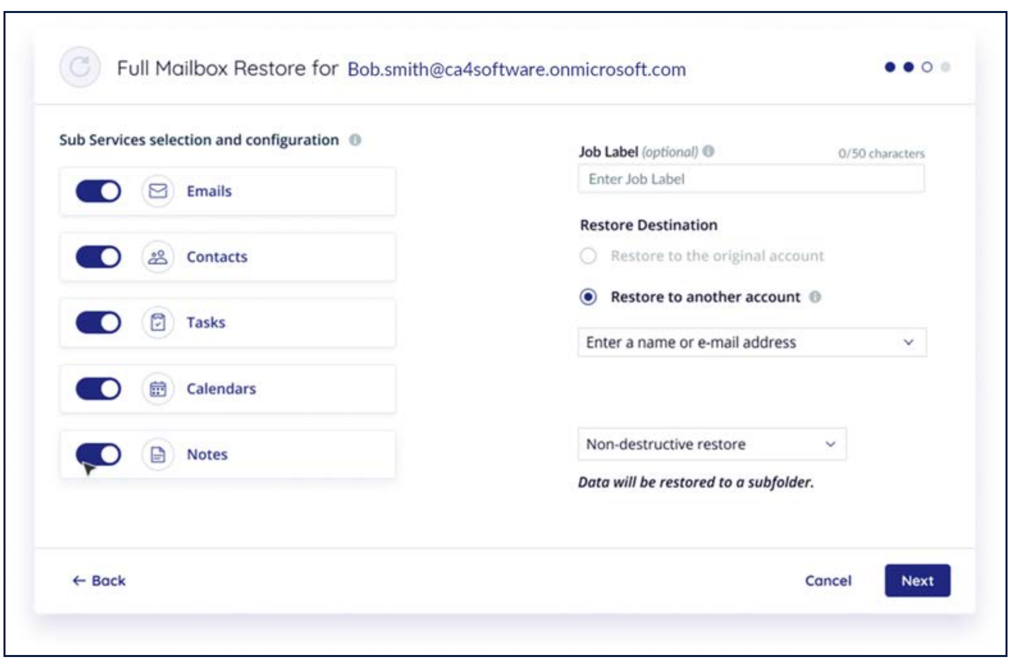
    b. Second option: click **Specific Backup Date** and select a backup date from the calendar with a backup status indication. Once you click a particular date, a card will open, indicating whether the backup was successful, partially successful, or if it failed.



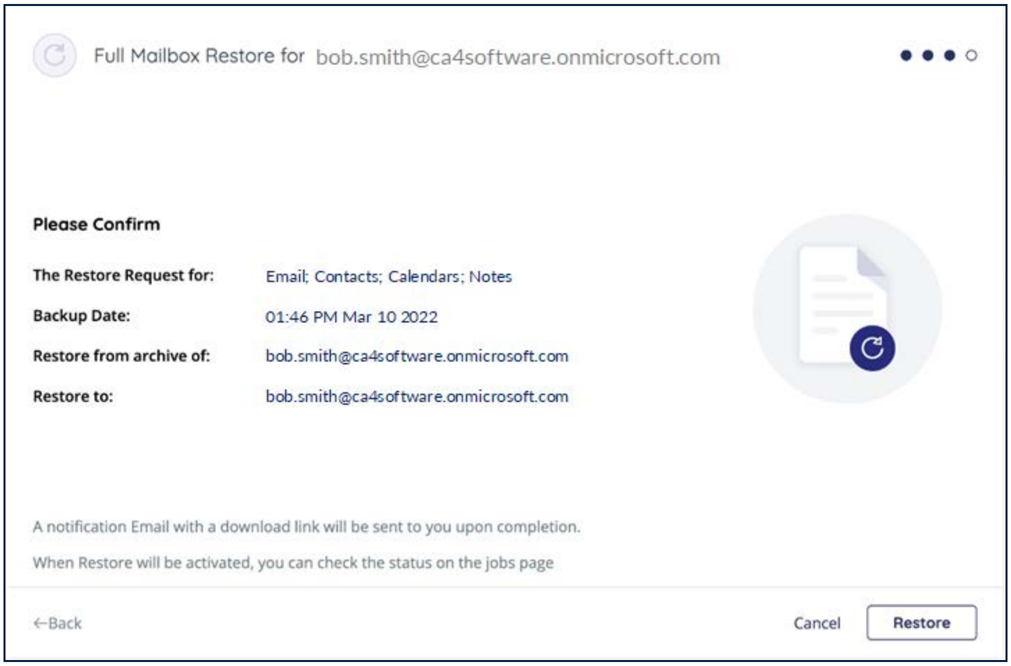
Dot Color	Meaning
Green	Successful backup
Orange	Partially successful backup
Two dots	Multiple backups on that date



11. Select which sub-services to restore.
    a. The default is to restore all sub-services.
    b. Click a toggle to the “off” position to remove individual sub-services.



12. Add an optional Job Label to describe this specific job. It will appear on the Jobs page so you can distinguish between your different restores.
13. **Restore Destination**: Choose where to restore your backup to:
    a. The default is to restore to the original account.
    b. Alternatively, you could restore to a different account, provided it is within the same domain. Click that option, and select an account from the drop-down list.
14. **Restore Type**:Choose one of the following:
    a. **Non-destructive restore**:
        i. Existing data will remain as-is.
        ii. Deleted items and folders will be restored from the snapshot to a new, dedicated folder with the name [Restored] *name*. The original folder structure will be preserved.
        iii. Use this option: to keep restored data separate, enabling manual drag & drop of items to relevant folders
    b. **Replace restore**: The restored items will be located in the same place as the existing items, not in a separate folder, which is created when you choose non-destructive restore.
        i. Deleted items and folders will be restored from the snapshot.
        ii. Existing items will be overwritten with the snapshot version.
        iii. **Use this option:** to restore or repair deleted / modified items
    c. **Bypass restore**: Restored content will be located in the same place as the existing items.
        i. Deleted items and folders will be restored from the snapshot.
        ii. Existing items will be skipped.
        iii. **Use this option**: to restore deleted data
15. Review the information on the confirmation screen. If the information is correct, click **Next** and then **Restore** to begin the recovery task. (If the information is not correct, click **Cancel**.)



16. Check the *Jobs* page to track the progress of your job. See "Tracking Recovery Tasks on the Jobs Page" for details.
17. After the restore task completes, you will receive a Confirmation Report by email.

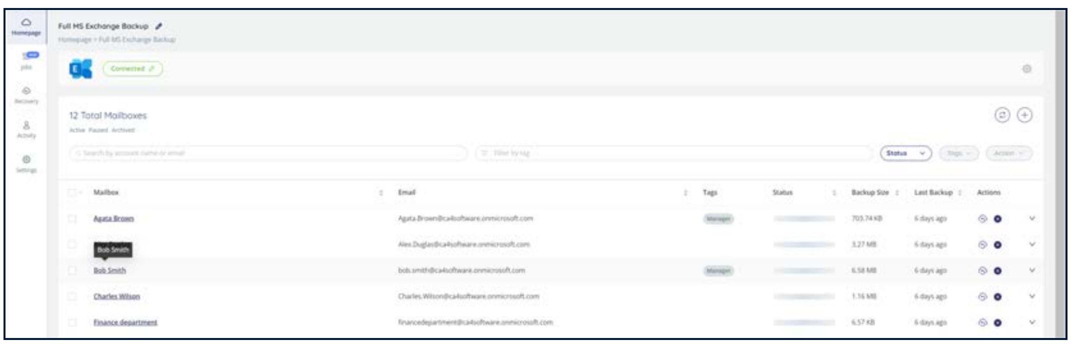
4.2 Recovering Microsoft 365 Exchange: New Recovery Page

4.2.1 Navigating to the Recovery Page

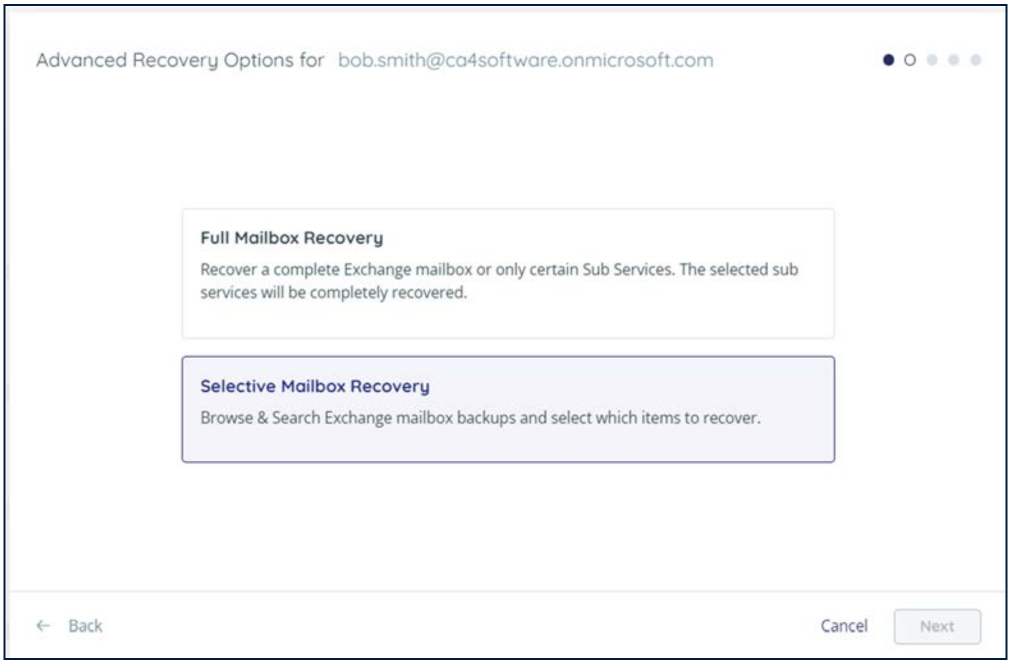
There are two ways to get to the recovery page:

- From the *Homepage*, locate a backup task, and click its name.

- And then click the name of the mailbox.

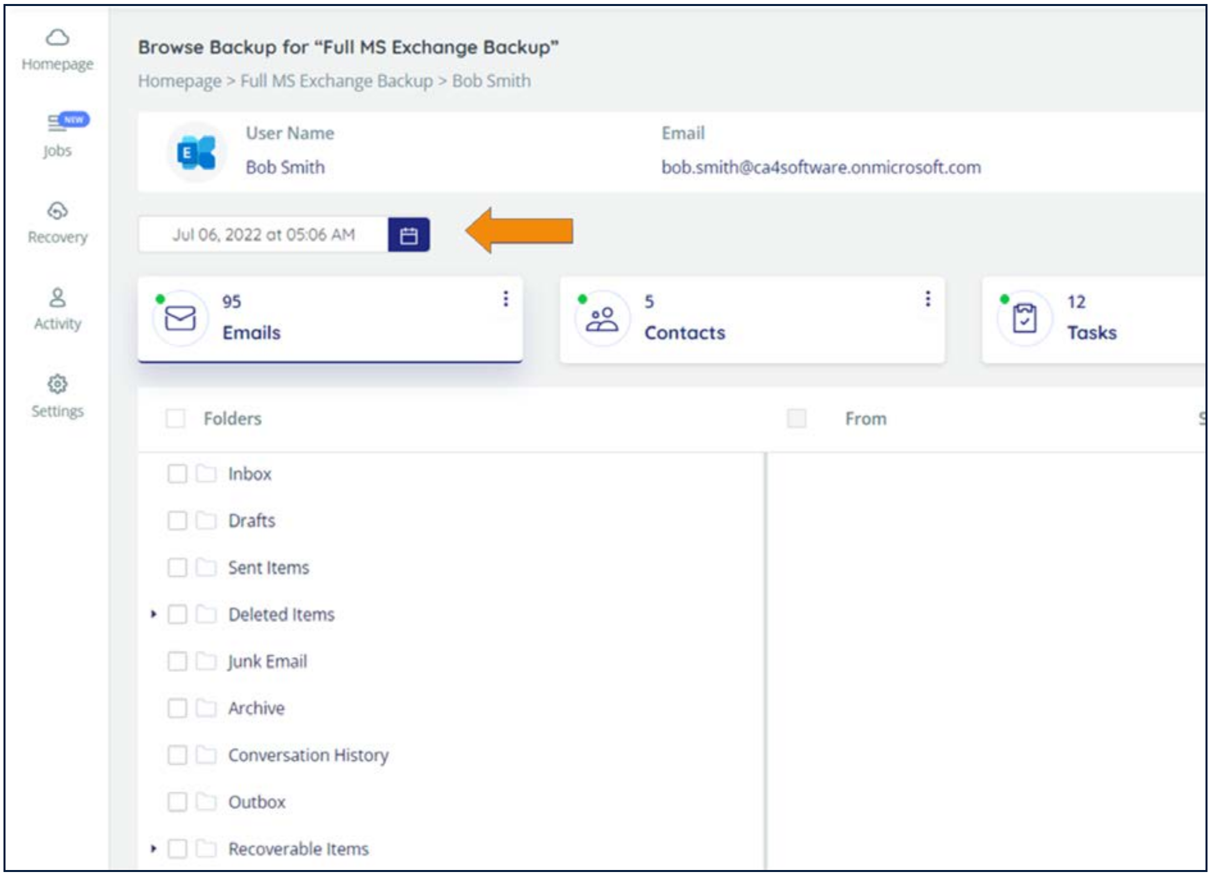


- Or, if you are on the home page, click **Recovery**
  - Look for the desired mailbox using the search bar, or scroll down the list until you find the one that you'd like to recover.
  - On the next screen, click **Selective Mailbox Recovery**

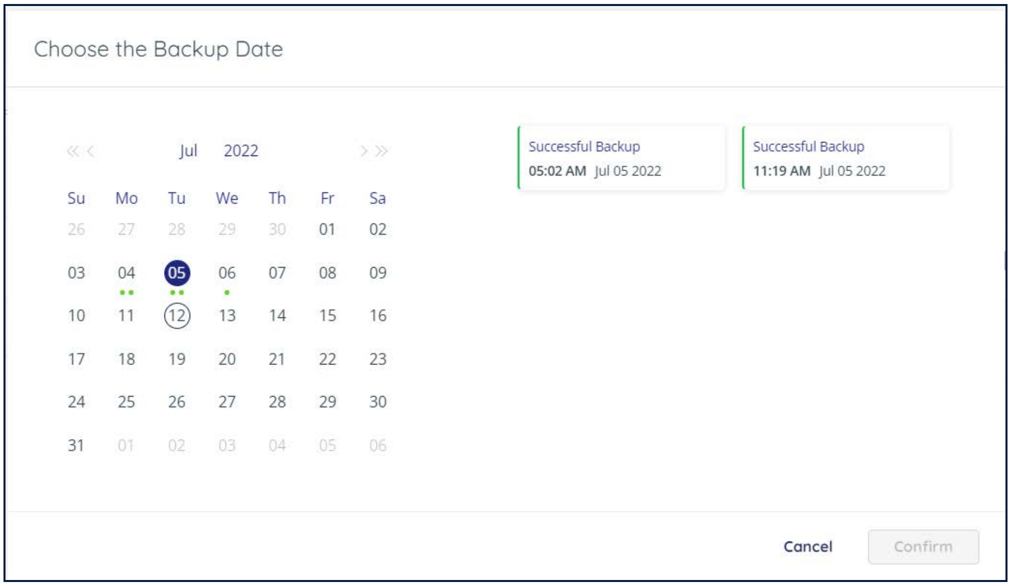

Advanced Recovery Options for bob.smith@ca4software.onmicrosoft.com
Full Mailbox Recovery
Recover a complete Exchange mailbox or only certain Sub Services. The selected sub services will be completely recovered.
Selective Mailbox Recovery
Browse & Search Exchange mailbox backups and select which items to recover.
Back
Cancel
Next

4.2.2 Choosing a Backup Date

Which backup are you looking for? The default is the last backup date, but if you'd like to change to an earlier date, click the calendar icon.



The dots indicate that one or more backups were performed on that day. Two dots indicate that multiple backups were performed on that day. Once you click a particular date, a card will open, indicating whether the backup was successful, partially successful, or if it failed.



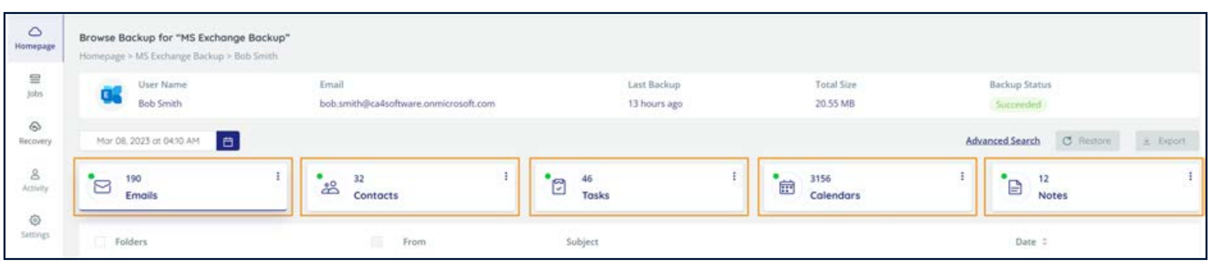
Legend: Meaning of Calendar Dots

Dot Color	Meaning
Green	Successful backup
Orange	Partially successful backup
Two dots	Multiple backups on that date

- Select your desired date, and click **Confirm**.

4.2.3 Browsing Your Backups

Each of the backed up sub-services has a card: Emails, Contacts, Tasks, Calendars and Notes.



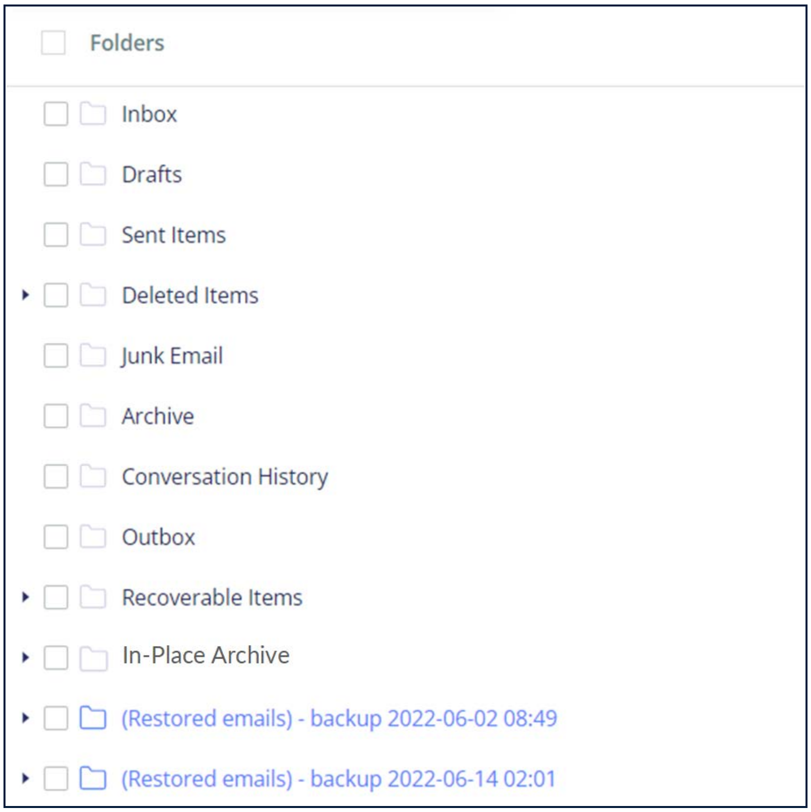
- Each of the cards has a number on it, which shows how many items there are on that date – in the mailbox, in the list of contacts, in the list of tasks, in the calendar, or in the list of notes.

- Each of the cards also has a colored status indicator, which lets you know whether the sub-service was successfully backed up, whether it was partially successful, or if it failed.

Choosing Items to Restore or Export

After you have selected the date of the backup, and the sub-service to recover, you need to choose which items to restore or export.

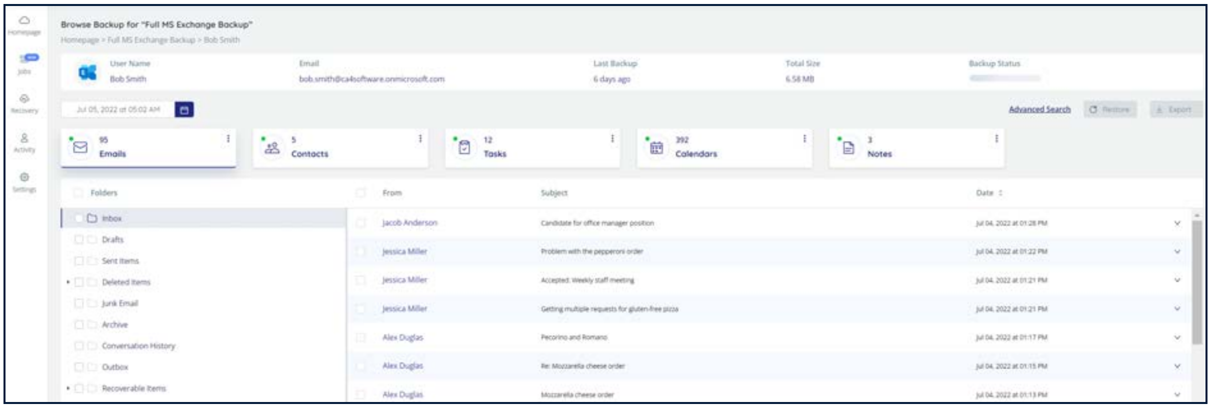
The Recovery folders are in the same familiar order as they are in Outlook, to make it easy for you to find the item you are looking for.



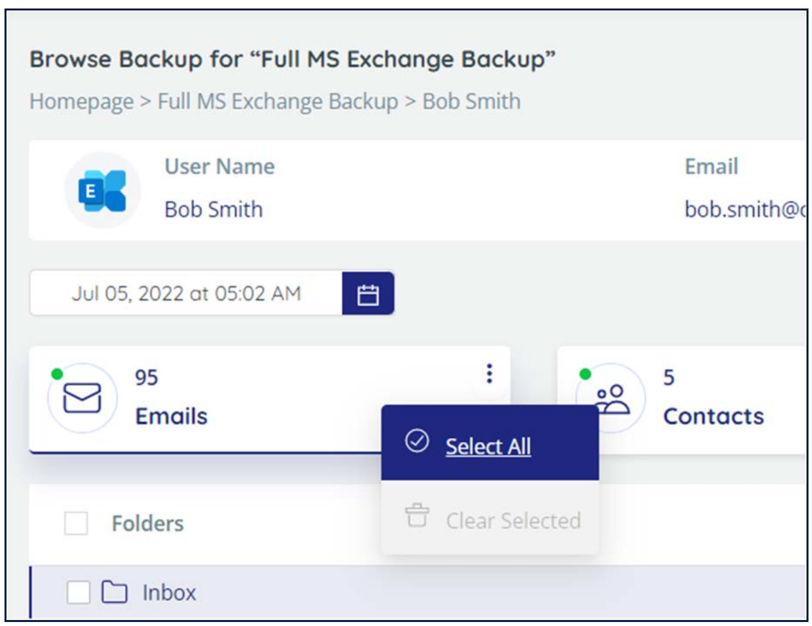
In addition to the usual folders, such as Inbox, Sent Items, and Deleted Items, at the bottom of the list you will find the Recoverable Items folder, and the In-Place Archive folder (if it has been activated) followed by CloudAlly Restored folders, indicated by "Restored emails" and the date of the restore.

4.2.3.1 Email

- Select the Inbox to see its contents.

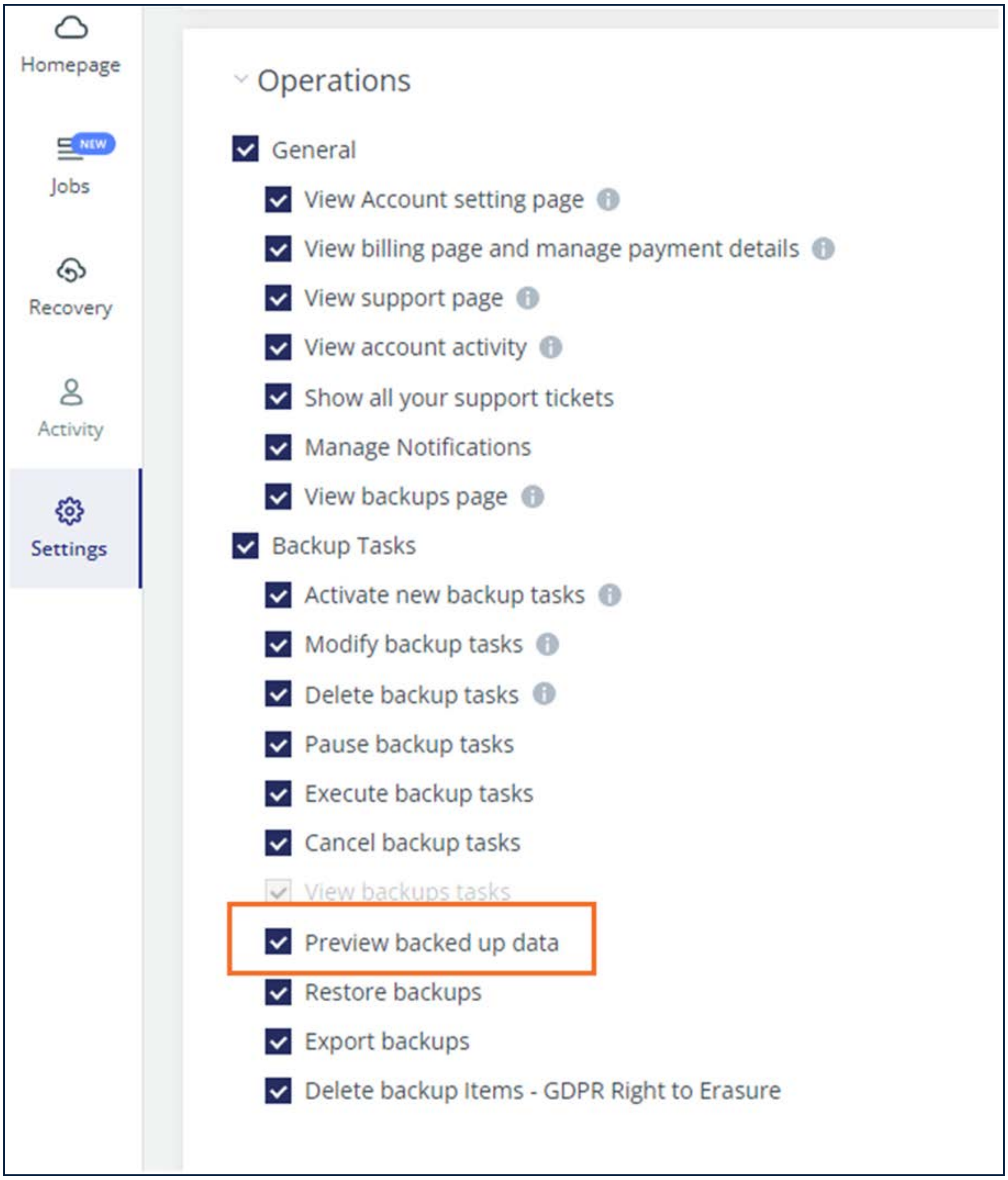


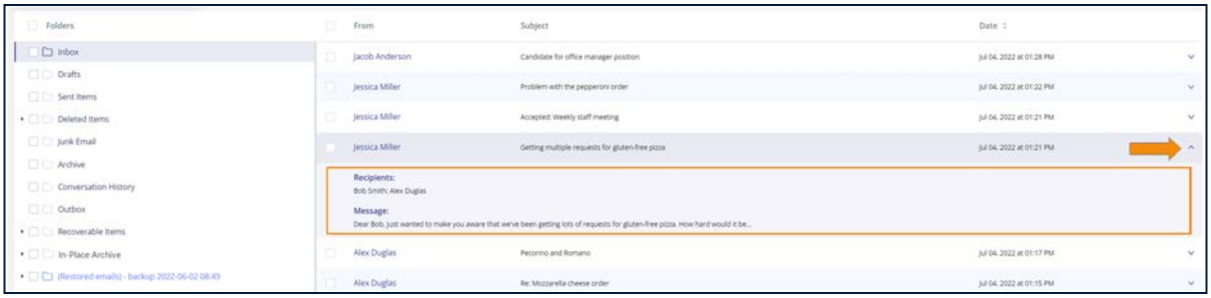
- You can choose one or more messages, or you can choose the entire Inbox.
  - To restore everything, all of the folders and their contents, click **Folders**.
  - Or, select the menu in the Email card, and then **Select All**.



- If you looking for a specific email, click the arrow of the email to see the first line of the message.

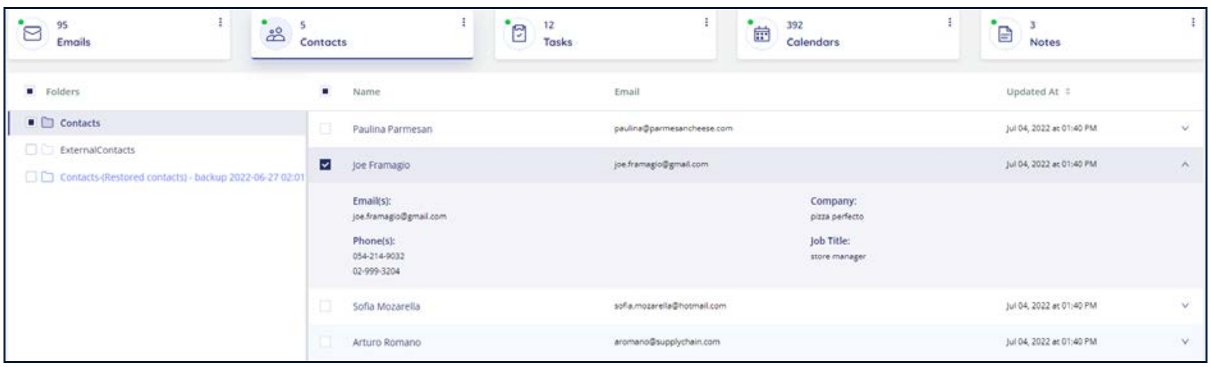
> **Note:** The option to expand a sub-service item and view additional information, such as the first line of an email message, is only available for users with "Preview backed up data" permission. This feature is set by the backup account administrator.





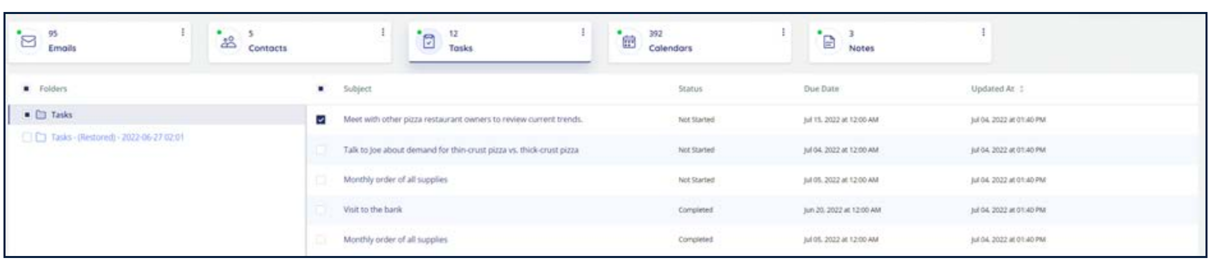
4.2.3.2 Contacts

When you select Contacts, you can see all of the details about the people in your list: Name, Email, Phone, Address, Job Title, and Company name.



4.2.3.3 Tasks

When you select the Tasks sub-service, you can see the Subject, Status and Due date.

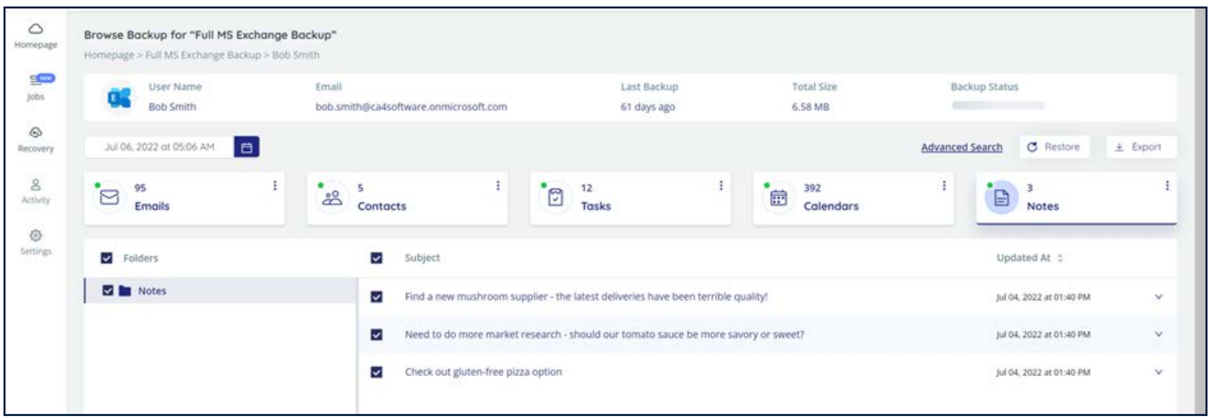


4.2.3.4 Calendar

When you select a Calendar event, you can see the start and end dates, and if you select it, you can see the description.

4.2.3.5 Notes

When you choose a note, you can preview its contents.



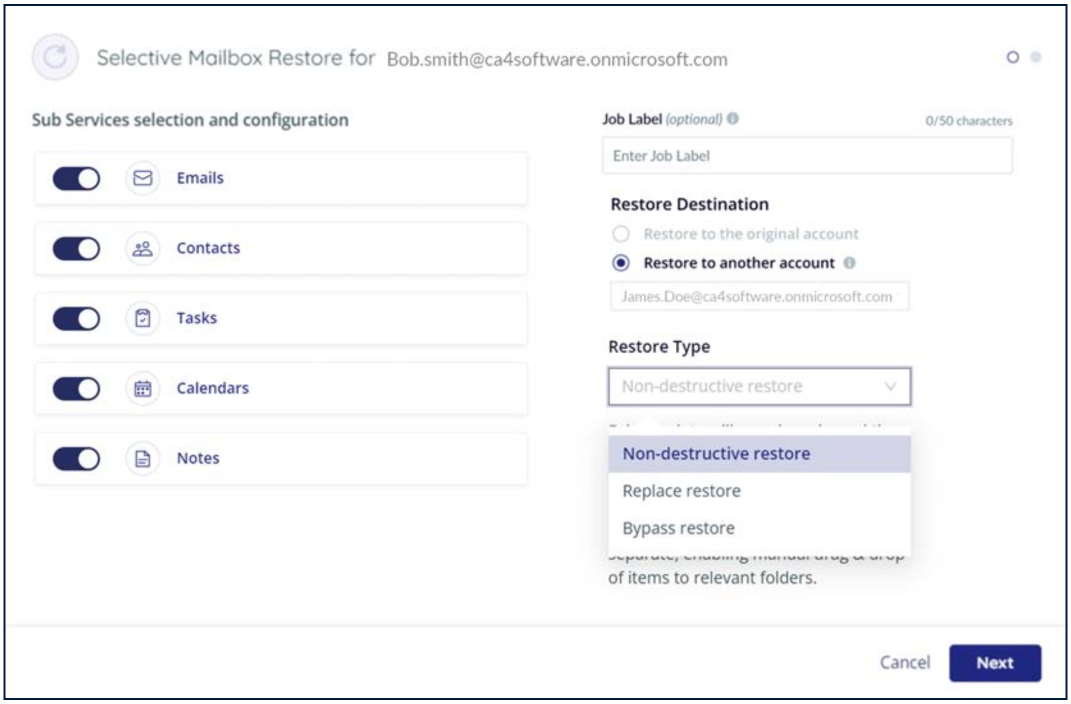
4.2.4 Restore

Once you select one or more items, the **Restore** button becomes active. When you click **Restore**, you will see all of the sub-services that you selected.

- You can choose to remove any of the sub-services by sliding the toggle bar to the left.
- By default, CloudAlly assumes you want to restore to the original account, or you can restore to a different account, as long as it is in the same domain.

4.2.4.1 Restore Options

When you click Restore, you will see the following screen:



Add an optional **Job Label** to describe this specific job. It will appear on the Jobs page so you can distinguish between your different restores.

Restore Destination

You will have the option of:

- Restoring to the original account
- Restoring to another account in the same domain.

Restore Type

Choose one of the following:

- **Non-destructive restore**:
  - Existing data will remain as-is.
  - Deleted items and folders will be restored from the snapshot to a new, dedicated folder with the name [Restored] name. The original folder structure will be preserved.

- **Use this option**: to keep restored data separate, enabling manual drag & drop of items to relevant folders

- **Replace restore**:The restored items will be located in the same place as the existing items, not in a separate folder, which is created when you choose non-destructive restore.
  - Deleted items and folders will be restored from the snapshot.
  - Existing items will be overwritten with the snapshot version.
  - **Use this option**: to restore or repair deleted / modified items
- **Bypass restore**: Restored content will be located in the same place as the existing items.
  - Deleted items and folders will be restored from the snapshot.
  - Existing items will be skipped.
  - **Use this option:** to restore deleted data

Restore Options

If you choose Replace Restore, the following options become available:

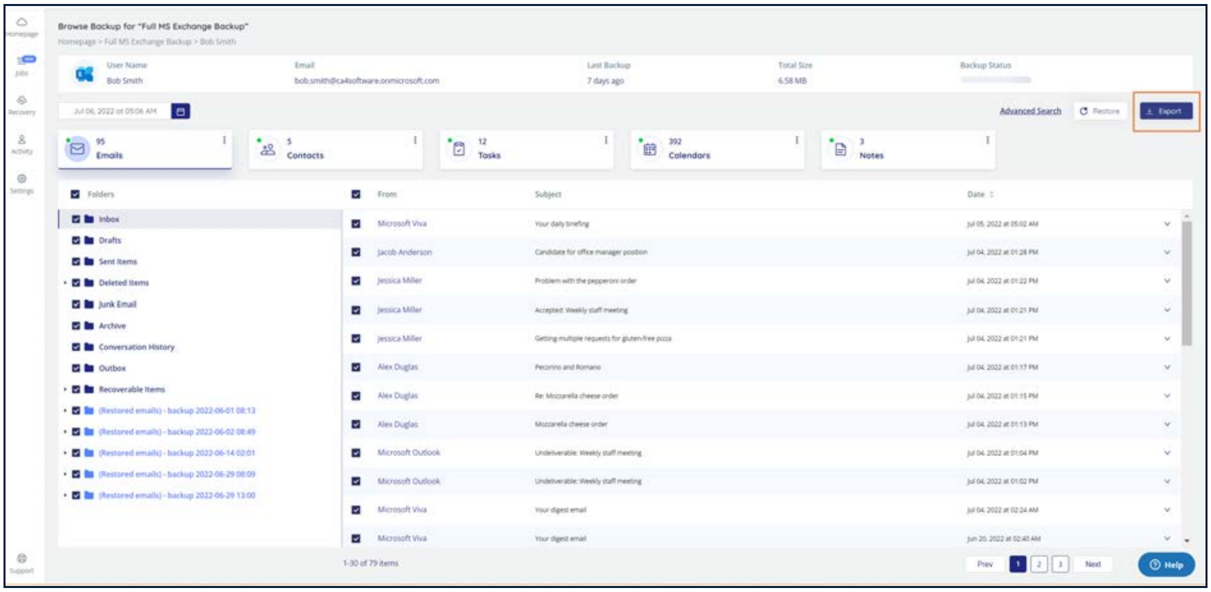
- Add a "restored..." tag to restored items, so you will be able to identify which items were added to your account.
- Add "restored..." to Outlook folders and calendars that the Restore process created.
- Create a snapshot of the restore endpoint prior to data upload - This is a local backup of the current contents of your account before the restore is implemented.

After you choose all of your **Restore** options, you can check the *Jobs* page to see the status of your job. See Tracking Recovery Tasks on the Jobs Page for details.

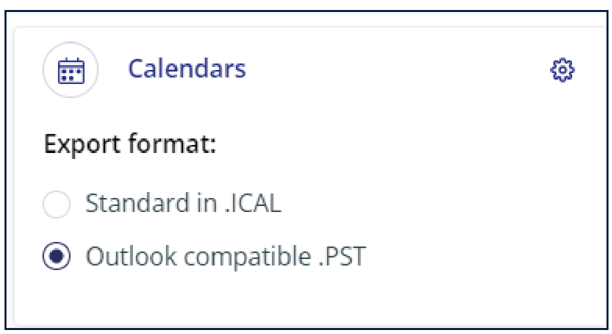
When the restore is complete, you will receive a notification email .

4.2.5 Export

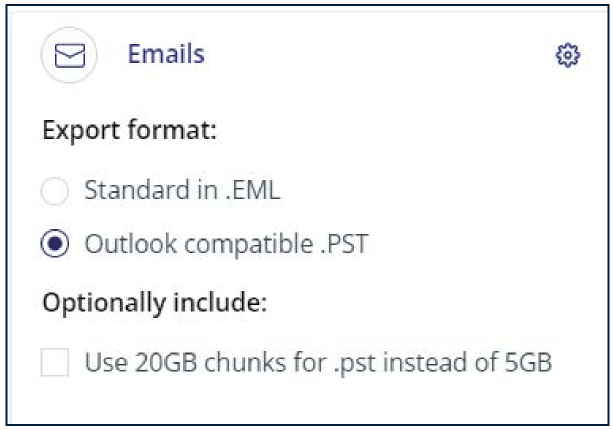
Once you select one or more items, the **Export** button becomes active. Click **Export**.



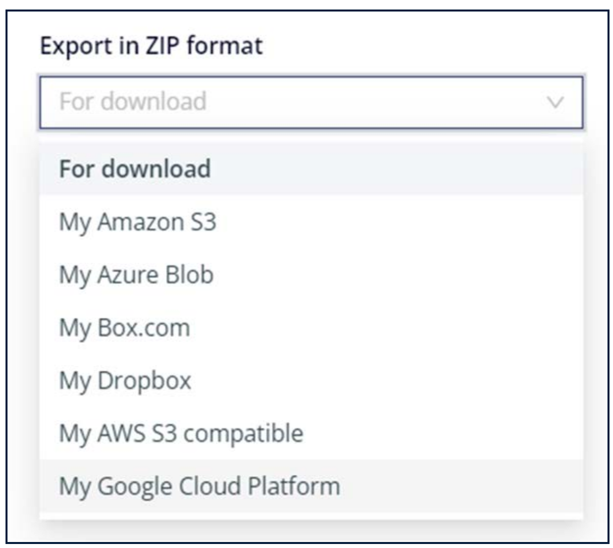
- When you export multiple sub-services, the format will be a single PST file.



- When you export a single sub-service, you can choose to customize the export format in the following ways.
  - If you click the gear-shaped settings icon, you can choose the export format: EML or PST.
  - You can also choose to have larger, 20 GB .pst files, instead of 5 GB files.



- The gear-shaped settings icon allows you to choose the format of the download file: iCAL or PST.
- The other option that you have when you export is to choose the destination: Amazon S3, Azure Blob, Box, DropBox, AWS S3 Compatible (if you are bringing your own storage), Google Cloud Platform, or a simple Zip file.

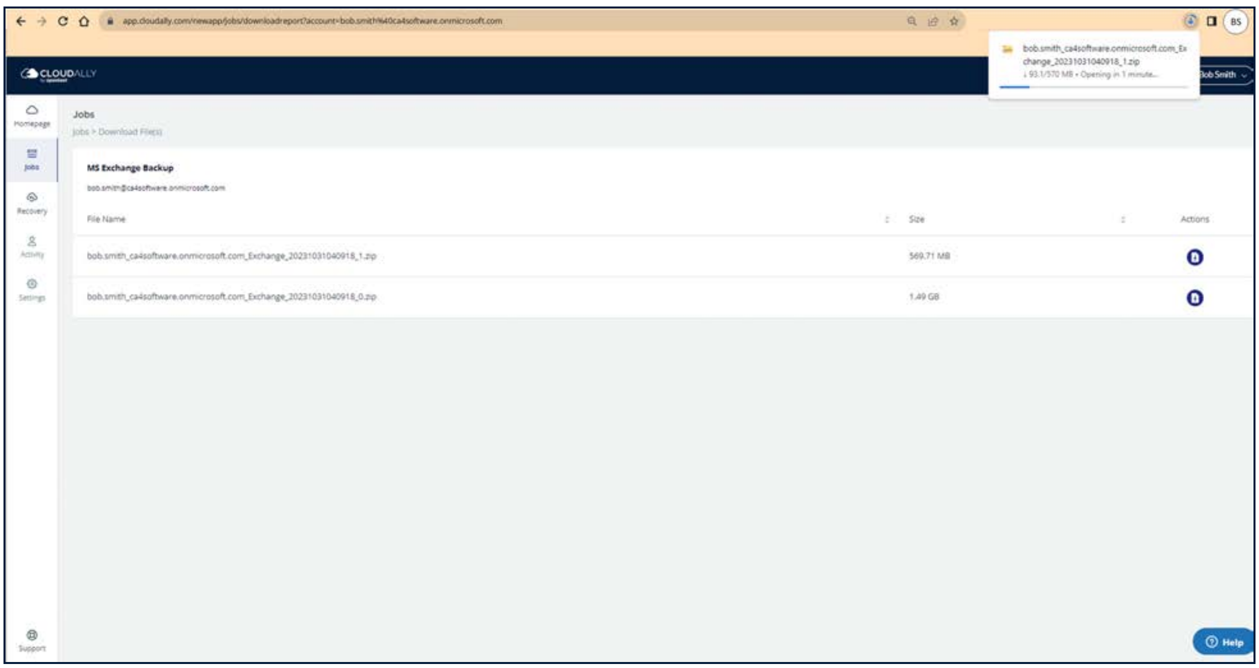


> **Note:** The default "for download" option exports the file to your local storage device.

- Check the *Jobs* page to track the progress of your job. "Tracking Recovery Tasks on the Jobs Page" on page 93

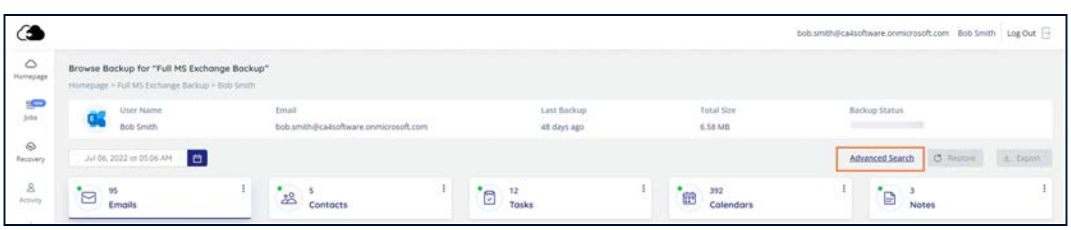
- When the export is complete, click **Download Results**.

A new page will open which will enable you to download your data file.

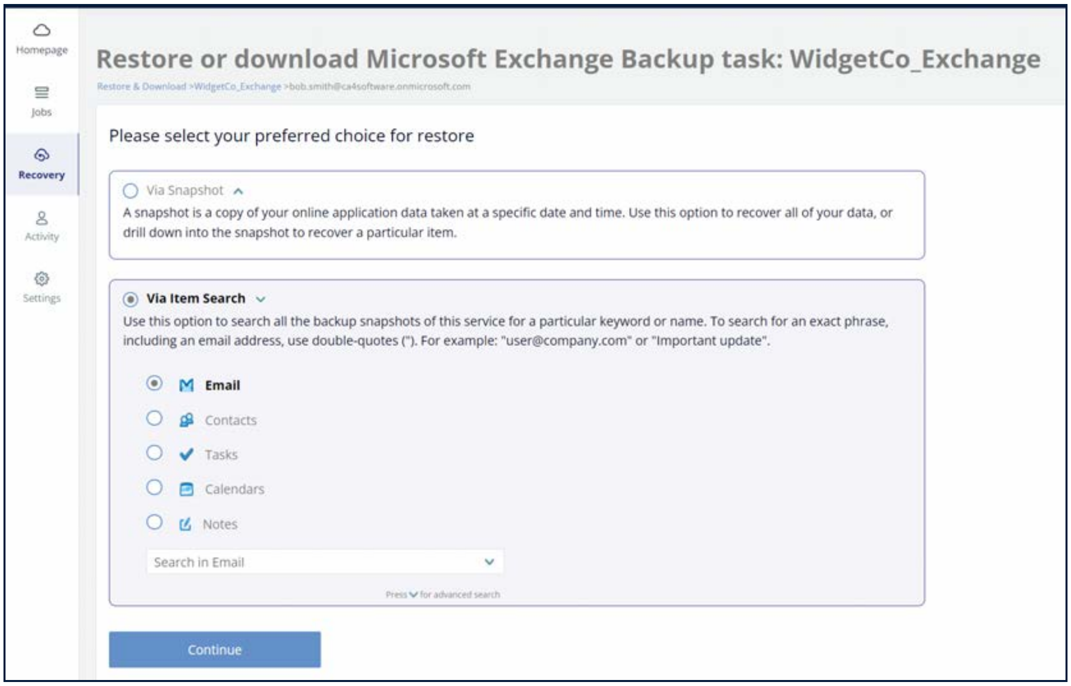


4.2.6 Advanced Search

To perform a granular, keyword search, click **Advanced Search**.



You will see the following screen:



Enter your search criteria for any of these sub-services:

- **Email** – Enter a keyword in the Search for field. For advanced search options, click the down-arrow and provide the following details in the drop-down form:
  - **From**: Enter a name or email address from which the email was received.
  - **To**: Enter a name or email address to which the email was sent.
  - **Subject**: Enter a keyword that matches any text in the email subject.
  - **Date from / Date to**: Enter the date range of the emails you would like to restore.
- **Contacts**: Enter a name in the Search for field.
- **Tasks**: Enter a keyword in the Search for field.
- **Calendars**: Enter a keyword in the Search for field. For advanced search options, click the downward-facing arrow, and provide the following details in the drop-down form:
  - **Description**: Enter all or part of the event description.
  - **Owner**: Enter the user name or the email address

- **Date from / Date to**: Enter the date range of the calendar you would like to restore.

4.3 How to Restore a Deleted Microsoft Exchange Mailbox

This procedure should be performed by a user with Administrator permissions.

1. Recreate all users in the Active Directory that have been deleted.
2. Recreate their mailboxes. Alternatively, restore the mailboxes to an existing user, but ensure that the users have a license with a mailbox.
3. From the Homepage, locate the Microsoft Exchange backup task you would like to restore, and then click the Recovery icon.
4. Select one of the active mailboxes on the list, and click **Next**.
5. In the **Full Mailbox Recovery** box, click **Restore**, and then **Next**.
6. Choose the backup you want to restore.
   a. First option: restore the **Last Backup**.
   b. Second option: click **Specific Backup Date** and select a backup date immediately prior to when the mailbox was deleted.
7. Select which sub-services to restore, or accept the default of restoring all services (recommended).
8. Select which sub-services to restore, or accept the default of restoring all services (recommended).
9. Choose where to restore your backup to:
   a. The default is to restore to the original account.
   b. Alternatively, you could restore to a different account, provided it is within the same domain. Click that option, and select an account from the drop-down list.
10. Review the information on the confirmation screen. If the information is correct, click **Next** and then **Restore** to begin the recovery task. (If the information is not correct, click **Cancel**.)
11. Check the *Jobs* page to track the progress of your job. After the restore task completes, you will receive a Confirmation Report by email.

12. The restored data will be in a newly created "(Restored)" folder. After the recovery, move the recovered data back into the appropriate mailbox folders.

> **Note:** For multiple Microsoft Exchange mailboxes, please contact Support for assistance.

4.4 Recovering Microsoft 365 OneDrive and Microsoft 365 SharePoint

> **Note:** The screens below are from a OneDrive recovery, but the functionality is identical for SharePoint.

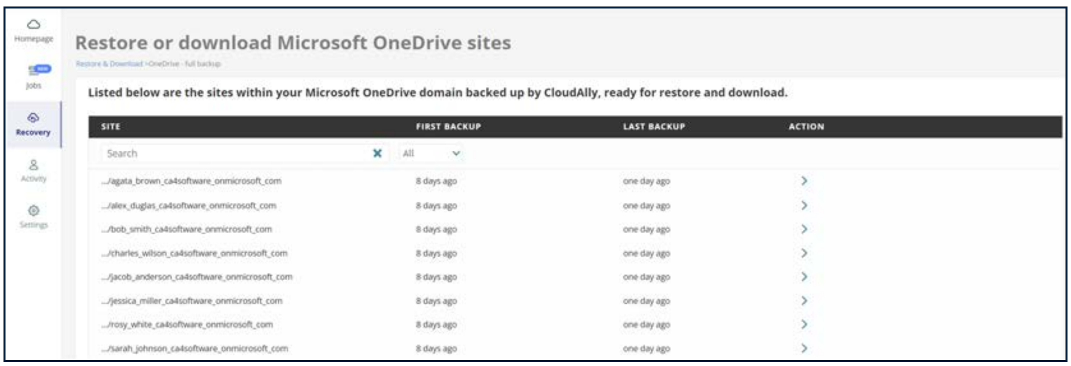
The Recovery Menu provides you with options at a fine granularity for selecting which sites to restore or export.

To recover your backed up data:

> **Note:** In order to restore all data, CloudAlly assigns the backup user to be the site collection administrator. If CloudAlly is unable to do so (for example, because the user doesn't have proper permissions), then the user needs to be added manually.

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

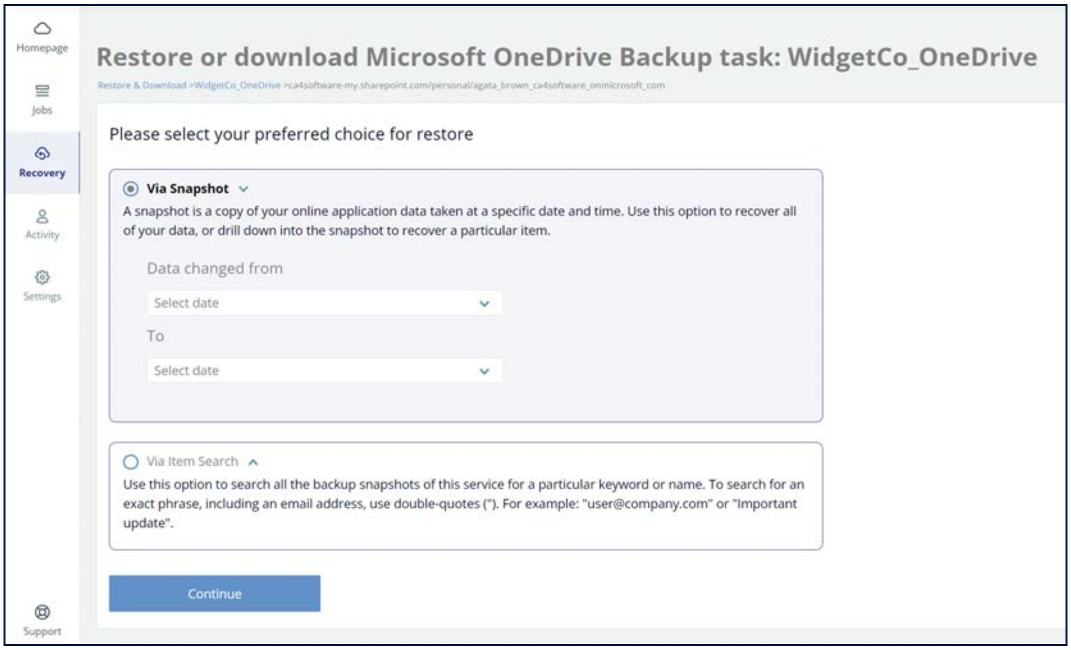
2. Click the OneDrive or SharePoint backup task from which you wish to recover the data. The *Restore or Download Active Mailboxes* page is displayed.



This page displays all your OneDrive and SharePoint domains backed up with the details such as Site name, First Backup date, Last Backup date, and available Actions. Your backed-up data is ready for download, from this page.

- You can filter the list using the following options:
  - Filter by statuses such as All, Active, In Process, Not Active, Scheduled, Paused, Backed-up in another task, or Archived, from the drop-down list.
  - Or: search by part or all of the Site name.
- Click the arrow icon at the end of the line of the site which you want to restore or export (download).

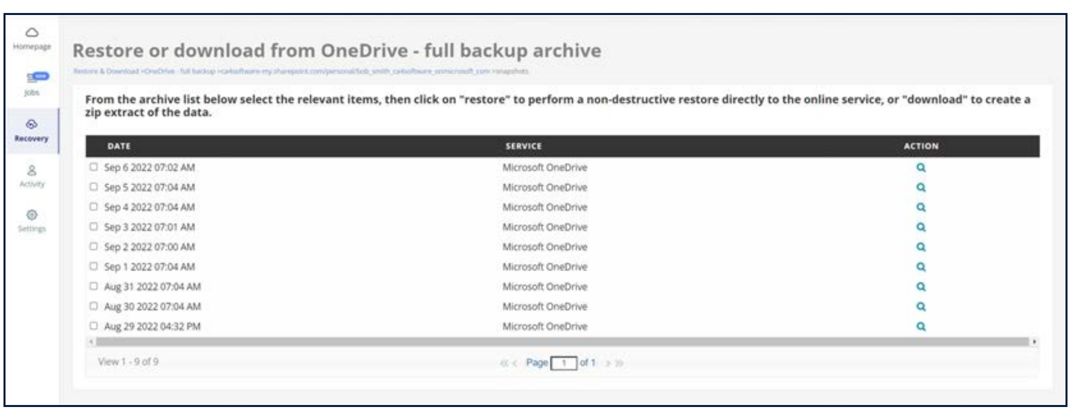
The *Restore or download Microsoft* page is displayed.



- Select the radio button for your preferred restore method:
  - [Via Snapshot]
  - [Via Item Search]

4.4.1 Restore or Download Via Snapshot - OneDrive or SharePoint

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 icon 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.

4.4.1.1 Restore - OneDrive or SharePoint

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

- Do you want to restore to another tenant? If so, provide the email address of the administrator, the password, and the site to restore to.

> **Note:** The administrator should have read/write access to the destination site. Therefore we suggest using a Microsoft account that has a Global Admin or SharePoint Admin role.

- Do you want to perform a **non-destructive restore**, where the existing data will remain as-is, and the restored data will be in a dedicated folder, preserving the original folder structure?
  - Use this option to keep restored data separate, enabling manual drag & drop of items to relevant folders.

> **Note:** The non-destructive restore option only works when you are restoring from OneDrive to a SharePoint sub-site, and the option to create a SharePoint sub-site is enabled in Microsoft.

- Or do you want to perform an **in-place restore**? You have three options for doing so:
  - **Replace**: The restored items will be located in the same place as the existing items, not in a separate folder when you choose nondestructive restore. Deleted items and folders will be restored from the snapshot. Existing items will be overwritten with the snapshot

version.

Use this option: to restore or repair deleted / modified items.

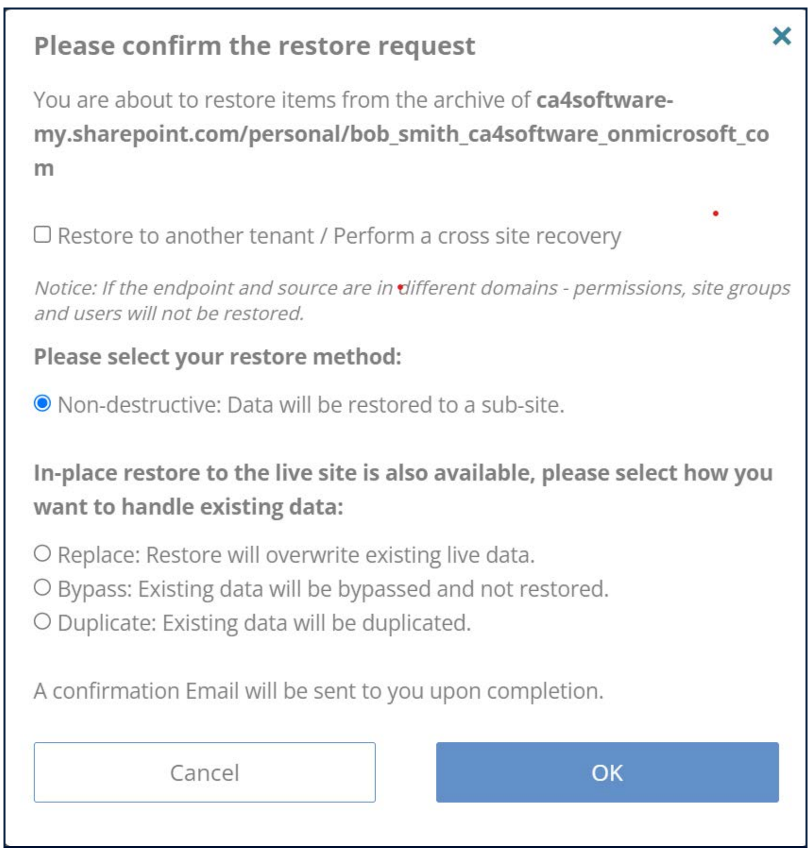
- **Bypass:** the restored content will located in the same place as the existing items. Deleted items and folders will be restored from the snapshot. Existing items will be skipped.

  Use this option: to restore deleted data.

- **Duplicate**: the restored data will be duplicated in the same location as the existing data, with a suffix that indicates that it is a copy. (The suffix contains the year, month, day, hour, minutes, and seconds, e.g., 20230401000525.) Deleted items and folders will be restored from the snapshot.

  Use this option: to compare both versions of each file, to ensure the correct version is preserved.

■ When you have completed the confirmation form, click **OK**.



5. 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."

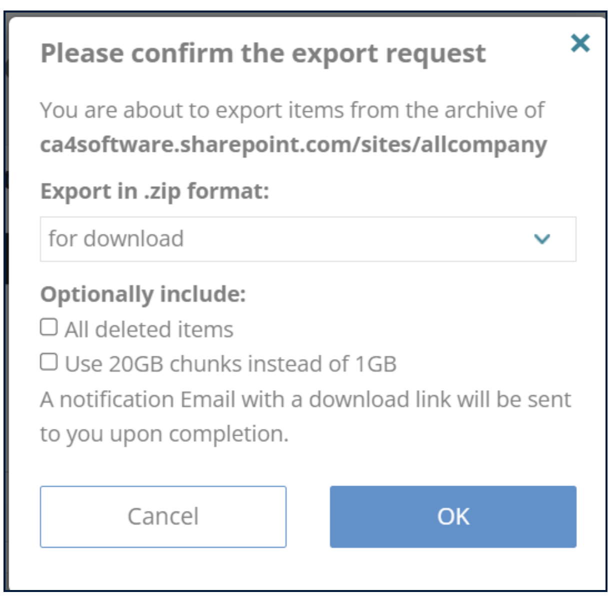
A Note About OneNote

CloudAlly is able to back up and restore OneNote, both from within SharePoint and within OneDrive. CloudAlly backs up and restores all content, except for the following items:

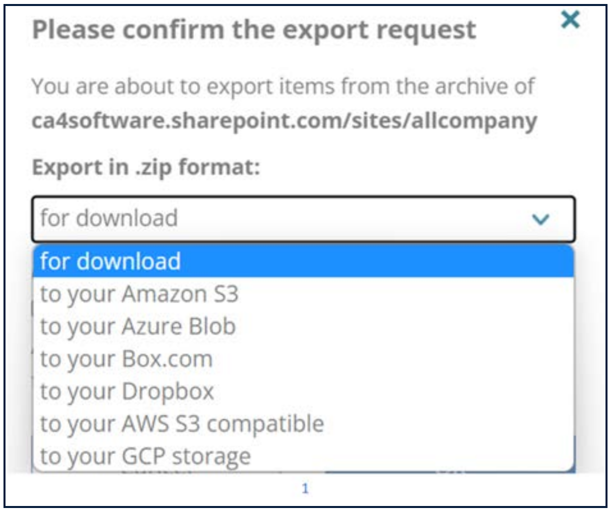
- Audio recordings (*.wav files)
- Images created with the Draw menu
- Tables
- Page color
- Rule lines
- Text styles (e.g., Headings, Normal, etc.)
- Attachments, except for image files, which are restored (Microsoft limitation)
- Tags

4.4.1.2 Export/Download - OneDrive or SharePoint

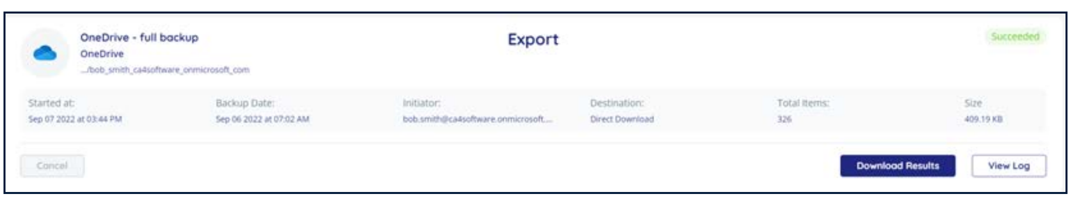
If you click **Download**, the following confirmation window appears.



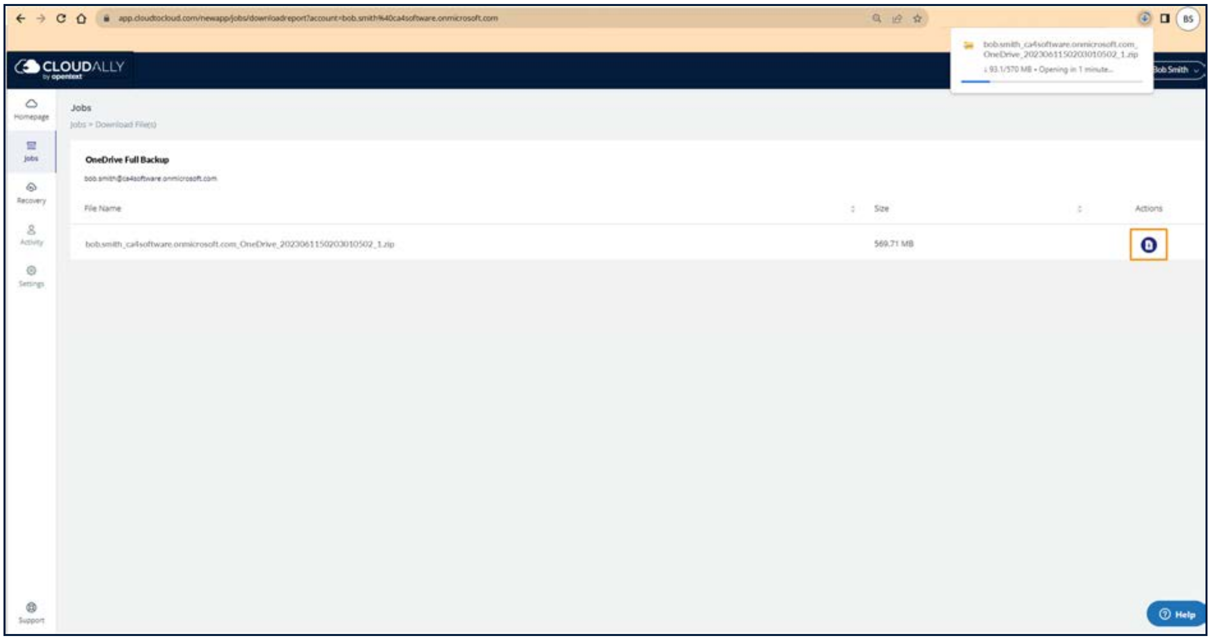
1. Click the drop-down list and select one of the following storage locations:



2. If you select options other than “for download,” you may be asked for additional credentials and/or access tokens for the selected storage locations.
3. By default, we download data in 1 GB files. But if your backed up data is large, you can choose to download in 20 GB chunks instead.
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.

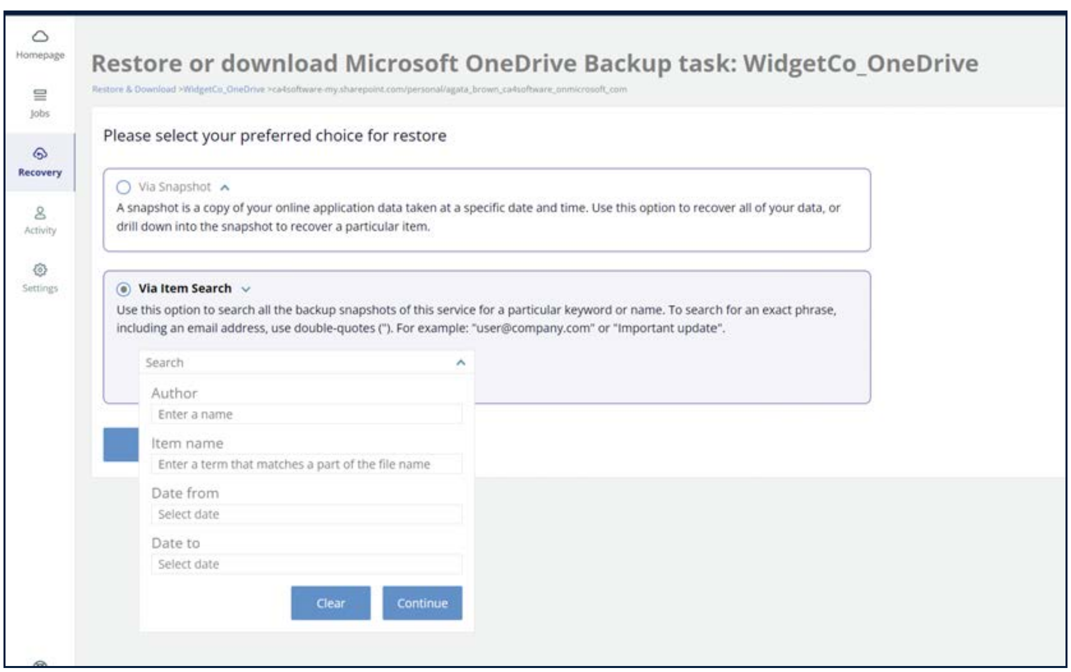


6. Click **Download Results**, and a page will open, where you can access your backup file.



4.4.2 Restore or Download Via Item Search - OneDrive or SharePoint

1. Select **Via Item Search**, and enter a word or phrase to search for.
2. Or, click the arrow to the right of the search bar, and enter search criterion in any of the Advanced fields: Author, filename or date.



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

4.4.3 How to Restore Deleted SharePoint Collections

1. Recreate all of the deleted Site Collections in Microsoft SharePoint.
2. Click **Recovery** from the Navigation Panel, and then click on the SharePoint backup task.
3. Locate the Site Collection that you want to restore, and then click the arrow icon to the right of the site. The *Restore or download* page is displayed.
4. Select the **Via Snapshot** radio button
5. Enter the date range that you would like to select from, or just click **Continue** for a full list of backups.
6. Select the backup you want to recover – the one closest to the date that all of your SharePoint data was deleted.
   a. Go to the bottom of the page, and click **Restore**.
   b. From the pop-up dialog, click **Replace: Restore will overwrite existing live data** and then click **OK**.
   c. Click **Yes** to the question about overwriting live data.

> **Note:** You will receive an email notification when the restore is complete and can view the job status from the Jobs page.

4.4.4 How to Restore Deleted OneDrive Sites

1. Click **Recovery** from the Navigation Panel, and then click on the OneDrive backup task.

2. Locate the Site that you want to restore and then click the arrow icon to the right of the site. The *Restore or download* page is displayed.
3. Select the **Via Snapshot** radio button.
4. Enter the date range that you would like to select from, or just click **Continue** for a full list of backups.
5. Select the backup you want to recover – the one closest to the date that all of your OneDrive data was deleted.
    a. Go to the bottom of the page, and click **Restore**.
    b. From the pop-up dialog, click **Replace: Restore will overwrite existing live data** and then click **OK**.
    c. Click **Yes** to the question about overwriting live data.

> **Note:** You will receive an email notification when the restore is complete, and you can view the status from the *Jobs* page.

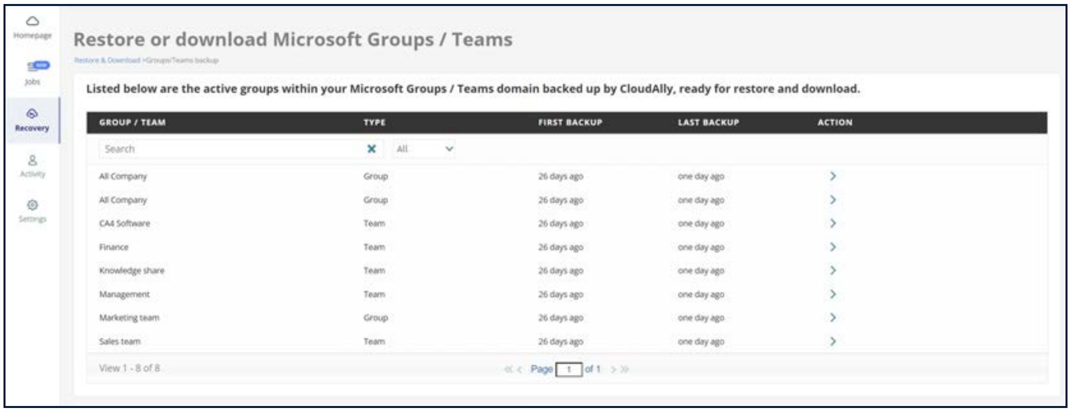
4.5 Recovering Microsoft 365 Teams & Groups

The Recovery Menu provides you with options at a fine granularity for selecting which account, team or site to restore or export.

To recover your backed up Teams & Groups data:

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

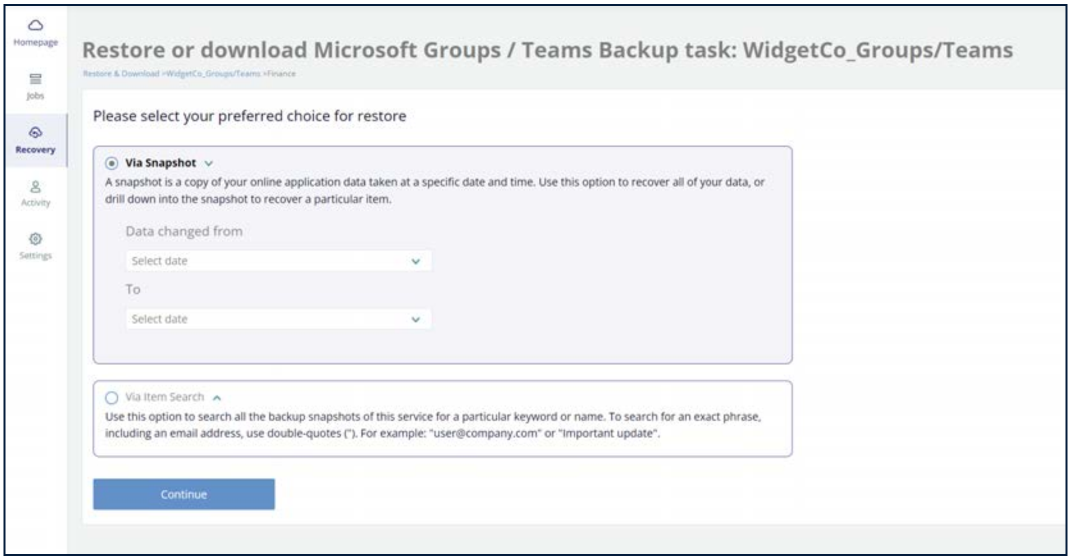
2. Click the Teams / Groups backup task from which you wish to recover the data. The *Restore or Download Microsoft Groups/Teams* page is displayed.



This page displays all of your backed up Teams & Groups, with details such as Team/Group name, First Backup date, Last Backup date, and available Actions. Your backed-up data is ready for download from this page.

- You can filter the list using the following options:
  - Filter by statuses such as All, Active, In Process, Not Active, Scheduled, Paused, Backed-up in another task, or Archived, from the drop-down list.
  - Or: search by part or all of the Team/Group name.
- Click the arrow icon at the end of the line of the group or team which you want to restore or export (download).

The *Restore or download Groups/Teams* page is displayed.



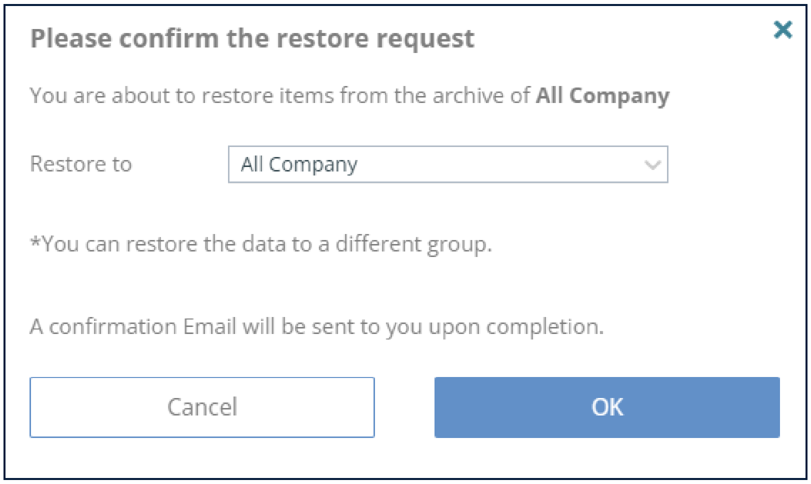
- Select the radio button for your preferred restore method:
  - Via Snapshot
  - Via Item Search

4.5.1 Restore or Download Via Snapshot

See the instructions in "Restore or Download Via Snapshot."

4.5.1.1 Restore - Teams & Groups

1. If you click **Restore**, the restore confirmation window appears, asking for the group/team to which you would like to restore the data. Enter the address, and click **OK**.



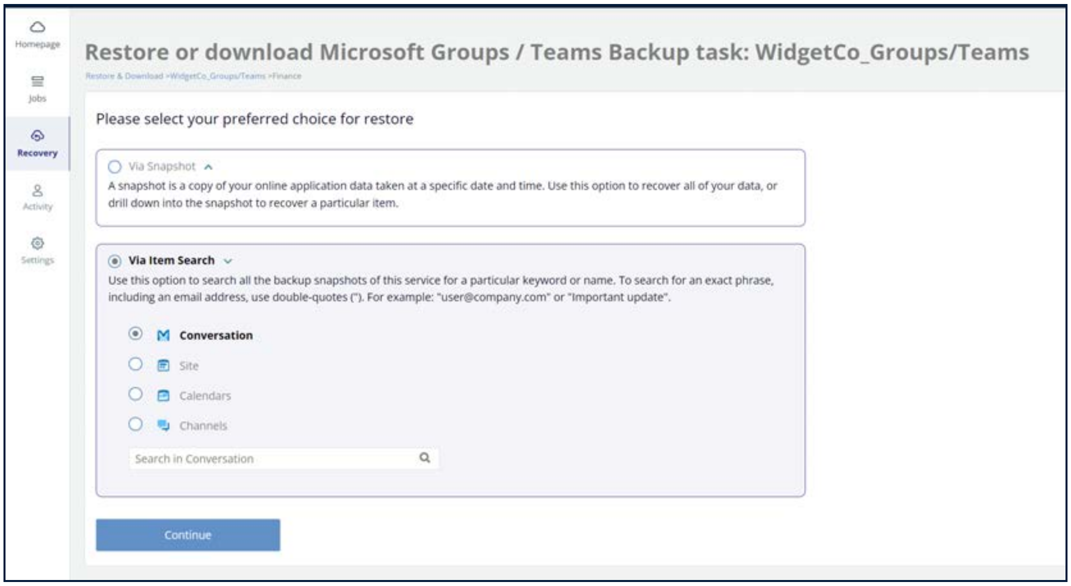
2. The backup data that you selected will be restored to the location that you specified. When the recovery process is complete, a summary will be sent to your email. You can also check the *Jobs* page to see the progress of your task. See "Tracking Recovery Tasks on the Jobs Page."

4.5.1.2 Export/Download - Teams & Groups

See the instructions in "Export/Download OneDrive or SharePoint."

4.5.2 Restore or Download Via Item Search - Teams & Groups

1. Select one of the following options:



- **Conversation**: Enter a keyword in the Search for field.
- **Site**: Sites refer to the SharePoint site where Teams files are stored. Enter a keyword in the Search for field. For advanced search options, click the arrow and provide the following details in the drop-down form:
    - **Author**: Enter the name of the person who created the file in the Teams channel.
    - **Item Name:** Enter a term that matches part of the file name.
    - **Date from / Date to**: Enter the date range during which files were sent in the Teams channel.
- **Calendars**: Enter a search keyword in the Search for field. For advanced search options, click the arrow and provide the following details:
    - **Description**: Enter a keyword that matches part of the event description.
    - **Owner**: Enter a name or email address of the calendar owner.
    - **Date from / Date to**: Enter the date range of the calendars you would like to restore.
- **Channels**: Enter a search keyword in the Search for field. For advanced search options, click the arrow and provide the following details:
    - **Date from / Date to**: Enter the date range of the data you would like to restore.
    - **Sender**: Enter a name of the person who sent messages within that

channel.

- **Channel**: Enter part or all of the channel name.

2. Click **Continue**. The *Restore or download* page is displayed, showing the search results with details such as **Date**, **Subject**, and **Folder**. 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.

4.6 How to Restore Deleted Teams Sites

Each of the deleted teams needs to be restored one at a time. If you need to restore a large number of teams, you can open a CloudAlly support ticket to help with the restore process.

4.6.1 First Step: Restore a Public Channel

> **Note:** Private channels need to be exported and then restored.

1. Click **Recovery** from the Navigation Panel. The *Restore & Download page* is displayed with all your active-backup account details.
2. Click the Microsoft Groups/Teams backup task from which you wish to recover the data. The *Restore or download Microsoft Groups & Teams page* is displayed.
3. Locate the Team (not the Group – that will come later) that you would like to restore. Click the arrow at the end of the row. The *Restore or download Microsoft Groups/Teams task* page is displayed.
4. By default, **Via Snapshot** is selected. Enter the appropriate date immediately before the Teams data was deleted, or simply click **Continue** without filling in the date fields to view all backups.
5. Locate the most recent Channel backup prior to the ransomware attack and select it. Go to the bottom of the page, click **Restore**, and then click **OK**.

> **Note:** This is a non-destructive restore – the data will be placed into a newly created Team called (Restored [date]).

6. Check the *Jobs* page to determine when the restore is complete.
7. Click the Homepage element from the Navigation Panel, and then click on the Teams backup task to return to the Teams backup. Click the CloudAlly refresh icon to display the newly restored Team. You will need to perform the following steps.

> **Note:** The refresh icon is not to be confused with the browser refresh button.

4.6.2 Second Step: Restore the Teams Sub-Services

Perform the following steps for each of these Teams sub-services in this order:

1. Sites
2. Calendars
3. Conversations
4. Metadata – this will finalize the restore, by recovering the Members, Owners, and most importantly, the Team Name.

For each sub-service, perform the following steps:

1. Click **Recovery** from the Navigation Panel, and then click the Microsoft Teams backup task from which you wish to recover the data.
2. Locate the most recent Team backup prior to the loss of your data. Click the arrow under the Action column to navigate to the **Restore** or **Download**

3. Locate the most recent Site, Calendar, Conversation, or Metadata (in that order) and select it. Go to the bottom of the page and click **Restore**.
4. Click the **Restore To** field and select the (Restored) channel.
5. For Sites, select the **Replace: Restore will overwrite existing live data** option.
6. Click **OK** to complete the restore.
7. Repeat these steps for the remaining sub-services.

4.6.3 How to Restore Deleted Groups

Groups are created by Microsoft when the Teams are created. When you restored the Channel, both the Team and the Group were created at the same time. Before you begin, verify that the Group was indeed created in Microsoft.

> **Note:** If you want to restore a Group, it can only be restored into a Group; Teams are restored into Teams.

Perform the following steps for each of these Group sub-services in this order:

1. Sites
2. Calendars
3. Conversations
4. Metadata – this will finalize the restore, by recovering the Members, Owners, and most importantly, the Group Name.

For each sub-service perform the following steps:

1. Click **Recovery** from the Navigation Panel, and then click the **Microsoft Groups** backup task from which you wish to recover the data.
2. Locate the most recent Group backup prior to the loss of your data. Click the arrow under the Action column to navigate to the **Restore** or **Download.**
3. Locate the most recent Site, Calendar, Conversation, or Metadata (in that order) and select it. Go to the bottom of the page and click **Restore**.
4. Click the **Restore To** field, a select the (Restored) channel.
5. For **Sites**, select the **Replace: Restore will overwrite existing live data** option.

6. Click **OK** to complete the restore.
7. Repeat these steps for remaining sub-services.

4.7 Tracking Recovery Tasks on the Jobs Page

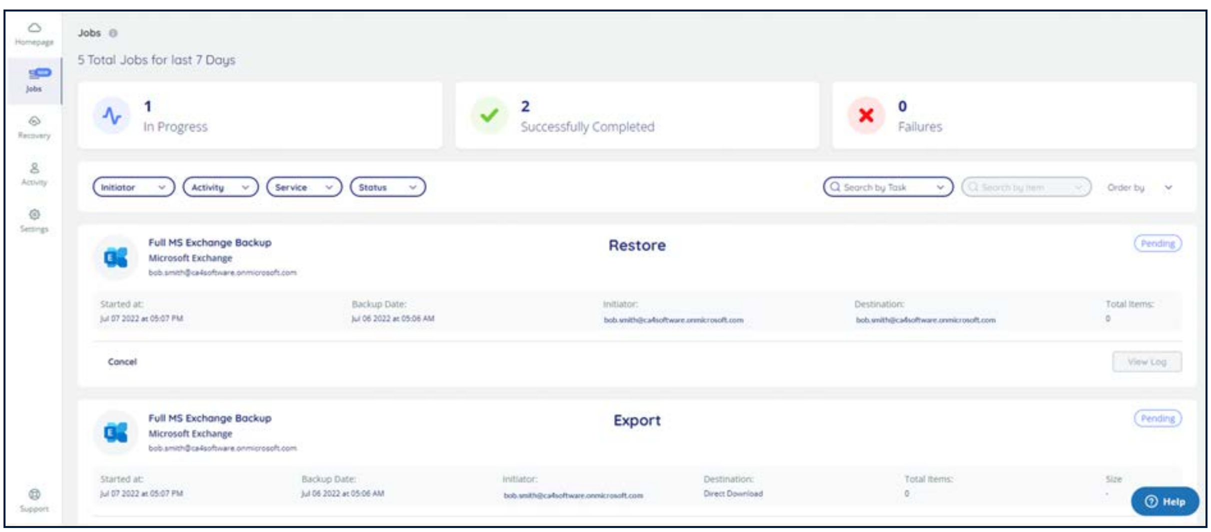
The *Jobs* page provides you with both high-level and drill-down views of your restore and export jobs over the last seven days.

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

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

4.7.1 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 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.

4.7.2 Filtering

The next section allows you to filter by numerous criteria:

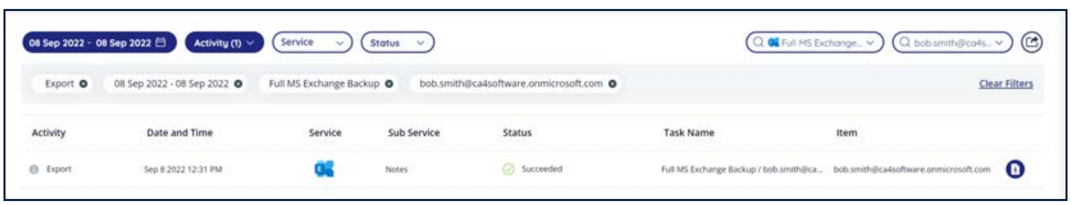
- **Initiator:** Who initiated the backup / restore?
- **Activity**: Filter by restores or exports.
- **Service**: Filter by one of the following services, such as:
  - Microsoft Exchange
  - Microsoft SharePoint
  - Microsoft Groups / Teams
  - Microsoft OneDrive
  - Google Workspace
  - Google Shared Drives
  - Salesforce
  - Box
  - Dropbox
  - Google Account
- **Status**: Filter by one of the following:
  - In progress
  - Succeeded
  - Failed
  - Pending
  - Canceled
- **Search by Task**: Filter by a task, such as:
  - Microsoft Exchange
  - Teams/Groups
  - OneDrive
  - SharePoint

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

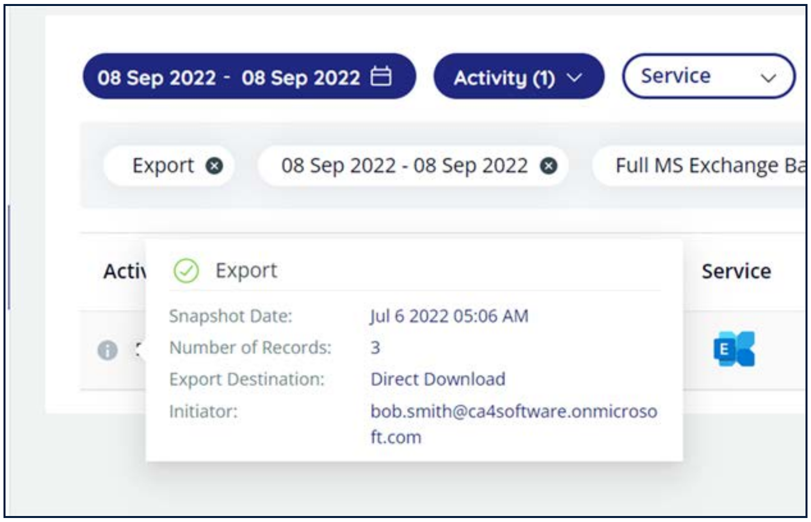
4.7.3 Description of Each Job

- 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 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:


08 Sep 2022 - 08 Sep 2022
Activity (1)
Service
Export
08 Sep 2022 - 08 Sep 2022
Full MS Exchange Ba
Export
Snapshot Date:
Jul 6 2022 05:06 AM
Number of Records:
3
Export Destination:
Direct Download
Initiator:
bob.smith@ca4software.onmicrosoft.com
Service

5 Compliance

5.1 Delete Backed Up Data: GDPR's "Right to Be Forgotten" Option

The way to delete data items - emails and files - from a CloudAlly backup is to enable the GDPR (General Data Protection Regulation) "right to be forgotten" option. CloudAlly supports deleting items from the following services:

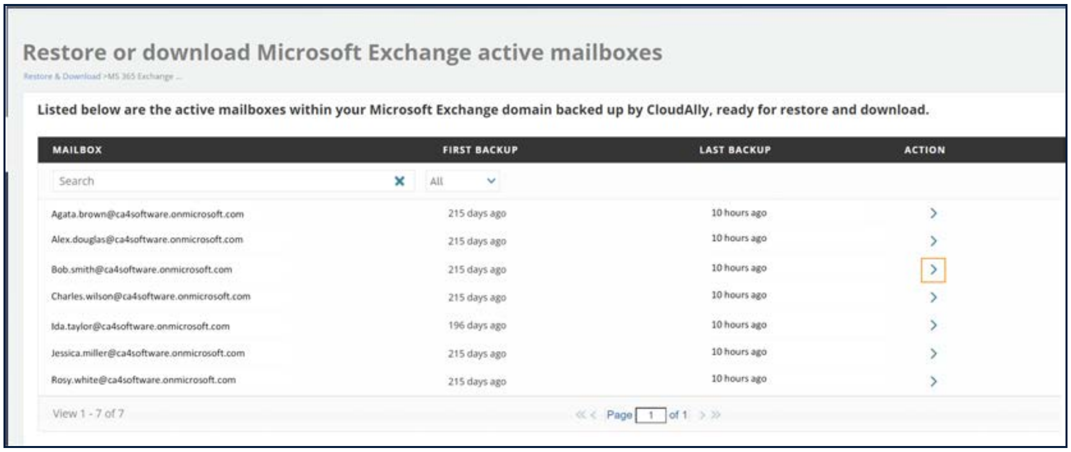
- Outlook: Mail, Contacts, Calendar, Tasks and Notes
- SharePoint
- OneDrive
- Teams & Groups: Conversations, Calendars, and Sites

To enable the ability to delete backed up items:

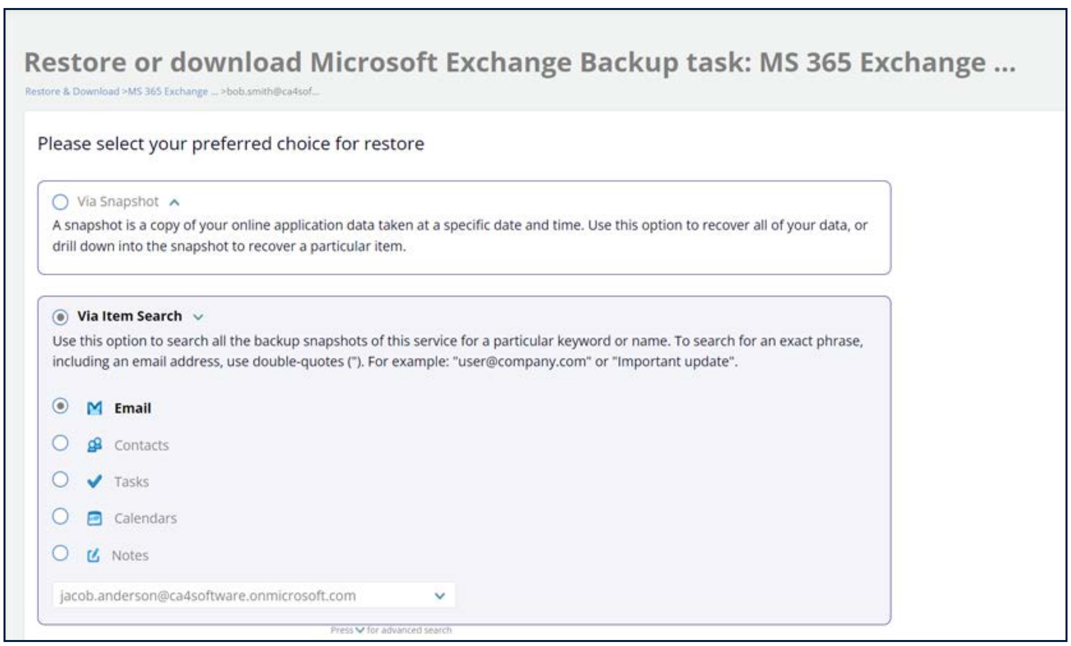
1. Request from Support that they enable the GDPR delete button for you. They will ask you for the name of your account, and the service for which you would like to enable this.
2. From the Homepage, click **Recovery**.
3. Click the service that contains the item you would like to delete.

Note: It is not possible to delete an entire folder, only one or more items.

4. Click the arrow at the end of the row of the account, team or site that contains the item you would like to delete.

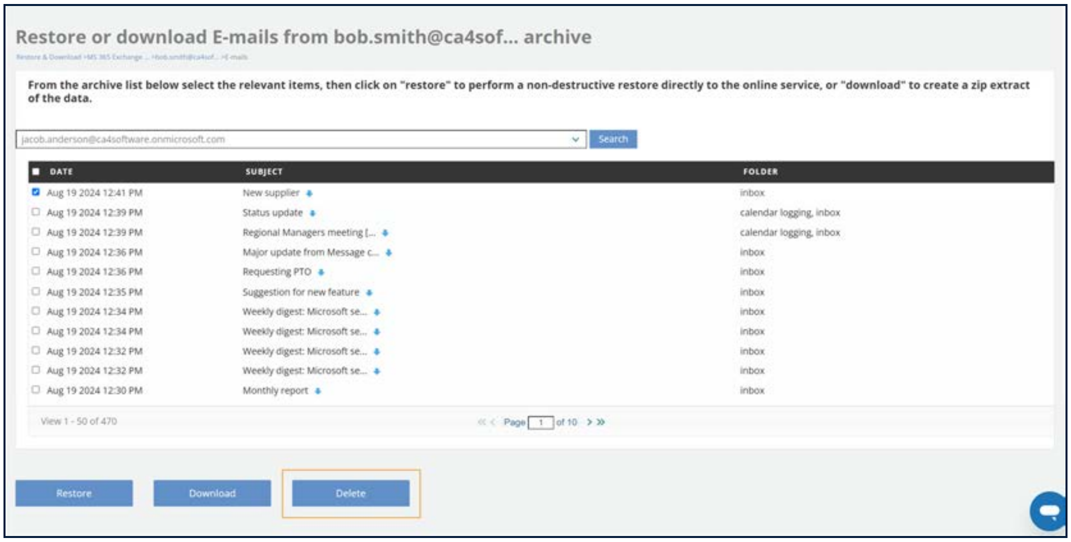


5. Click "Via Item Search" and enter the desired search criteria. For example, if you would like to delete all emails received from a specific person, type their email address. Or you can search by keyword.



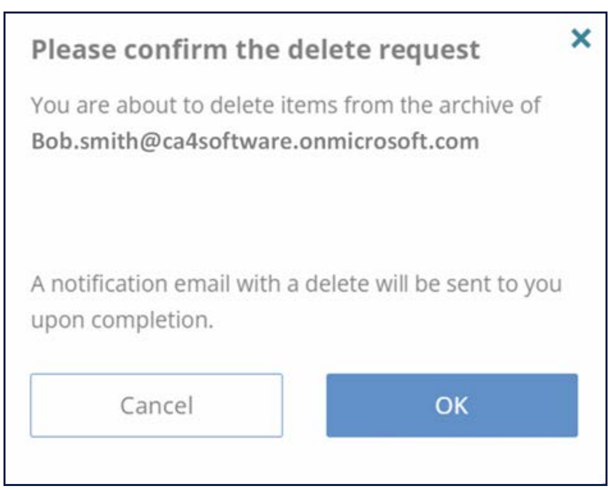
Note: It is not possible to perform a GDPR delete using "Via Snapshot."

6. Select the item(s) you would like to delete, and click **Delete**.



> **Note:** Ensure that the item you wish to remove is already removed from the source. If it is not, CloudAlly will continue backing it up, even if you deleted it using the "Delete" button.

7. The system will ask you to confirm the delete request. Once you have confirmed, the item will be removed from our system within a few days.

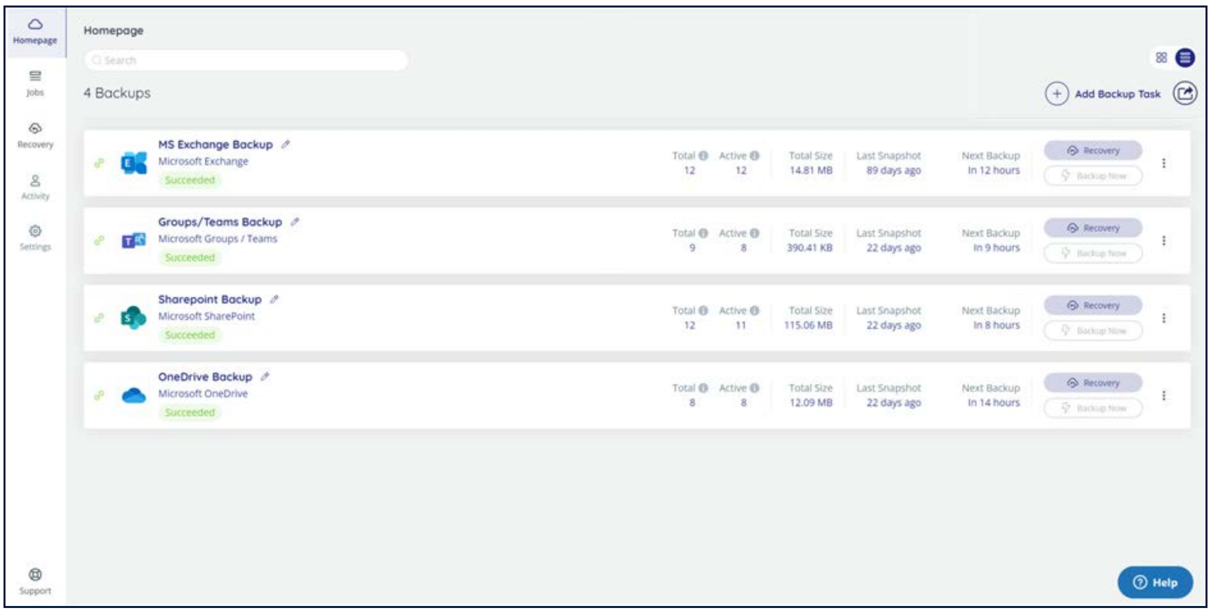


6 Filtering and Viewing Drill-Down Details

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

6.1 Filtering by Account, Team or Site

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



2. Click the desired service from the list or enter a keyword in the Search field to find a specific task. The specific service's backup page is displayed.

This page displays all the accounts, teams, or sites available for the account you are using. The page displays the details such as:

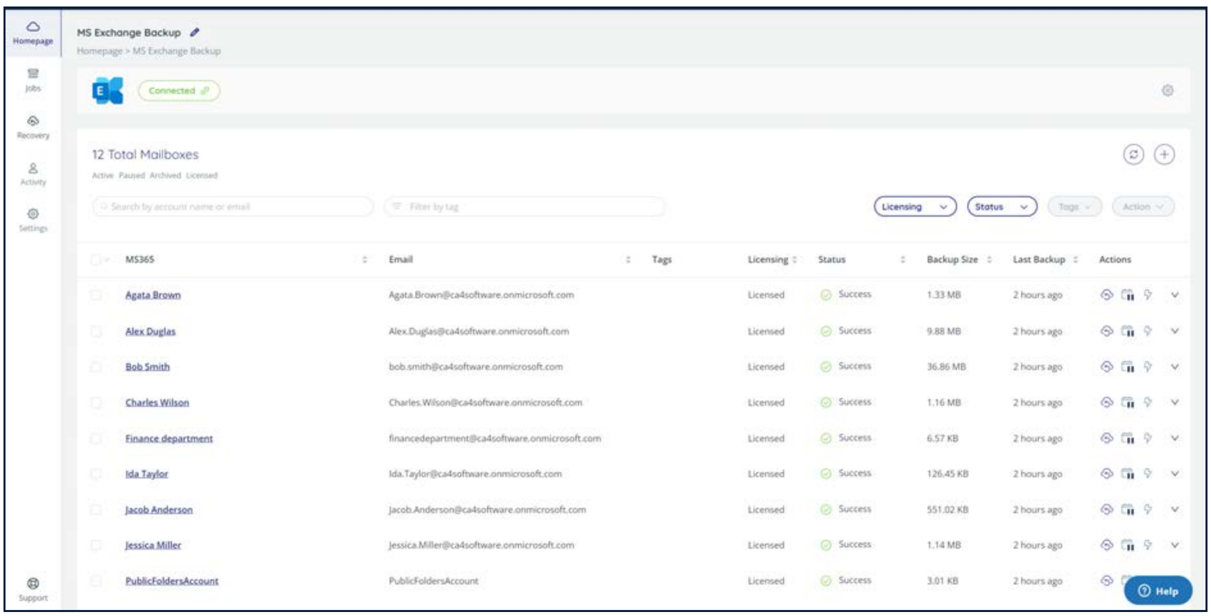
- **Microsoft Exchange:** Mailbox name, Email, Microsoft Licensed / Unlicensed, Status, Backup Size, and Last Backup date
- **Microsoft Teams & Groups**: Group/Team Name, Type (Group or Team), Tags, Status, Backup Size, and Last Backup date
- **Microsoft SharePoint and OneDrive**: Site name, Tags, Status, Backup Size, and Last Backup date

It also provides the means to filter and control the associated backup tasks.

6.1.1 Filtering Using Names, Statuses, or Licensing

You can filter accounts using the following options:

- Enter a search phrase in the *Search by* field to view all the accounts, teams or sites with the entered keyword.
- For Microsoft Exchange only: Filter by whether the mailboxes are Microsoft Licensed or Unlicensed.
- Filter by statuses such as Not Active, Scheduled, Success, In Process, Failed, Paused, Archived, or Partial.



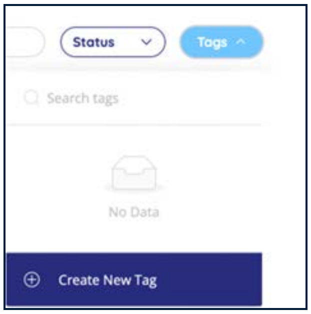
6.1.2 Filtering Using Tags

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 mailboxes, accounts, or sites that belong to Managers, or all those that belong to the Sales Team.

You can use tags to quickly filter your list of mailboxes, accounts or sites.

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

1. Select at least one account, team or site.
2. Click **Tags**, and the following screen appears.



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

6.1.3 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.

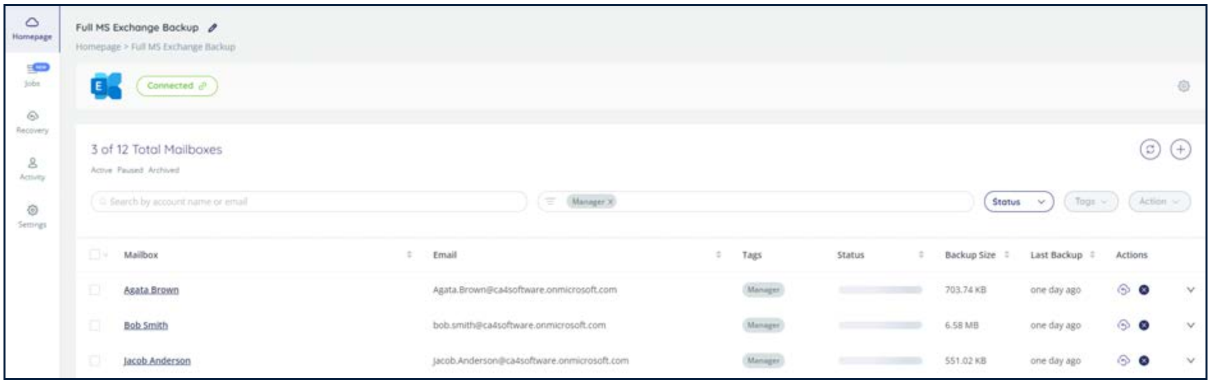
2. Enter a new tag name and click **Create.**

To apply tags to your accounts, teams or sites:

1. Select at least one account, team or site.
2. Click **Tag**.
3. Choose the desired tag for your account, team or sites.
4. Click **Apply**.

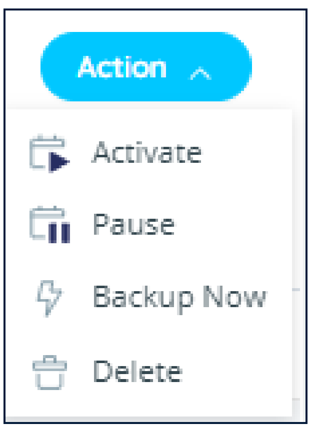
6.1.4 Filtering by Tag

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



6.1.5 Actions

To perform actions on an account, team or site, 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:

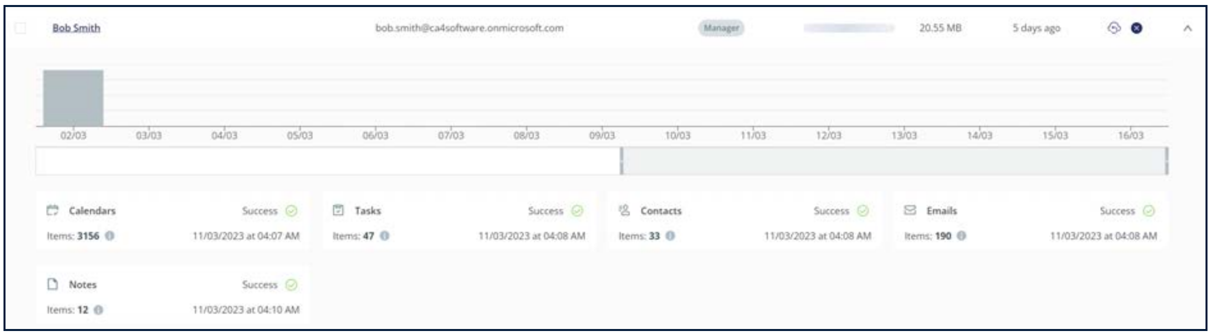


- **Activate** enables backup in all the selected account, team or sites.
- **Pause** halts the backup procedures on the selected account, team or sites.
- **Backup now** starts the backup immediately. The backup in this case starts as soon as a backup processing machine is available, which may take several minutes.

- **Delete** removes the backup task and backup data for the selected account, team or sites.

6.2 Viewing Backup Statistics with the Drill-down Feature

Select an account, team or site, and click the arrow button 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.

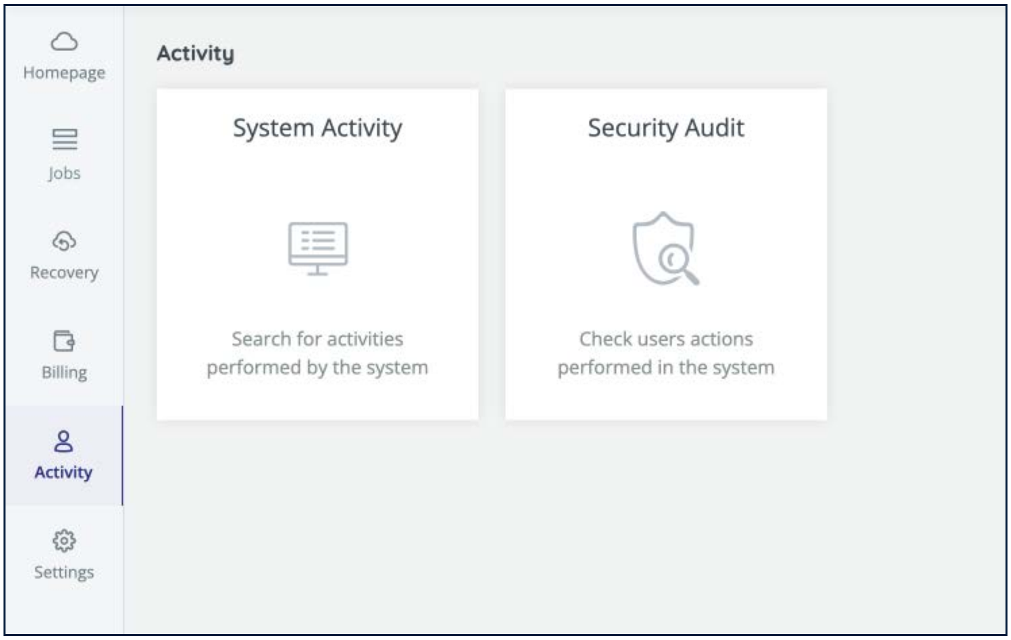
The summary tiles below the chart provide at-a-glance information about the backup: for each sub-service, they display the total number of items in the backup, the date of the last backup, and the outcome.

7 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.

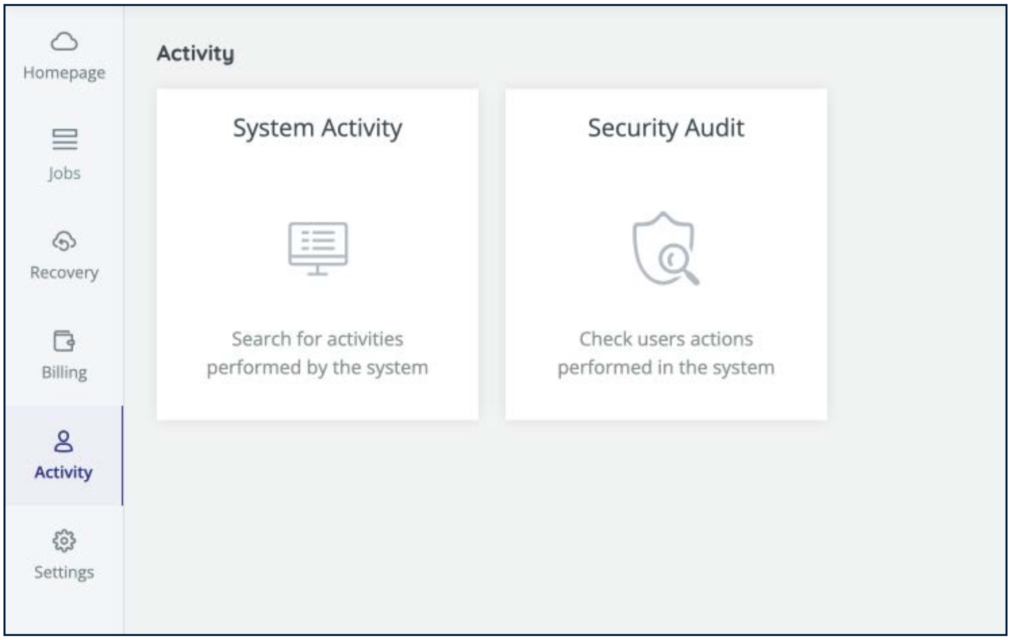
7.1 Viewing Account Activity

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

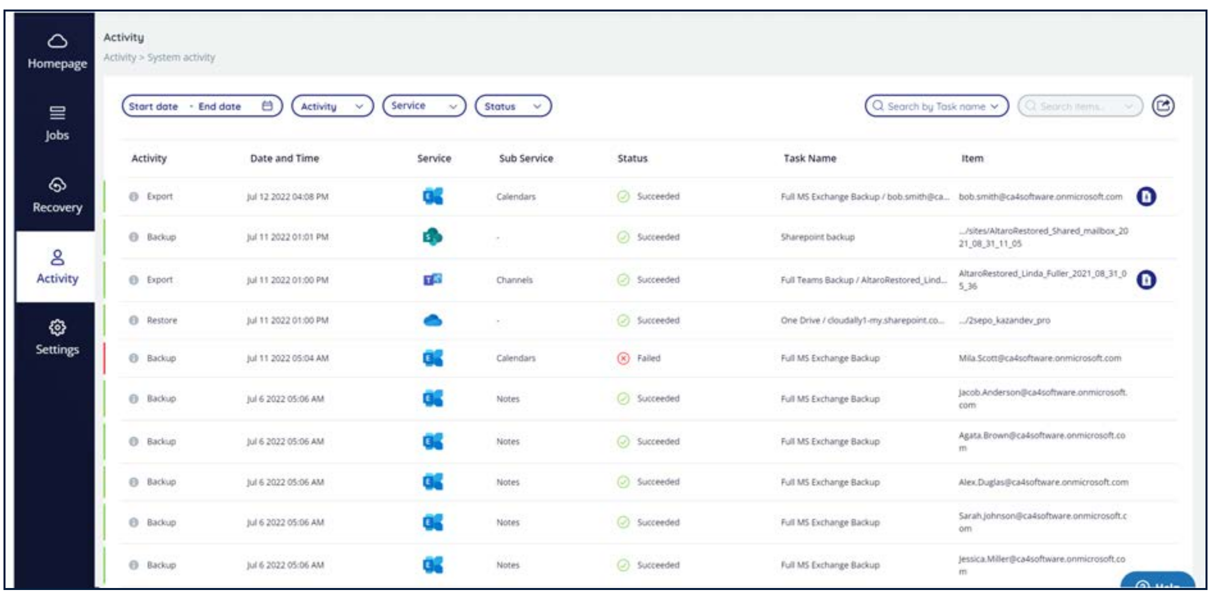


7.1.1 System Activity

Click **System Activity**.

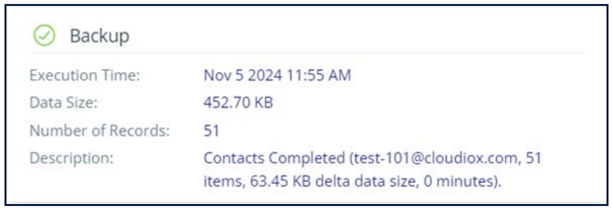


The *System Activity* page displays your account activity, with details such as Activity, Date and Time, Service, Sub-Service, Status, Task Name, and Item.

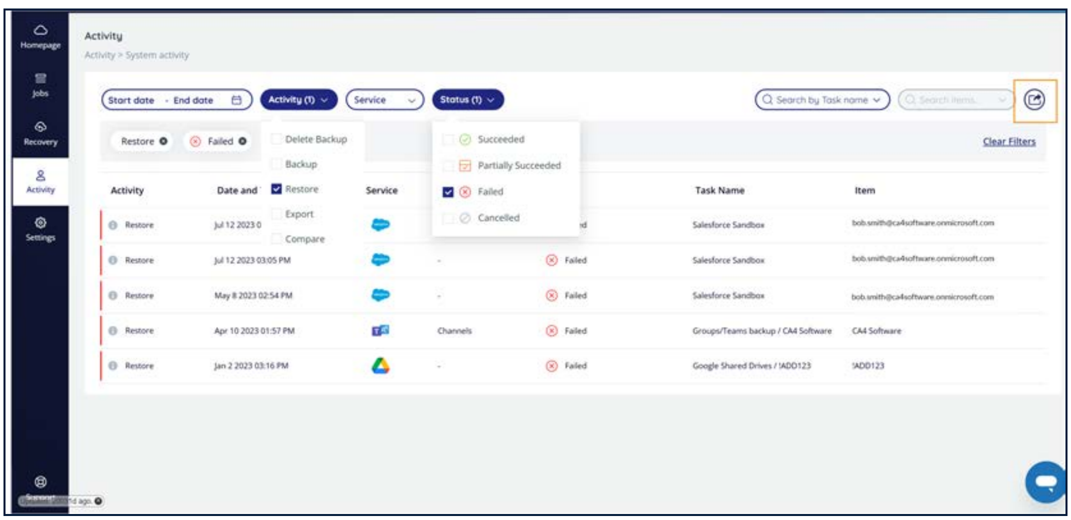


This page enables you to:

- 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.



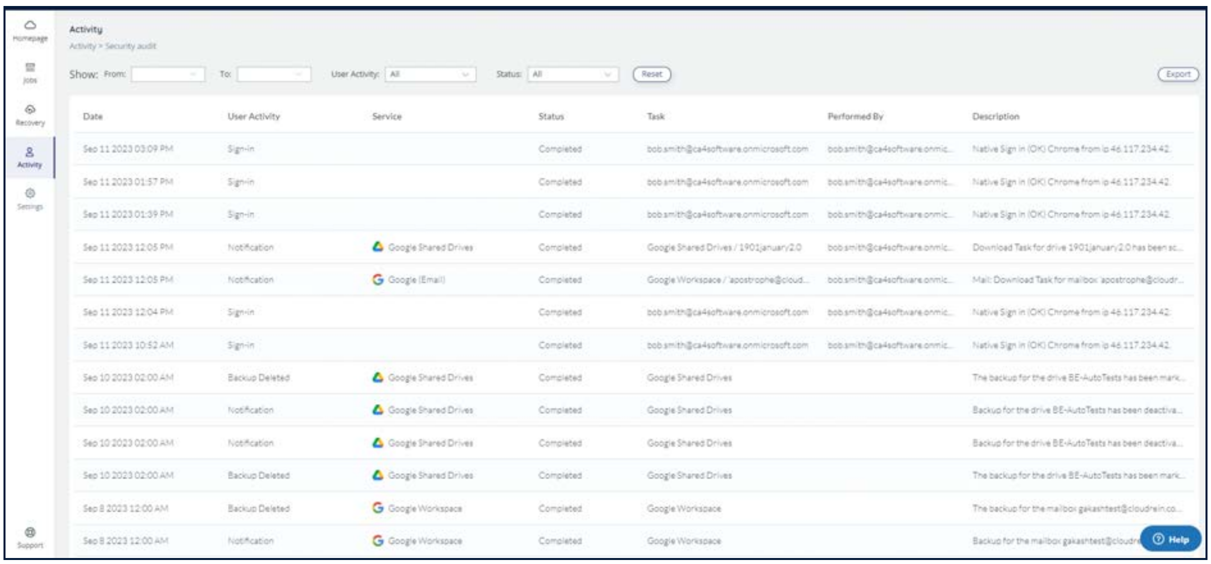
> **Note:** Administrators can grant users permission to see the *System Activity* page by clicking **Settings > User Management**, and checking "View Account Activity."

7.1.2 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**.

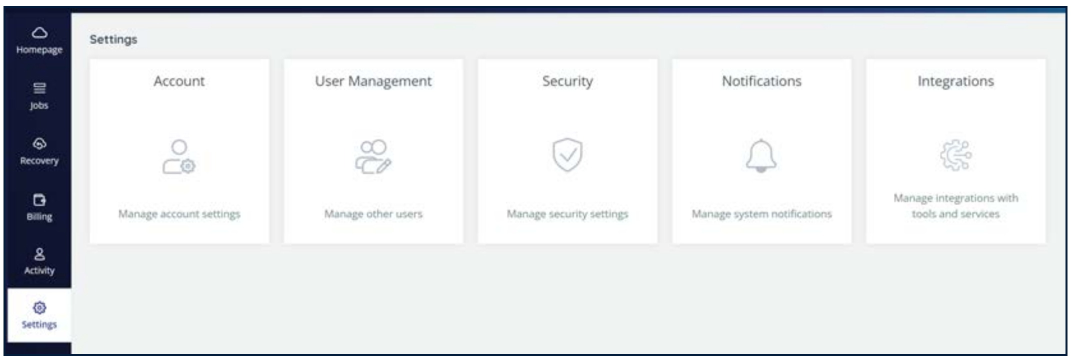
> **Note:** Administrators can grant users permission to see the *Security Audit* page by clicking **Settings > User Management**, and checking "View Security Audit Page."

7.2 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.

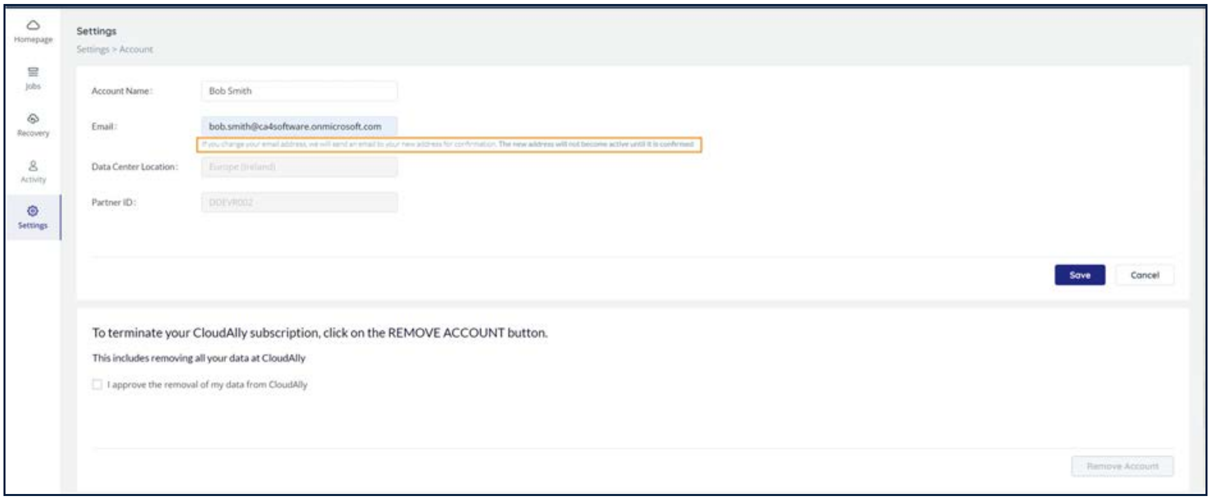


7.2.1 Account Settings

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 Support. Finally, this page also allows you to terminate your account.

To update or change your account details:

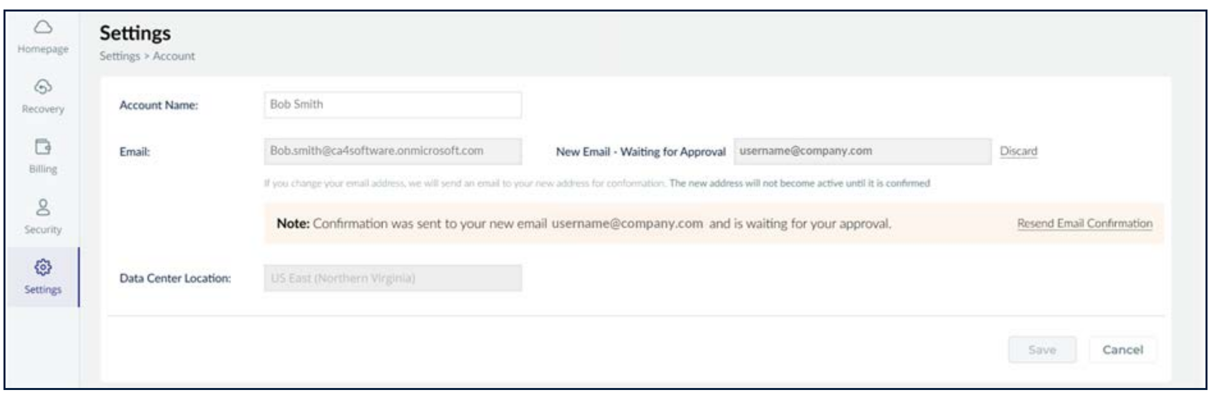
1. From the Navigation Panel, click **Settings** and then click **Account** . The *Settings > Account* page is displayed.



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.

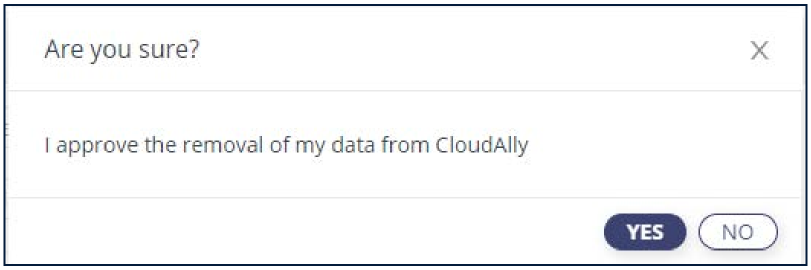
Click **SAVE**. The following screen will appear. If you did not receive the confirmation email, click **Resend Email Confirmation**



7.2.2 Canceling Your Subscription

To cancel your subscription:

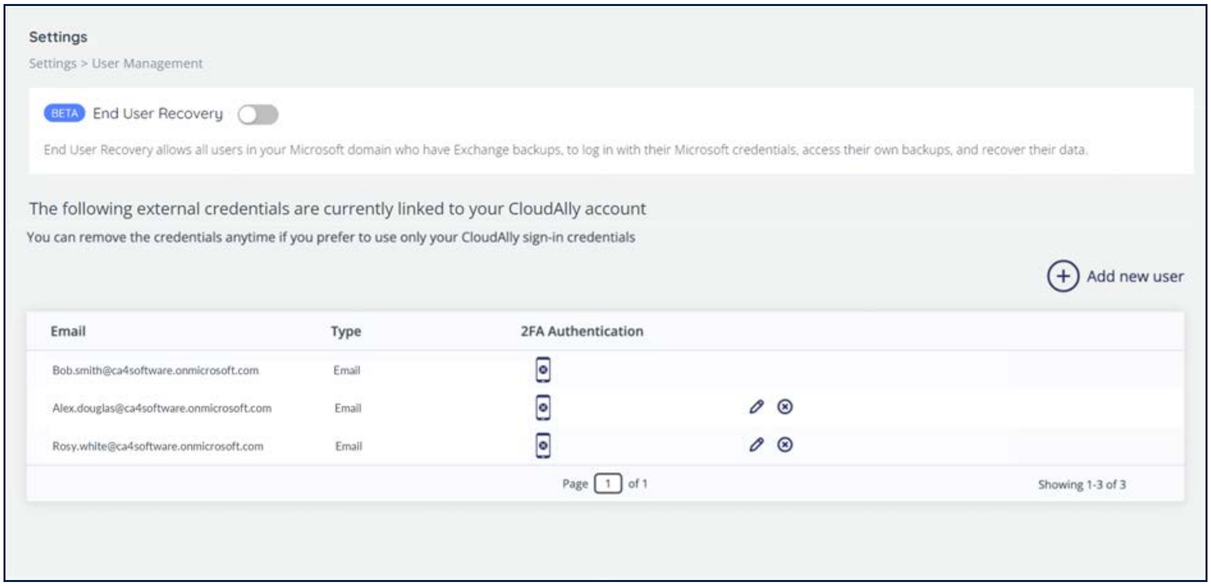
1. Check the box for "I approve the removal of my data from CloudAlly" field and click **REMOVE ACCOUNT**.
2. The *Are you sure?* pop-up window is displayed with a confirmation request.
3. Click **YES** to confirm the cancellation.



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.

7.3 User Management

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

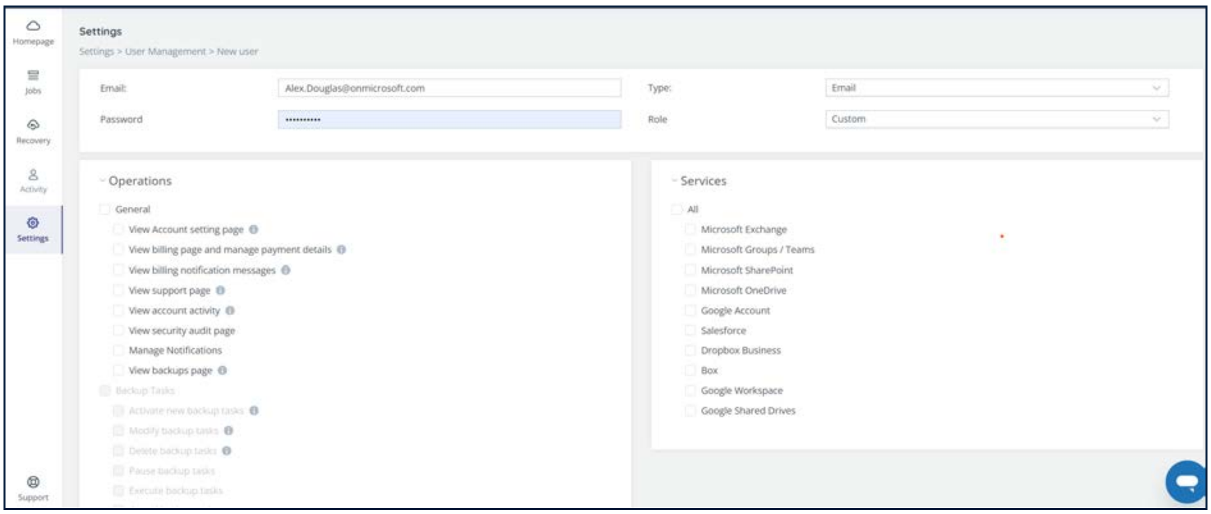


7.3.1 Adding a New User

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.

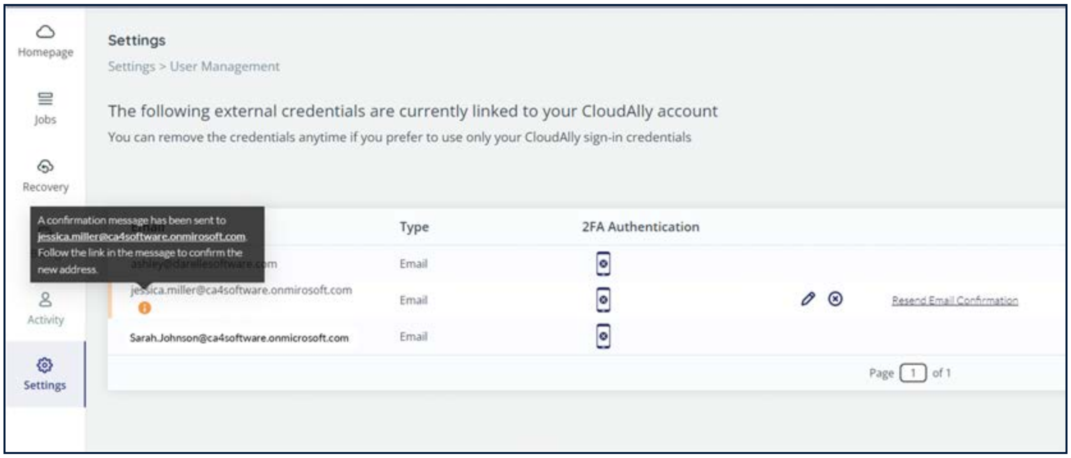
- Enter the new user's email address.
- Select the Authentication Type: Azure, Email, Google+, or Okta.
- Select the permissions role for the user. Selecting the role "Administrator" enables permissions to all services and operations. Or, you can selectively choose which permissions to grant from the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



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

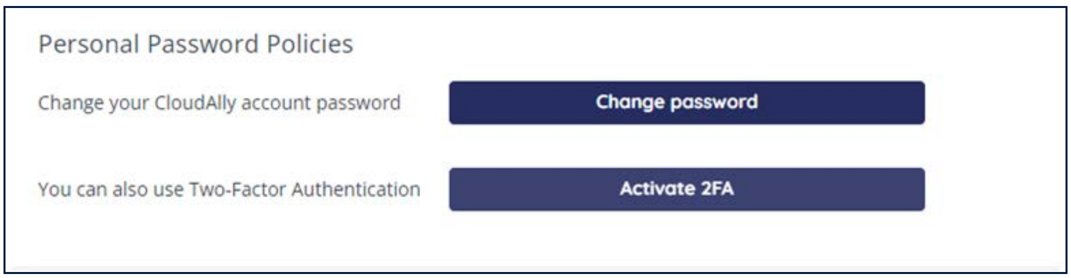
You will be returned to the Settings page. To complete the process, the user must confirm their email address using the link sent via email. This is a security measure, which ensures that the user's email address is valid.

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**.



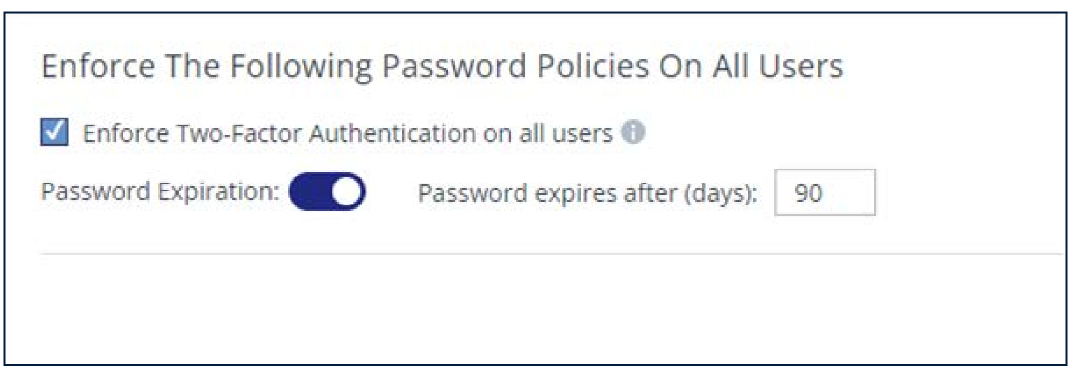
7.4 Security Settings

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.

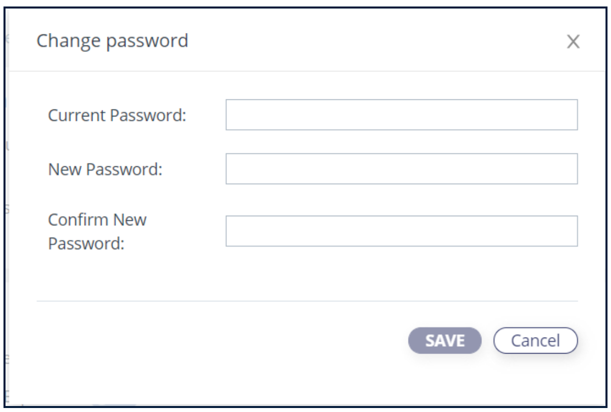


- With the **Enforce Two-Factor Authentication** option, you can make two-factor authentication mandatory for all the users in your account.
- By setting the **Password Expiration**, you can enable the password expiration option for all your users – you will be also be asked for the number of days before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

7.4.1 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.



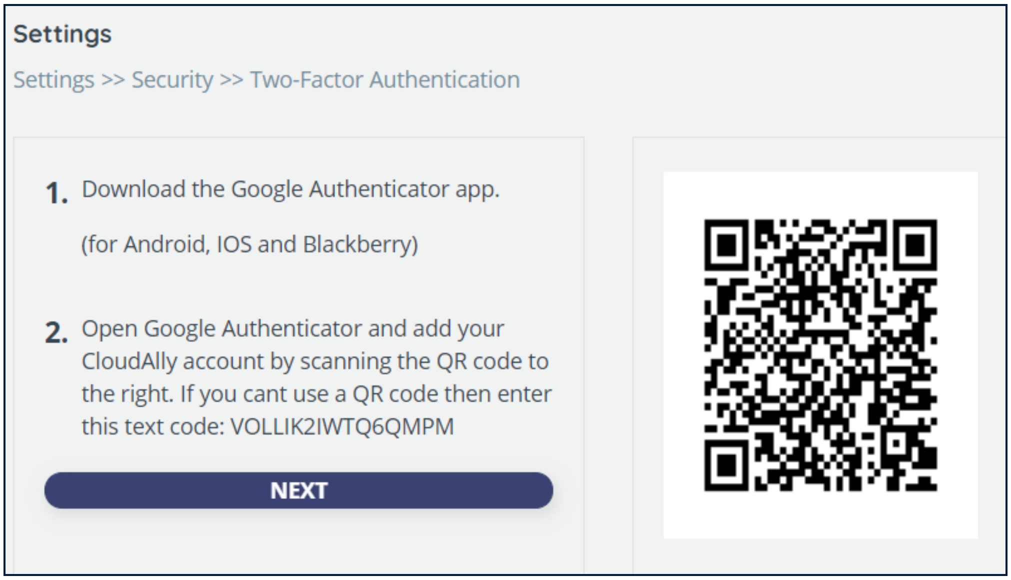
3. Enter the current password in the *Current Password* field.
4. Enter the new password in the *New Password* field.
5. Re-enter the new password in the *Confirm New Password* field.
6. Click **SAVE**. You can now use this password to access your account.

7.4.2 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.

7.4.3 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).

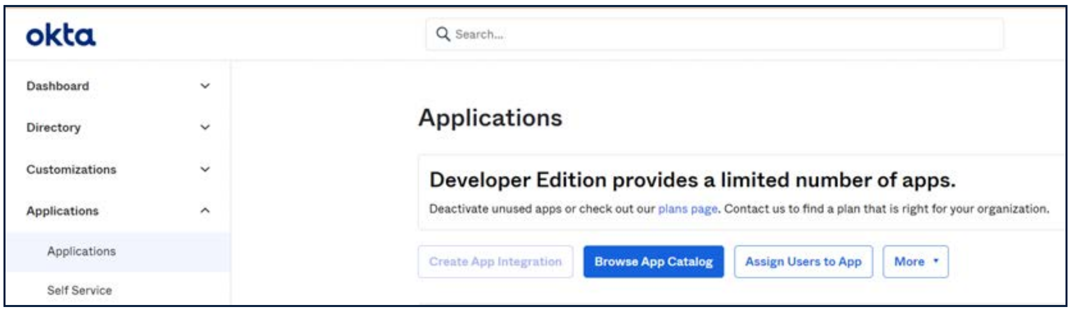
CloudAlly supports Okta as its SAML provider.

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

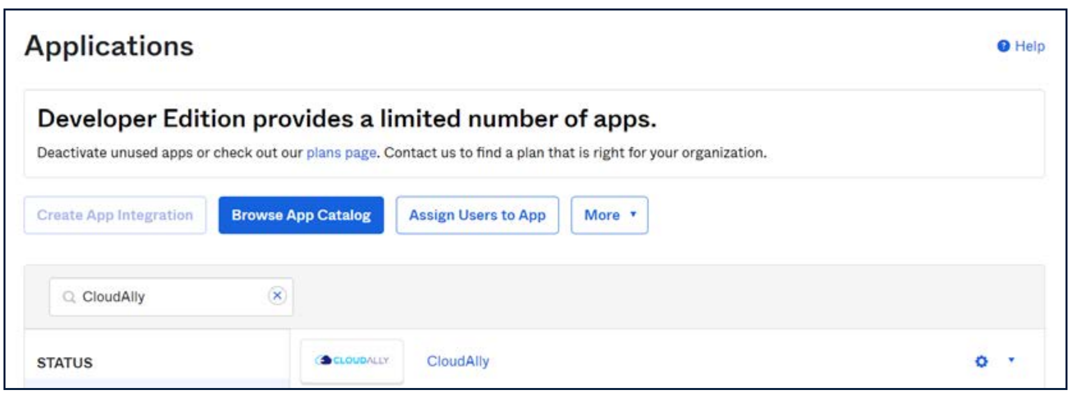
- Setting up CloudAlly in the Okta Application
- Setting up Okta in the CloudAlly application

7.4.3.1 Setting up CloudAlly in the Okta Application

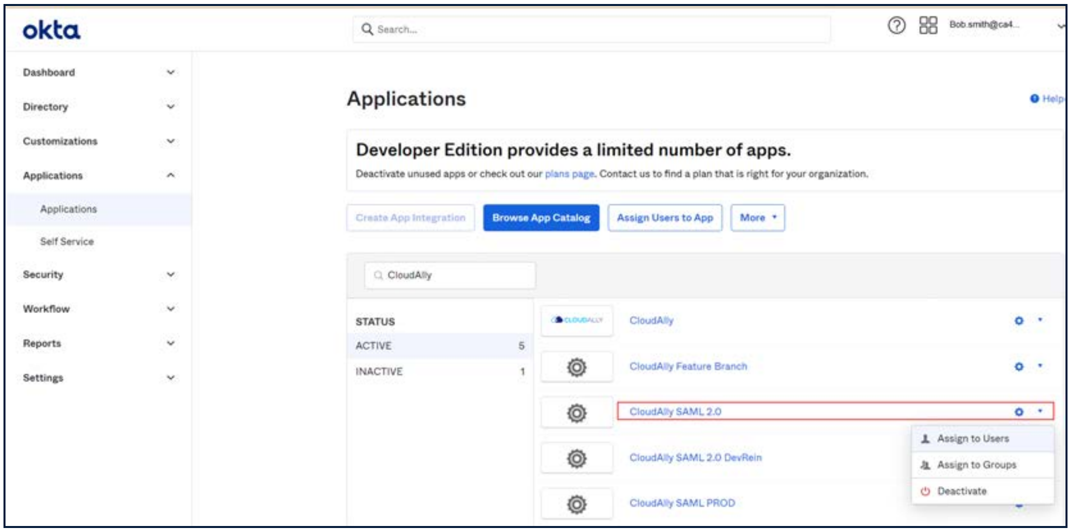
- In the Okta application, click **Applications** > **Applications** > **Browse App Catalog**.



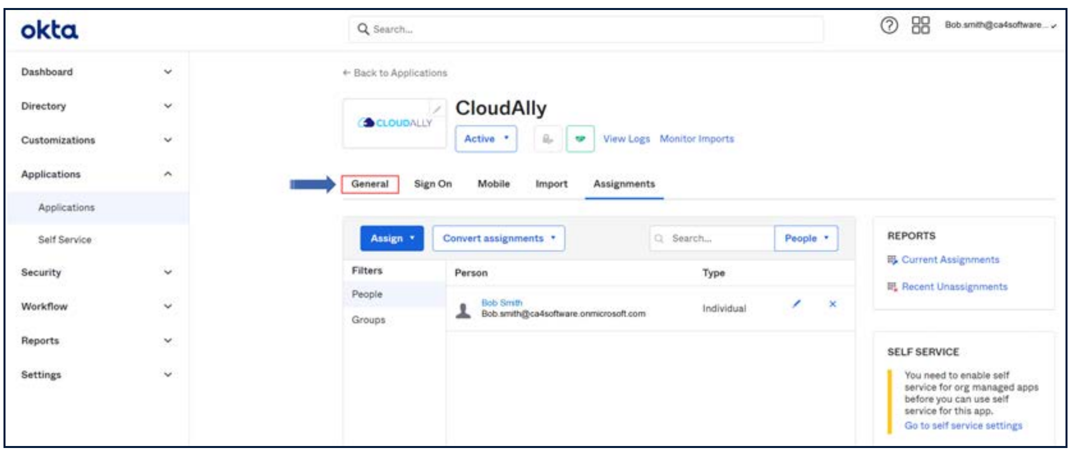
- In the search bar, enter CloudAlly.



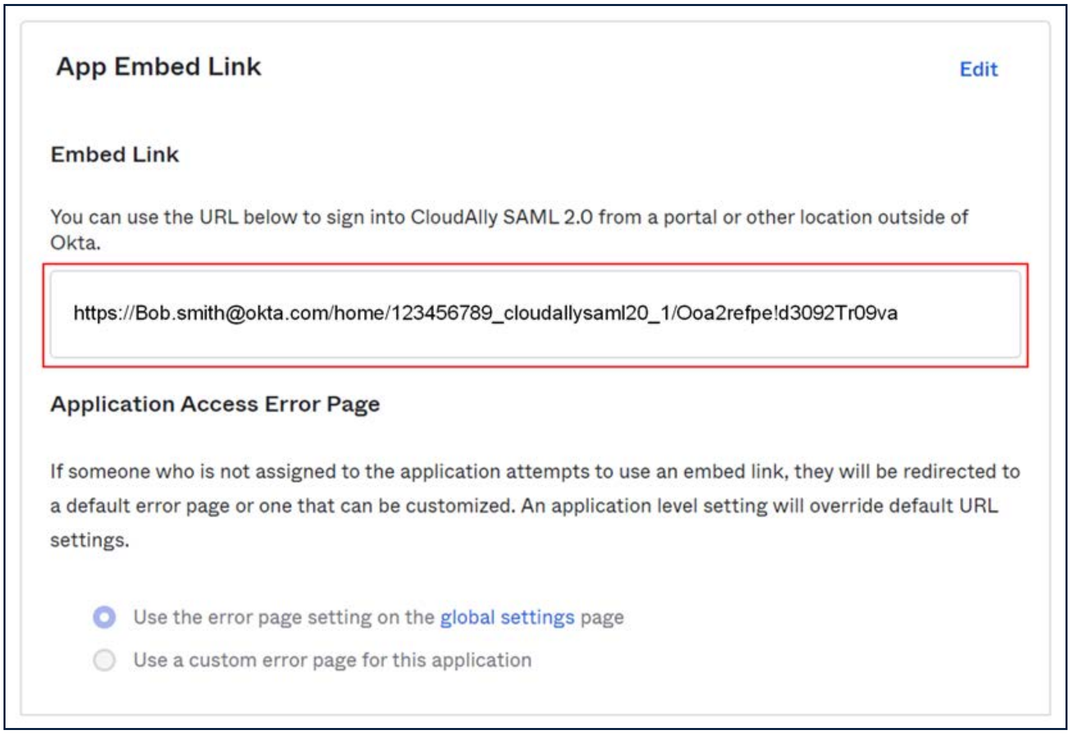
- Click the arrow next to CloudAlly SAML 2.0, and **Assign to Users** or **Assign to Groups**.



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

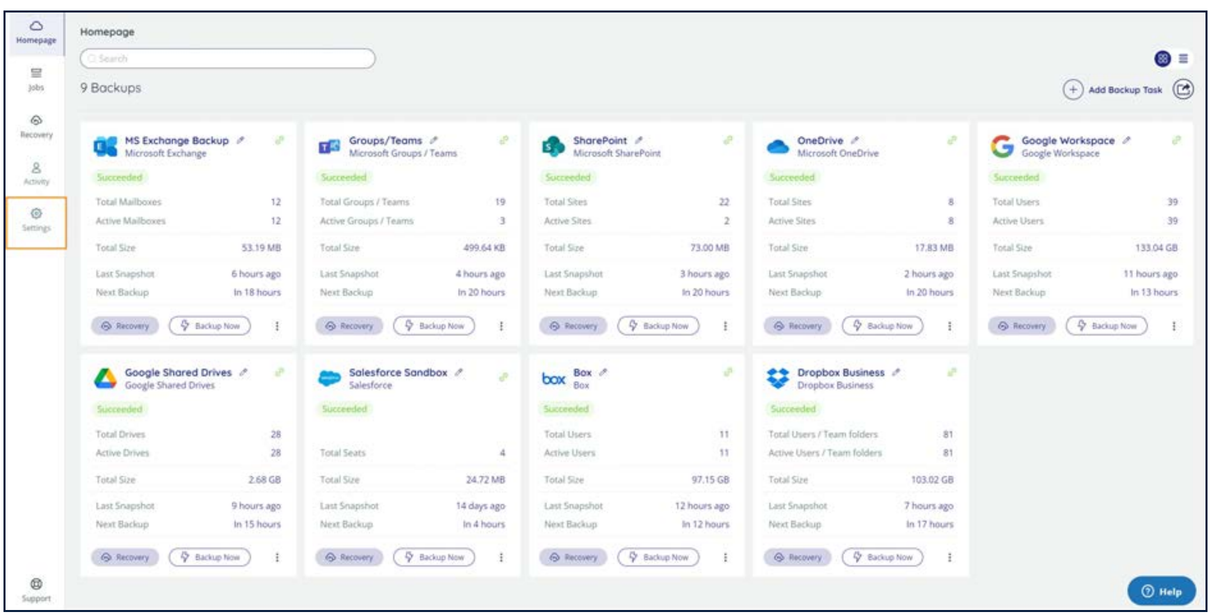


- Scroll down until you see the **App Embed Link** section. Copy the URL that is displayed - you will need this to set up Okta in the CloudAlly app.

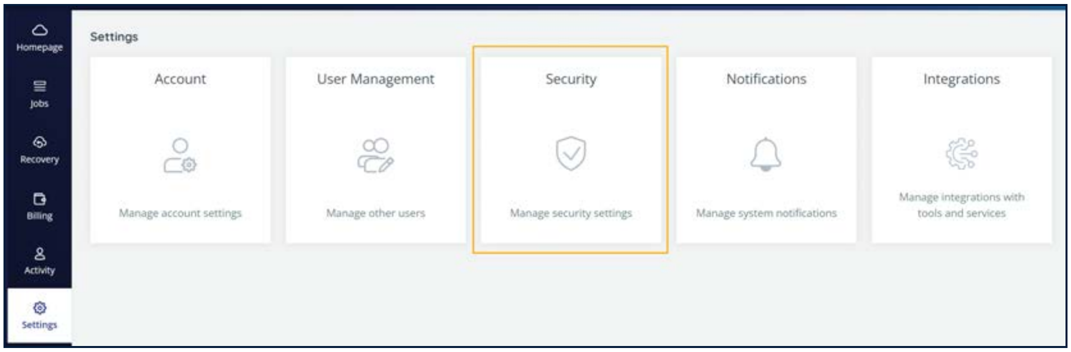


7.4.3.2 Setting Up Okta in the CloudAlly Application

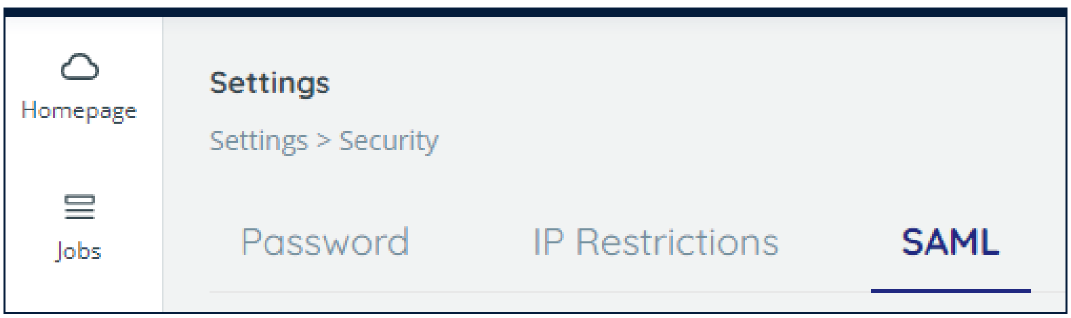
1. From the Homepage, click **Settings** in the Navigation panel.



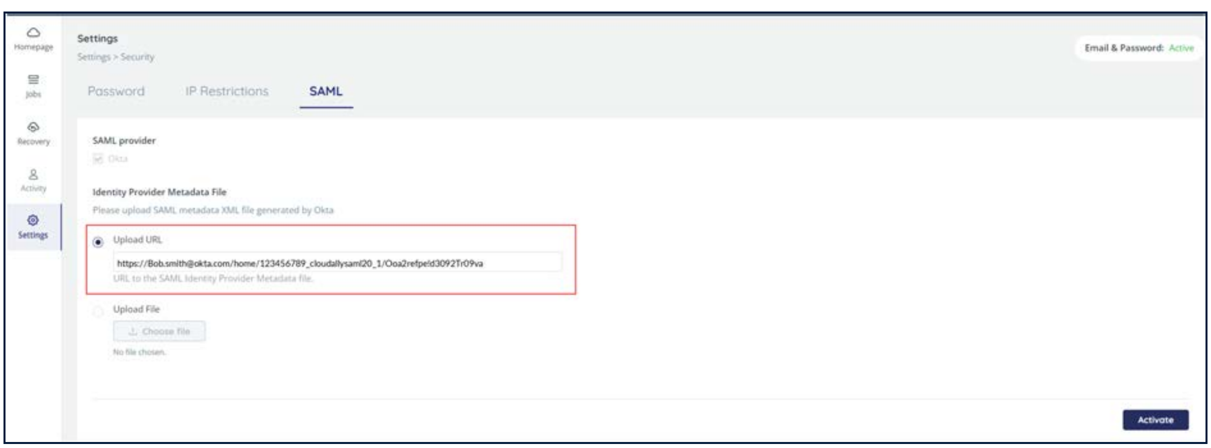
2. On the Settings page, click **Security**.



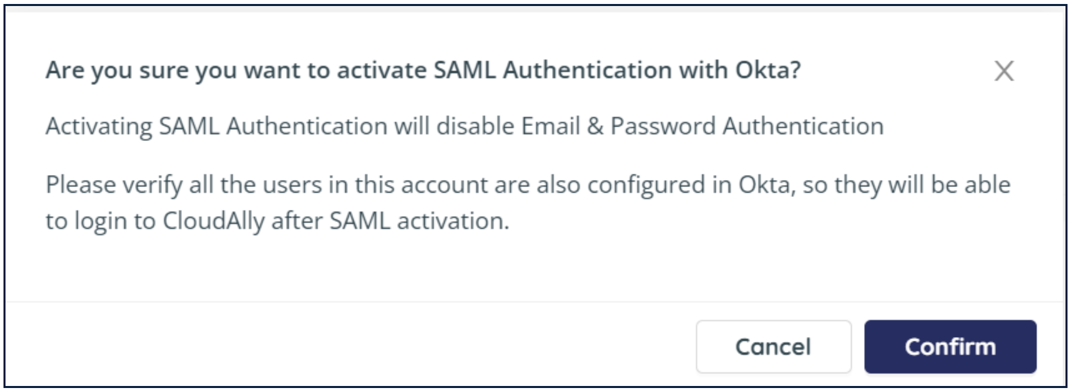
3. Click the **SAML** tab.



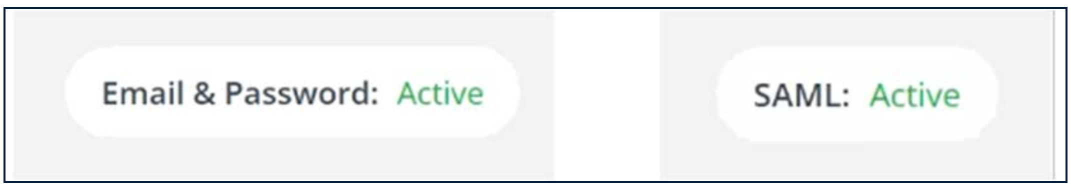
4. Paste the URL that you copied from the Okta site.



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.**



7.4.4 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.

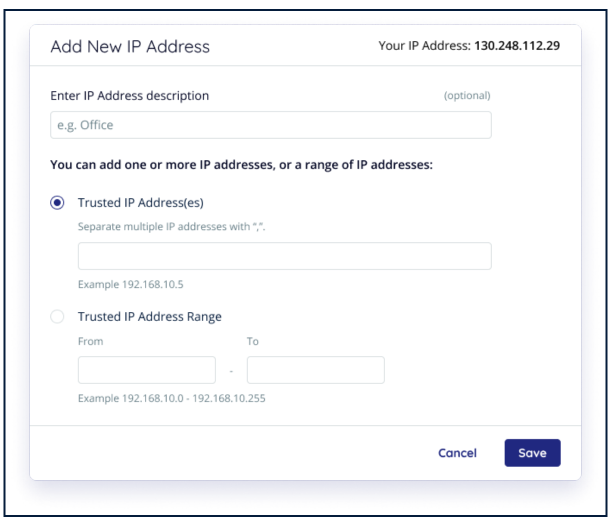
> **IMPORTANT!**

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

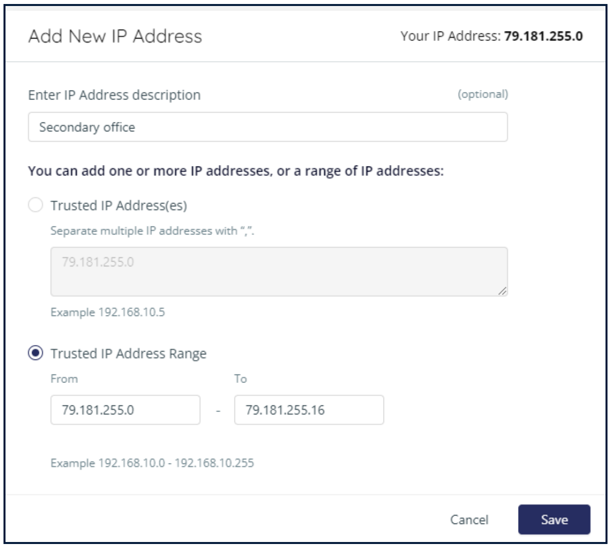
1. In the *Settings* panel, click **Security**, and then **IP Restrictions**.

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

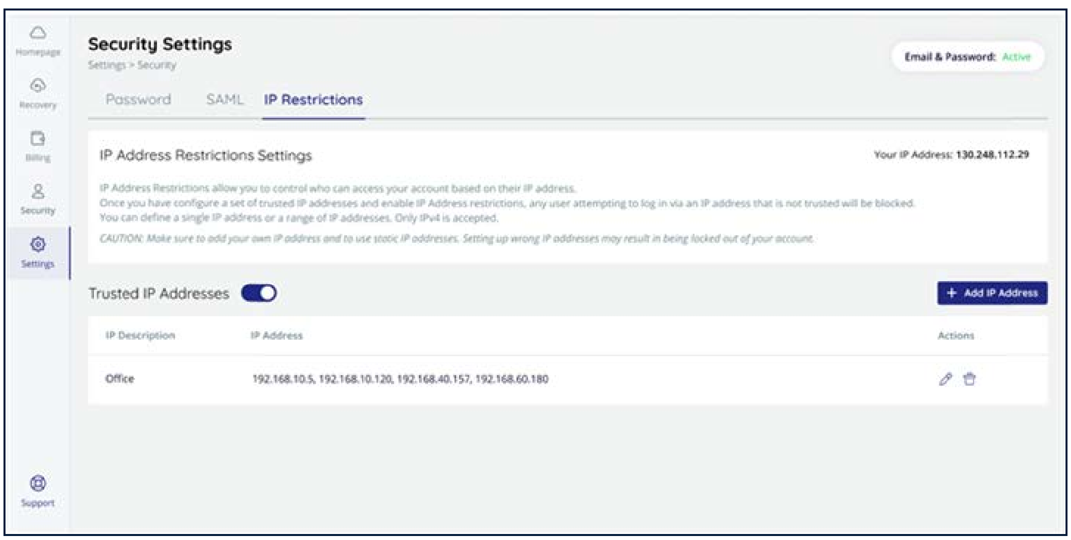
   a. Enter individual addresses separated by commas, and an optional description.



   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.



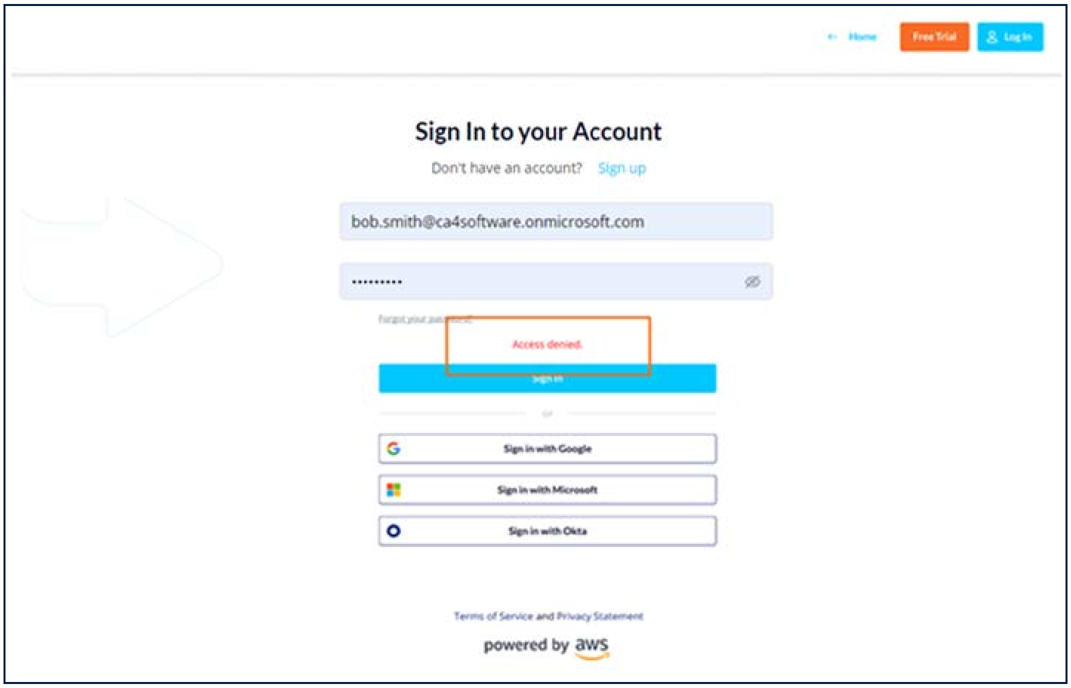
You can edit your list of addresses by clicking the pencil icon, or delete ones that you no longer want on your trusted list by clicking the trash icon.

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.

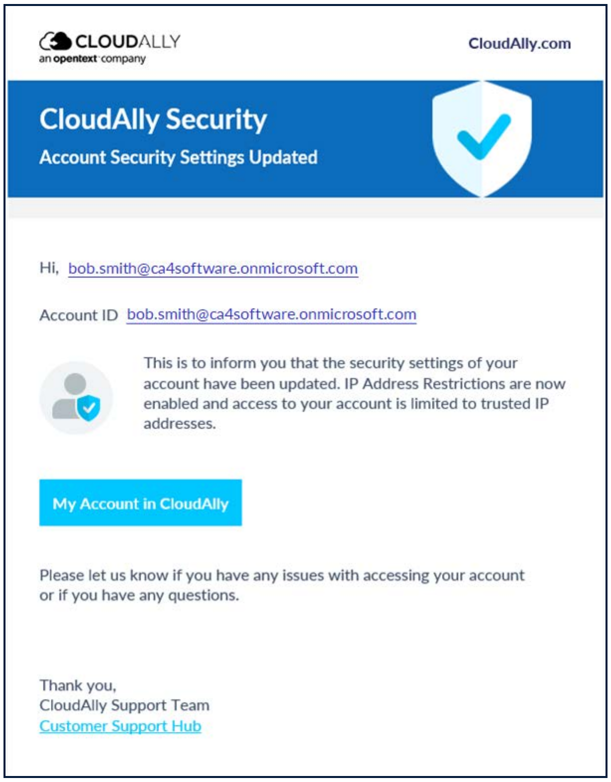
Blocking Access

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



7.4.5 Email Notifications

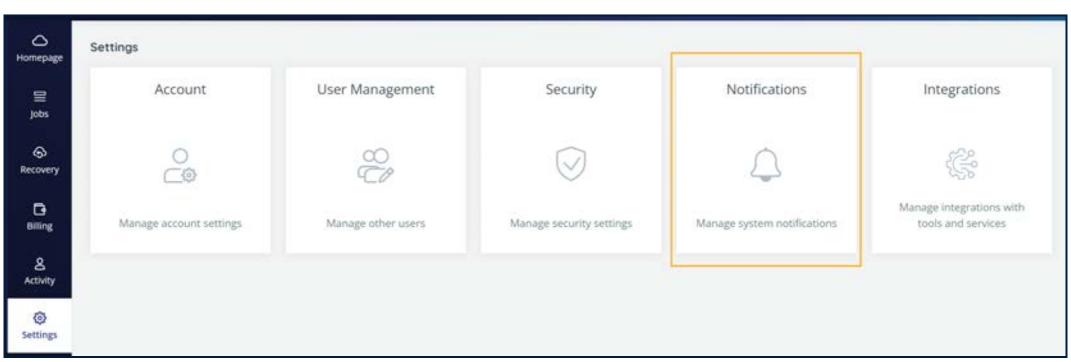
Whenever you enable or disable IP restrictions, or modify the addresses, CloudAlly will send you an email notification, letting you know what has changed.



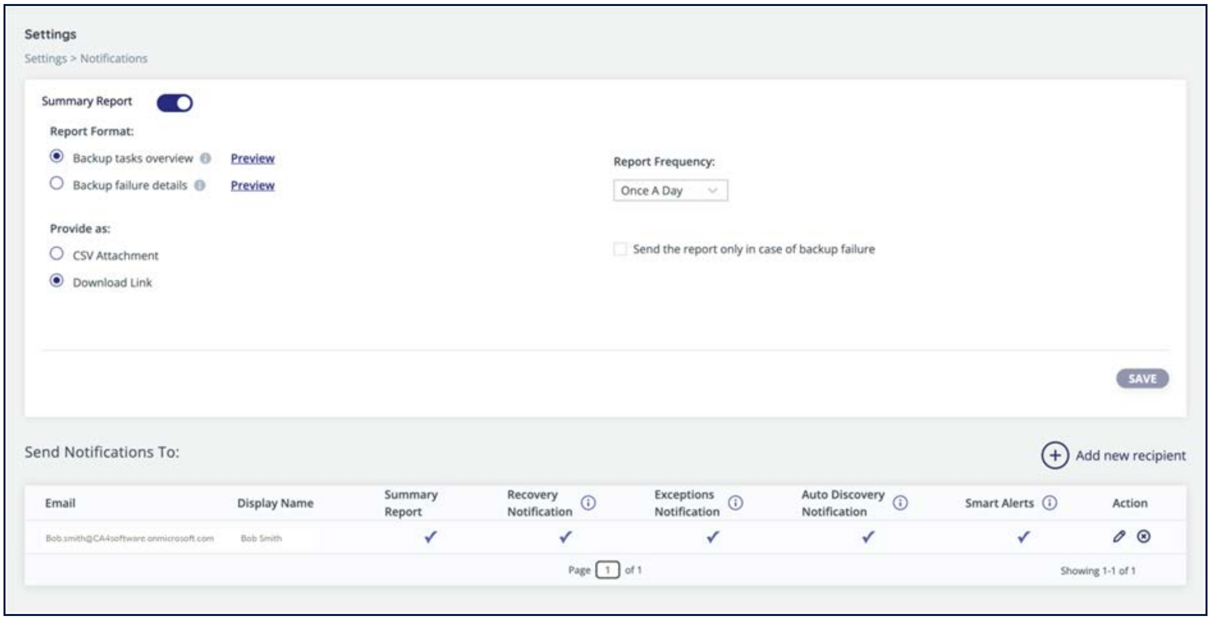
7.5 Notifications Settings

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:

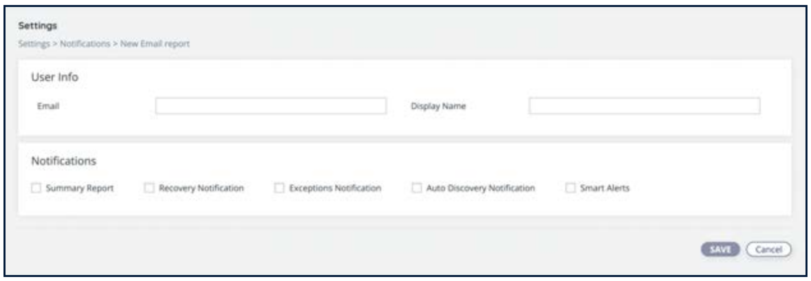
1. Click **+ Add new recipient**.
2. Enter the Email of the recipient and the Display name. The Display name is used in the report email to address the recipient.
3. Select the desired notification types:
    a. Summary Report
    b. Recovery Notification
    c. Exceptions Notification - This notification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

> **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.



7.6 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.

7.6.1 Splunk

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

Versions Supported:

7.6.2 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.

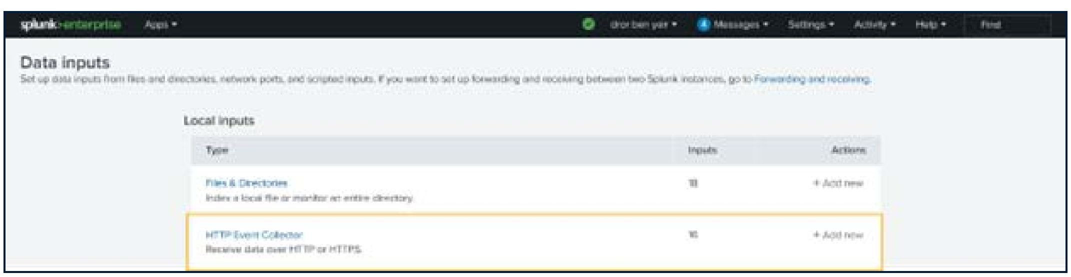
- Customers' activity events, such as backups and restores
- Customers' Security Audit logs (see " Security Audit" on page 108)

7.6.3 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**.

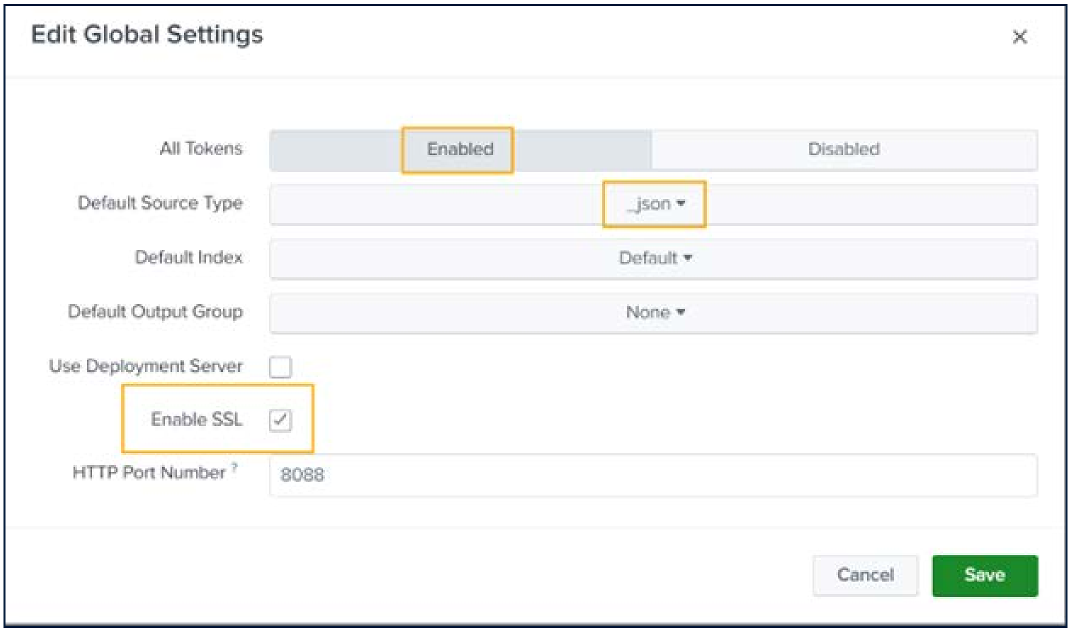


2. Under the Global Settings option:

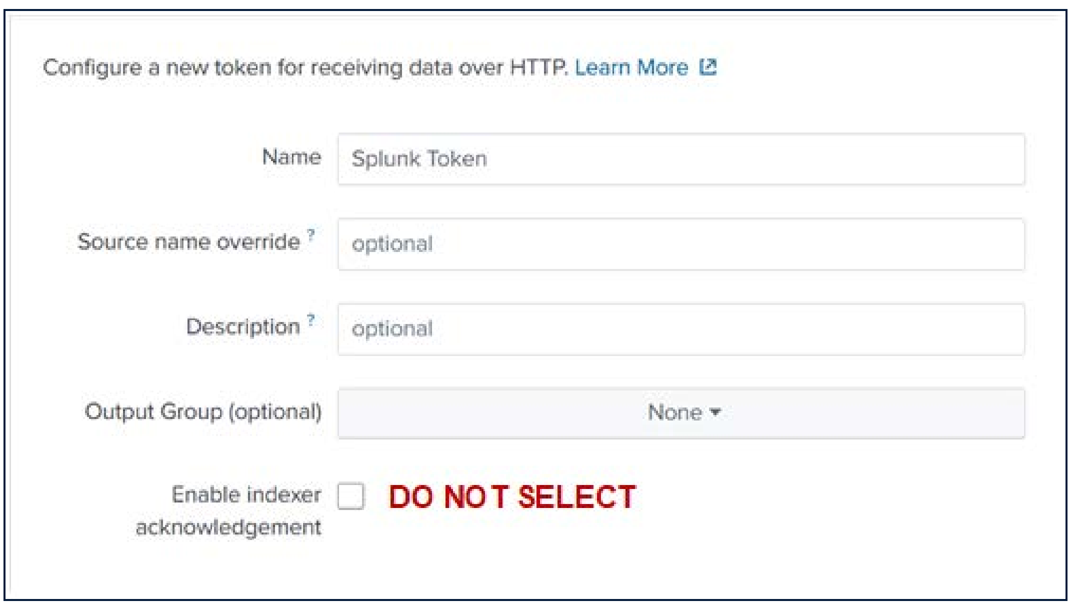
    a. Enable the HTTP Event Collector by setting All Tokens to **Enabled**.

    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".

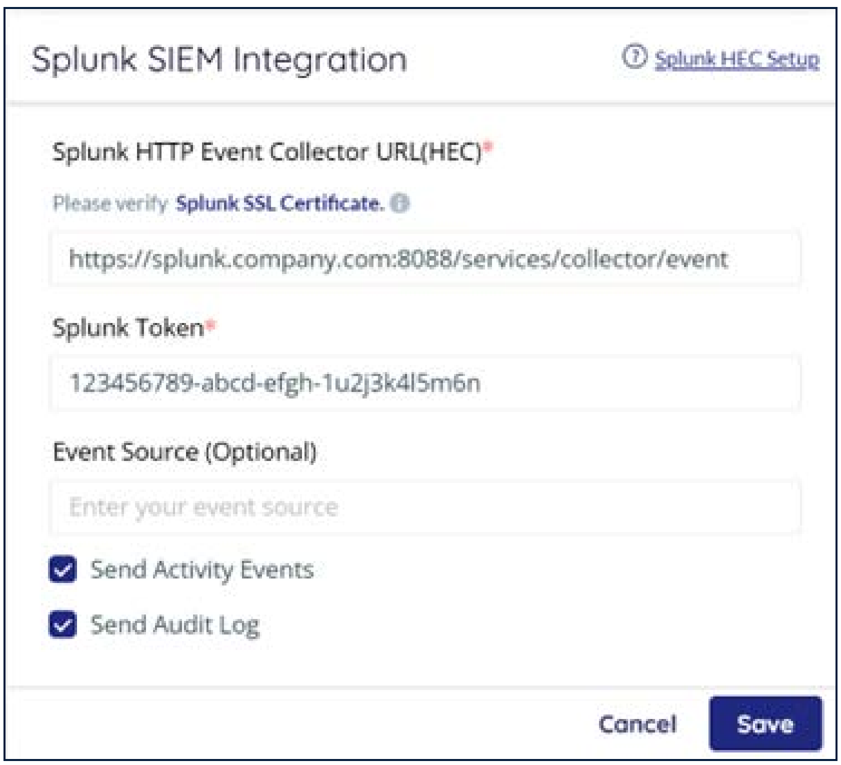
4. Find Your HEC URL.

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.

7.6.4 Setting Up Splunk in the Portal

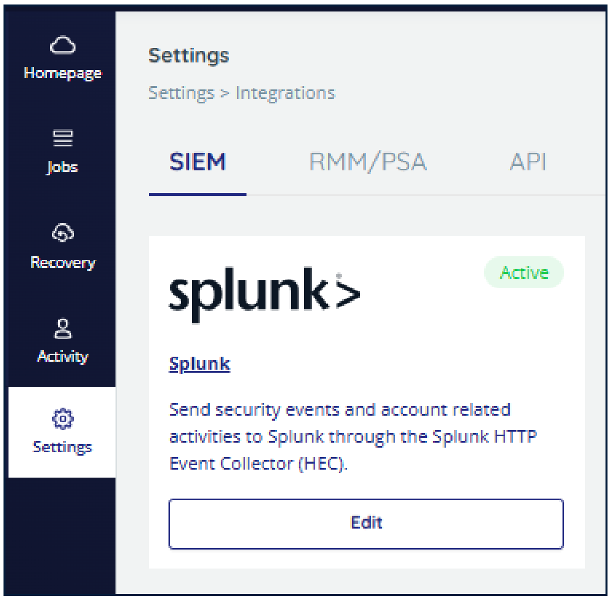
1. From the navigation pane, click **Settings > SIEM**.
2. Click **Splunk > Connect**. Complete the fields on the following screen:
    a. Enter the Splunk HTTP Event Collector URL.
    b. Paste the token value that you copied into the Splunk Token field.
    c. Optional: Add the Event Source, which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

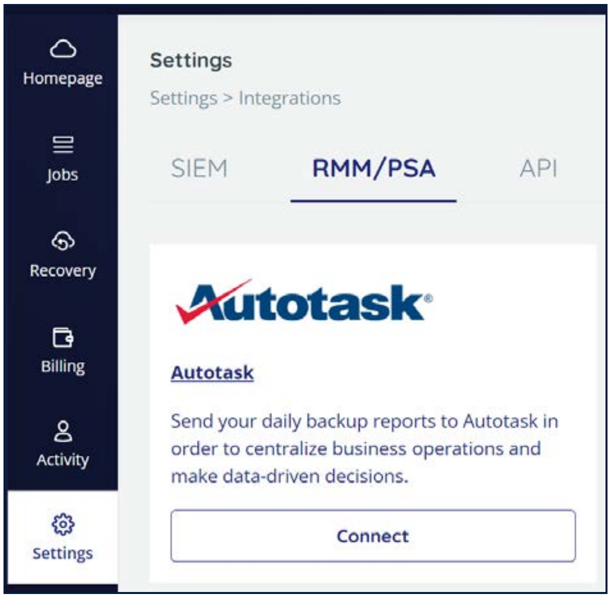
   a. Send customer activity events
   b. Send customer audit log

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



7.6.5 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 Password
- 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.

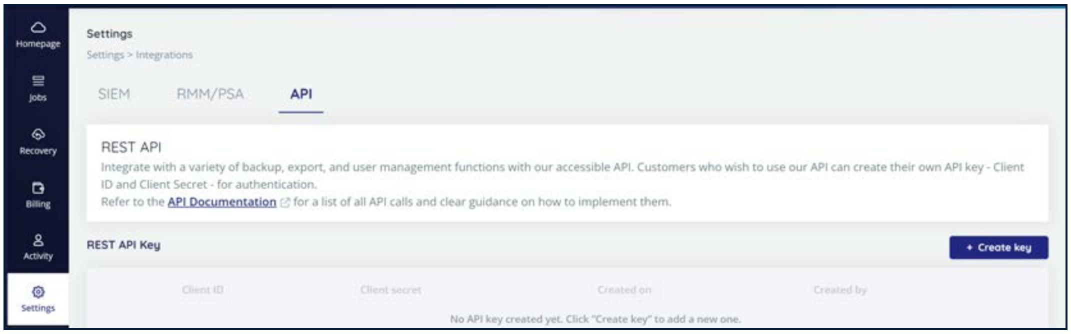
7.6.6 API

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

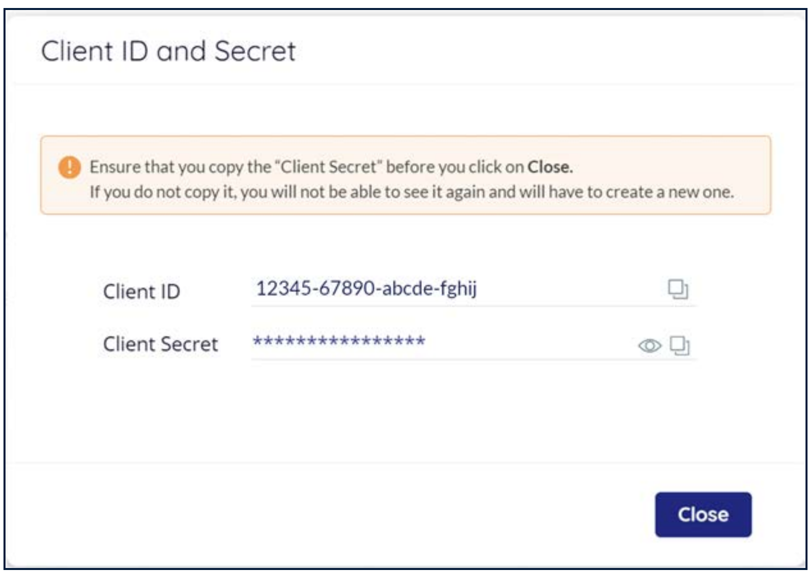
CloudAlly has a robust API, that enables you to perform billing management, backup, restore, and download management, Partner Portal management, and user management functions. It enables you to automate processes and integrate with the CloudAlly solution. The API can be used for many common business 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.

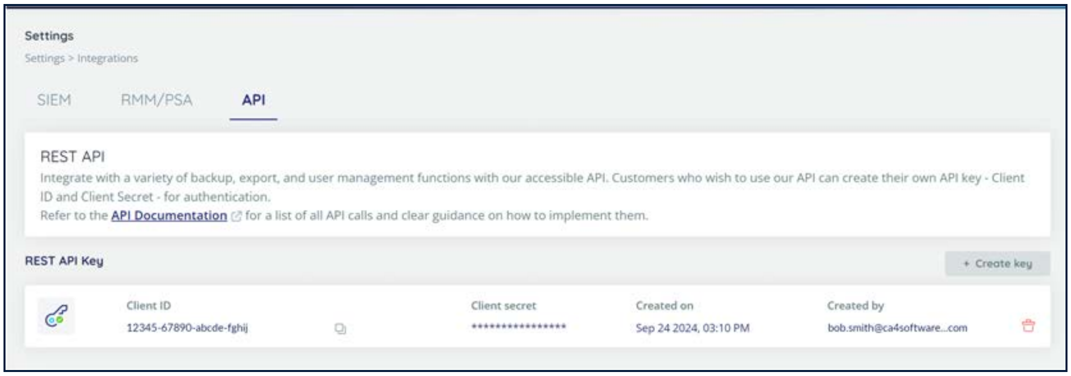
> **Note:** The Created On Date is not available for client IDs created prior to CloudAlly release 24.4.1.



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.

7.6.7 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.

8 Managing Subscriptions and Payments

8.1 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.

8.1.1 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.

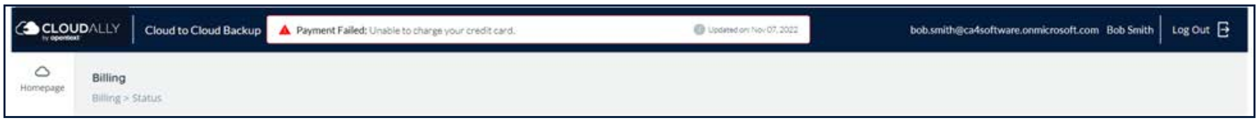
To finalize your subscription, enter your credit card details and general billing information, and then click **Subscribe**.

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 Support. Instead, you will start receiving monthly invoices for the payments.

8.1.2 Annual Subscriptions

When you subscribe to an annual plan, you will receive a confirmation message that your request has been submitted, and then 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.

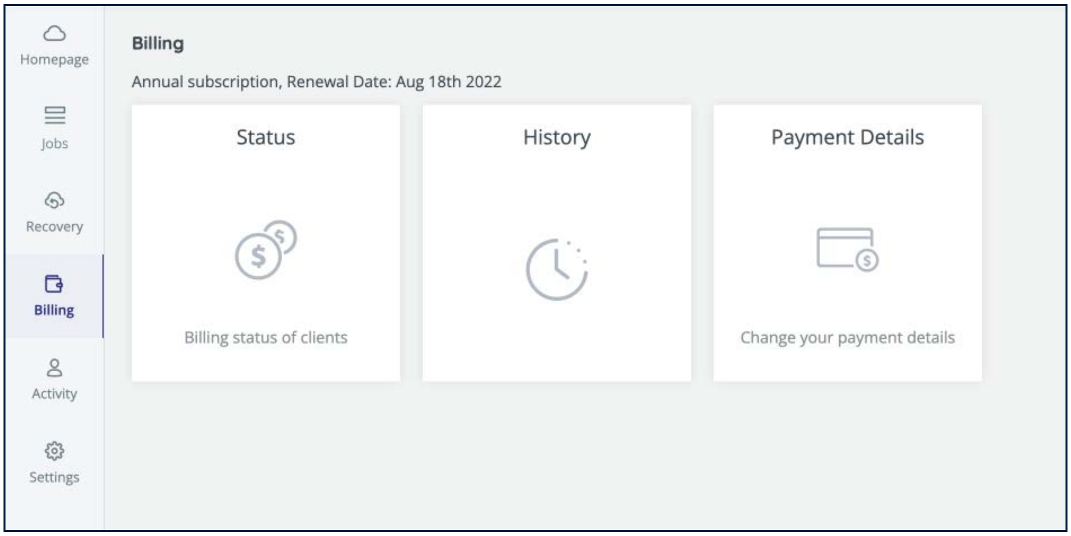
After the initial payment, CloudAlly will send you an invoice 30 days before your payment is due, in 11 months. You will also be reminded that your annual subscription is due online:

> **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.

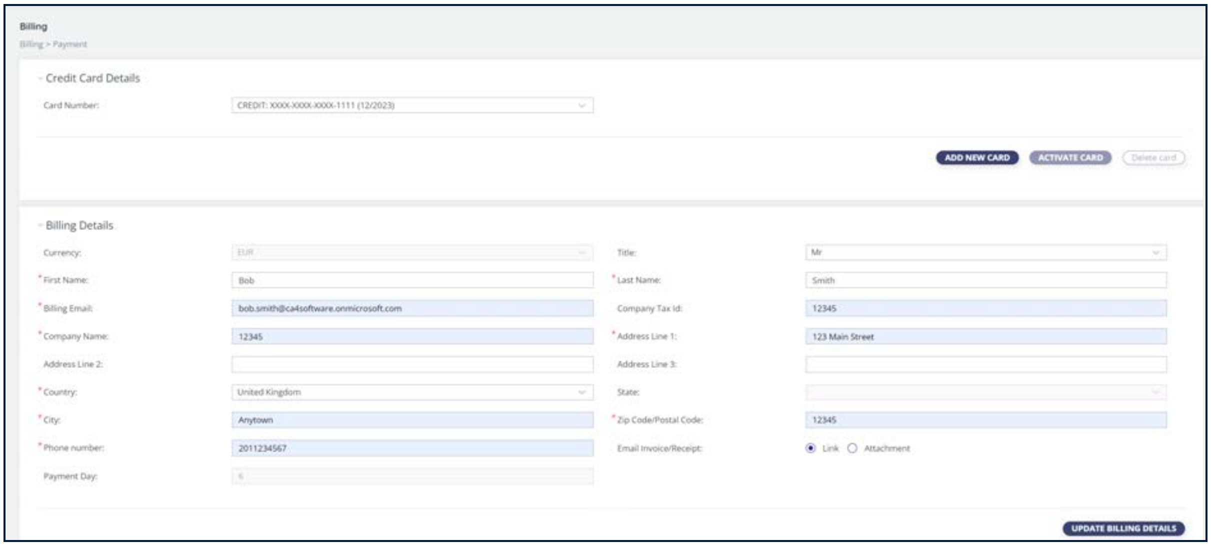
8.2 Payment Details



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

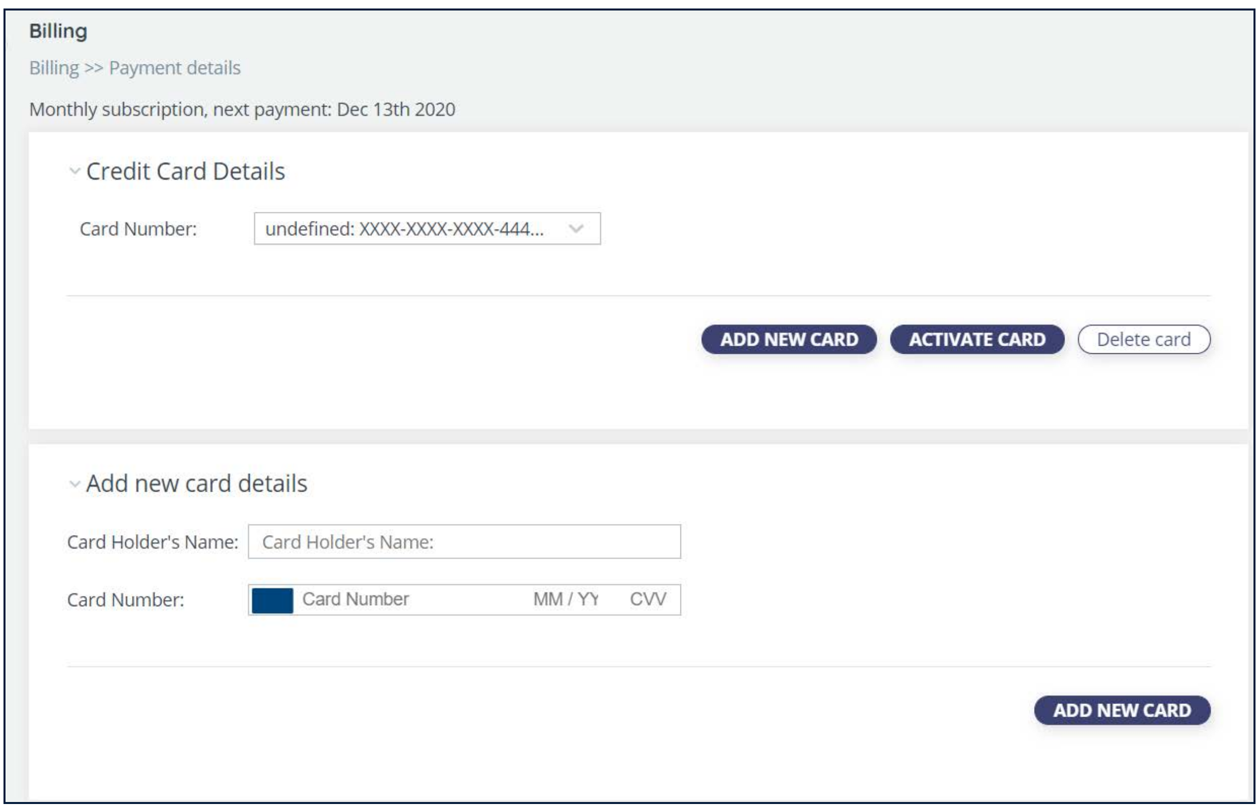
8.2.1 Monthly Subscriptions

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



8.2.1.1 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:

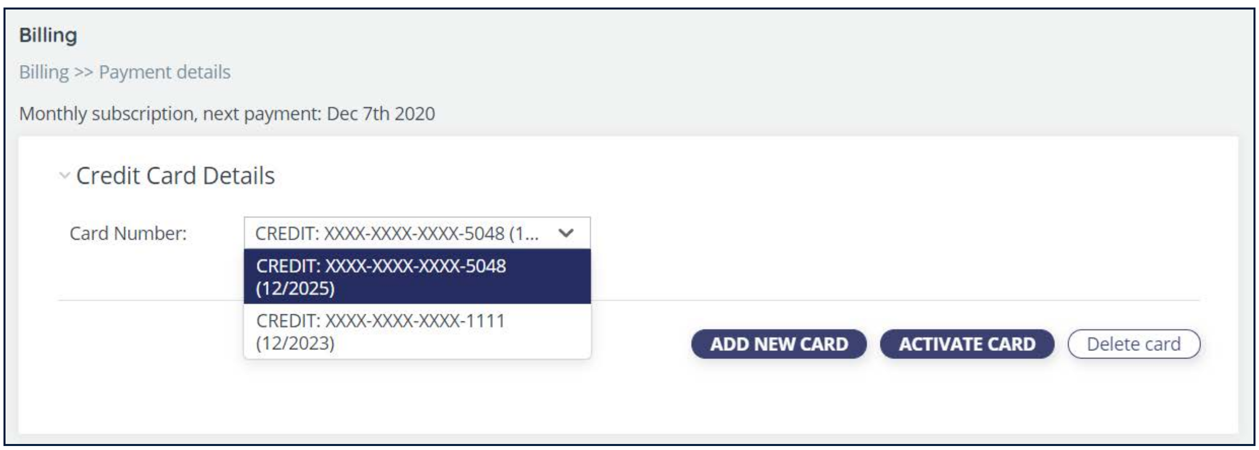
1. Click **ADD NEW CARD.**
2. Enter the card details such as Card Number, CVV, Card holder's name, and card expiry date.
3. Click **ADD NEW CARD**.

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

8.2.1.2 Change Payment Method

To change your existing payment method:

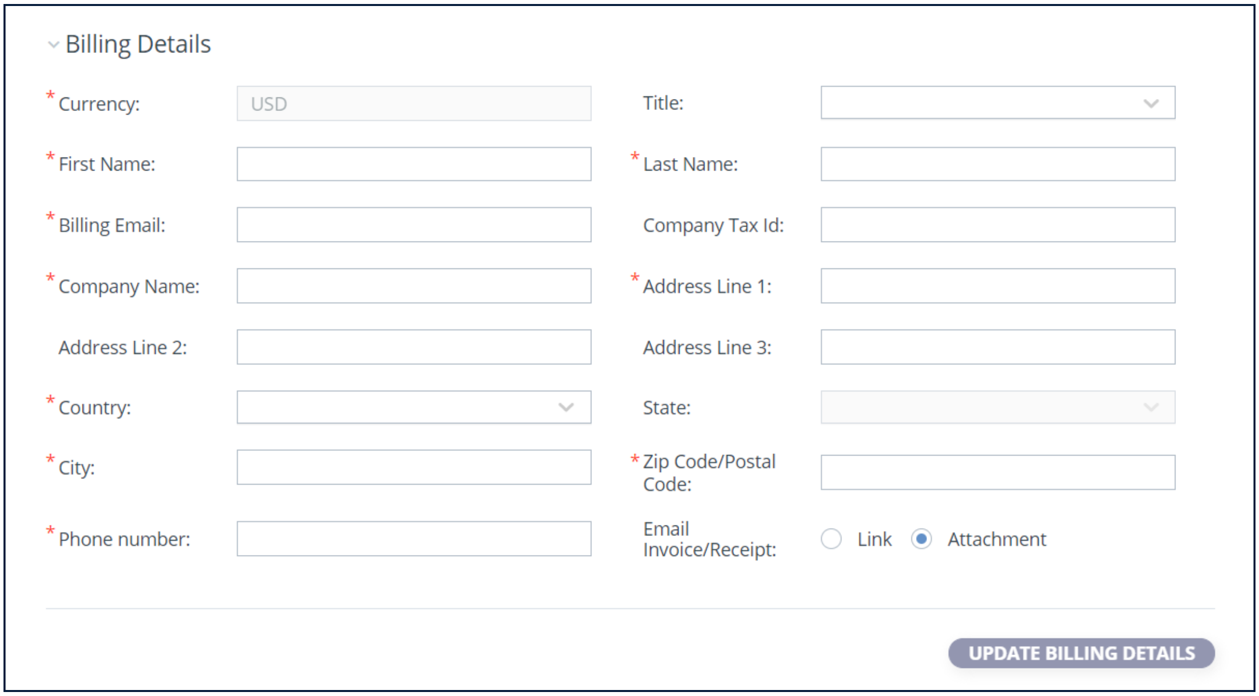
1. Click the drop-down list and select the payment method from the Cards Number drop-down list.
2. Click the payment method from the list (the screen shot below depicts choosing a different credit card).
3. Click **ACTIVATE CARD** to set the selected card as the preferred payment method.



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.



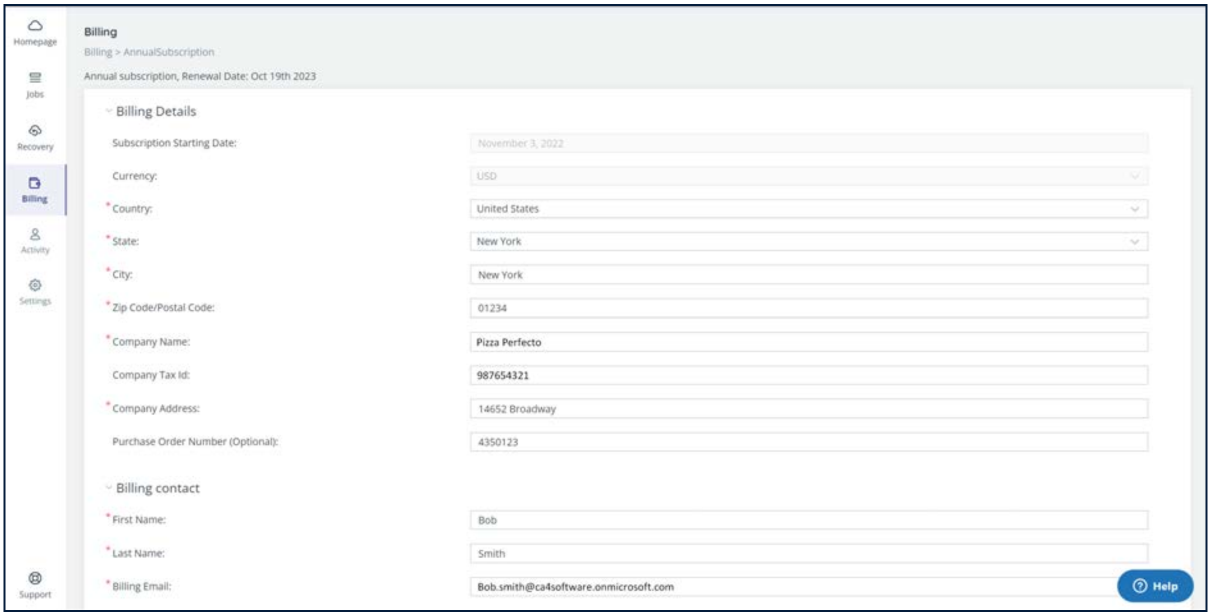
5. Update the required fields. The fields marked with the * symbol are mandatory.
6. Click **UPDATE BILLING DETAILS**.
7. The updates are saved.

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 Support.

8.2.2 Annual Subscriptions

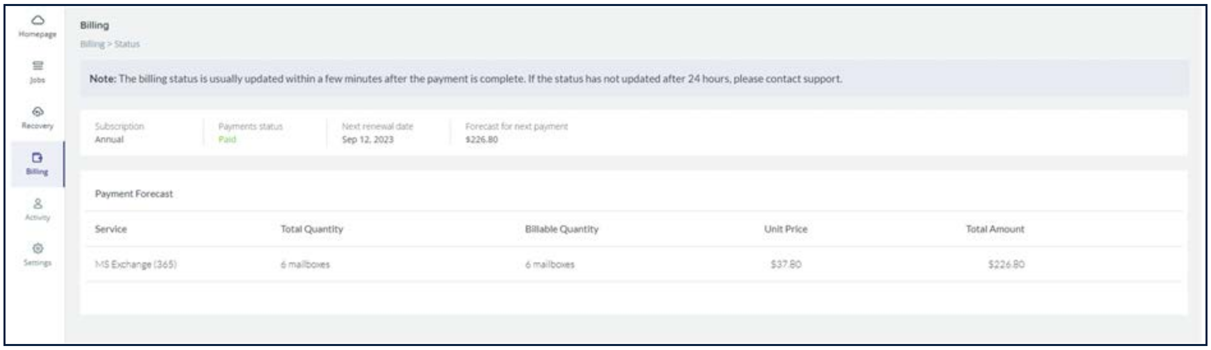
If you have chosen an annual payment plan, you can update your billing details here. When you are done, click **SAVE**.



8.3 Billing Status

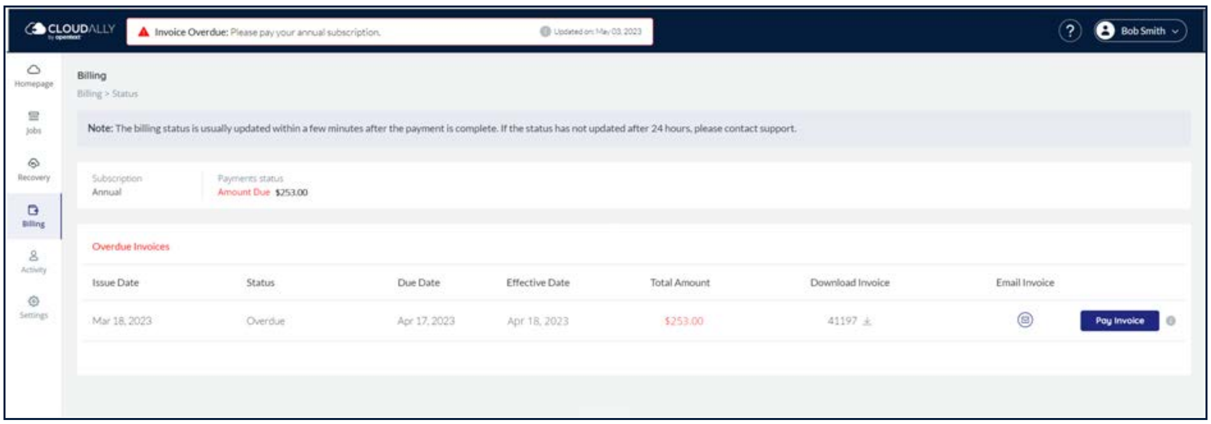
Annual Subscription

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.

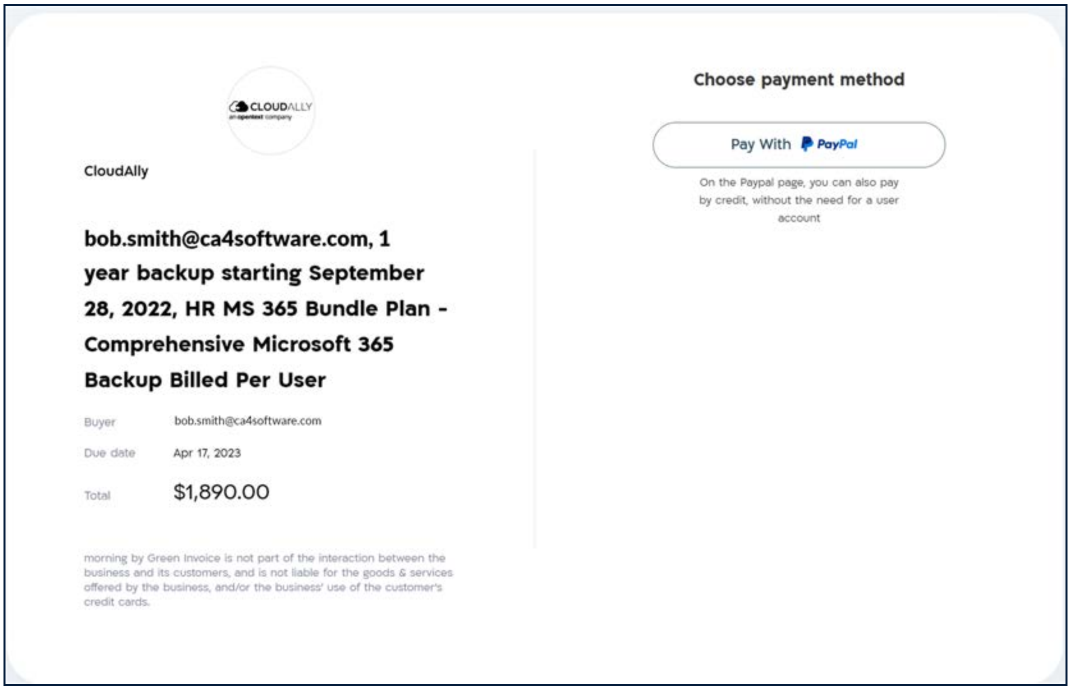


When your subscription amount becomes due, the Billing Status page displays the following information:

- **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.

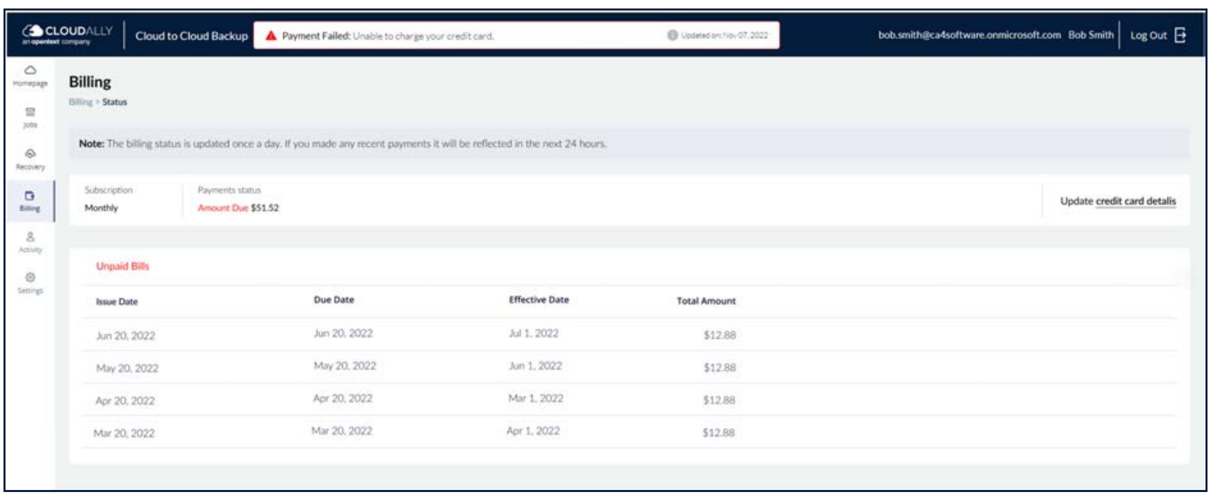


You can click **Pay Invoice**, and you will be directed to the following screen, where you can pay your invoice via PayPal or by credit card:



Monthly

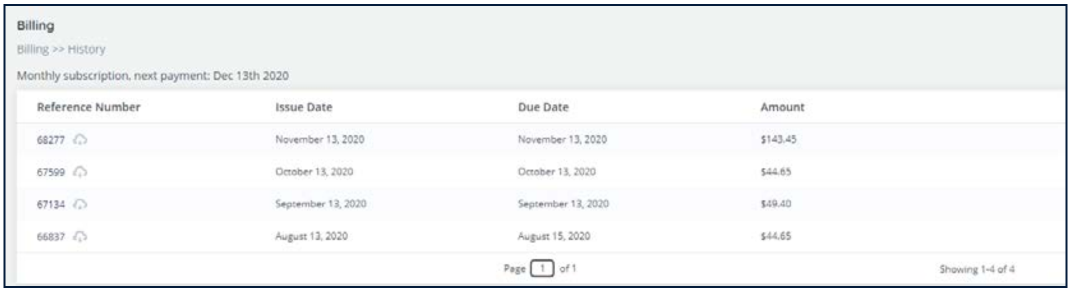
Similarly, if there was a problem with your monthly subscription payment, the status will look as follows:



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

8.4 History

This page displays the history of payments.



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**

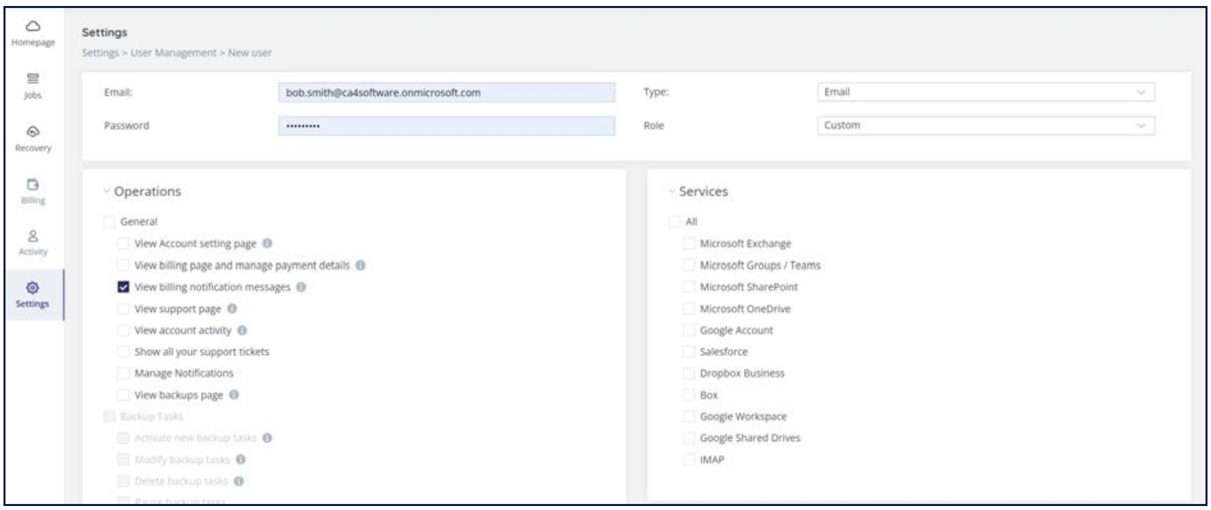
Created 26/04/2021 16:29 | Invoice / Receipt 51646 | page 1 of 1

8.5 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.



9 Helpful Resources

9.1 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.

9.2 Knowledge Base

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

9.3 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

9.4 Privacy

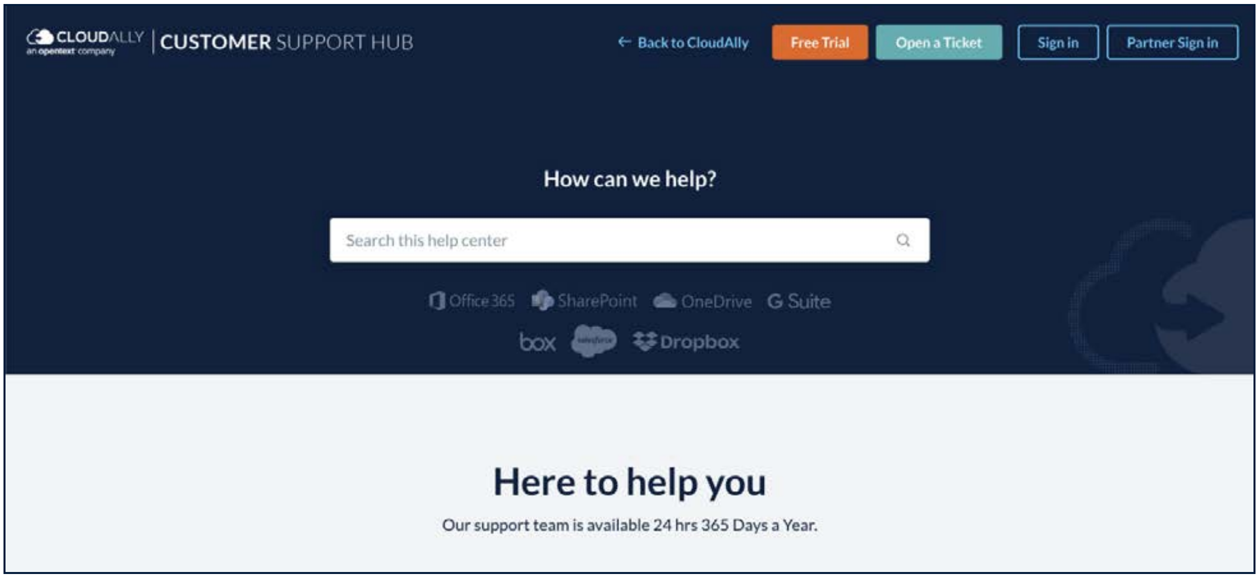
CloudAlly takes privacy seriously. Read our Privacy Policy at https://www.cloudally.com/privacy-policy

9.5 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/

10 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

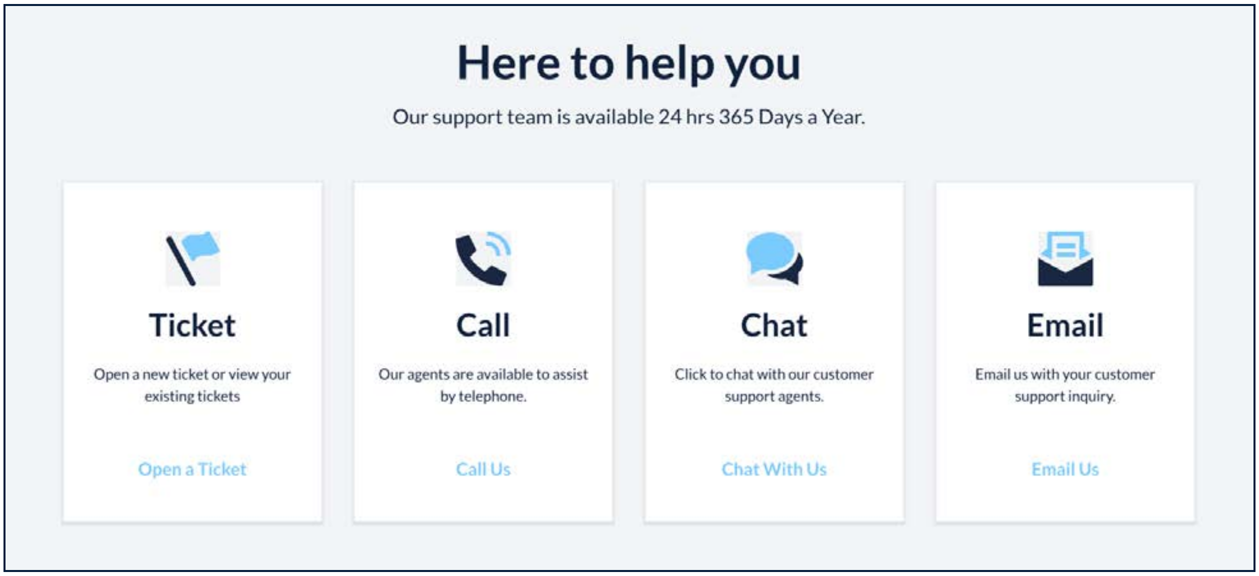
Email Addresses:

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.