CloudBacko Home

Quick Start Guide for Mac

CloudBacko Corporation

6 January 2025

Copyright Notice

© 2025 CloudBacko Corporation. All rights reserved.

The use and copying of this product is subject to a license agreement. Any other use is prohibited. No part of this publication ay be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without prior written consent of CloudBacko Corporation. Information in this manual is subject to change without notice and does not represent a commitment on the part of the vendor. CloudBacko Corporation does not warrant that this document is error free. If you find any errors in this document, please report to CloudBacko Corporation in writing.

Trademarks

CloudBacko Pro, CloudBacko Lite, CloudBacko Home, and CloudBacko App are trademarks of the CloudBacko Corporation.

Amazon S3 is a registered trademark of Amazon Web Services, Inc., or its affiliates.

Apple and Mac OS X, macOS, and iOS are registered trademarks of Apple Computer, Inc.

Dropbox is a registered trademark of Dropbox Inc.

Google Cloud Storage, Google Drive, Google Authenticator, and Android are registered trademarks of Google Inc.

Wasabi Hot Cloud Storage is a registered trademark of Wasabi Technologies Inc.

Backblaze B2 Cloud Storage is a registered trademark of Backblaze Inc.

MariaDB is a registered trademark of MariaDB Corporation AB.

Lotus, Domino, and Notes are registered trademark of IBM Corporation.

Microsoft Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, OneDrive, OneDrive for Business, Microsoft Authenticator, and Microsoft 365 are registered trademarks of Microsoft Corporation.

Oracle, Oracle Database, Java and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

OpenJDK is a registered trademark of Oracle America, Inc.

Rackspace and OpenStack are registered trademarks of Rackspace US, Inc.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. www.redhat.com in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the U.S. and other countries.

Ubuntu is a registered trademark of Canonical Ltd.

Debian is a registered trademark of Software in the Public Interest, Inc.

Rocky is a registered trademark of Rocky Brands.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

VMware ESXi, vCenter, and vSAN are registered trademarks of VMware, Inc.

Tibero® is a registered trademark of TmaxData Co., Ltd.

All other product names are registered trademarks of their respective owners.

Disclaimer

CloudBacko Corporation will not have or accept any liability, obligation, or responsibility whatsoever for any loss, destruction, or damage (including without limitation consequential loss, destruction, or damage) however arising from or in respect of any use or misuse of reliance on this document. By reading and following the instructions in this document, you agree to accept unconditionally the terms of this Disclaimer and as they may be revised and/or amended from time to time by CloudBacko Corporation without prior notice to you.

Revision History

Date	Descriptions	Version
23 May 2024	▪ Ch. 3.5 – updated twitter screenshot ▪ Ch. 6.2 – updated screenshots ▪ Ch. 7.8.1 – updated screenshots and options	5.9.14.0
2 September 2024	▪ Ch. 7.4.1.5 – updated screenshots and instructions ▪ Ch. 10 – updated screenshots and instructions ▪ Ch. 11.1 – updated screenshots and instructions	5.11
6 January 2025	▪ Ch. 11 – Updated Restore instructions ▪ Ch. 11.2 – Updated Restore Filter instructions	5.13

Table of Contents

1 Overview 6

1.1 What is this software? 6

1.2 System Architecture 6

1.3 Mobile Backup Server (MBS) 7

System Diagram 7

2 Requirements for CloudBacko app 10

2.1 Backup Software Version Requirement 10

2.2 Network Connection 10

2.3 Android and iOS Version Requirement 10

3 Requirements for CloudBacko Home on macOS 11

3.1 Hardware Requirements 11

3.2 Supported Platforms 11

3.3 Internet Connection 11

3.4 Firewall Settings 11

3.5 Social Media Accounts 11

3.6 Full Disk Access Permission 12

3.7 Supported Applications 12

3.8 Supported Features 12

3.9 Mobile Device Requirements 12

3.10 Supported macOS Big Sur on Intel and ARM (M1) CPU 13

3.11 Limitations 13

4 Get Started with CloudBacko Home 15

5 Download and Install CloudBacko Home 16

5.1 Download CloudBacko Home 16

5.2 Install CloudBacko Home 17

5.3 Upgrade CloudBacko Home 21

5.4 CloudBacko Home Services 22

5.5 Mobile Backup Server (MBS) Health Check and CloudBacko app connection Check 25

6 Start CloudBacko Home 28

6.1 Setup CloudBacko Home 28

6.2 Launch CloudBacko Home 35

6.2.1 Initial launch creating backup set and setting up mobile backup 35

6.2.2 Subsequent login with privacy lock 39

6.2.3 Subsequent login with no privacy lock 40
7 CloudBacko Home Overview 41
7.1 Language 42
7.2 About 42
7.3 Backup 43
7.4 Backup Sets 44
7.4.1 Backup Set Settings 46
7.4.1.1 General 46
7.4.1.2 Source 47
7.4.1.3 Backup Schedule 56
7.4.1.4 Destination 57
7.4.1.5 Others 59
7.5 Report 67
7.5.1 Backup 68
7.5.2 Restore 72
7.5.3 Usage 73
7.6 Restore 75
7.7 Settings 76
7.7.1 Proxy 77
7.7.2 Email Report 78
7.7.3 Authentication 79
7.7.4 Mobile Backup 85
7.8 Utilities 99
7.8.1 Data Integrity Check 100
7.8.1.1 Data Integrity Check Completed with Errors 111
7.8.1.2 Data Integrity Check Result 112
7.8.1.3 Test Mode Confirmation 114
7.8.2 Space Freeing Up 116
7.8.3 Export Settings 120
7.8.4 Delete Backup Data 122
7.8.5 Decrypt Backup Data 127
7.9 Social Media Icons 128
7.10 Online Help 128
8 Create a Backup Set 130
9 Overview on Backup Process 138
9.1 Periodic Data Integrity Check (PDIC) Process 139
9.2 Backup Set Index Handling Process 141

9.2.1 Start Backup Job 141
9.2.2 Completed Backup Job 142
9.3 Data Validation Check Process 143
10 Run Backup Jobs 144
11 Restore Data 146
11.1 Restore Data 146
11.2 Restore Filter 152
12 Mobile Backup and Restore to Cloud 156
13 Contact CloudBacko 159
Technical Assistance 159
Appendix 160
Appendix A: Uninstall CloudBacko Home 160
Appendix B: Example Scenarios for Restore Filter 162
Appendix C: Setting up Full Disk Access Permission 170
Appendix D: Exclude Filter System Files 174

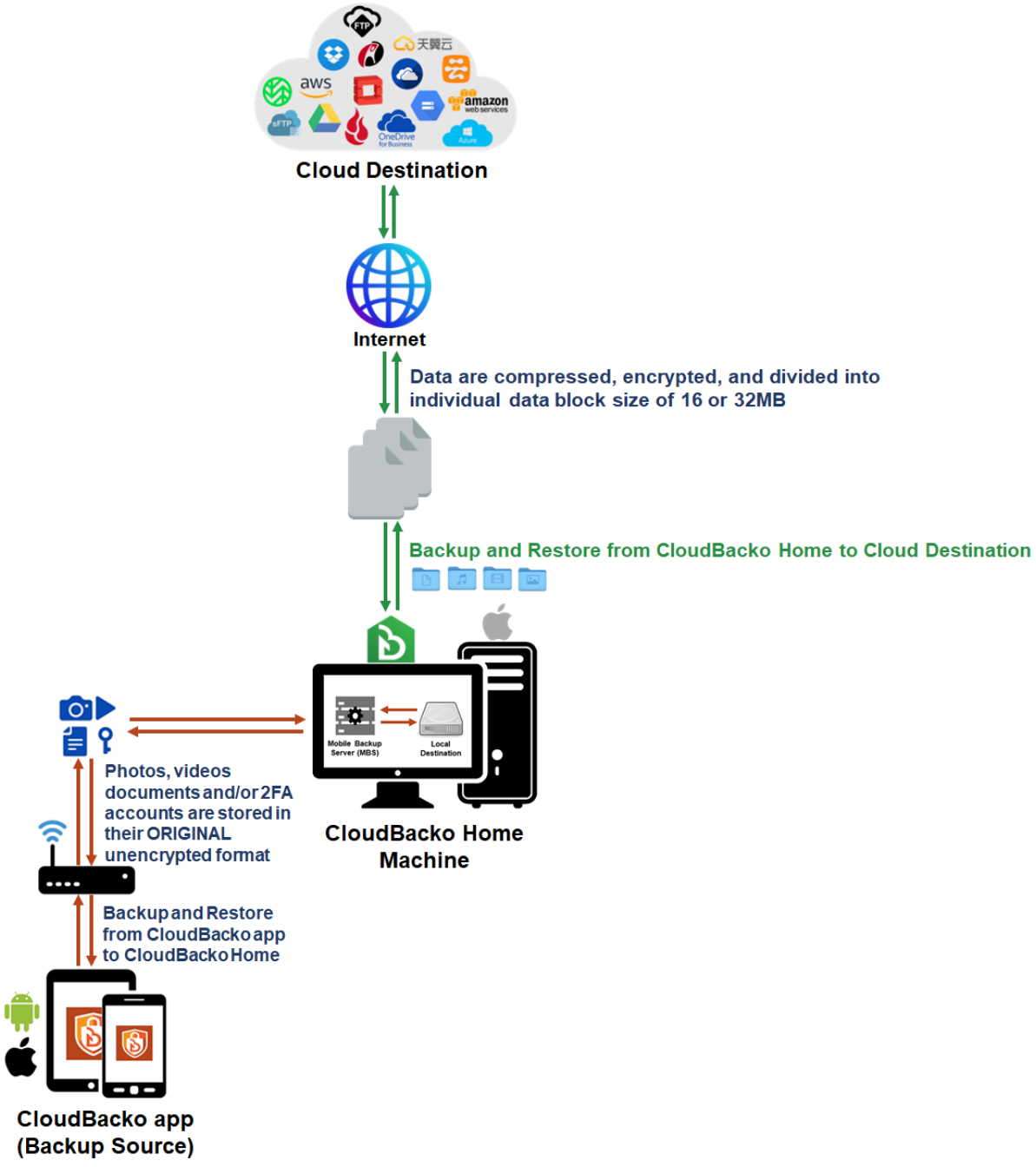
1 Overview

1.1 What is this software?

CloudBacko brings you specialized client backup software, namely CloudBacko Home, to provide a simple backup solution for protecting file(s) / folder(s) on your machine, with a wide variety of backup destinations (major cloud storage service providers, FTP/SFTP, local drive, etc.) of your choice.

1.2 System Architecture

Below is the system architecture diagram illustrating the major elements involved in the backup process among the backup machine CloudBacko Home and CloudBacko app.



1.3 Mobile Backup Server (MBS)

The Mobile Backup Server (MBS) will be utilized to handle mobile backup and restore of CloudBacko app. It is an integral part of CloudBacko Home, which is located in the “mbs” folder inside the CloudBacko Home folder.

System Diagram

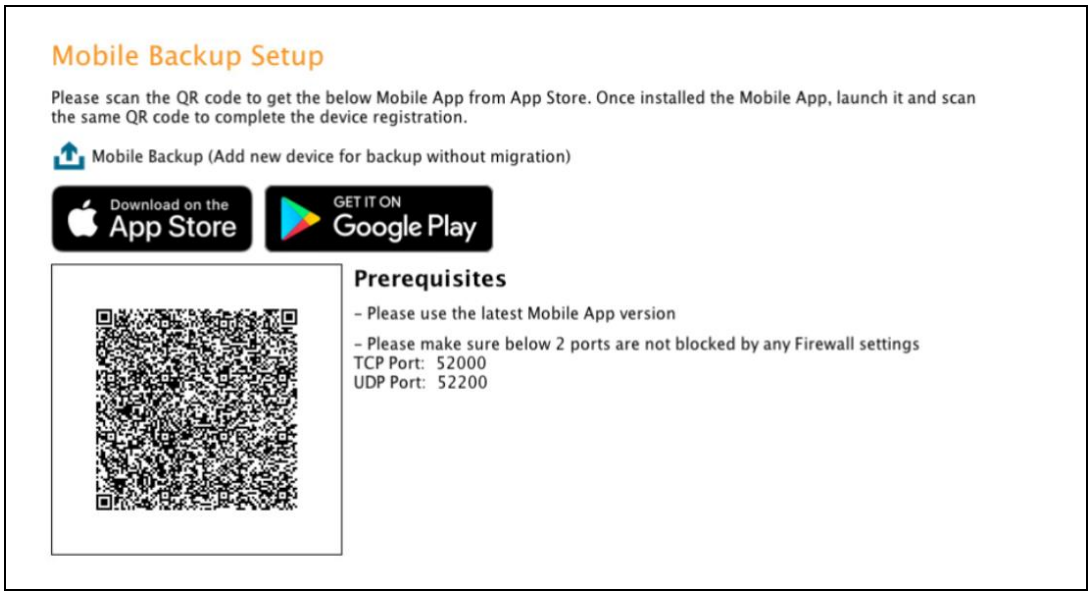
The Mobile Backup Server (MBS) will be activated automatically when a mobile device installed with the CloudBacko app is successfully registered for mobile backup with CloudBacko Home. Afterwards, it will be automatically restarted whenever the CloudBacko Home services is restarted or when the CloudBacko Home machine is rebooted or powered on. The MBS will be deactivated when all mobile devices have deregistered from the mobile backup settings and the CloudBacko Home services is restarted.

The MBS will use the following port ranges:

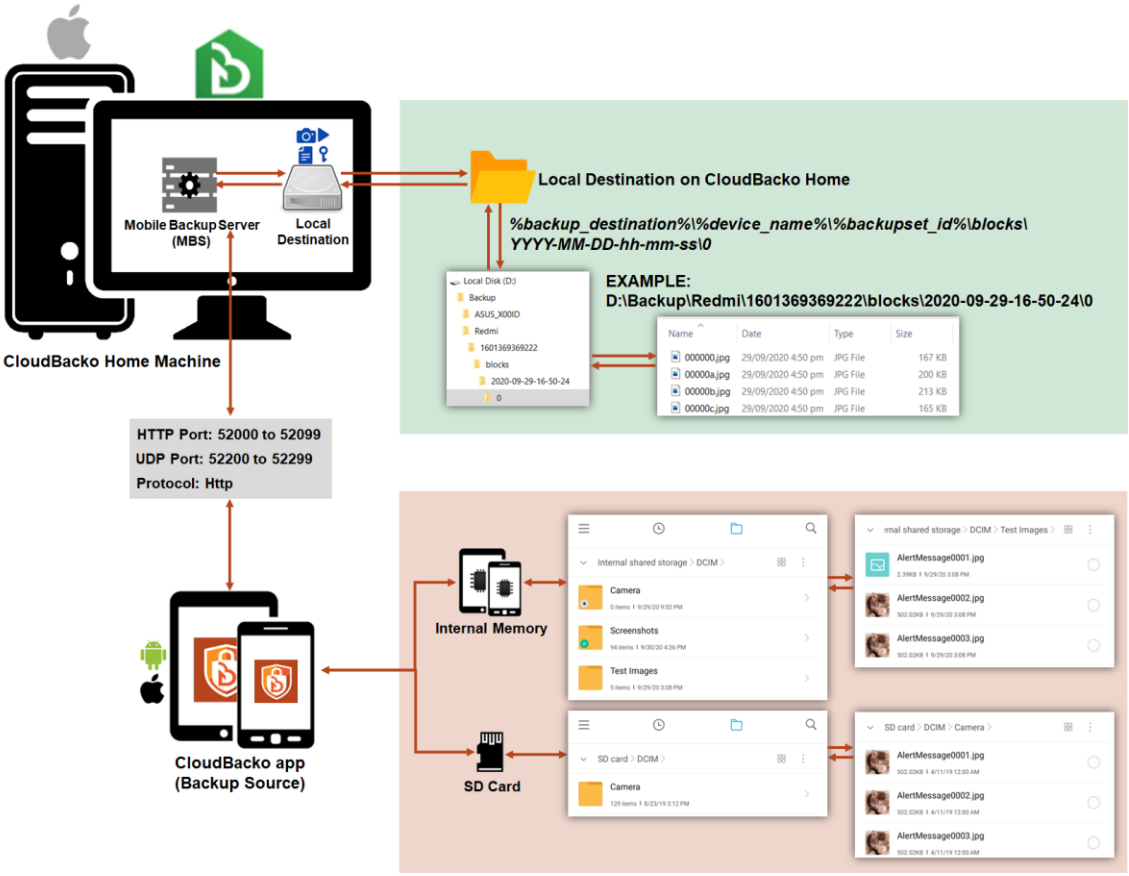
- **TCP Port:** 52000 to 52099
- **UDP Port**: 52200 to 52299
- **Protocol:** Http, for the request of CloudBacko app.

The default TCP and UDP ports are **52000** and **52200**, if these ports are already in use by other applications or services, then the MBS will automatically acquire another port.

The actual TCP and UDP port can be seen on the CloudBacko Home when pairing a mobile device for mobile backup.



Photos, videos, documents and 2FA accounts are stored either in mobile device's internal memory or SD Card. These are selected as backup source using the CloudBacko app and will be backed up to the local destination of the CloudBacko machine, that can be a Hard Drive, Flash Drive, and/or Network Drive in their *original* unencrypted format. For Android devices, photos and videos will retain all EXIF. While for iOS devices, photos and videos will retain most of the EXIF including, capture date, location, and lens.

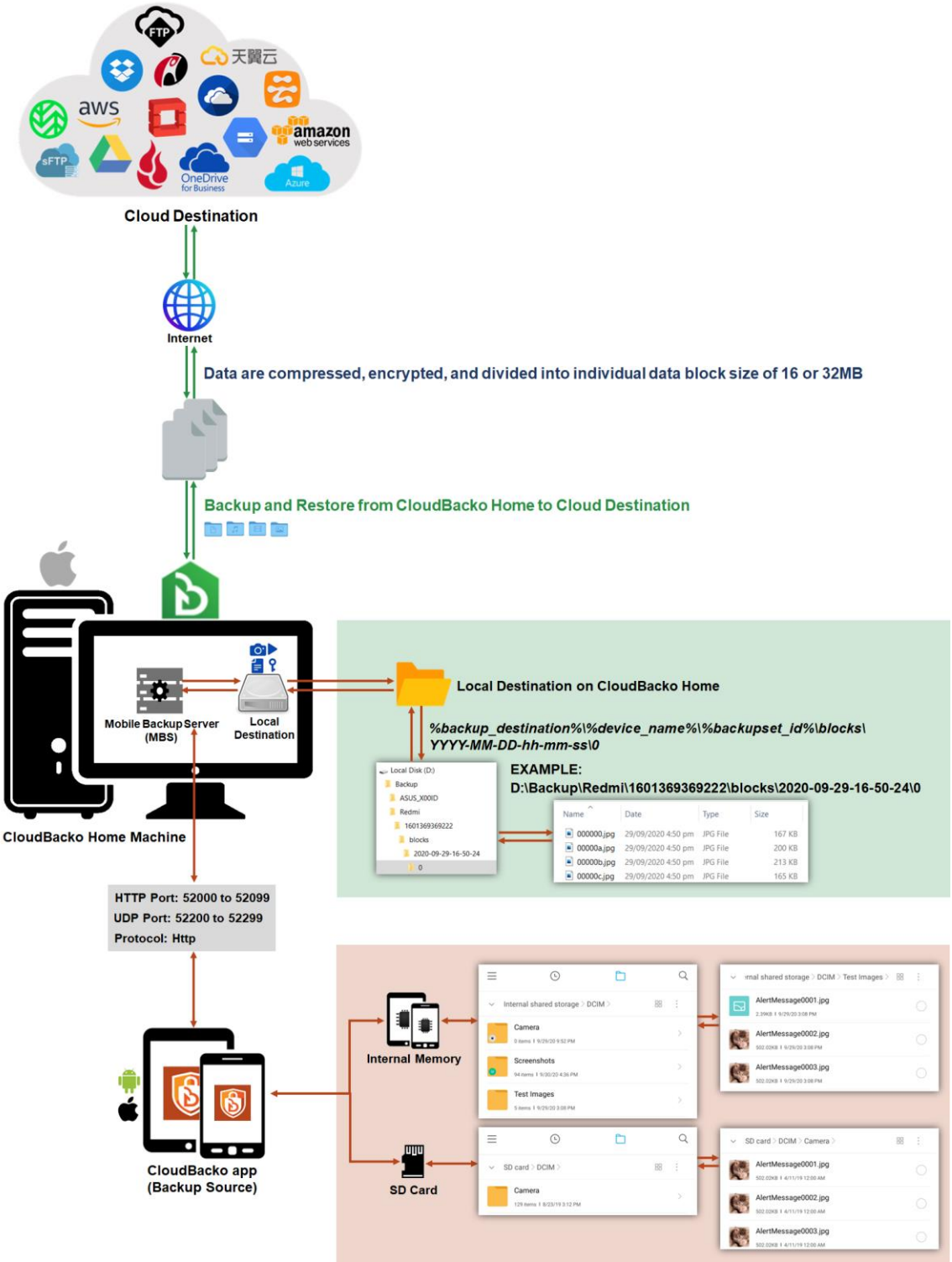


If storage of photos, videos, documents and 2FA accounts to a cloud destination is required, then this can be done using CloudBacko Home to perform a secondary backup and restore of the photos, videos, documents and 2FA accounts on the local drive to the cloud.

To back up and restore photos, videos, documents and 2FA accounts from CloudBacko app to CloudBacko Home and Cloud, is a two-step process.

1st: Back up photos, videos, documents and/or 2FA accounts from CloudBacko app to the CloudBacko Home local destination.

2nd: Create a File backup set using CloudBacko Home, using the local backup destination as the backup source, and then back up this backup set to cloud destination.



2 Requirements for CloudBacko app

2.1 Backup Software Version Requirement

- Download and install the latest version of CloudBacko Home.
- Download and install the latest version of CloudBacko app on the Play Store for Android mobile devices and on the App Store for iOS mobile devices.

2.2 Network Connection

Ensure that CloudBacko app is connected to the same local WiFi network with CloudBacko Home. Failure to do so will prevent the CloudBacko app from performing backup/restore.

2.3 Android and iOS Version Requirement

- For Android device, Android version must be Android 8 or above.
- For Apple device, iOS version must be 12.0 or above.

3 Requirements for CloudBacko Home on macOS

3.1 Hardware Requirements

Refer to the link below for details of the minimum and recommended requirements for installing CloudBacko Home.

CloudBacko Home: Hardware Requirement

3.2 Supported Platforms

Refer to the following link for details of the operating systems supported by CloudBacko Home.

CloudBacko Home: Supported Operating Systems

3.3 Internet Connection

CloudBacko machine must have a fixed internet connection

3.4 Firewall Settings

For mobile backup inbound / outbound network traffic must be allowed through the following default ports: HTTP port: 52000 and UDP port: 52200..

The actual ports used may be different, please refer to Chapter 1.3: Mobile Backup Server (MBS) for more details.

3.5 Social Media Accounts

One of the following social media accounts is required, as part of the CloudBacko Home setup you will have to login using one of these accounts to activate CloudBacko Home.

Google

Twitter

Facebook

Microsoft

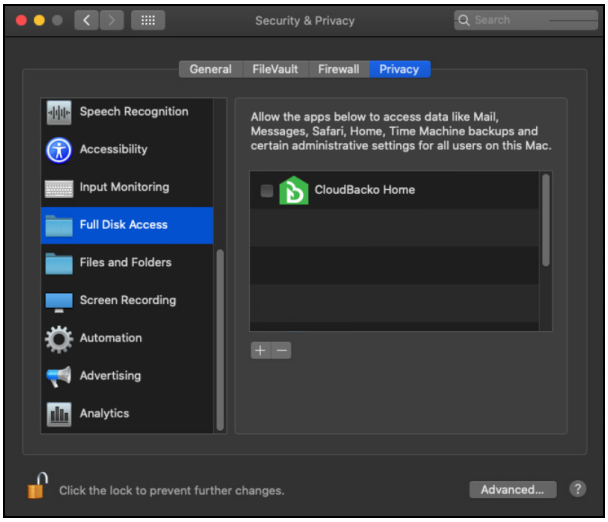
Sina Weibo

Tencent Weibo

3.6 Full Disk Access Permission

macOS 10.15 or higher "Full Disk Access" permission needs to be granted in, **System Preferences**>**Security & Privacy**>**Privacy tab to CloudBacko Home**.

Due to an upgrade in security on macOS 10.15 or higher, additional security settings are required to allow applications to access the machine. CloudBacko Home requires "Full Disk Access" permission to be able to access your files for selection and backup. Also, without "Full Disk Access" permission, CloudBacko Home will not be able to restore files to the machine.



For more details on how to setup the Full Disk Access permission, please refer to Appendix C: Setting up Full Disk Access Permission.

3.7 Supported Applications

CloudBacko Home supports File Backup Set only.

For backup of VMware, Hyper-V, Databases, and Microsoft 365, please consider upgrading to CloudBacko Pro or CloudBacko Lite.

3.8 Supported Features

Refer to the link below for the details of the supported features by CloudBacko Home.

CloudBacko Home: Supported Features

3.9 Mobile Device Requirements

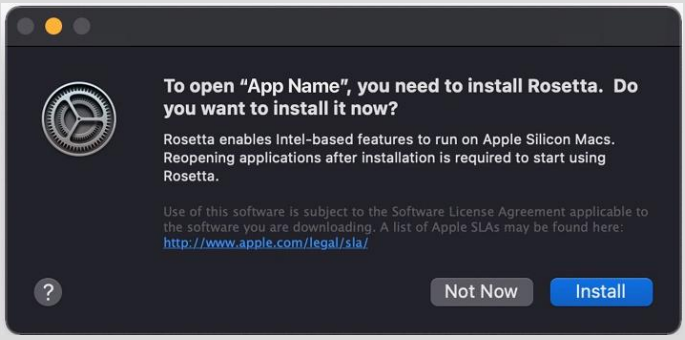
Refer to the CloudBacko App v1 User Guide for Android and iOS for details of the minimum and recommended requirements for installing CloudBacko app.

3.10 Supported macOS Big Sur on Intel and ARM (M1) CPU

CloudBacko Home v4.5.2.3 and above supports macOS Big Sur on both Intel and ARM (M1) CPU. For macOS on ARM (M1) CPU, Rosetta 2 must be installed. Refer to the link for more details: [Apple Support: If you need to install Rosetta on your Mac]

NOTE

If CloudBacko Home v4.5.2.3 and above is installed and run for the first time on macOS 11 or above - ARM M1 CPU machine, there will be a pop-up to request installation of Rosetta. Then click **Install** to proceed.



3.11 Limitations

If you require any of the following features, please consider upgrading to CloudBacko Pro or CloudBacko Lite.

- **Advanced In-File Delta Setting**

  Advanced In-File Delta Setting is not supported on CloudBacko Home.

- **Advanced Retention Policy**

  Advanced Retention Policy is not supported on CloudBacko Home.

- **Bandwidth Control**

  Bandwidth Control is not supported on CloudBacko Home.

- **Case-Insensitive File System**

  For volume with a case-insensitive file system, target file of a symbolic link will be backed up twice (in both upper case and in lower case), hence, doubling the backup quota storage requirement.

- **Command Line Tool**

  Pre-Backup / Post-Backup Commands are not supported on CloudBacko Home.

- **Continuous Backup**

  Continuous Backup is only supported on Windows platform.

- **Email Report**

  Email Report is not supported on CloudBacko Home.

- **File Permissions**

  Backup of file permissions is enabled by default and the setting cannot be changed.

- **Follow Link**

  Follow Link is enabled by default and the setting cannot be changed.

- **Immutable Destination**

  Immutable Destination is not supported on CloudBacko Home.

- **Installation on Root Drive**

  CloudBacko Home must be installed on the root drive of a volume (e.g. /Applications/...).

- **Resource Fork Files**

  Resource fork files cannot be restored with CloudBacko installation on macOS 10.8 above.

- **Restore Drill**

  Restore Drill is not supported on CloudBacko Home.

- **Scheduled Backup**

  Scheduled backup is not supported on CloudBacko Home

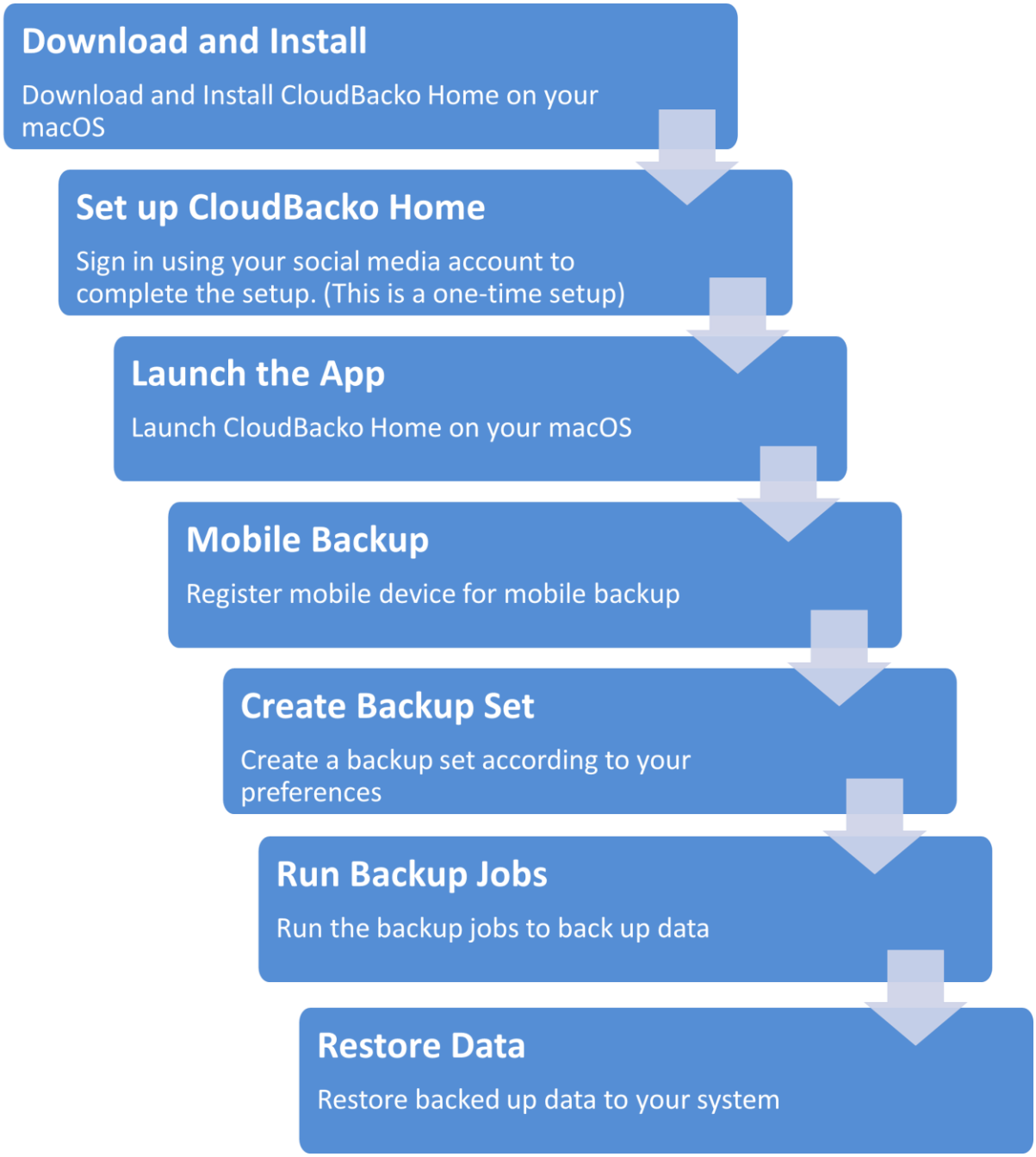
- **Software Update**

  Automatic software update is not supported for CloudBacko Home.

  To upgrade CloudBacko Home, please download the latest version from the CloudBacko website.

4 Get Started with CloudBacko Home

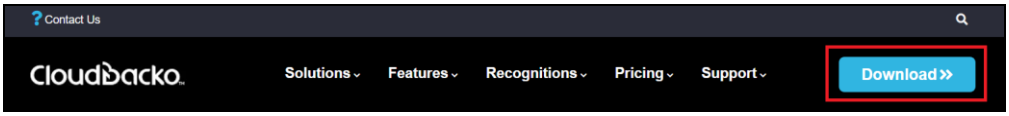
This quick start guide will walk you through the following seven (7) major parts to get you started with using CloudBacko Home.



5 Download and Install CloudBacko Home

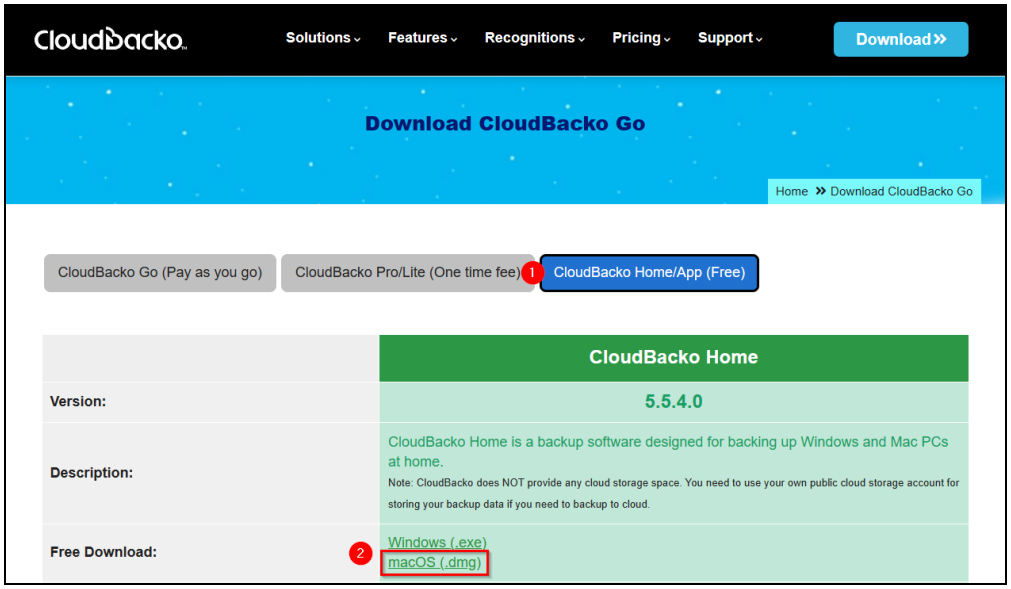
5.1 Download CloudBacko Home

1. In a web browser, go to the CloudBacko website and click **Download**.



NOTE
Screenshot was taken as of 2023-September-12, it may be different in the future.

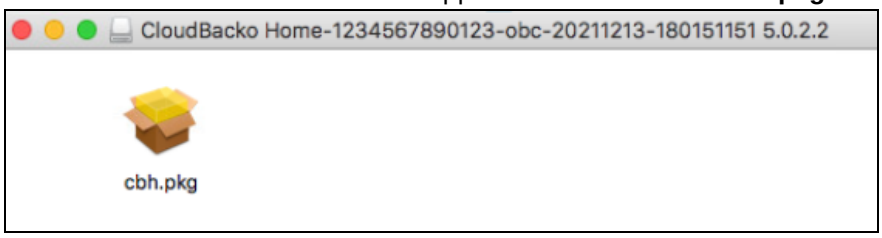
2. Click **CloudBacko Home/App**. Under CloudBacko Home you can choose the installer by operating system and click the corresponding link to start downloading. In this case click **macOS (.dmg)**.



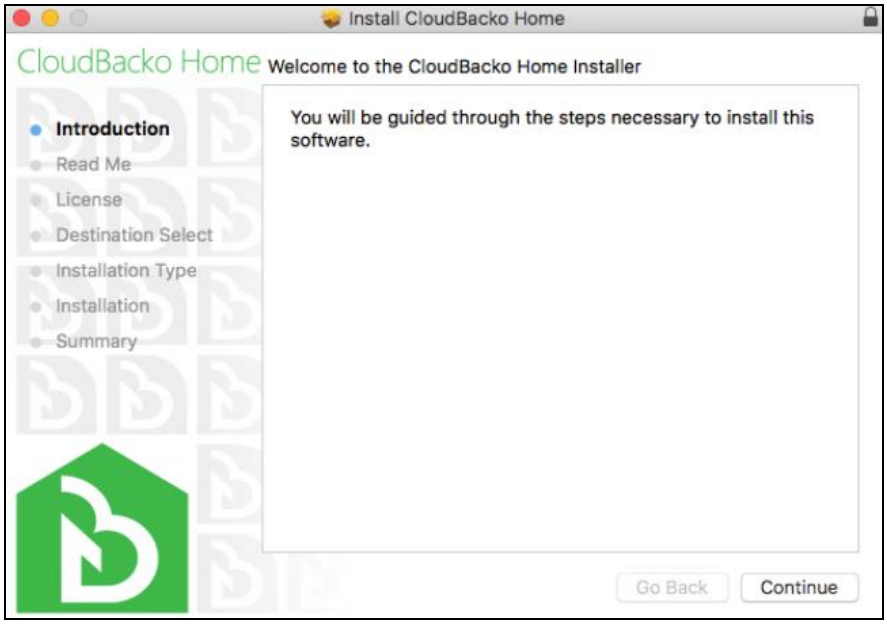
5.2 Install CloudBacko Home

1. Double-click the icon of the CloudBacko installation package **.dmg** file you have downloaded.

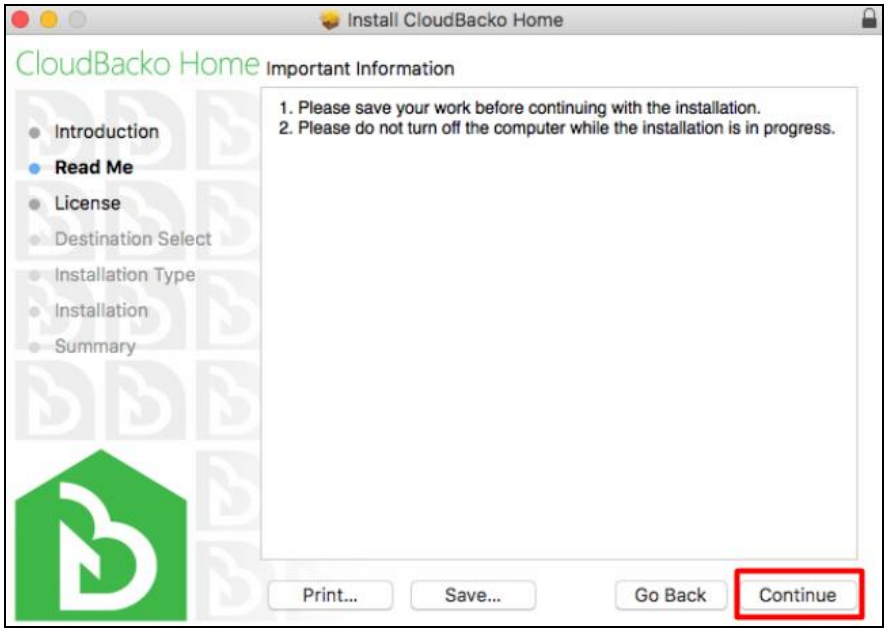
2. The CloudBacko Home window will appear. Double-click the **cbh.pkg** file.



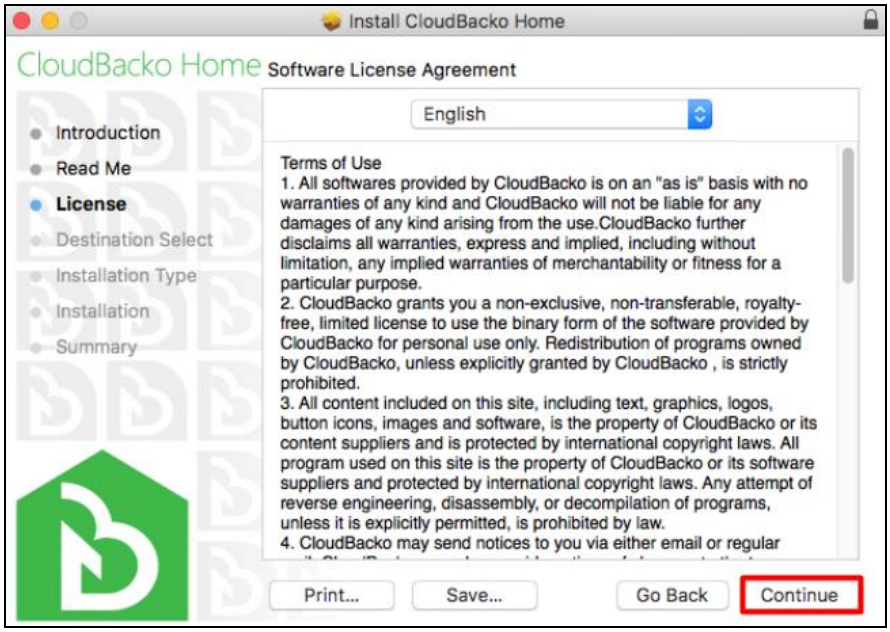
3. When the CloudBacko Home Installer wizard appears, click **Continue** to proceed.



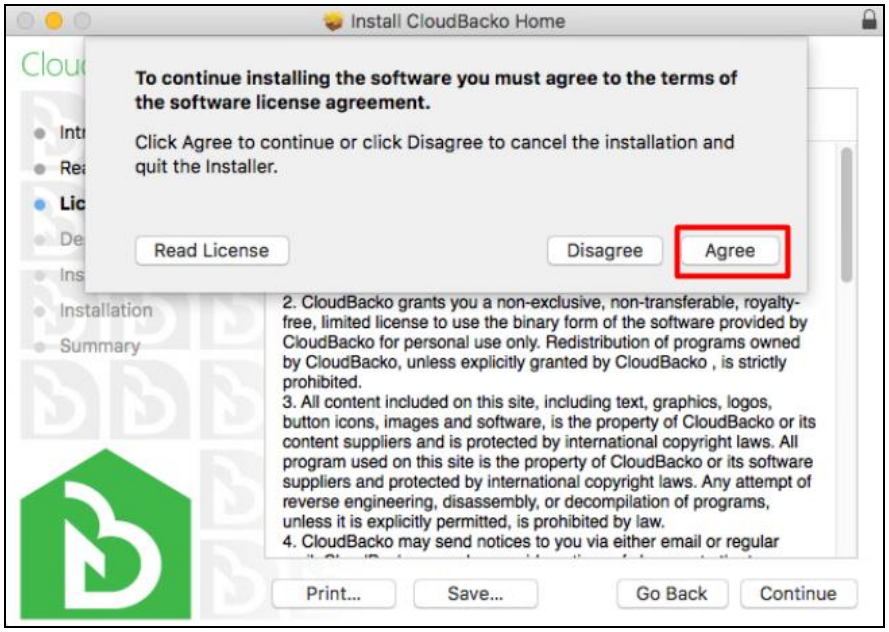
4. When the Important Information screen appears, read the information and then click **Continue** to proceed.



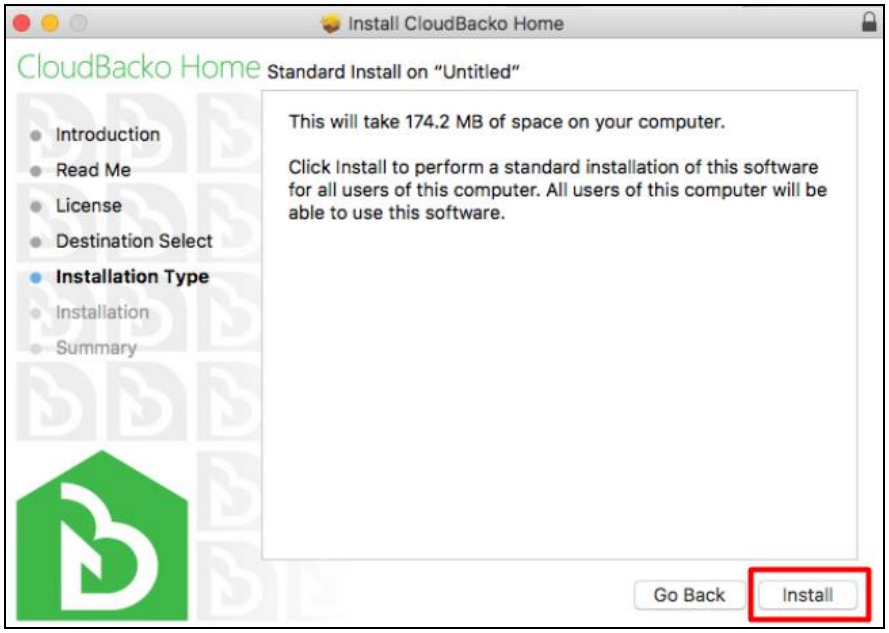
5. When the Software License Agreement appears, the agreement content will be displayed in English by default. If you prefer to read it in a different language, click the dropdown menu to change the language. After reading the agreement carefully, click **Continue** to proceed.



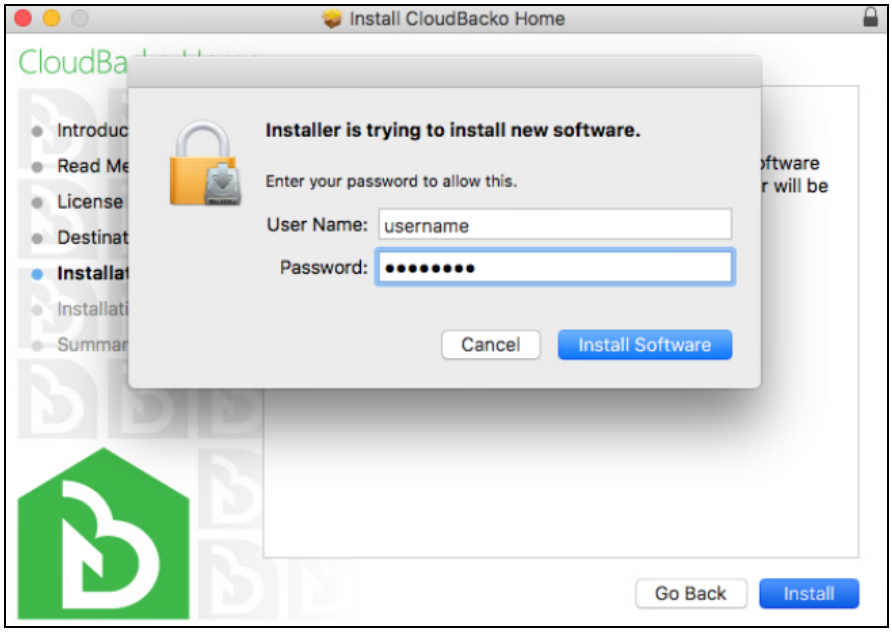
6. The following message will appear in a pop-up window. Click **Agree** to accept the software license agreement.



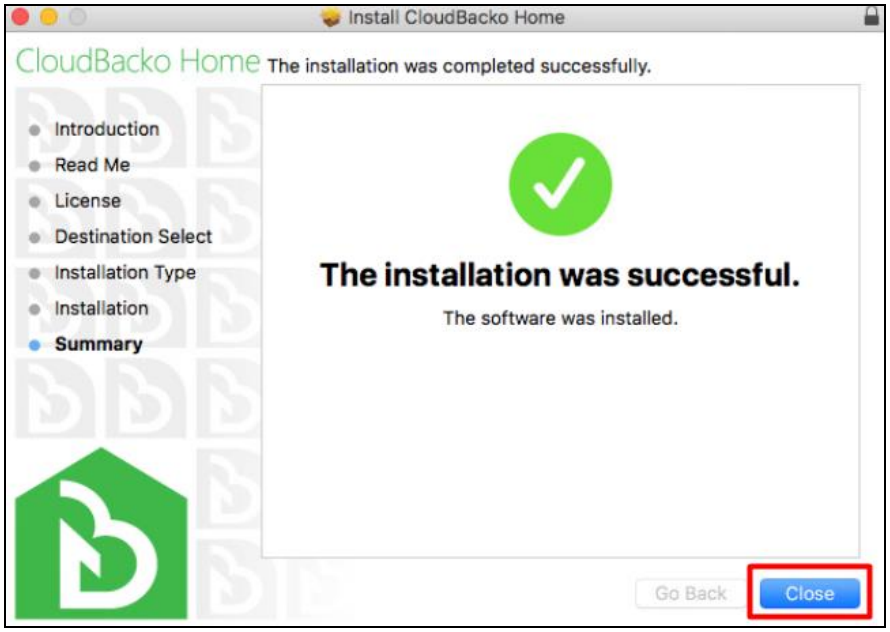
7. Click **Install** to start installing CloudBacko Home to the default location.



8. When the following screen appears, enter your macOS login credentials then click **Install Software** to start the installation process.



9. The following screen indicates a successful CloudBacko Home installation. Click **Close** to continue.



5.3 Upgrade CloudBacko Home

To upgrade CloudBacko Home to the latest version, follow the instructions below:

1. Uninstall CloudBacko Home. For more details, please check Appendix A: Uninstall CloudBacko Home.
2. Download the latest version of CloudBacko Home from the CloudBacko website. For more details, please refer to Chapter 5.1 Download CloudBacko Home.
3. Install CloudBacko Home. For more details, please check Chapter 5.2: Install CloudBacko Home.

5.4 CloudBacko Home Services

The CloudBacko Home Services is a key component which regulates and controls several important functions on CloudBacko.

Function	Description
Continuous Backups (Windows platform only)	Ensures that Continuous backups are run according to the backup interval.
Reminder (Windows platform only)	Ensures that a reminder popup is displayed when the last time a backup was run exceeded the tolerance period.
Mobile Backup Server (MBS)	Ensure that registered mobile devices can perform backups to CloudBacko Home. The MBS will be activated when a mobile device is registered for mobile backup on CloudBacko Home. The MBS will be deactivated when all mobile devices have been deregistered from the mobile backup settings and the CloudBacko Home services is restarted.

Therefore, it is very important to ensure the CloudBacko Home Services is running after,

a new CloudBacko installation

a CloudBacko software update

when the machine rebooted

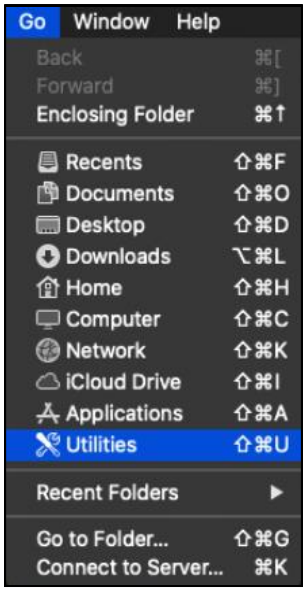
the machine is powered on

the machine wakes up from hibernation or standby mode

Otherwise, all of the functions above will stop working.

This option is used to kick automated or scheduled backup jobs.

1. To start, click **Go** at the top menu bar and select **Utilities**.



2. Open the **Terminal** application.

3. Use the command highlighted in red to enter the CloudBacko Home folder.

```
[admins-Mac:bin admin$ cd /Applications/CloudBacko\ Home.app/bin
[admins-Mac:bin admin$
```

4. To check if the CloudBacko Home Services is running, use the **ps** command. You will see that the CloudBacko Home Services is running, highlighted in red.

```
admins-Mac:~ admin$ ps -ef|grep java
0 5735 1 0 9:05PM ttys000 0:02.07 /Applications/CloudBacko\
Home.app /jvm/bin/ java -Xms128m -Xmx768m -Djava.library.path=.
-cp .:./cbs.jar cbs /Applications / CloudBacko\ Home.app
501 5741 5705 0 9:05PM ttys000 0:00.00 grep java
```

There are two (2) options to **stop** and **start** the CloudBacko Home Services.

Option 1

- **Stop CloudBacko Home Services**

  To **stop** the CloudBacko Home services, use the command highlighted in red. If you run this command for the first time, you will need to enter the login password of your local machine.

  To check if the CloudBacko Home Services has stopped running, use the **ps** command.

```
admin-admins-Mac-2~% sudo /Applications/CloudBacko\
Home.app/bin/StopScheduler.sh

Password:

admin-admins-Mac-2% ps -ef|grep java

501 5721 5705 0 9:02PM ttys000 0:00.00 grep java
```

- **Start CloudBacko Home Services**

  Use the command highlighted in red to **start** the CloudBacko Home Services then use the **ps** command. You will see that the CloudBacko Home Services is running, highlighted in red.

```
admin-admins-Mac-2~% sudo /Applications/CloudBacko\ Home.app
/bin/Scheduler.sh

admin-admins-Mac-2~% ps -ef|grep java

0 5735 1 0 9:05PM ttys000 0:02.07 /Applications/CloudBacko Home.app
/jvm/bin/java -Xms128m -Xmx768m -Djava.library.path=. -cp .:./cbs.jar
cbs

/Applications/CloudBacko Home.app

501 5741 5705 0 9:05PM ttys000 0:00.00 grep java
```

Option 2

- **Stop CloudBacko Home Services**

  To **stop** the CloudBacko Home Services, use the command highlighted in red. Use the **ps** command to check if the CloudBacko Home Services has stopped running.

```
admin-admins-Mac-2~% sudo launchctl unload -F
/Applications/CloudBacko\ Home.app/bin/com.cb.scheduler.plist
Password:
admin-admins-Mac-2~% ps -ef|grep java
0 5735 1 0 9:05PM ttys000 0:02.07 /Applications/CloudBacko Home.app
/jvm/bin/java -Xms128m -Xmx768m -Djava.library.path=. -cp .:./cbs.jar
cbs
/Applications/CloudBacko Home.app
501 5741 5705 0 9:05PM ttys000 0:00.00 grep java
```

- **Start CloudBacko Home Services**

  Use the command highlighted in red to start the CloudBacko Home Services then use the ps command.

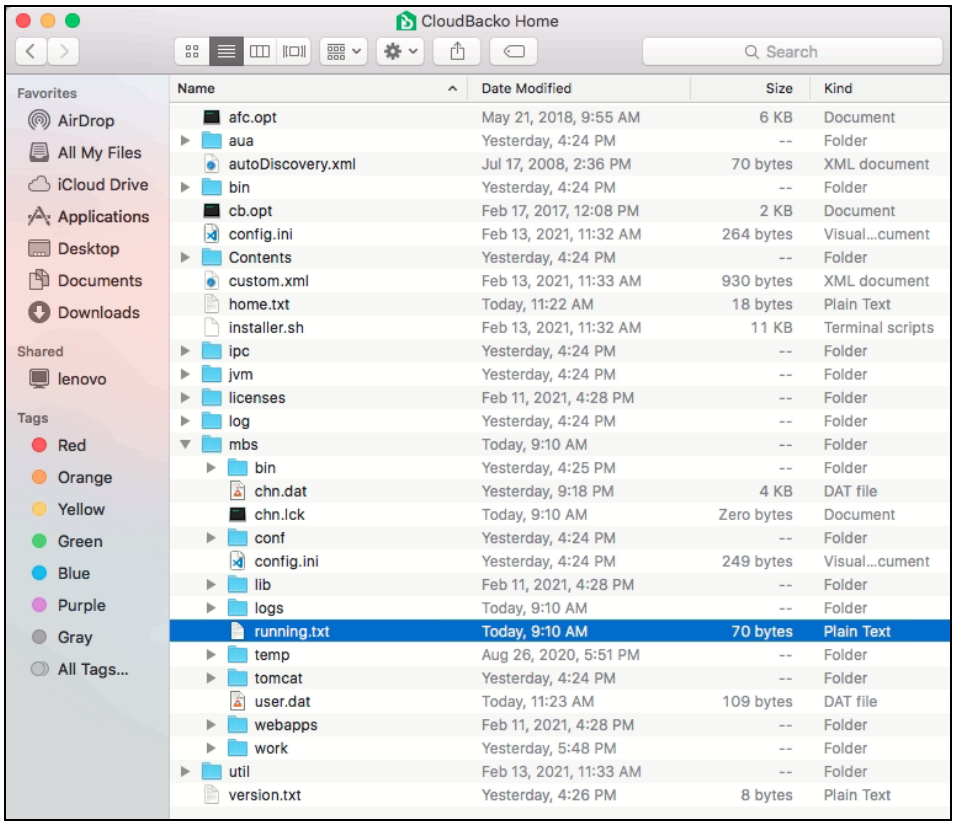
  You will see that the CloudBacko Home Services is running, highlighted in red.

```
admin-admins-Mac-2~% sudo launchctl load -F /Applications/CloudBacko\
Home.app/bin/com.cb.scheduler.plist
Password:
admin-admins-Mac-2~% ps -ef|grep java
0 5805 1 0 9:21PM ?? 0:01.92 /Applications/CloudBacko
Home.app/jvm/bin/java -
Xms128m -Xmx768m - Djava.class.path=/Applications/CloudBacko Home.app
/bin:/Applications/CloudBacko Home.app/bin/cbs.jar -
Djava.library.path=/Appli
cations/CloudBacko Home.app/bin cbs /Applications/CloudBacko Home.app
501 5811 5793 0 9:21PM ttys000 0:00.00 grep java
```

5.5 Mobile Backup Server (MBS) Health Check and CloudBacko app connection Check

Before starting a backup on your mobile device, check the following first:

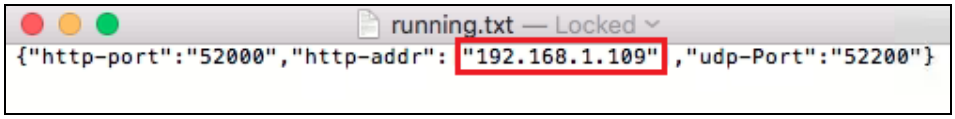
1. Check the IP address, HTTP port, and UDP port in the “running.txt” file. Go to */Applications/CloudBacko Home/mbs*.



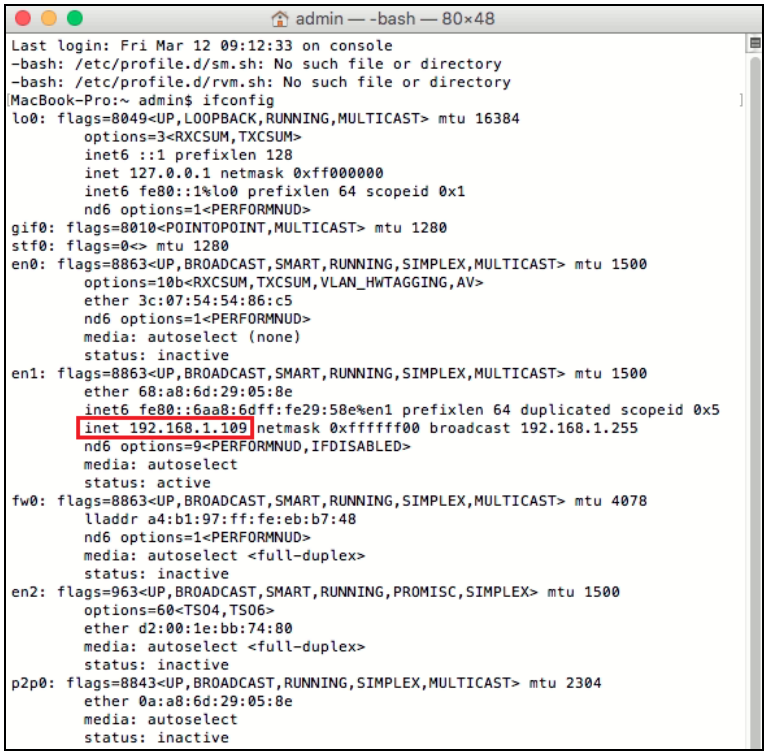
NOTE:

If the “running.txt” file does not exist then the MBS is not running, restart the CloudBacko Home services

After opening the file it will show the HTTP port, IP address, and UDP port which are in actual use by the MBS.

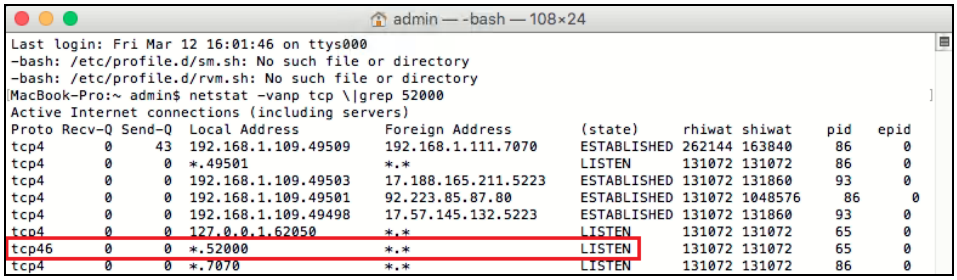


2. Open a command prompt and check if the IP address captured in the running.txt is the correct IP address of the machine where CloudBacko Home is installed.



3. To verify the actual HTTP port used by MBS, type the command:

```
MacBook-Pro:~ admin$ netstat -vanp tcp \|grep 52000
```

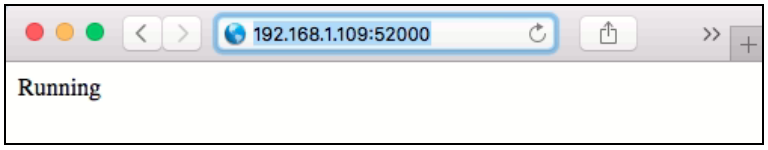


4. Make sure that your firewall setting allows network traffic through the following HTTP and UDP ports to ensure that the communication between your machine and mobile device is successful, otherwise mobile backup and restore will not work.

5. To perform a health check on the MBS. Open a browser on the CloudBacko Home machine and type the IP address, followed by TCP port.

   For example: If the HTTP port used is 52000, http://192.168.109:52000, you should get the following result that shows the “Running” status, which means that the MBS is running.

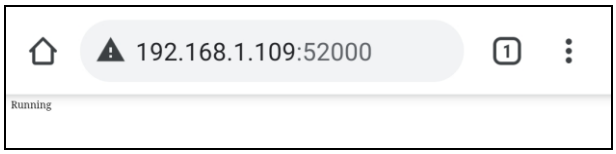
   In the CloudBacko Home machine



6. To run a connection test between the mobile device and machine, open a browser in your mobile device and type the IP address, followed by TCP port.

   For example If the HTTP port used is 52000, http://192.168.109:52000 you should get the following result, which shows the “Running” status. This means that the CloudBacko app can successfully connect to the MBS and both backup and restore can proceed on the mobile device.

   In the mobile device



6 Start CloudBacko Home

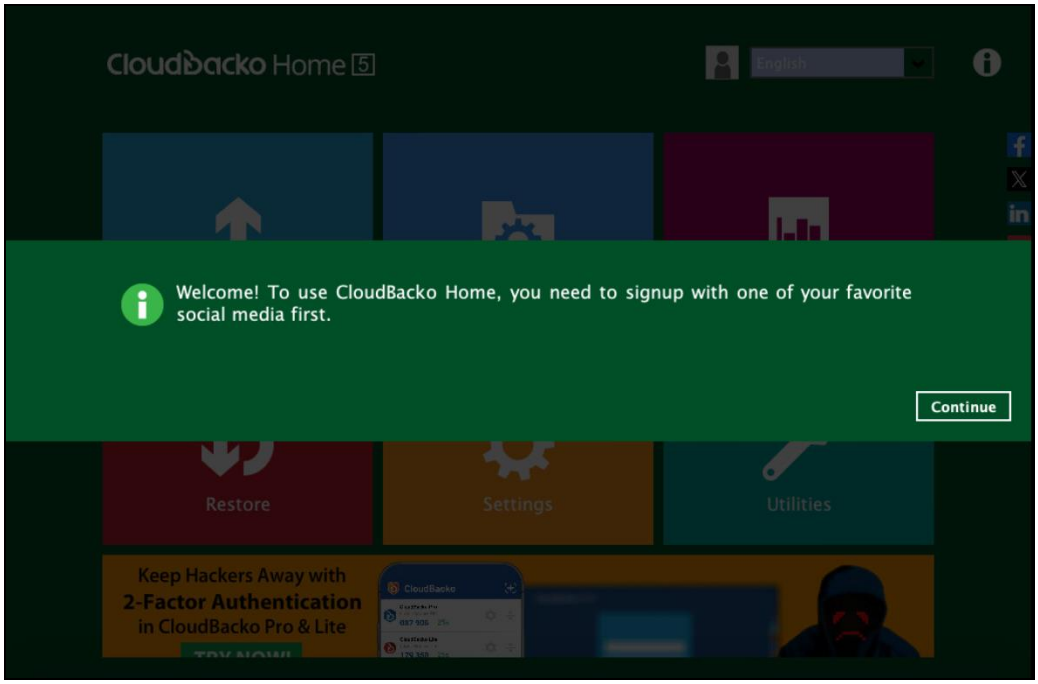
Several scenarios will be encountered during log in. Login steps for the different scenarios will be discussed in this chapter.

6.1 Setup CloudBacko Home

Before using CloudBacko Home, it is required to set it up by signing in to one of the available social media accounts. This is a one-time setup only even when upgrading to a newer version.

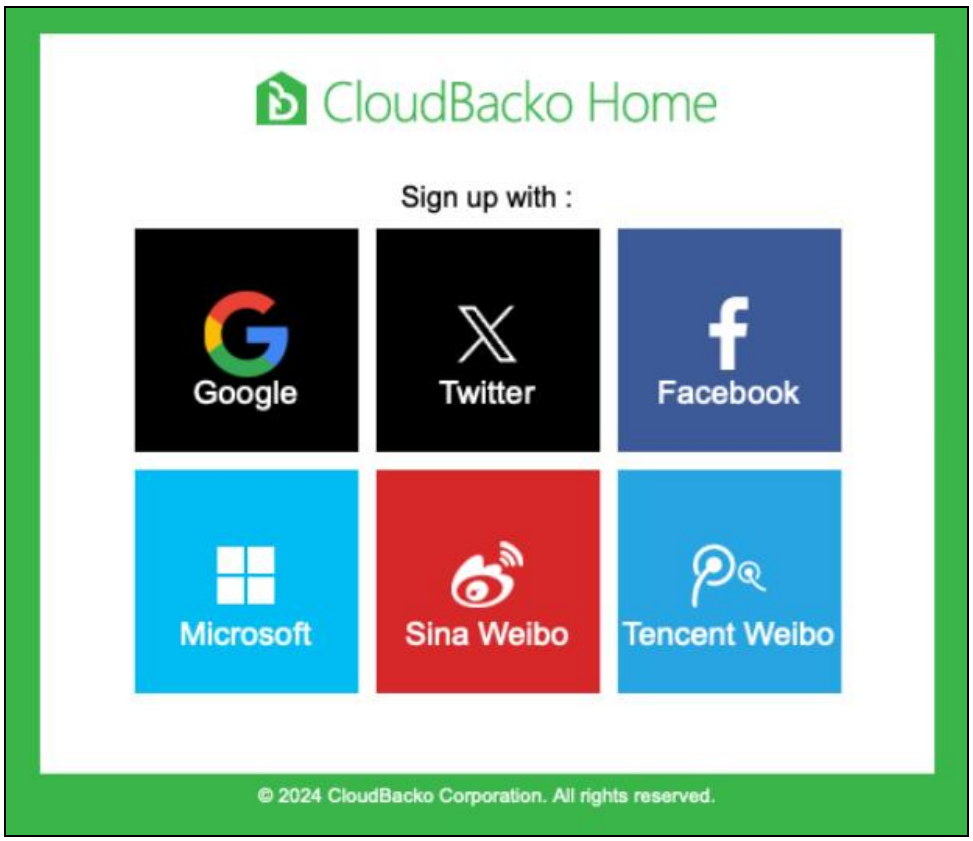
1. Double-click the **CloudBacko Home** icon to launch the application.

2. The following screen will appear. On the first launch of CloudBacko Home, it is required to sign up to one of the social media accounts. Click **Continue** to proceed.

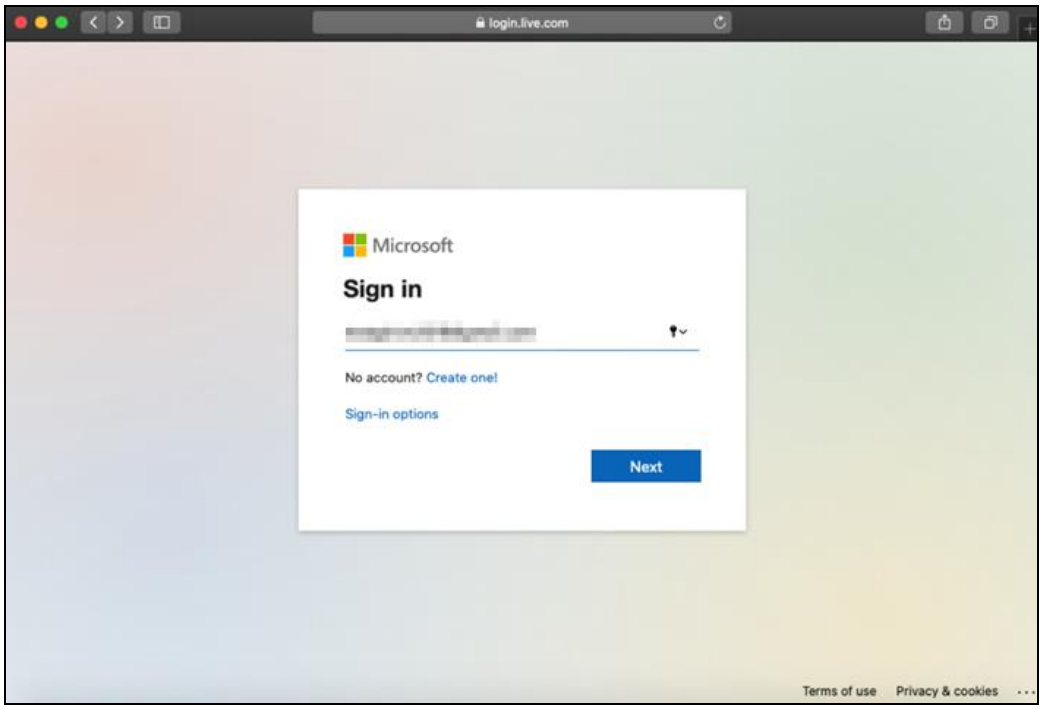


3. This will redirect to a web browser where you can choose from the following social media platforms:

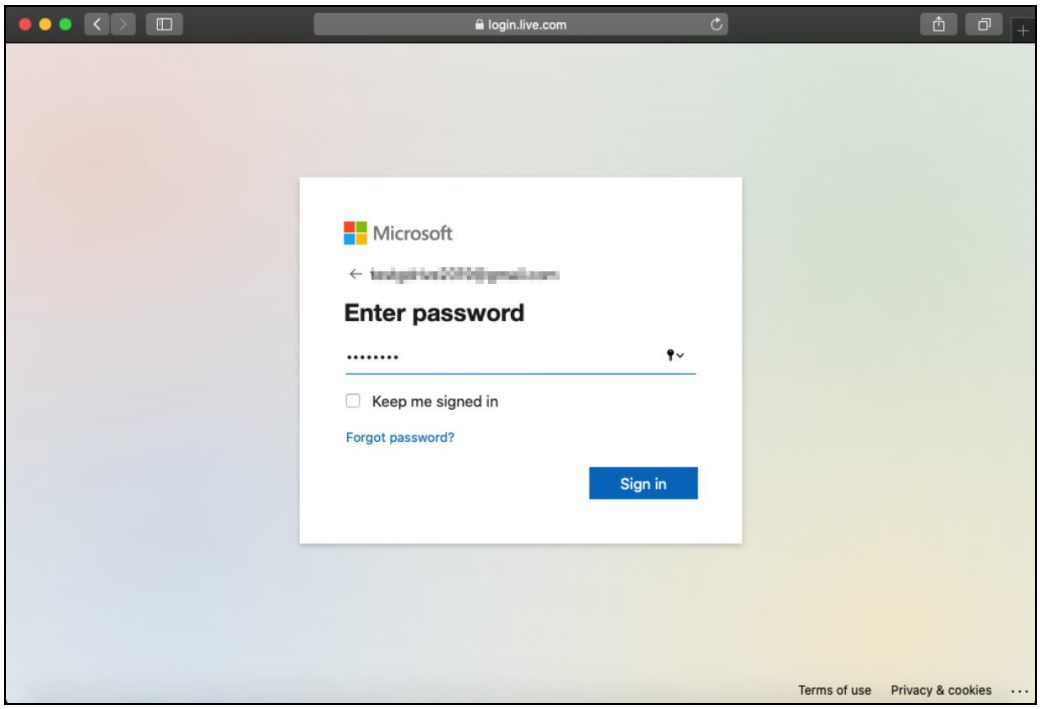
    Google
    Twitter
    Facebook
    Microsoft
    Sina Weibo
    Tencent Weibo



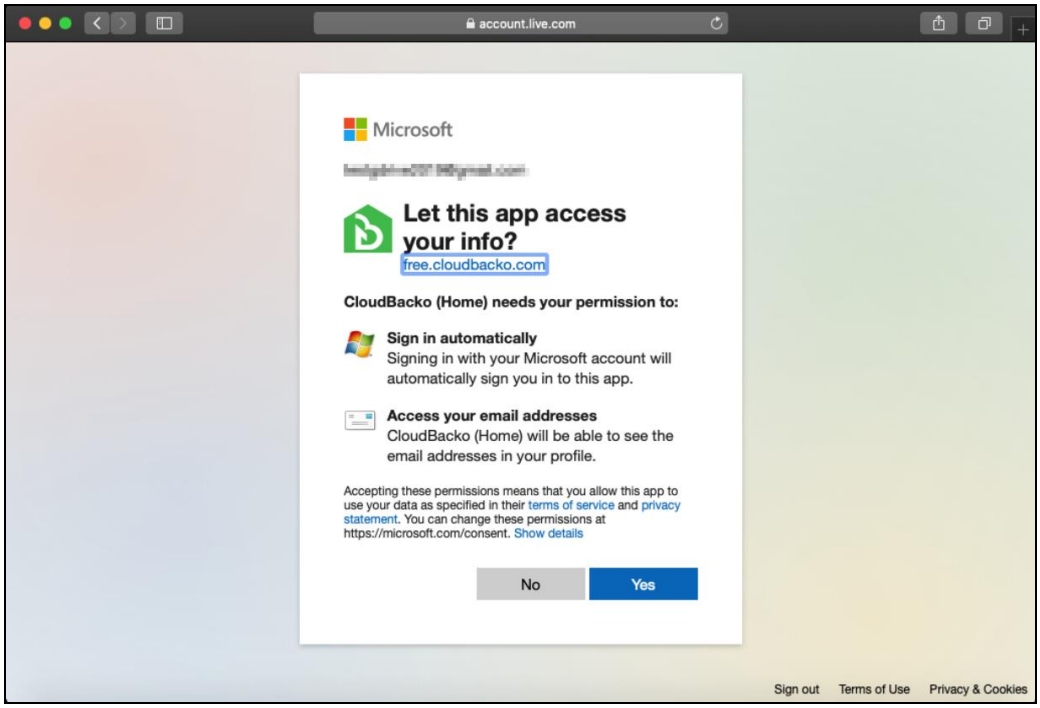
In this example, Microsoft is selected. Input a valid email address then click **Next** to proceed.


login.live.com
Microsoft
Sign in
No account? Create one!
Sign-in options
Next
Terms of use
Privacy & cookies

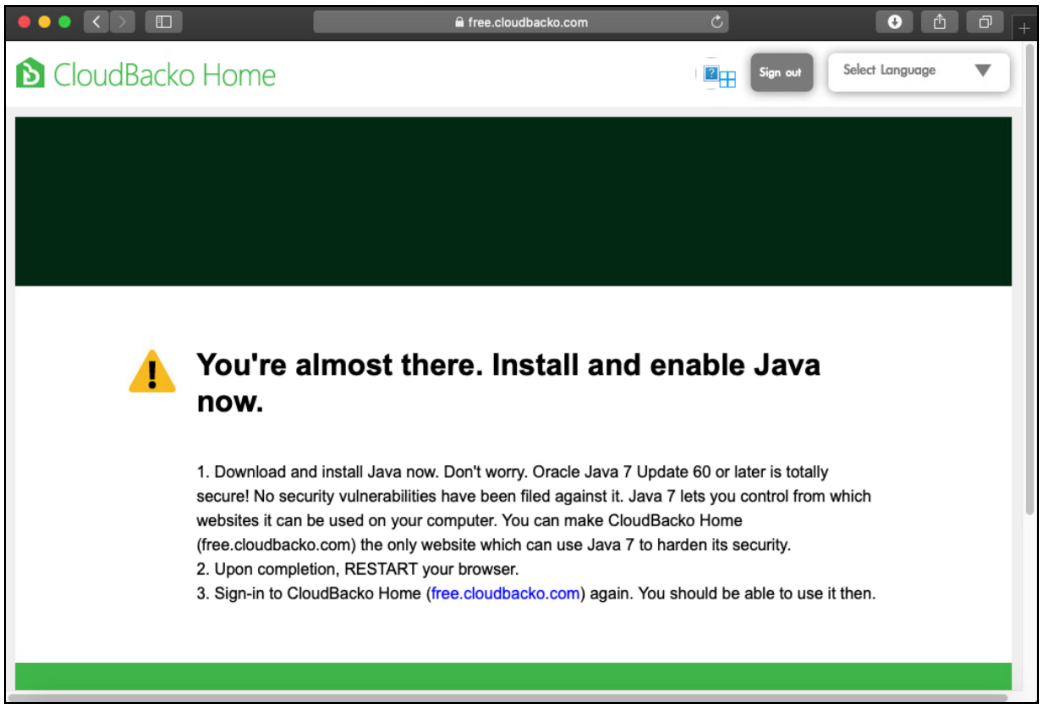
Enter a valid password then click **Sign in** to proceed.



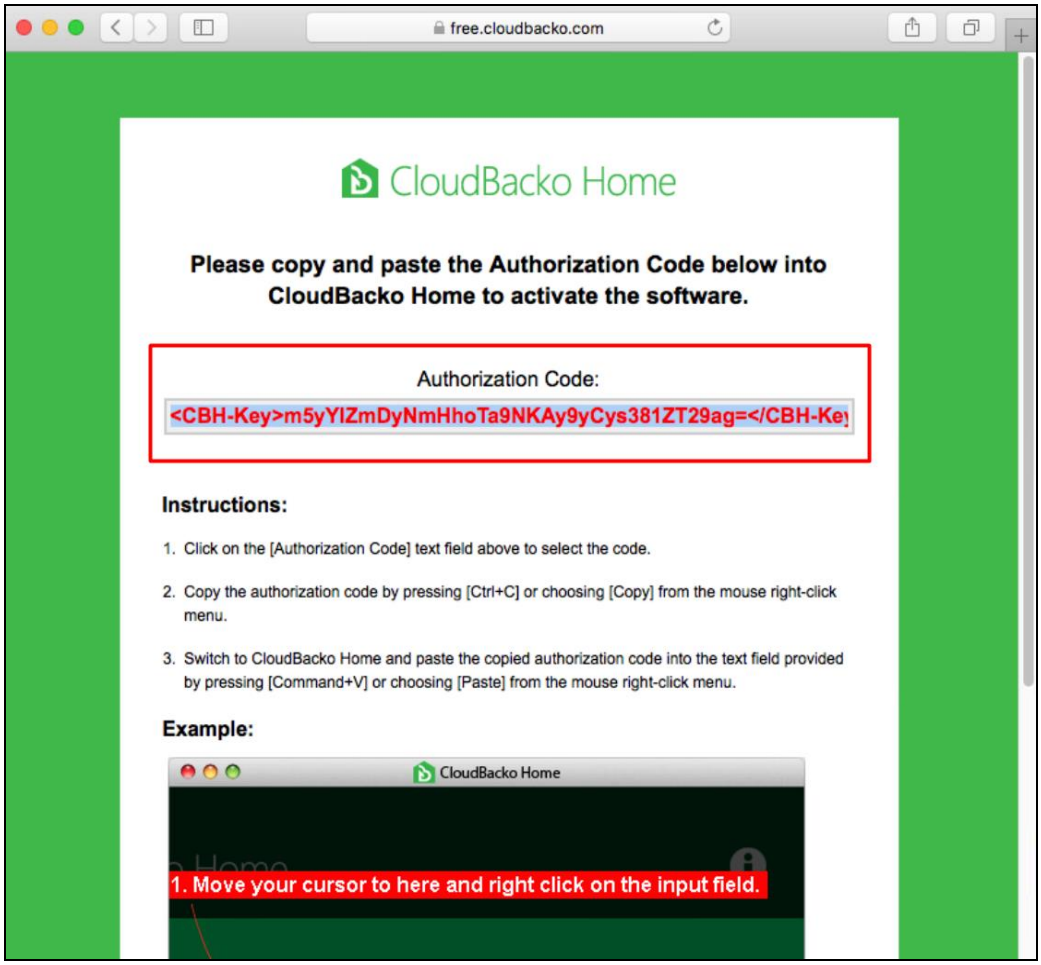
4. Click **Yes** to allow CloudBacko Home to access the Microsoft account.

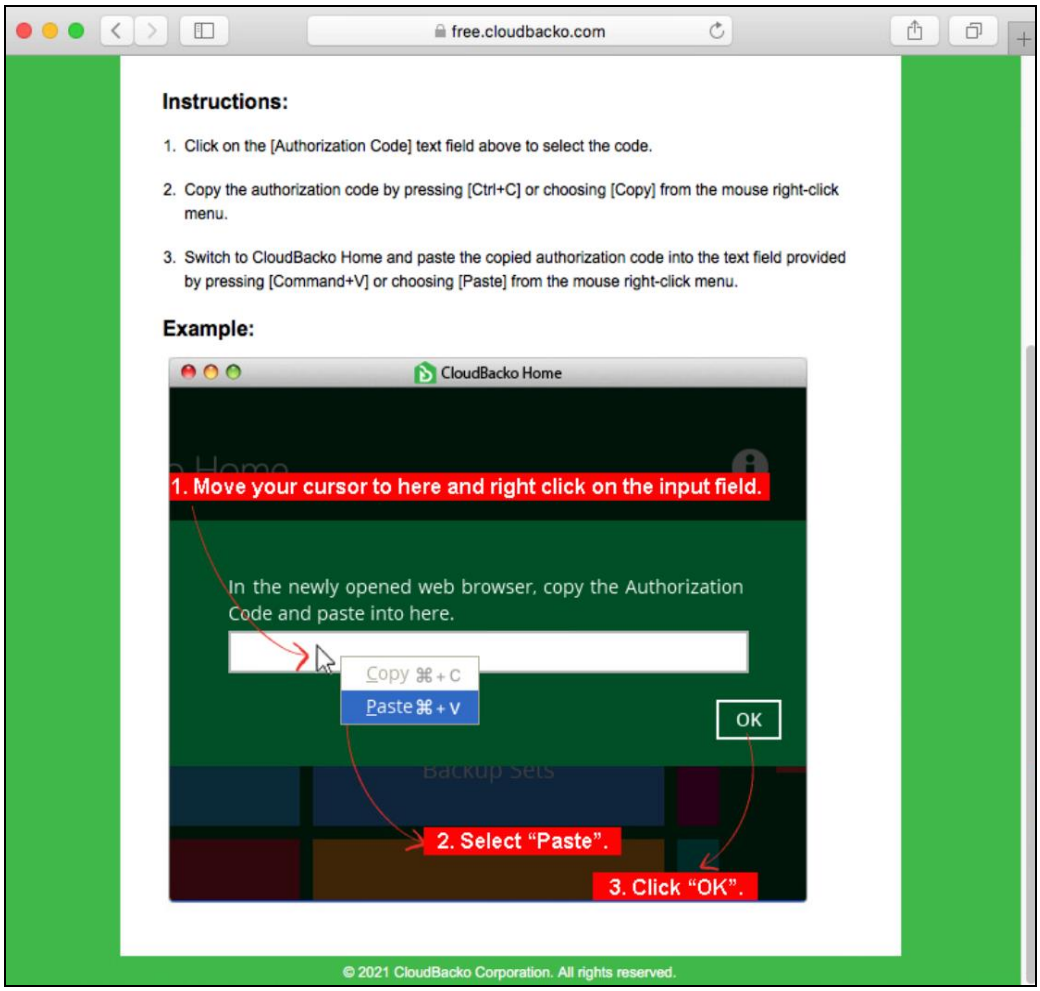


Note: This warning message will appear to install and enable Java.

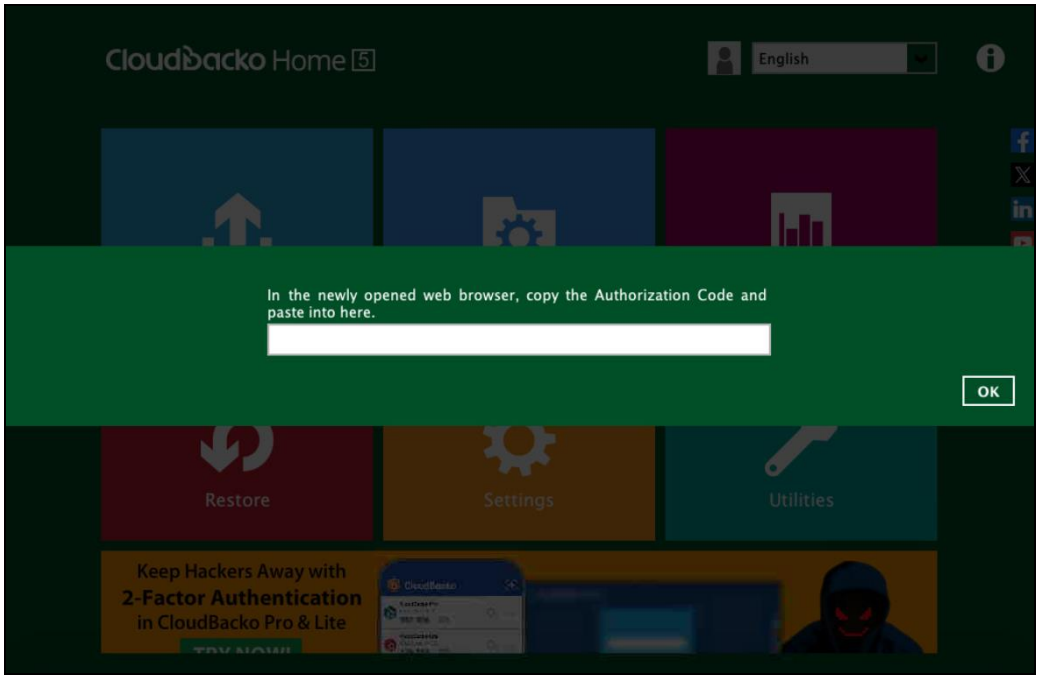


The CloudBacko Home authorization code will be displayed. Copy and paste the authorization code to CloudBacko Home. You may scroll-down the screen to see the detailed steps.

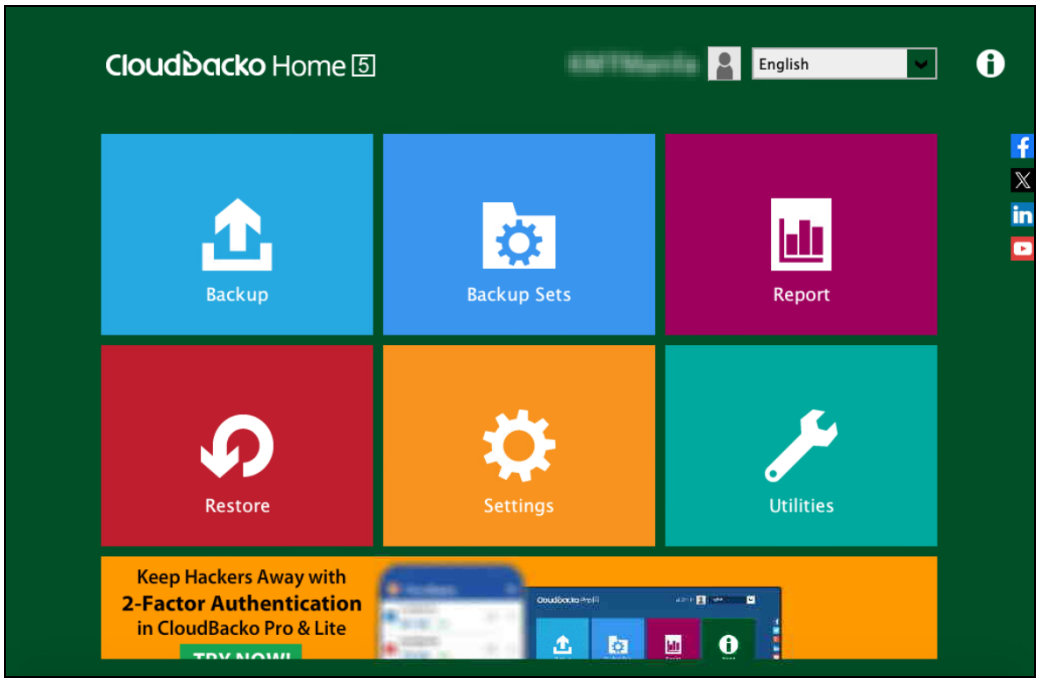




5. After pasting the copied authorization code, click **OK** to proceed.



6. The CloudBacko Home main screen will be displayed after a successful setup.

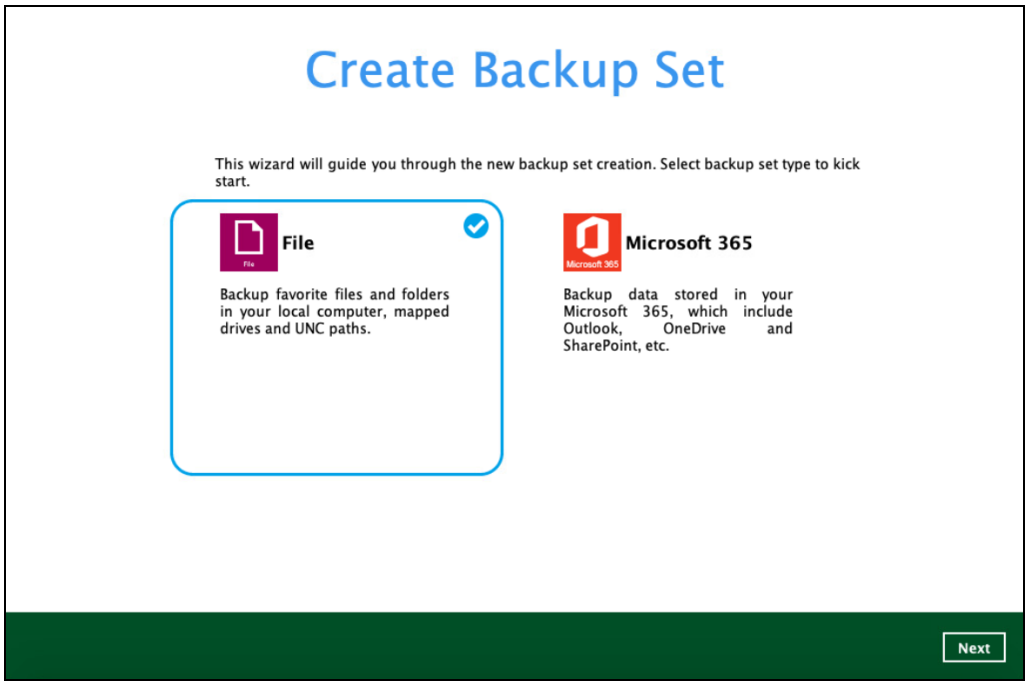


6.2 Launch CloudBacko Home

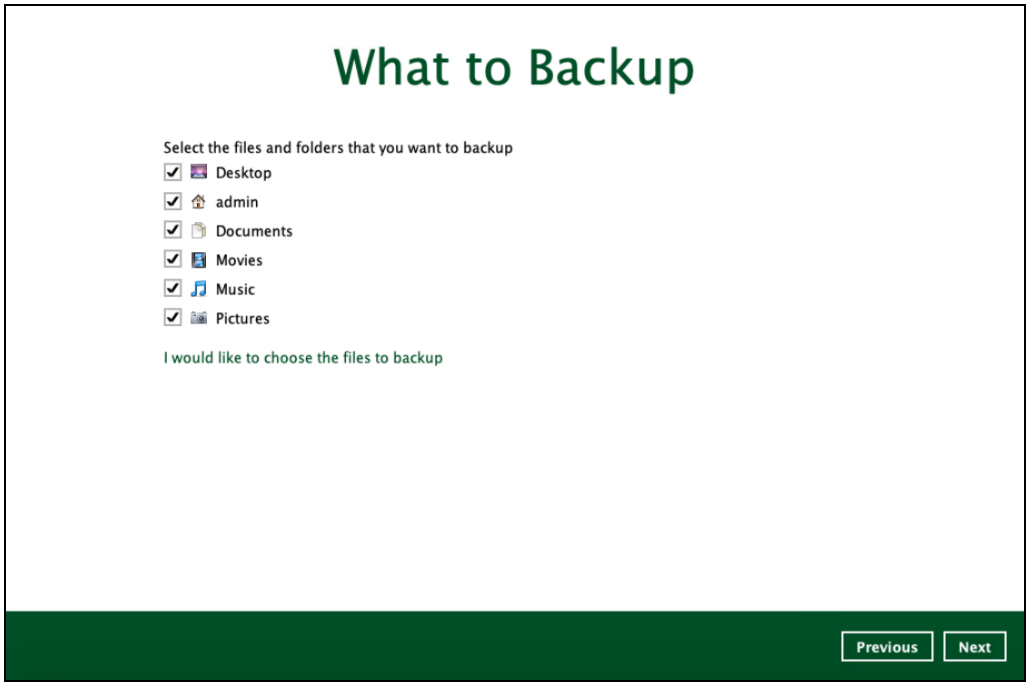
6.2.1 Initial launch creating backup set and setting up mobile backup

When launching the CloudBacko Home for the first time, creating a backup set and setting up mobile backup feature, please follow the steps below:

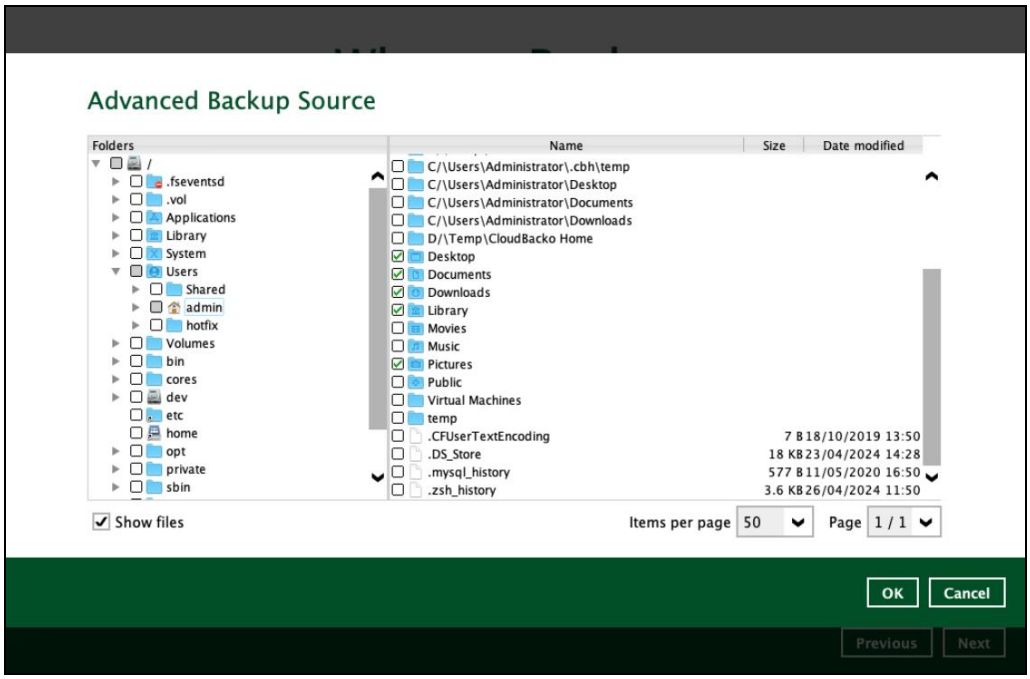
1. Select the type of backup set to create, whether File or Microsoft 365.



2. In the **What to Backup** window, select the backup source for your backup set. Click **I would like to choose the files to backup** if you would like to select files for backup individually.

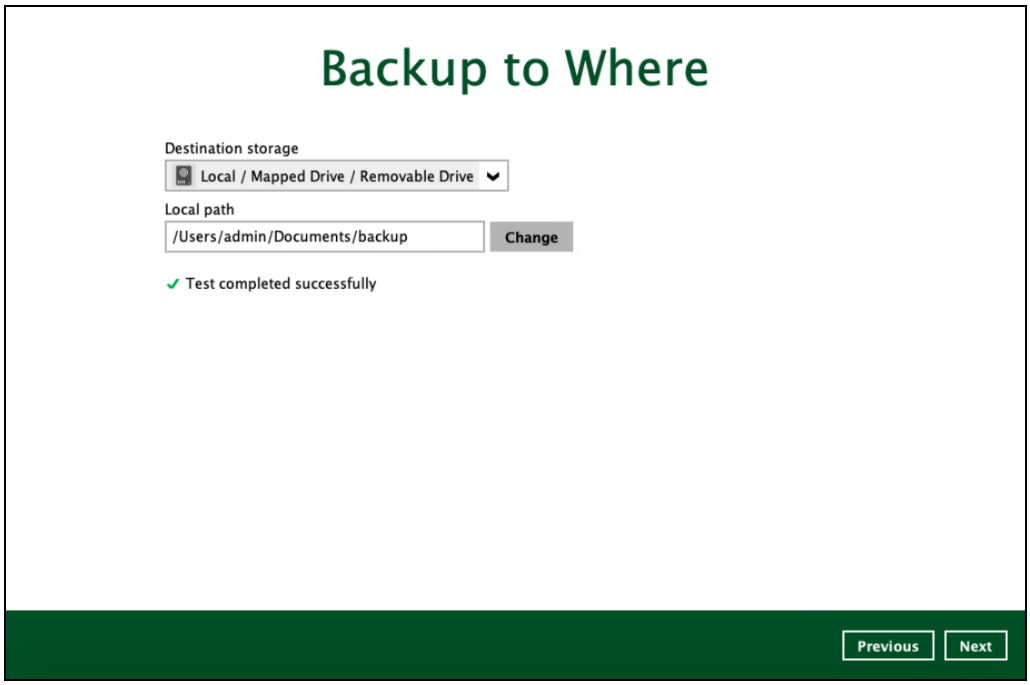


Click **I would like to choose the files to backup** if you would like to select specific files/folders to backup.

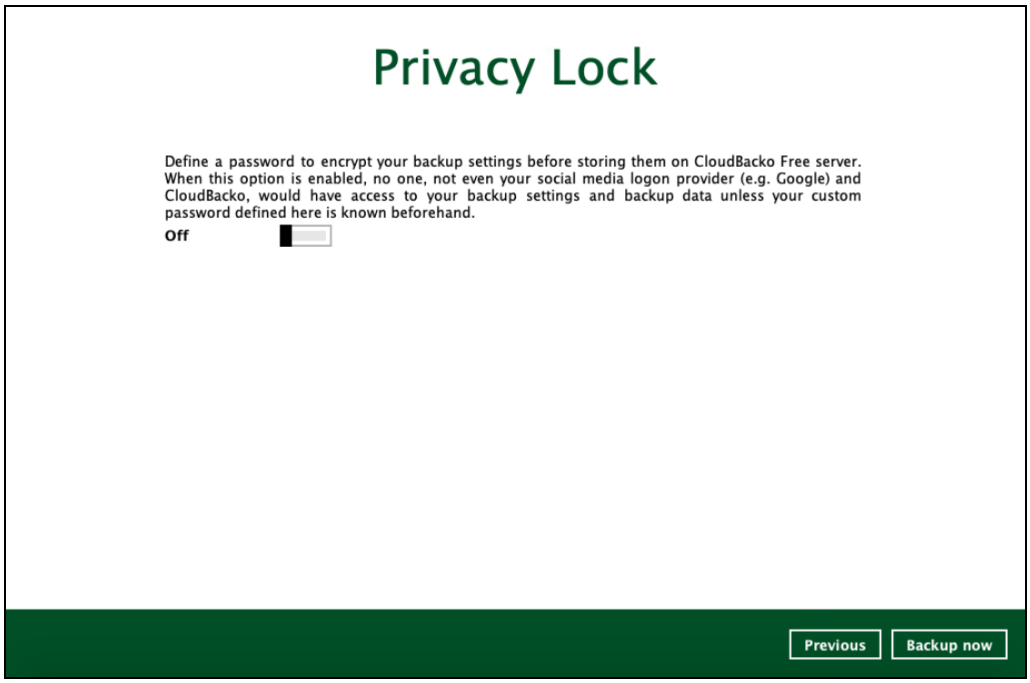


Once done selecting items to back up in the **What to Backup** window, click **Next** to proceed.

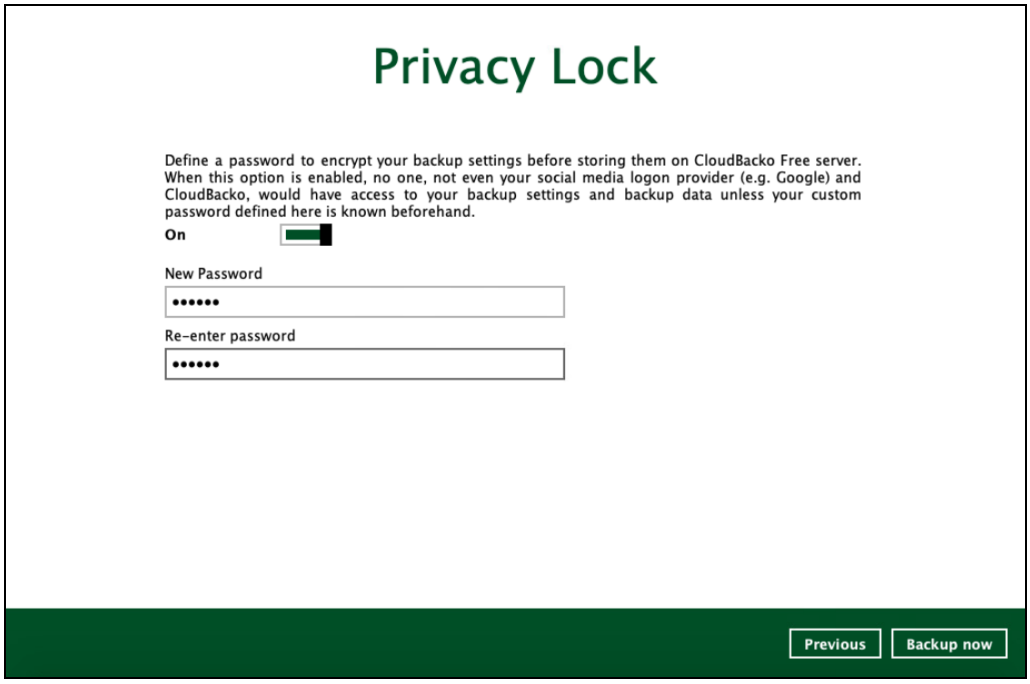
3. The **Backup to Where** window will appear. Select a backup destination for the backup data storage, then click **Next** to proceed.



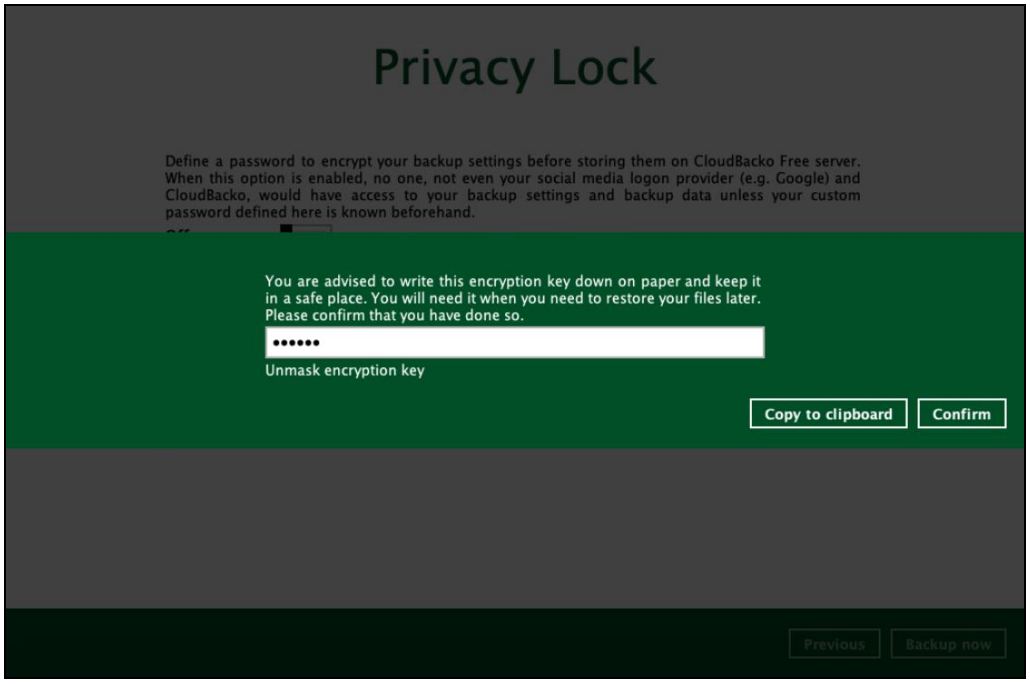
4. Slide the switch to the right hand to turn on the Privacy Lock.



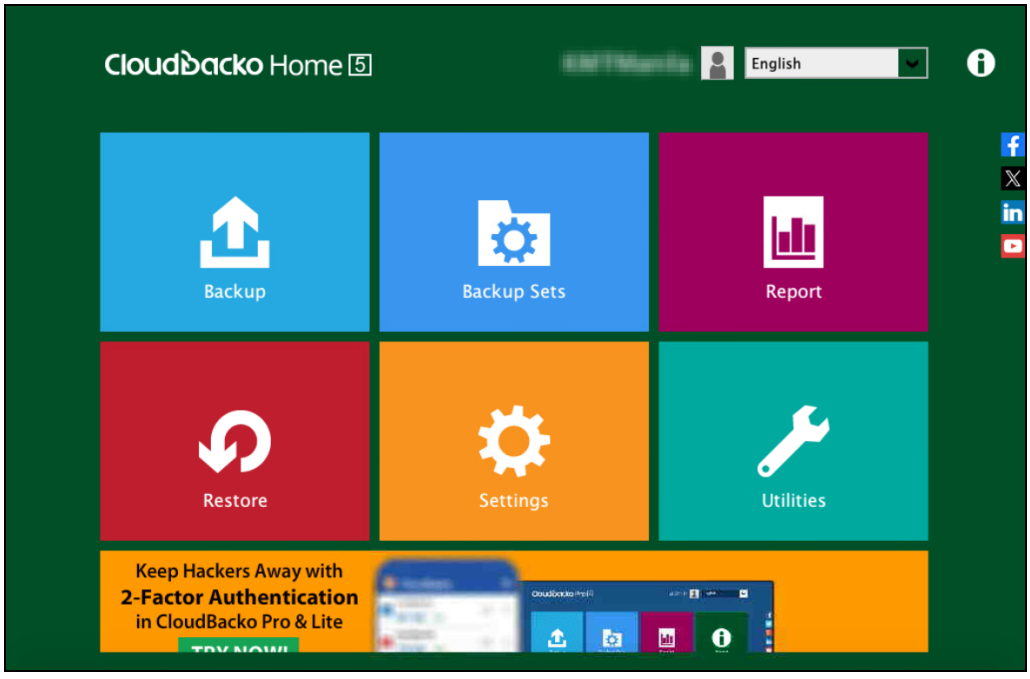
Enter new password and re-enter password for confirmation. Once done with the setup, click **Backup Now**.



5. Click **Copy to clipboard** to copy the encryption key or click **Confirm** to start the backup process.



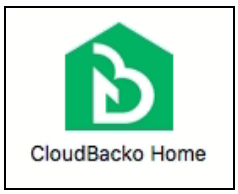
6. After successful backup, the following screen will appear.



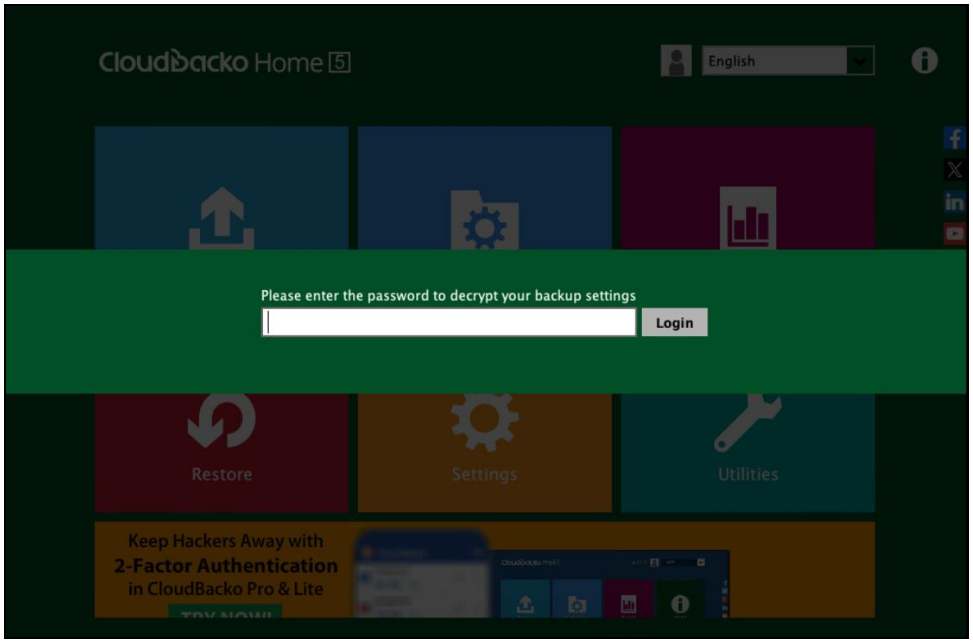
6.2.2 Subsequent login with privacy lock

For succeeding logins to CloudBacko Home with privacy lock, please follow the steps below:

1. Double-click the **CloudBacko Home** icon to launch the application.



2. Enter password for privacy lock.

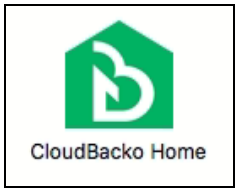


3. The following screen will appear.

6.2.3 Subsequent login with no privacy lock

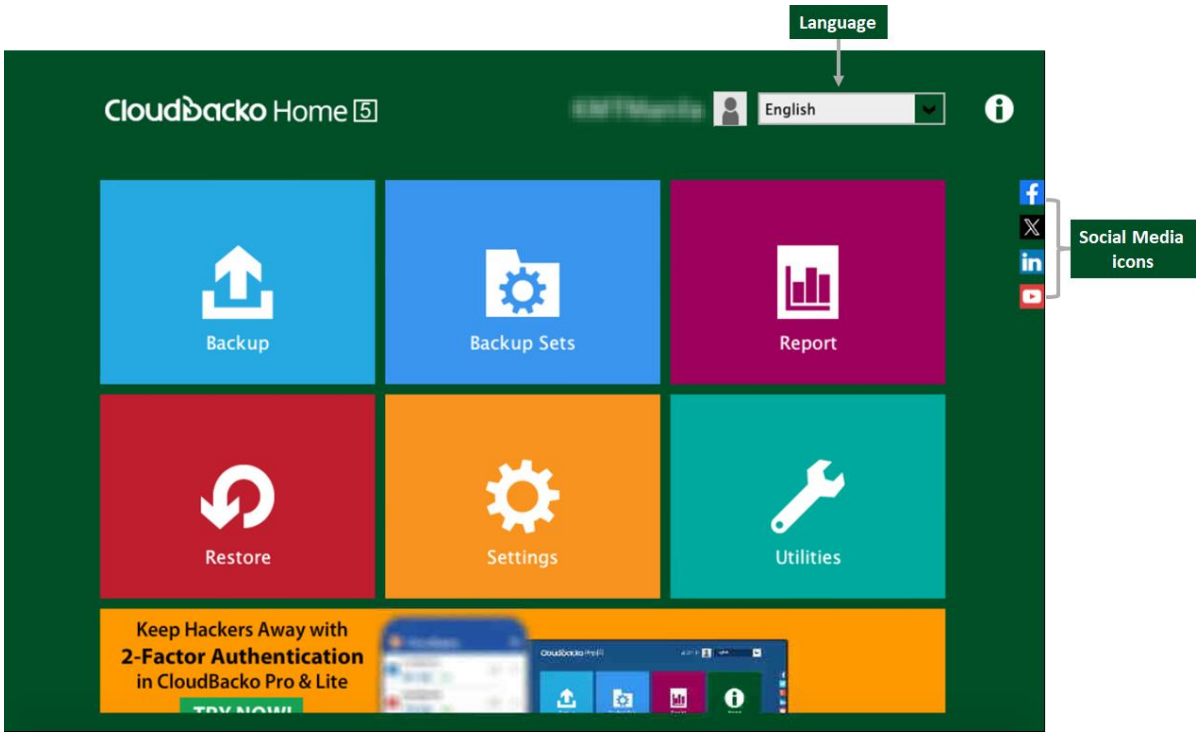
For succeeding logins to CloudBacko Home with no privacy lock, please follow the steps below:

1. Double-click the **CloudBacko Home** icon to launch the application.



2. The following screen will appear.

7 CloudBacko Home Overview

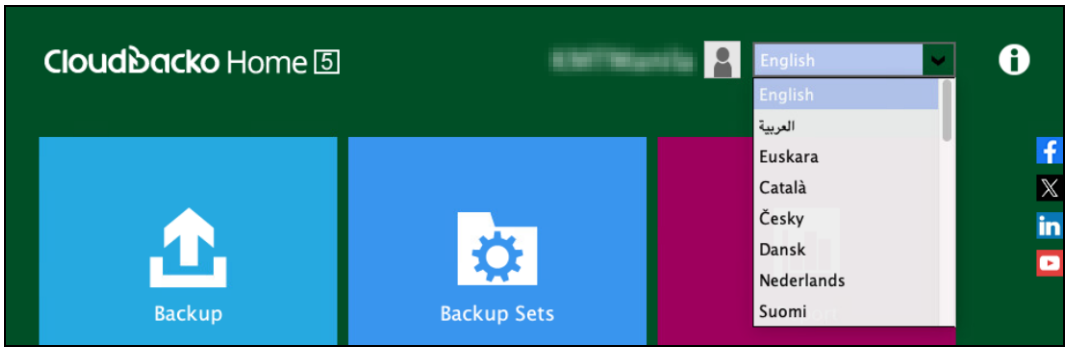


CloudBacko Home main interface has nine (9) icons that can be accessed by the user:

- Language
- About
- Backup
- Backup Sets
- Report
- Restore
- Settings
- Utilities
- Social Media Icons

7.1 Language

This option is used to change the language of the CloudBacko Home interface. The list of the available languages depends on the backup service provider.



Once the language is set, it will reflect on the CloudBacko Home interface right away.

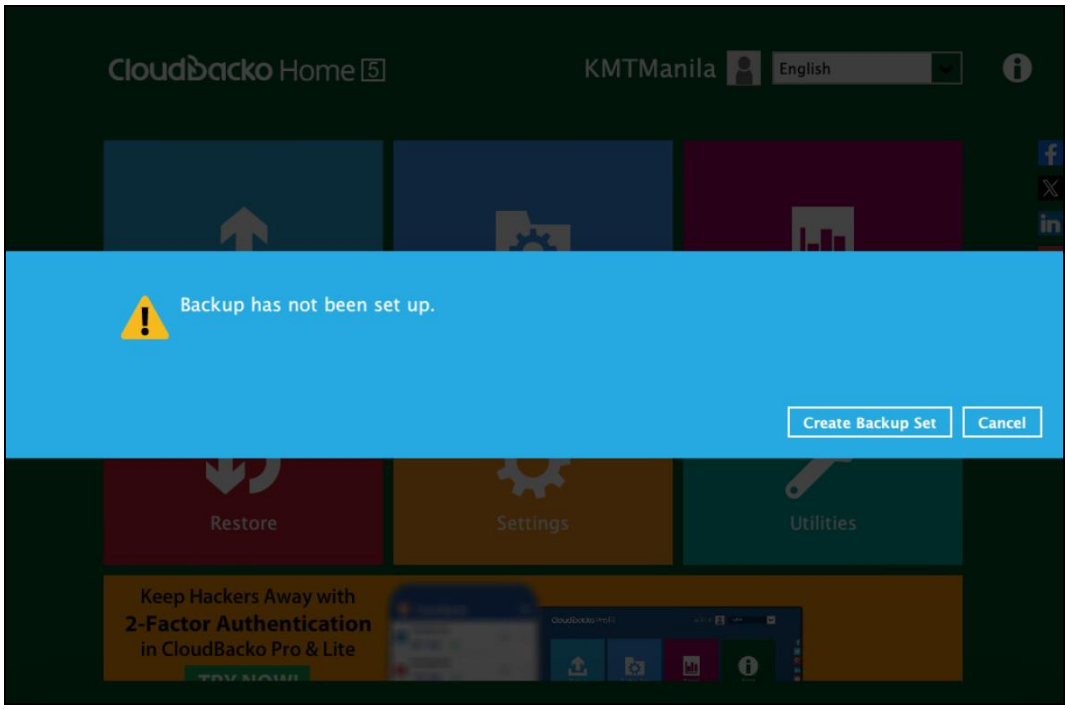
7.2 About

This **About** module displays the product version and system information of the machine where the CloudBacko Home is installed.

7.3 Backup

This feature is used to run your backup set(s).

When using CloudBacko Home for the first time, you will be asked to create a new backup set first.

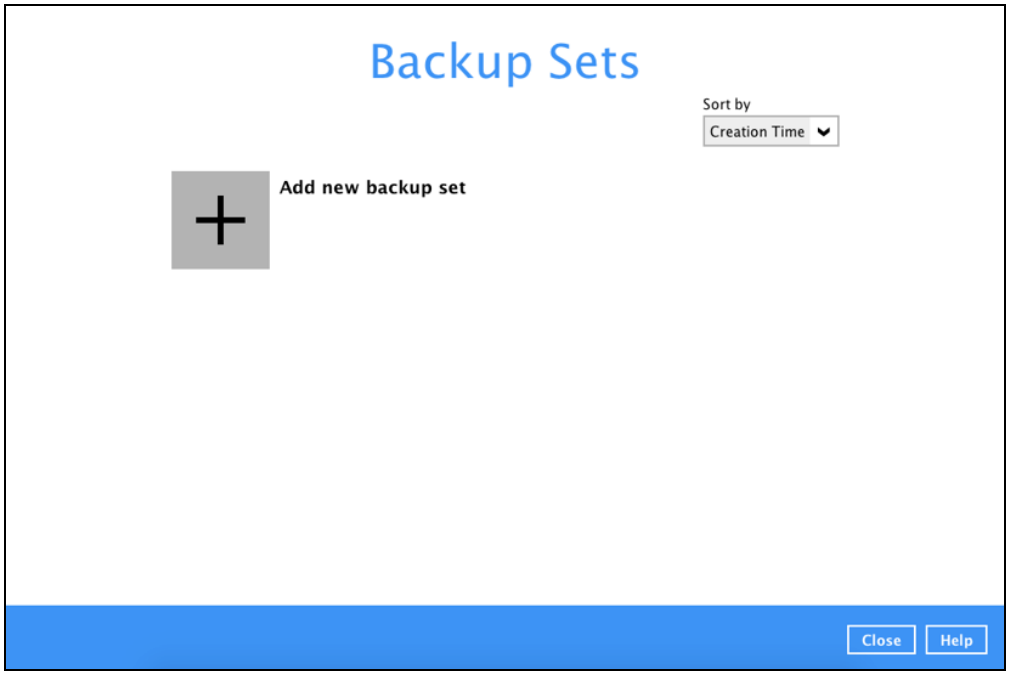


For instructions on how to start a backup, refer to Chapter 10 Run Backup Jobs.

7.4 Backup Sets

The backup set is where you will select files and/or folders to be backed up as well as configure other settings related to it. This feature allows the user to select files individually or an entire folder to backup. It is also used to delete backup set(s).

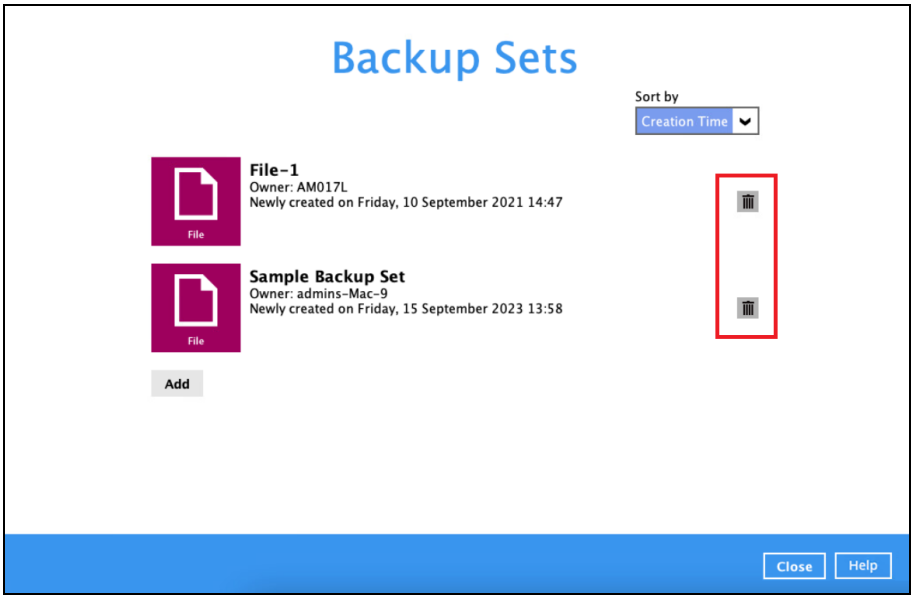
When using CloudBacko Home for the first time, you must add a new backup set first.



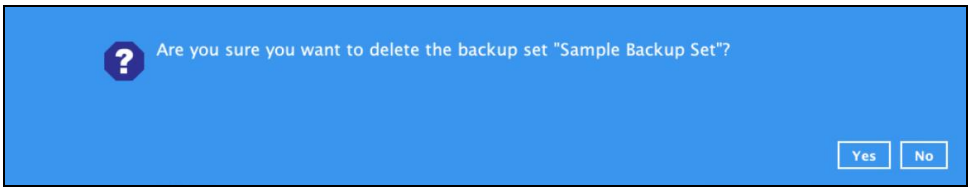
To create or modify a backup set, follow the instructions on Chapter 8 Create a Backup Set.

To delete a backup set, follow the instructions below:

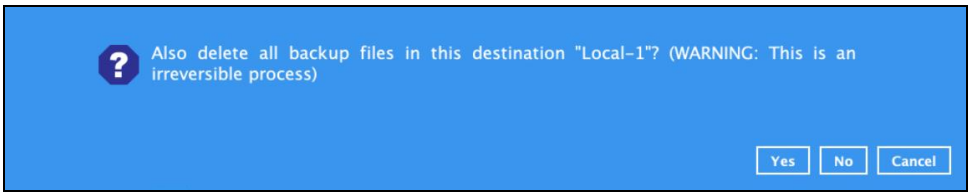
1. Click on the delete icon on the right side of the backup set that you want to delete.



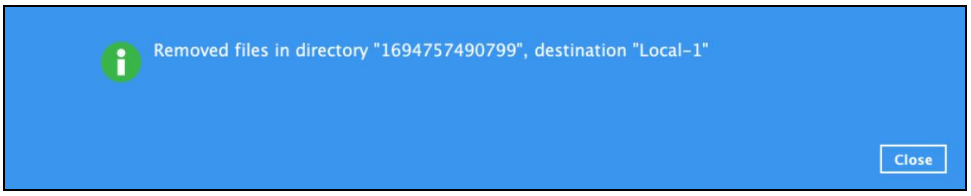
2. Click the Yes button to delete the backup set or click the No button to abort the deletion.



3. If Yes is selected, it will also display another alert message confirming the deletion of all backup files in the destination. Click **Yes** to proceed. Otherwise, click **No** to abort the deletion.



4. The backup set is successfully deleted as well as the files from the directory.



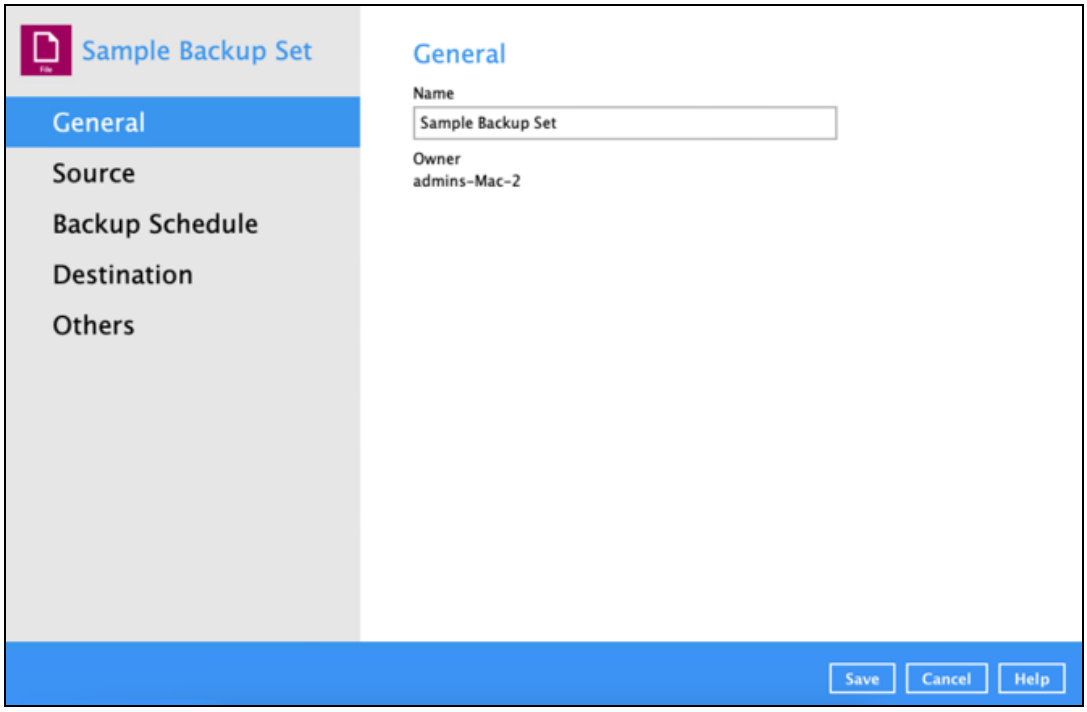
7.4.1 Backup Set Settings

Below is the list of configurable settings under a Backup Set:

- General
- Source
- Backup Schedule
- Destination
- Others
- Delete Backup Set

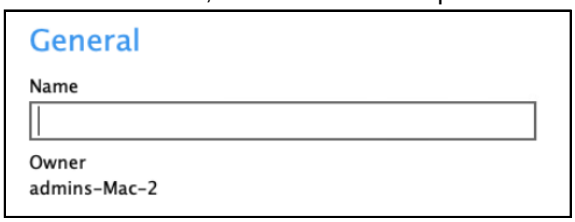
7.4.1.1 General

This feature allows the user to modify the current name of the backup set.

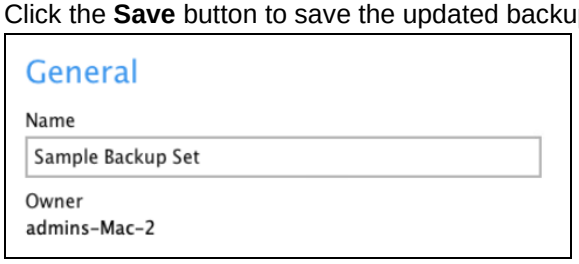


To modify the name of a backup set, follow the steps below:

1. In the Name field, enter a new backup set name.

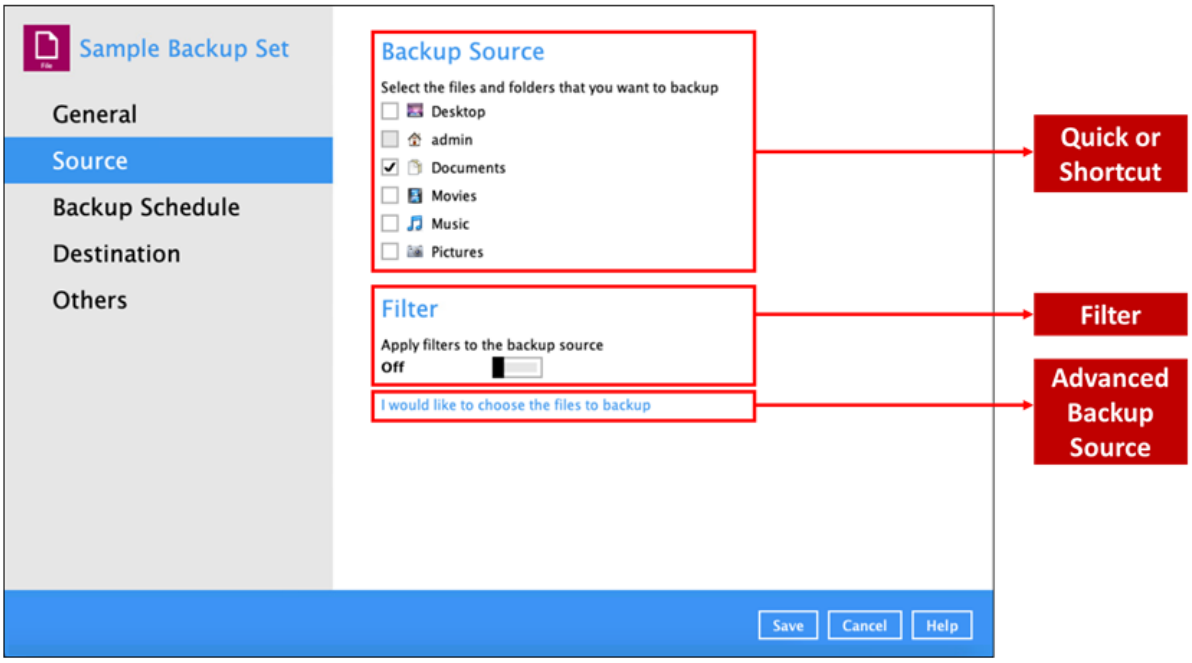


2. Click the **Save** button to save the updated backup set name.



7.4.1.2 Source

This feature allows the user to select files and/or folders in the backup source.

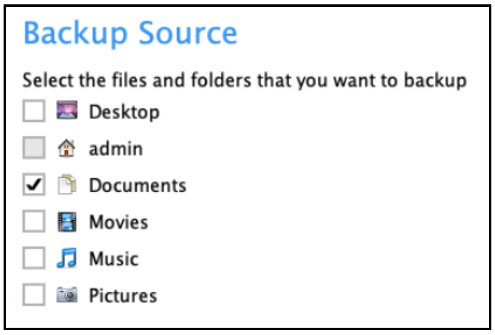


There are three (3) ways to select files and/or folders to back up:

Option	Description
Quick or Shortcut	This allows the user to back up files and/or folders in the selected backup source entirely.
Filter	This allows the user to select or exclude files and/or folders from the backup job.
Advanced Backup Source	This allows the user to select files and/or folders individually to back up.

Option 1: Quick or Shortcut

This option allows the user to quickly select a backup source to be backed up. For our example below, we assume the account name is admin.



To know the locations of the folder(s) that will be backed up for each selected backup source, refer to the following table:

Backup Source		Description
Desktop		If Desktop is selected, all files and/or folders in the following location will be backed up: ***%UserProfile%/Desktop*** Example: If the account name is **admin**, the location is ***/Users/admin/Desktop***
Admin		If home for admin is selected, all files and/or folders located in the following location ***/Users/admin/*** will be backed up this includes: ***/Users/admin/Desktop*** ***/Users/admin/Documents*** ***/Users/admin/Downloads*** ***/Users/admin/Movies*** ***/Users/admin/Music*** ***/Users/admin/Pictures*** ***/Users/admin/Public*** This selection also includes some macOS system level folders and CloudBacko system folders which are hidden. It is recommended these folders are excluded from the backup source using the Exclude Filter. ***/Users/admin/Library*** ***/Users/admin/Downloads*** ***/Users/admin/.Trash*** ***/Users/admin/.bash_sessions*** ***/Users/admin/.cbh*** **Note**: If you select admin during the creation of backup set, the entire Backup Source in the Quick or Shortcut option will also be selected (e.g. Desktop, Documents, Movies, Music, and Pictures), but you may choose to unselect any of each.

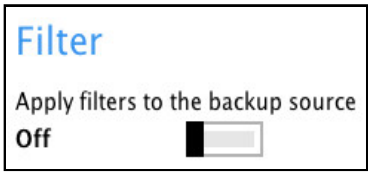
Documents		If Documents is selected, all files and/or folders located in the following location will be backed up: ***%UserProfile%/Documents*** Example: If the account name is **admin**, the location is ***/Users/admin/Documents***
Movies		If Movies is selected, all files and/or folders located in the following location will be backed up: ***%UserProfile%/Movies*** Example: If the account name is **admin**, the location is ***/Users/admin/Movies***
Music		If Music is selected, all files and/or folders located in the following location will be backed up: ***%UserProfile%/Music*** Example: If the account name is **admin**, the location is ***/Users/admin/Music***
Pictures		If Pictures is selected, all files and/or folders located in the following location will be backed up: ***%UserProfile%/Pictures*** Example: If the account name is **admin**, the location is ***/Users/admin/Pictures***

To select files and/or folders to back up using the Quick or Shortcut option, follow the steps below:

1. Select a backup source.
2. Click the **Save** button to store the selected backup source.

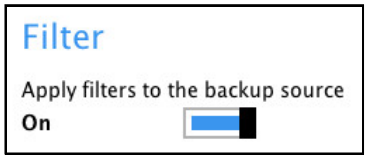
Option 2: Filter

This option allows the user to manually select files and/or folders in the selected location(s) to back up.



To select files and/or folders to back up using the Filter Backup Source, follow the steps below:

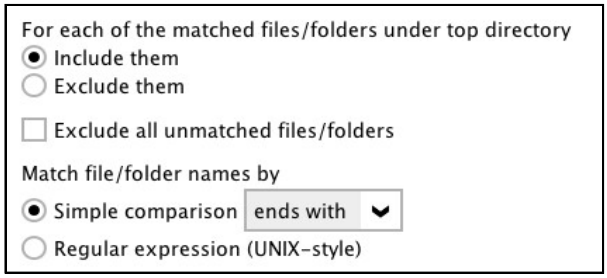
1. Slide the lever to the right to turn on the filter setting.



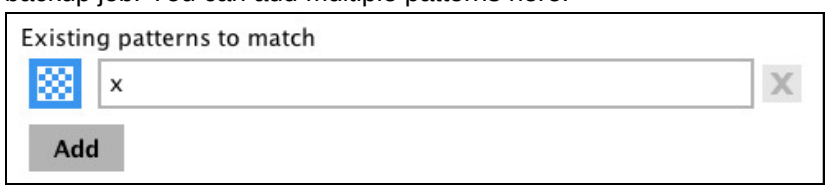
2. Click the **Add** button to create a filter.

3. Assign a desired name to the backup filter.

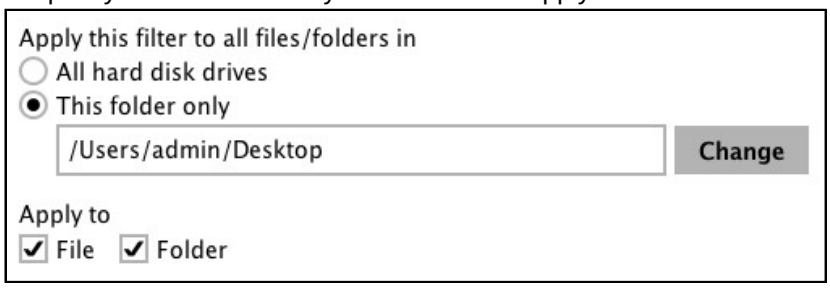
4. Configure the following options.



5. In this example, all files and/or folders that end with the letter 'X' will be included to the backup job. You can add multiple patterns here.

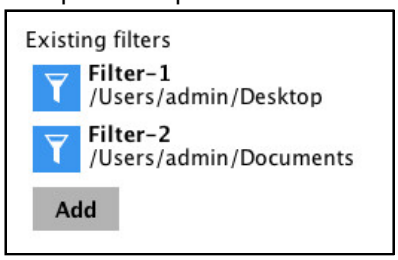


6. Select whether you would like to apply the filter to all files and/or folders in all hard disk drives or to a specific folder only. If 'This folder only' is selected, click the [Change] button to specify the folder where you would like to apply the filter to.



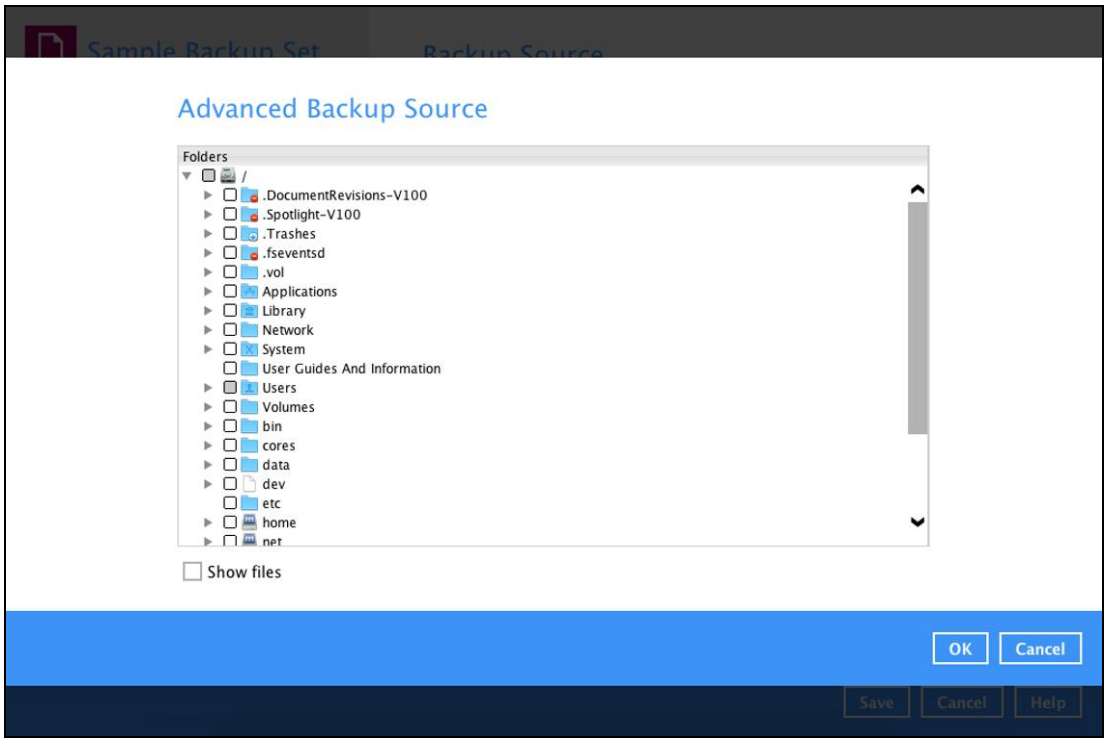
7. Click the **OK** button to save the created filter, then click the **Save** button to store settings. Once you run a backup, all files and/or folders that match the applied filter will be backed up.

8. Multiple backup filters can be created by clicking the **Add** button.



Option 3: Advanced Backup Source

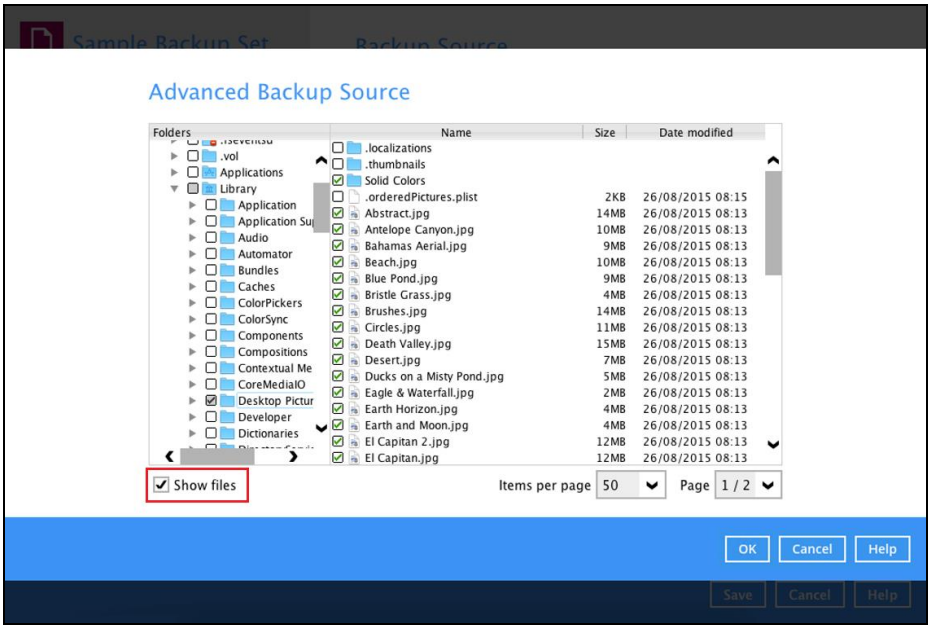
This option allows the user to display the locations in the backup source to select files and/or folders to back up.



To select files and/or folders using the Advanced Backup Source, follow the steps below:

1. In the Source window, select 'I would like to choose the files to backup'.

2. Select 'Show files' to display the files inside each folder, then select the files and/or folders that you would like to back up.



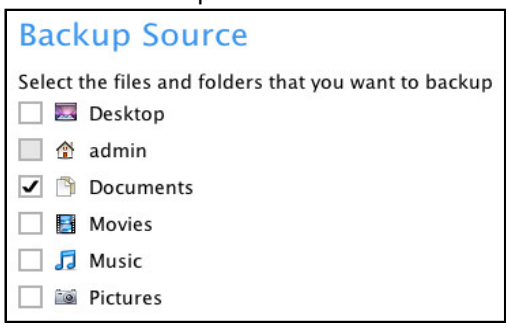
3. Click the **OK** button to save the selection, then click the **Save** button to store settings.

In selecting files and/or folders to back up, the three (3) options can be used simultaneously. For more details, please refer to the example scenarios below:

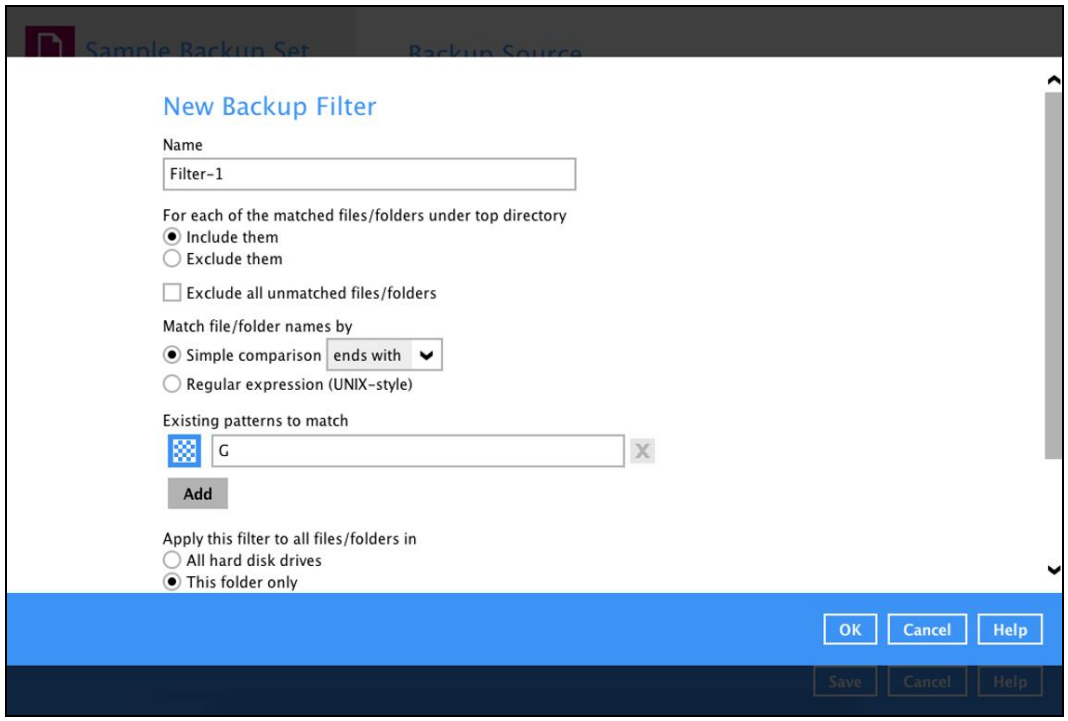
Scenario 1 (Quick or Shortcut + Filter)

You can use the quick or shortcut option and apply filter to the selected backup source at the same time. To use this type of combination, follow the steps below:

1. Choose a backup source.



2. Create a filter that will be applied to the backup source.

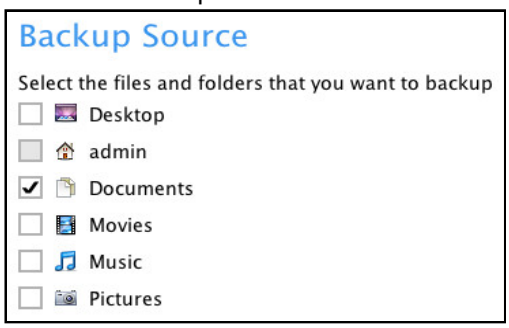


3. Click the **OK** button to save the created filter, then click the **Save** button to save settings.

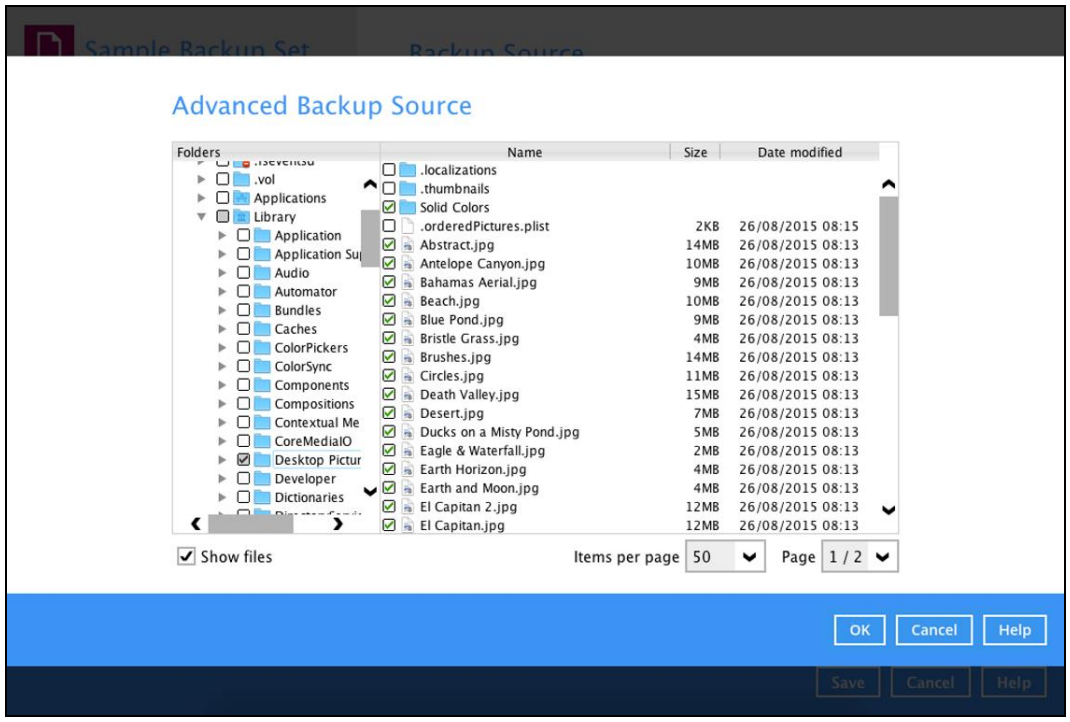
Scenario 2 (Quick or Shortcut + Advanced Backup Source)

You can use the quick or shortcut option and select files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

1. Choose a backup source.



2. In the Source window, click 'I would like to choose the files to backup', then select the files and/or folders that you would like to back up.

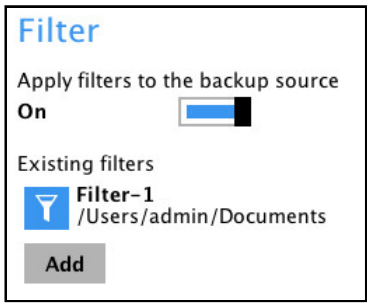


3. Click the **OK** button to save the selection, then click the **Save** button to store settings.

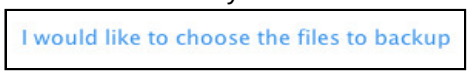
Scenario 3 (Filter + Advanced Backup Source)

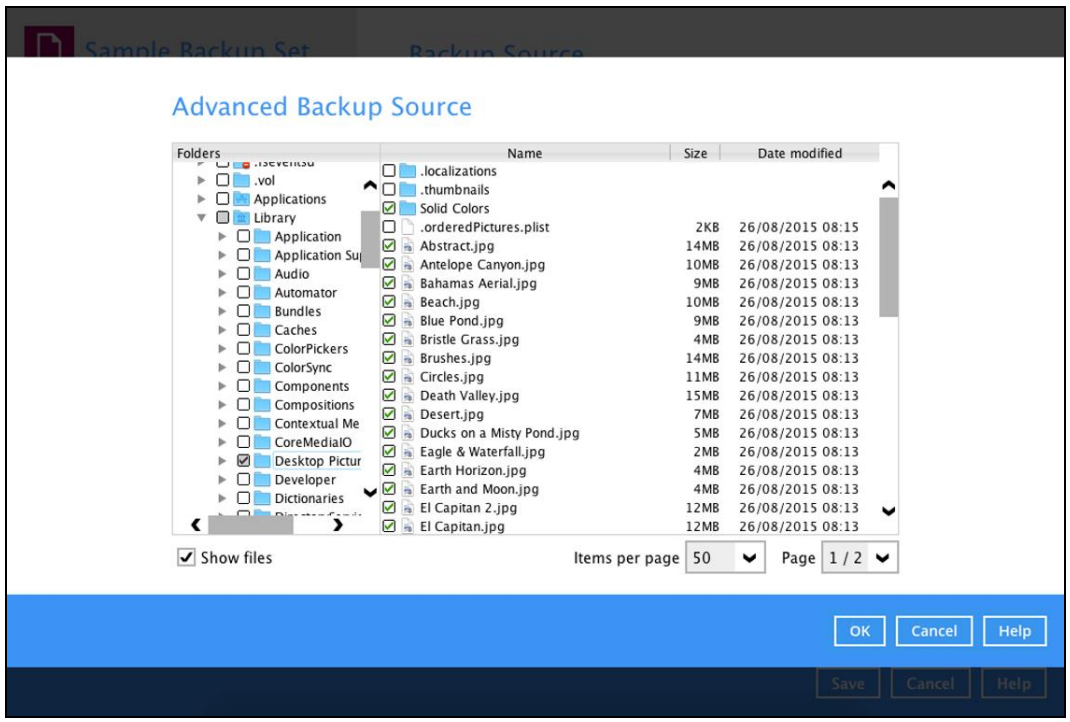
You can use the filter backup source and select files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

1. Create a filter.



2. In the source window, click 'I would like to choose the files to backup', then select the files and/or folders that you would like to back up.

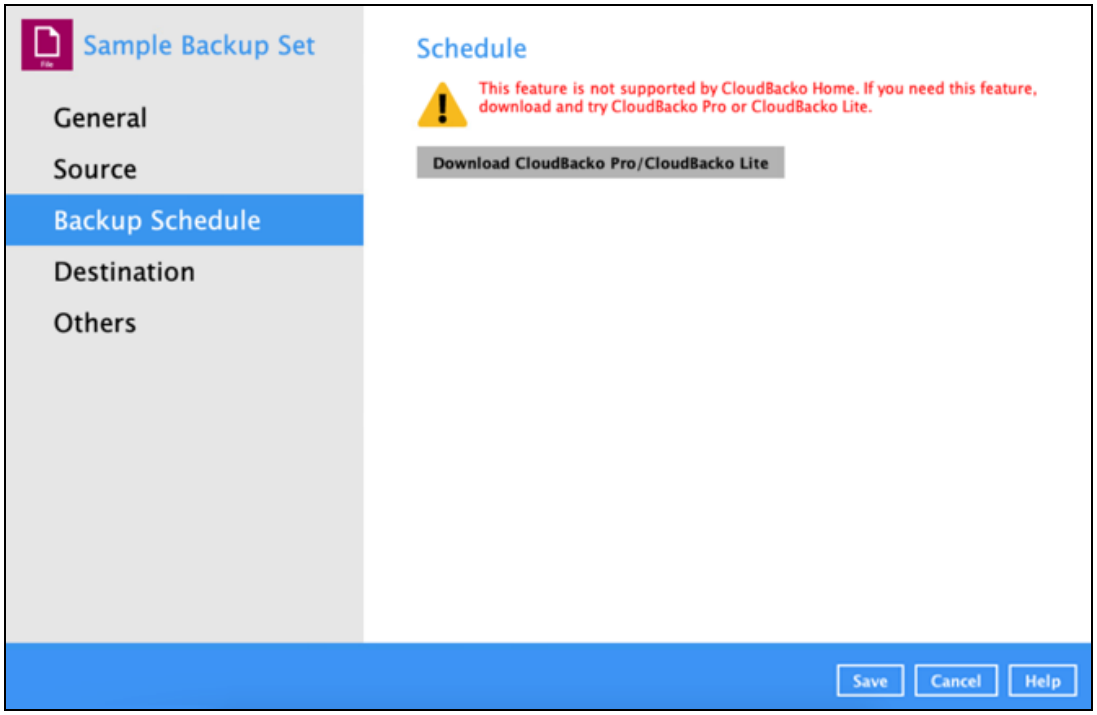




3. Click the **OK** button to save the selection, then click the **Save** button to store settings.

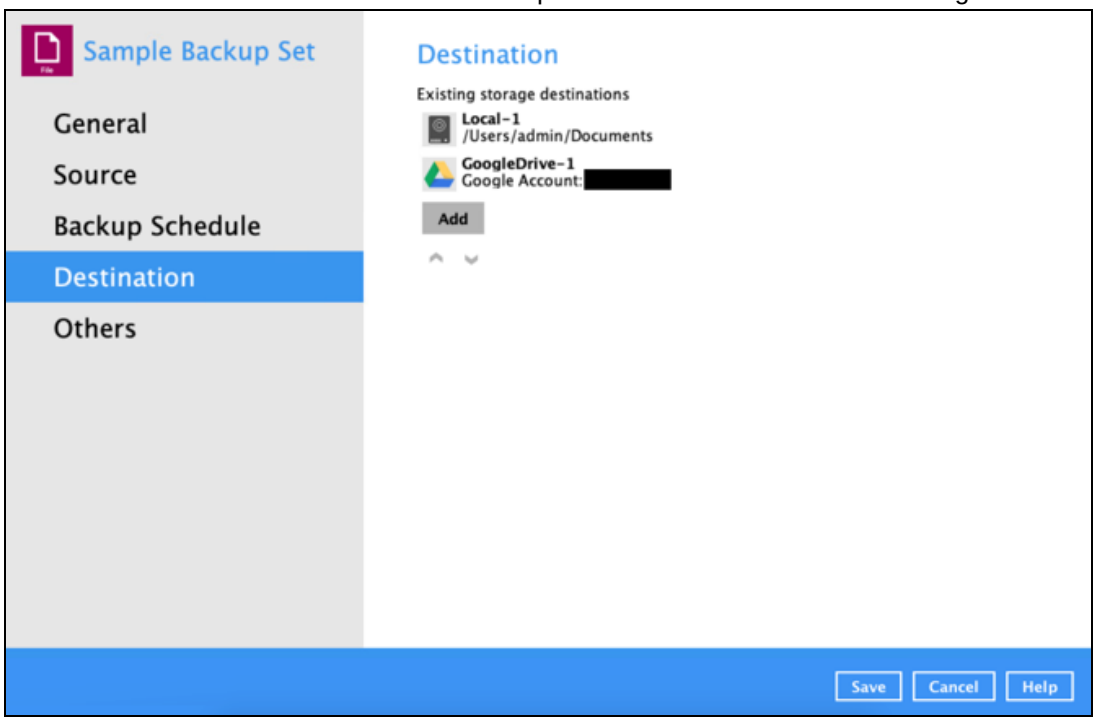
7.4.1.3 Backup Schedule

Backup Schedule is not supported for CloudBacko Home. This feature is only available for CloudBacko Pro or CloudBacko Lite. Click **Download CloudBacko Pro/CloudBacko Lite** for more details.



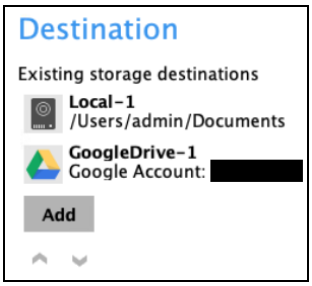
7.4.1.4 Destination

This feature allows the user to select a backup mode and add an additional storage destination.



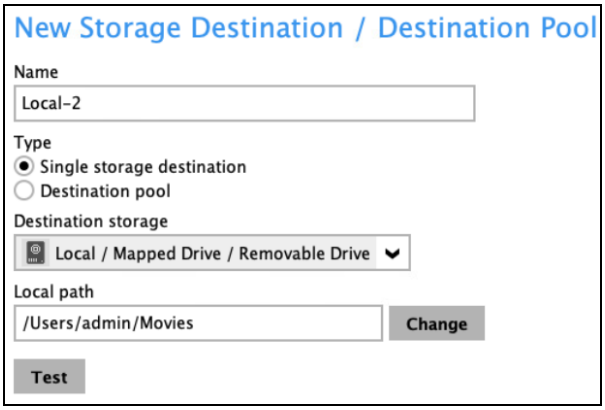
To add a new storage destination, follow the steps below:

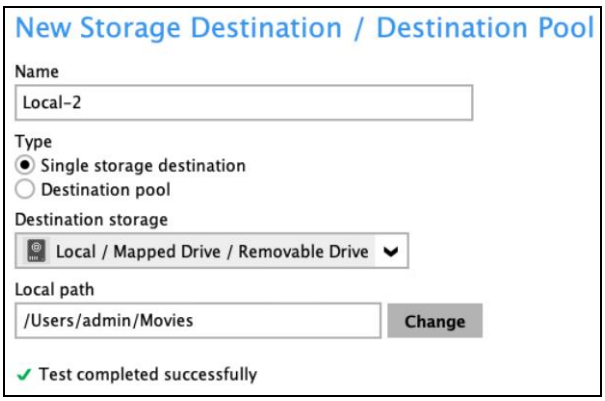
1. Click the **Add**.



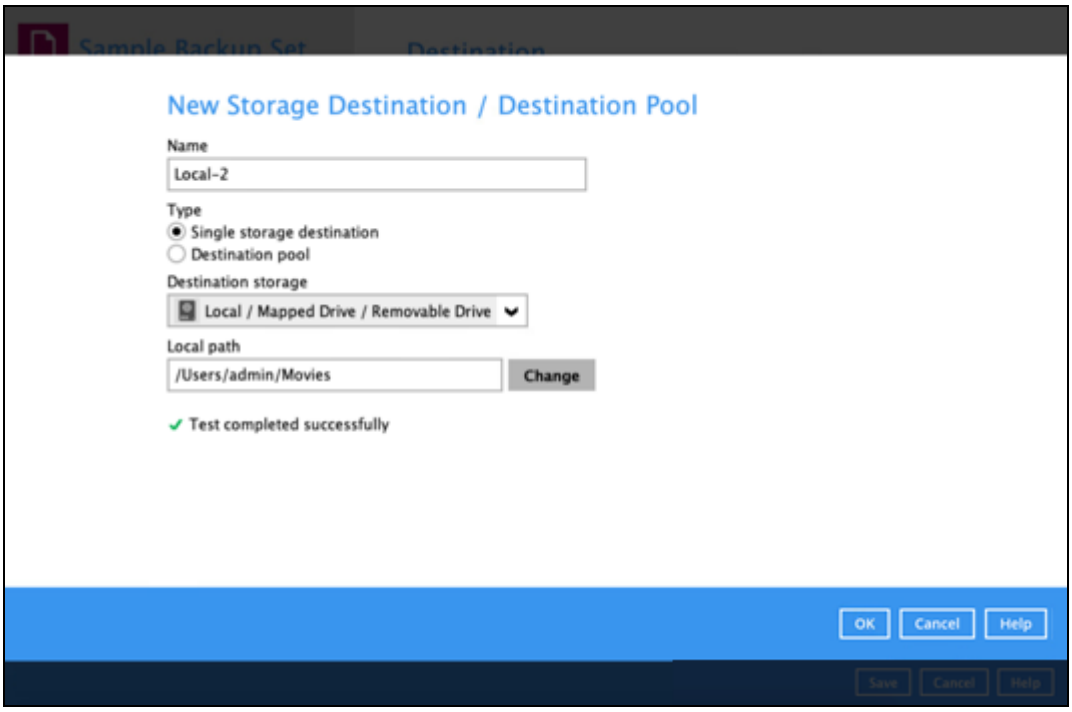
2. Click the drop-down button to select a backup destination.

3. If the **Local / Mapped Drive / Removable Drive** is selected, click the **Change** button to select a new storage destination, then click the **Test** button to validate access to it.





4. Click **OK** to save the added storage destination, then click **Save** to store the updated backup mode and added storage destination.



7.4.1.5 Others

Below is the list of other configurable options under the backup set settings:

- Retention Policy
- Temporary Directory
- Compressions
- Encryption
- Recycle Bin
- Restore Drill

Retention Policy

When the CloudBacko Home identifies files and/or folders that are deleted, updated, or with updated permission/attributes during a backup job, these files and/or folders will then be moved from the Data Area to the Retention Area.

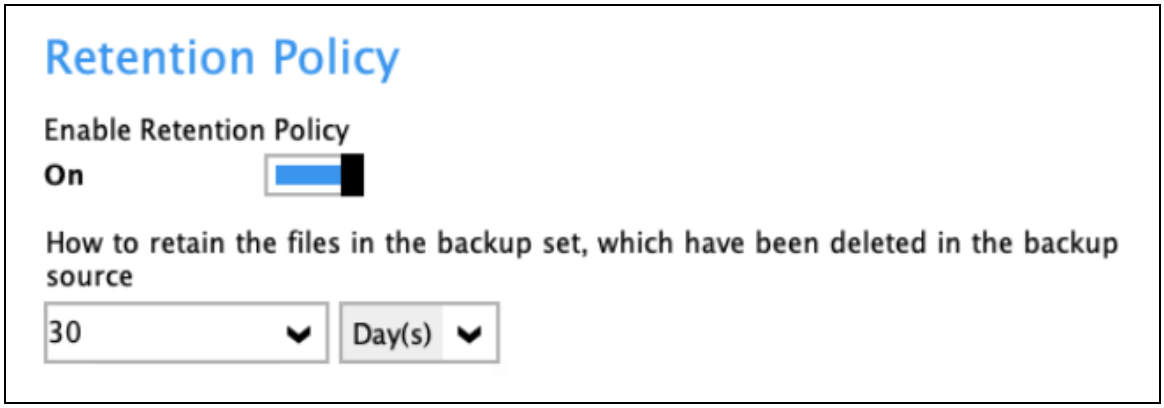
Data Area is the place where backed up files and/or folders are stored.

Retention Area is a place used as a temporary destination to store these files (deleted, updated, or with updated permission/attributes during a backup job). Files and/or folders in the Retention Area can still be restored.

The **Retention Policy** is used to control how long these files remain in the Retention Area when they are removed which can be specified in the number of days, weeks, months, or backup jobs. Retained data within all backup destinations (e.g. local drive, SFTP/FTP, and cloud storage) are cleared by the Retention Policy job.

The Retention Policy job will be run whenever a backup job is performed as long as this is enabled for the backup set. It will also be run when Space Freeing Up is performed. For further information on Space Freeing Up, refer to Ch. 7.8.2 Space Freeing Up.

The default Retention Policy setting for a File Backup Set is 30 days.



NOTE

There is a trade-off between the Retention Policy and backup destination storage usage. The higher the Retention Policy setting, the more storage is used, which translates into higher storage costs.

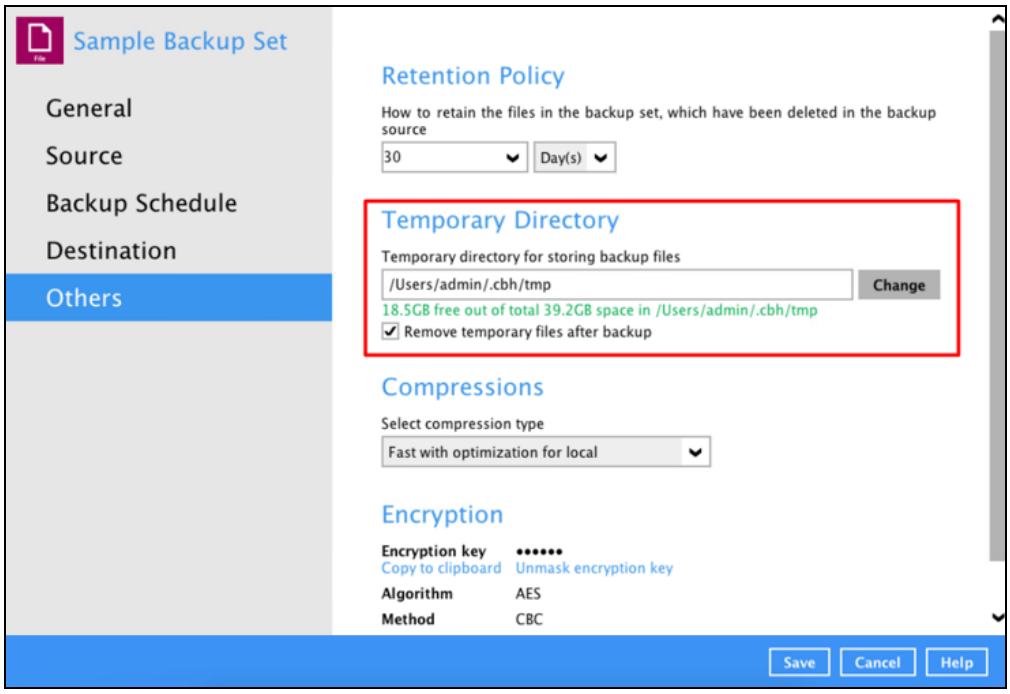
To configure the Retention Policy, follow the steps below:

1. Select the **Others** tab in the Backup Set Settings.
2. Slide the switch to the right to turn on **Enable Retention Policy**.
3. Click the drop-down button to define the number of day(s) or job(s) that the deleted files will be retained. This is configured as thirty (30) days by default.
4. Click **Save** button to store the configured Retention Policy.

WARNING
When files and/or folders in the Retention Area exceed the Retention Policy setting, they will be permanently removed from the backup set and cannot be restored.

Temporary Directory

The CloudBacko Home uses the temporary directory for both backup and restore operations.



For a **backup job**, it is used to temporarily store backup set index files. An updated set of index files is generated after each backup. The index files are synchronized to each individual backup destination at the end of each backup job.

For a **restore job**, it is used to temporarily store temporary restore files.

NOTES

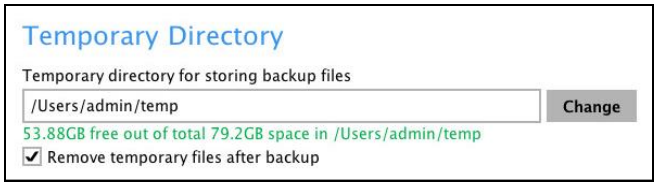
1. For best practice, the temporary directory should be located on:
   - A local drive for optimal backup and restore performance.

   And should not be located on:
   - System drive, as the System drive is used by Mac and other applications. There will be frequent disk I/O activity which may affect both backup and restore performance.
   - A network drive, as it could affect both backup and restore performance.

It is recommended to select the 'Remove temporary files after backup' option on the backup set to keep the temporary drive clear.

To change the temporary directory, follow the steps below:

1. Click **Change** to select a directory path for storing temporary data.



2. Locate the directory that you would like to use, then click **OK** to select the folder. Click the **Save** button to apply the settings.

Compressions

This feature is used to enable compression of data during a backup job. When this feature is enabled, the CloudBacko Home will compress all files before it is backed up to the backup destination(s).

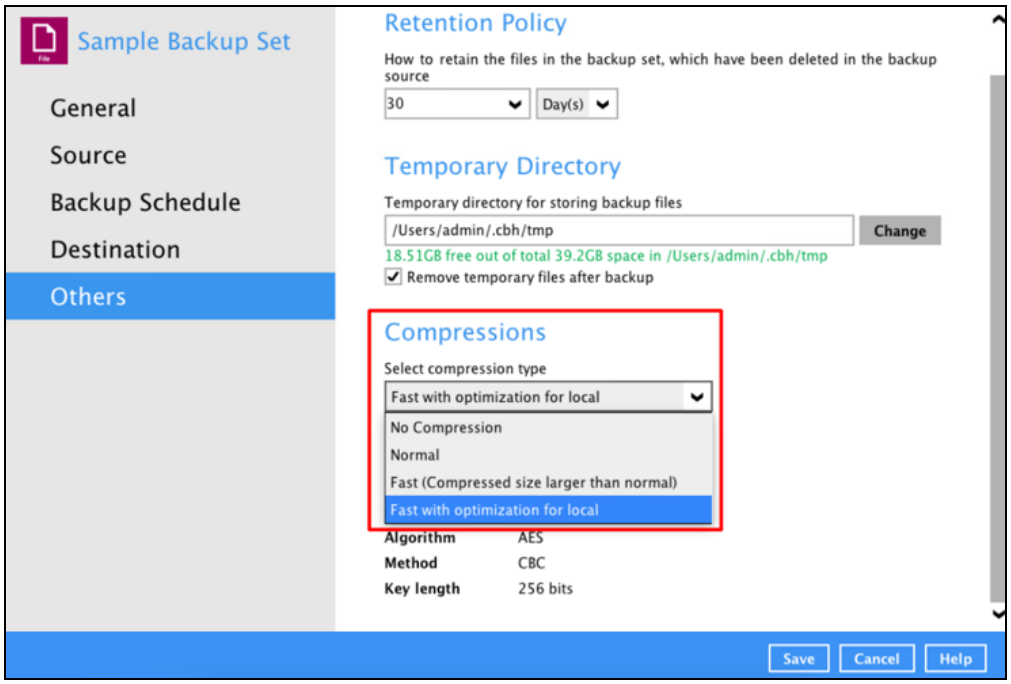
For newly created backup set(s), “Fast with optimization for local” is selected by default.

These are the four (4) compression types:

- **No Compression** - file will not be compressed before backup.
- **Normal** - compression is comparable to gzip Normal compression ratio
- **Fast (Compressed size larger than normal)** - Compression will be faster but with less compression and lower CPU usage compared to Normal.
- **Fast with optimization for local** - Uses Snappy compression library when baking up to local destination only, otherwise setting will default to gzip if baking up to other destinations. Has the lowest CPU usage, very high speed and reasonable compression but compressed file size may be larger that Fast.

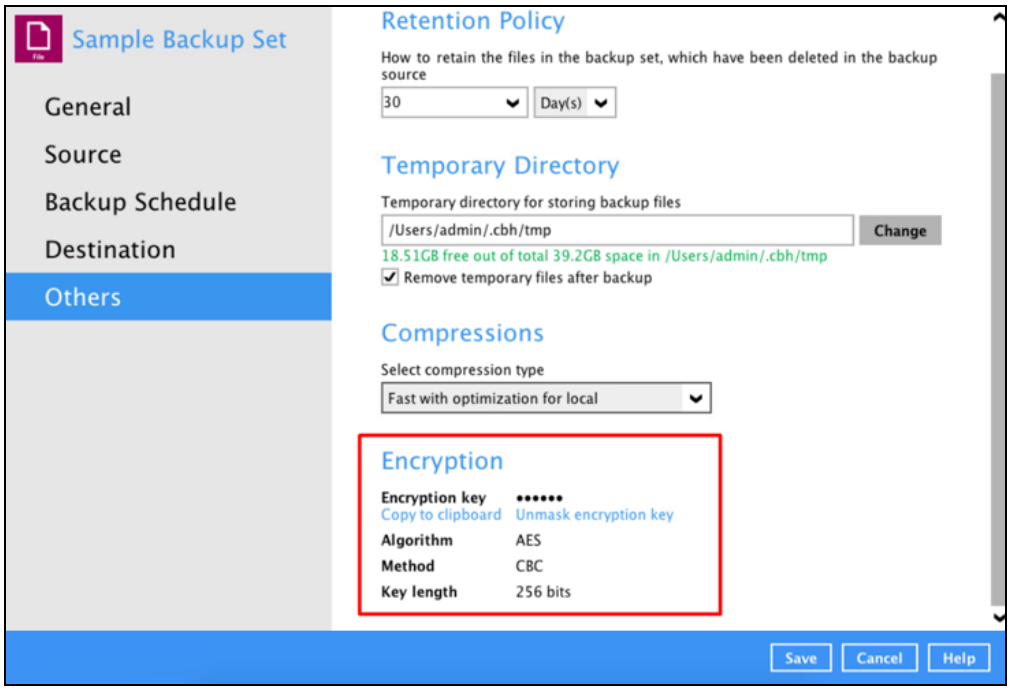
WARNING

The compression type can be changed anytime even after a backup job. The modified compression type will be applied on the next run of a backup.



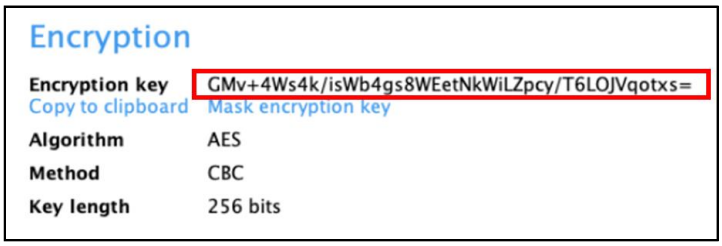
Encryption

This feature allows the user to view the encryption settings.

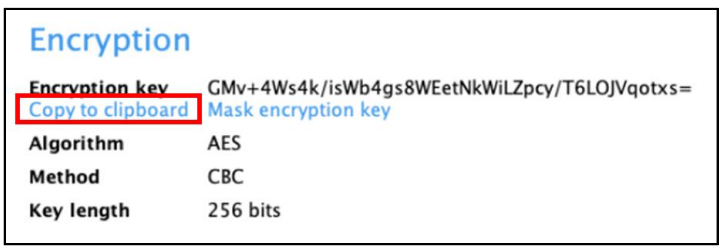


To view the encryption key of the backup set, follow the steps below:

1. In the backup set settings, select the **Others** tab. Scroll-down to display the **Encryption**.
2. Click **Unmask encryption key** to display the encryption key of the backup set.



3. Click **Copy to clipboard** to copy the encryption key of the backup set.



Recycle Bin

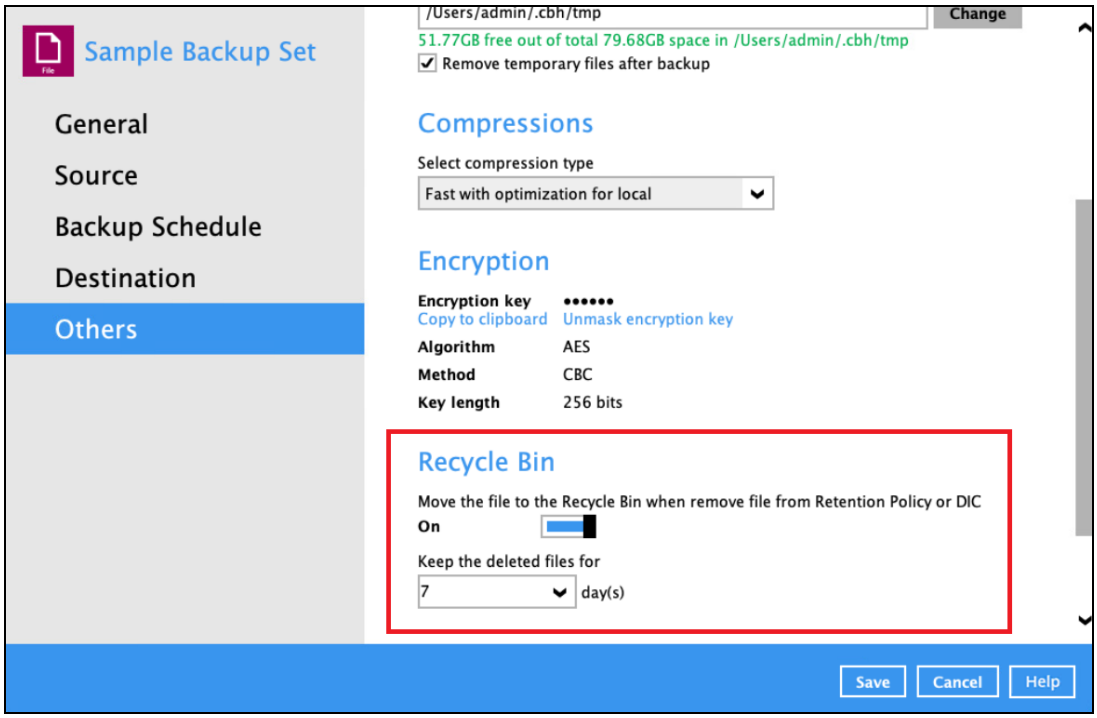
This feature is for protection of the BAK (block) files stored in the Backup Set's destination, allows the user to set the number of days BAK files that were deleted due to Retention Policy or Data Integrity Check, will be held under Recycle Bin as added protection.

This is how the Recycle Bin will treat deleted data:

- Data in the Recycle Bin will consume Quota.
- It does not move the data in another location within the storage, instead the index tracks the xxxxxx.bak files and the remaining time in the Recycle Bin.
- If the index is reverted to a previous timestamp, the settings of the Recycle Bin in the reverted index will be followed.
- Recoverability of data is not affected when the Recycle Bin is alternately enabled or disabled.
    - When enabled, it will only check if the data inside the Recycle Bin is still within the set number of days. Once it is beyond the set number of days it will only be deleted when the following operations are run: Backup, Space Freeing Up, Data Integrity Check and Delete Backup Data.
    - When disabled, if there are already deleted files it will not automatically delete the data inside the Recycle Bin. It will remain in the Recycle Bin even if it is beyond the set number of days. It will only be deleted when the following operations are run: Backup, Space Freeing Up, Data Integrity Check and Delete Backup Data.
- Once the Recycle Bin is disabled, deleted files will be removed immediately and will not be moved in the Recycle Bin.
- The setting applies to all destinations for the backup set.
- Viewing Recycle Bin contents is not available.
- Recycle Bin cleanup is done at the start of the backup job process.
- Recovering from Recycle Bin requires reverting the index. For instructions on how to revert the index please refer to this article: FAQ: How to un-delete backup data moved to Retention, or revert indexes to a healthy state from an earlier successful backup.

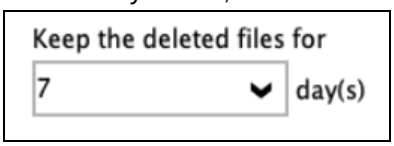
WARNING
When reverting index, new data will be lost.

This is enabled by default set with 7 days.



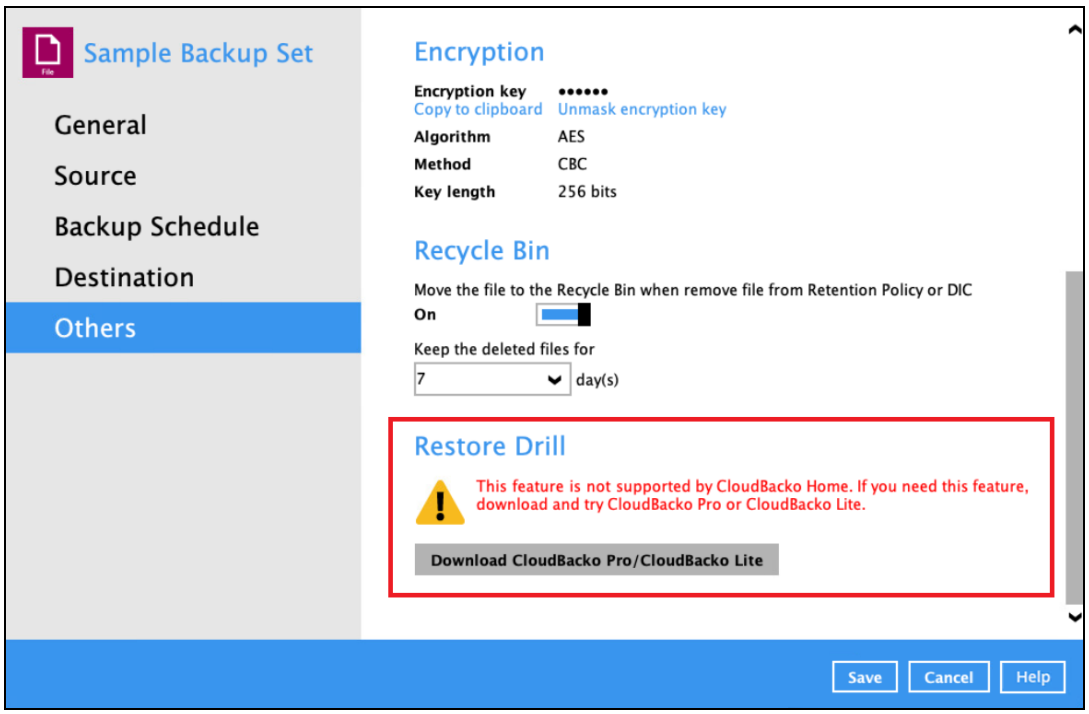
To set the number of days, follow the steps below:

1. Go to Backup Sets, then select a backup set.
2. Click the **Others** tab in the backup set settings.
3. Under Recycle Bin, select the number of days or you can enter it manually.



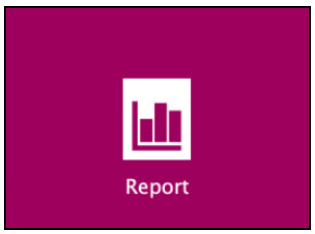
Restore Drill

Restore Drill is not supported for CloudBacko Home. This feature is only available for CloudBacko Pro or CloudBacko Lite. Click the **Download CloudBacko Pro/CloudBacko Lite** button for details.



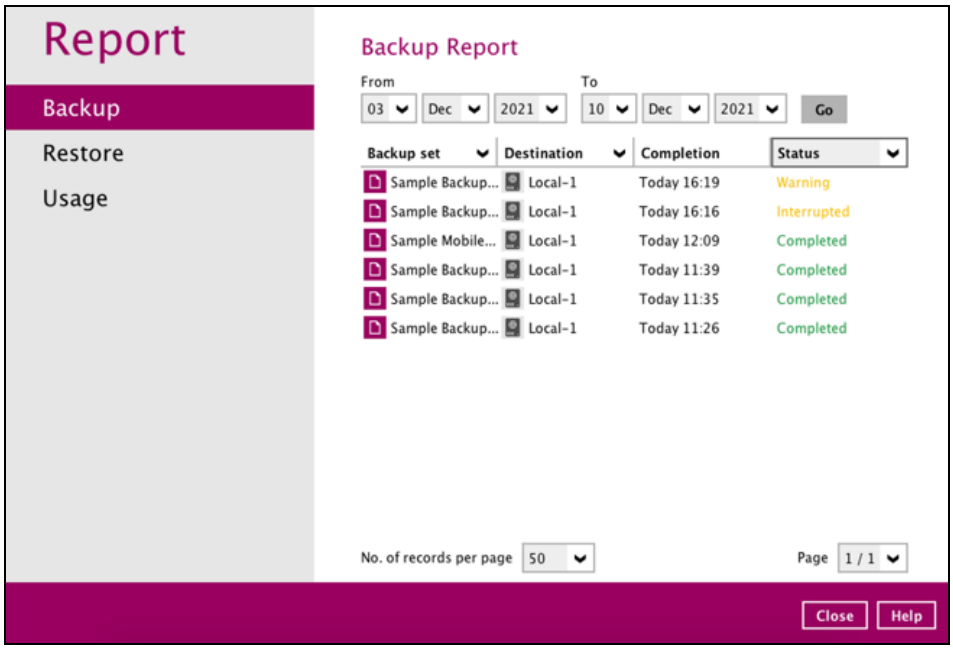
7.5 Report

This feature allows user to run and view backup and restore reports.



There are three (3) options available for this feature:

- Backup
- Restore
- Usage



7.5.1 Backup

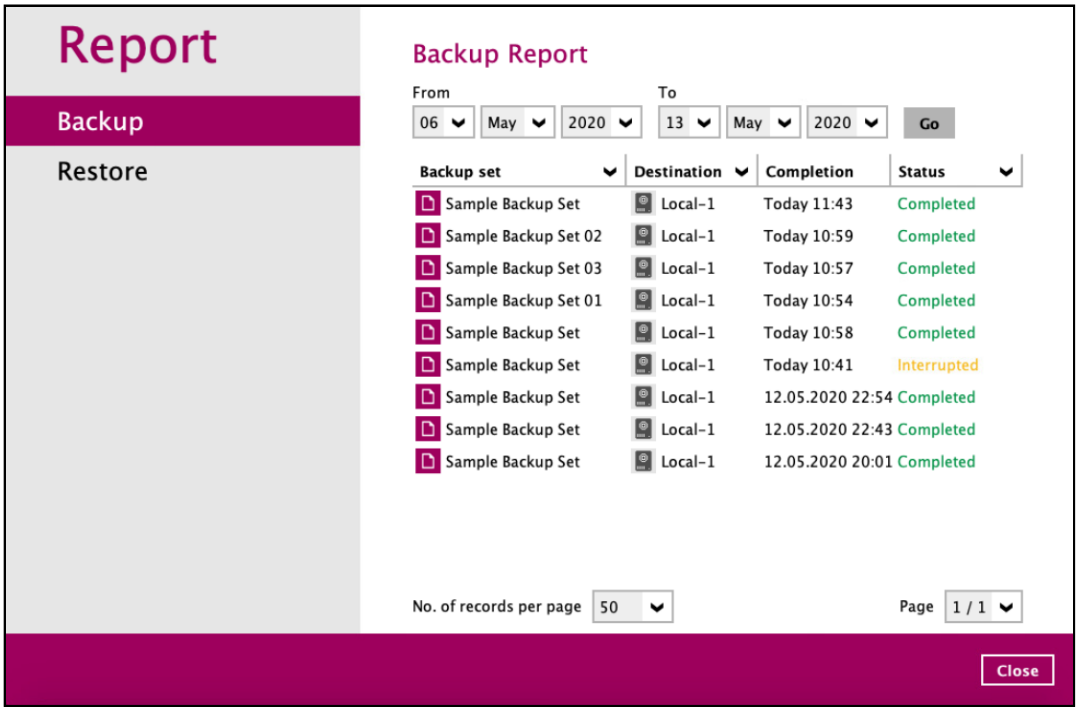
This option is used to run and view backup reports. There are four (4) filters that can be applied on this feature, namely:

Date

Backup set

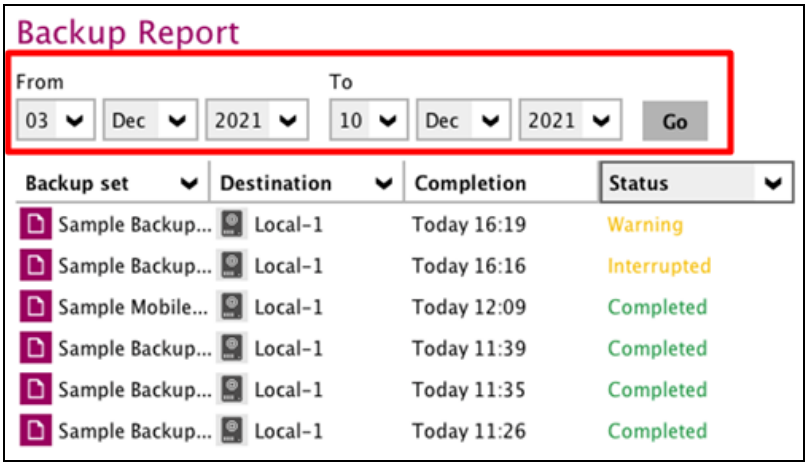
Destination

Status



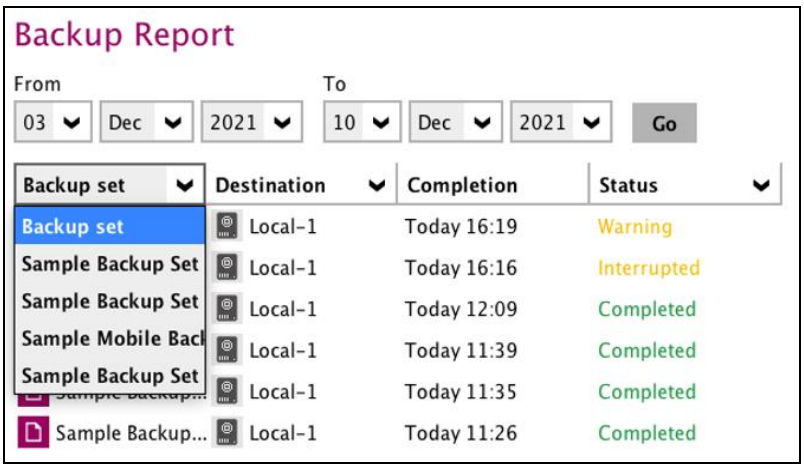
Date

Use this filter to display all the available backup report(s) within a date range.



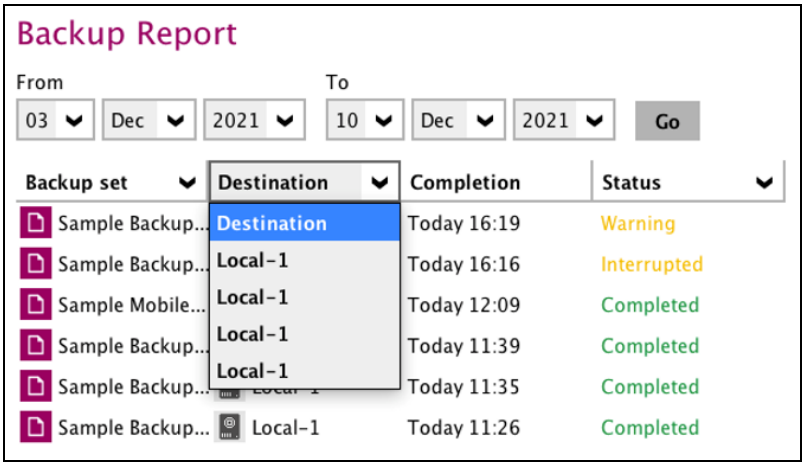
Backup set

Use this filter to display all the available backup set(s) with a backup report. Then select which backup set with backup report that you would like to view.



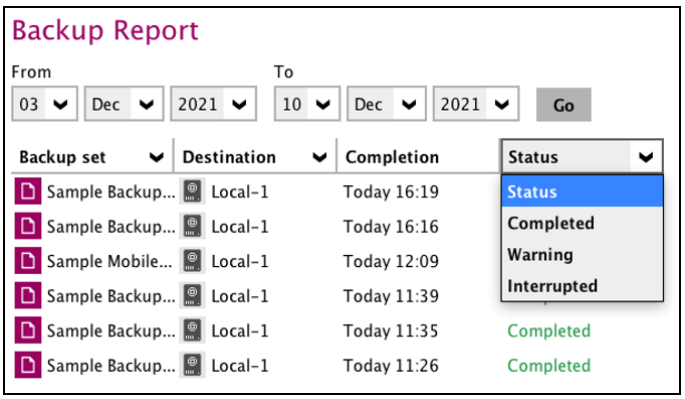
Destination

Use this filter to view the backup report for the selected storage location.



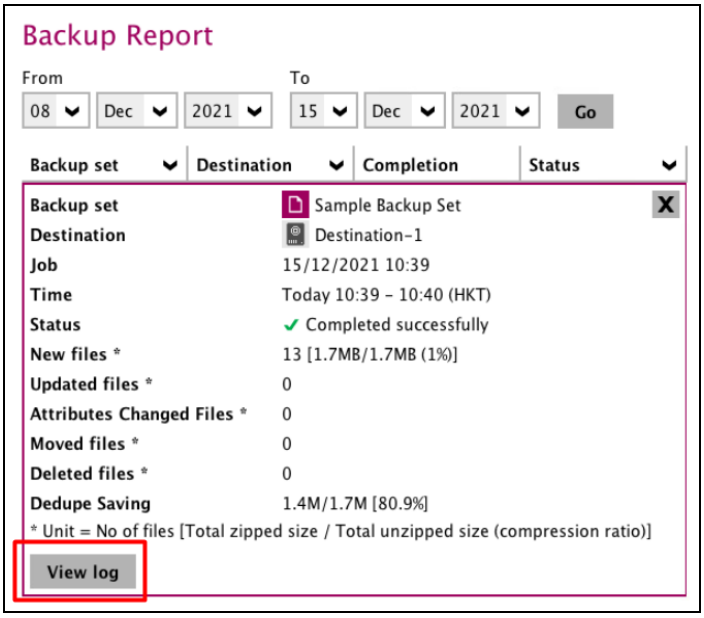
Status

Use this filter to view all the backup report(s) with the same status (i.e., Completed, Warning, Interrupted, Interrupted with error(s), Failed and In progress).

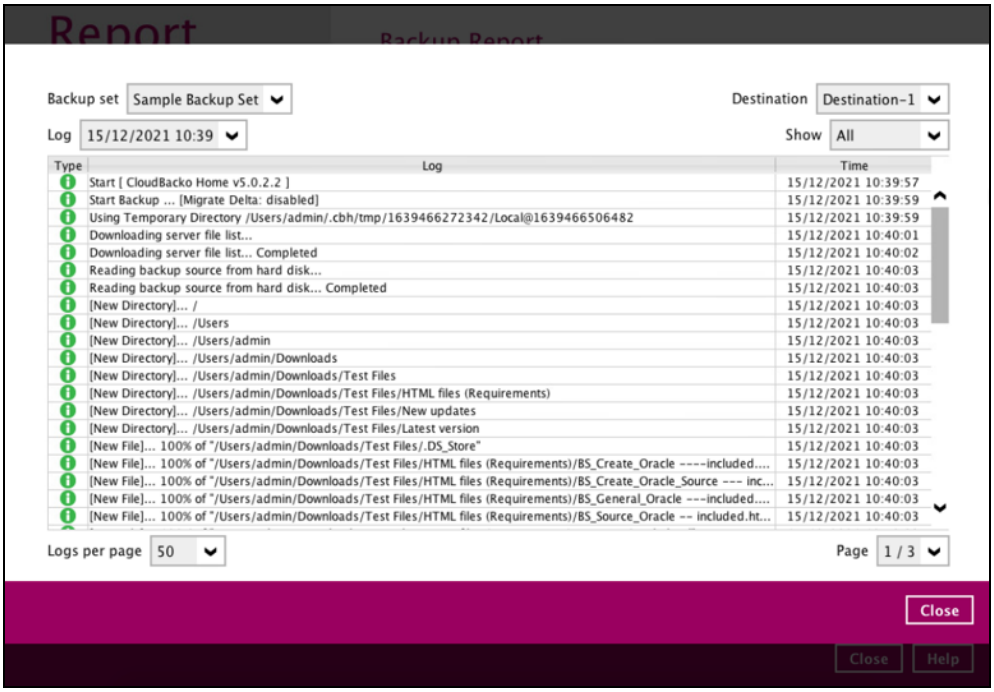


To view the backup log, follow the instructions below:

1. Select and click the backup report, then click the **View log** button.



2. The **Backup set**, **Destination**, **Log Date and Time**, **Status**, the number of Logs per page, and Page can be filtered when viewing the backup report.



7.5.2 Restore

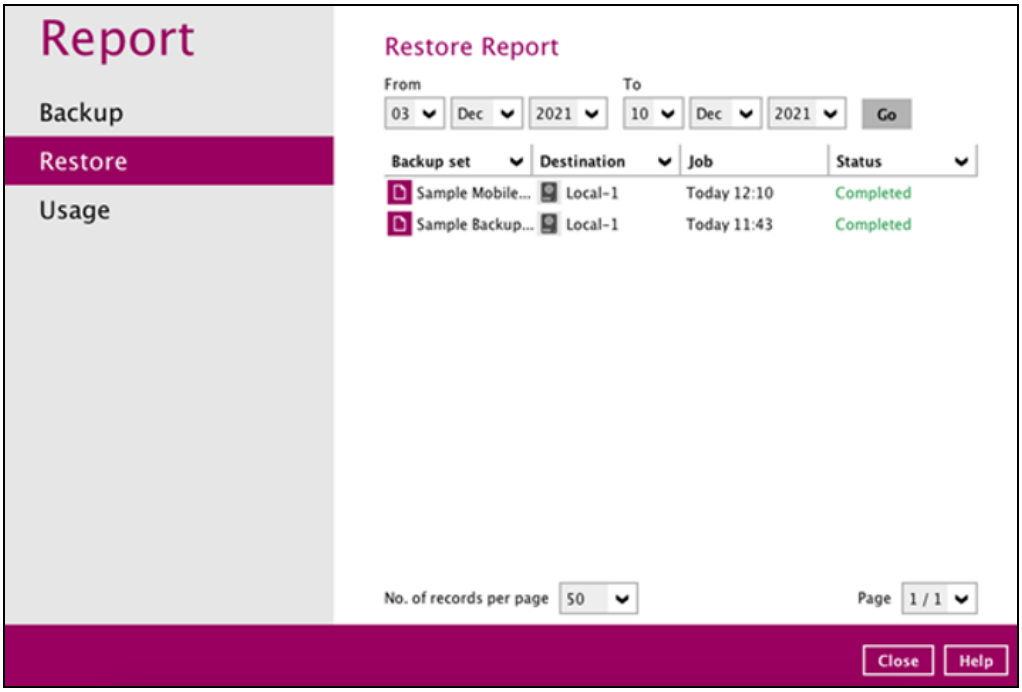
This feature displays the restore report logs for each backup set. Similar to the **Backup** tab, this feature also consists of the following filters:

Date

Backup set

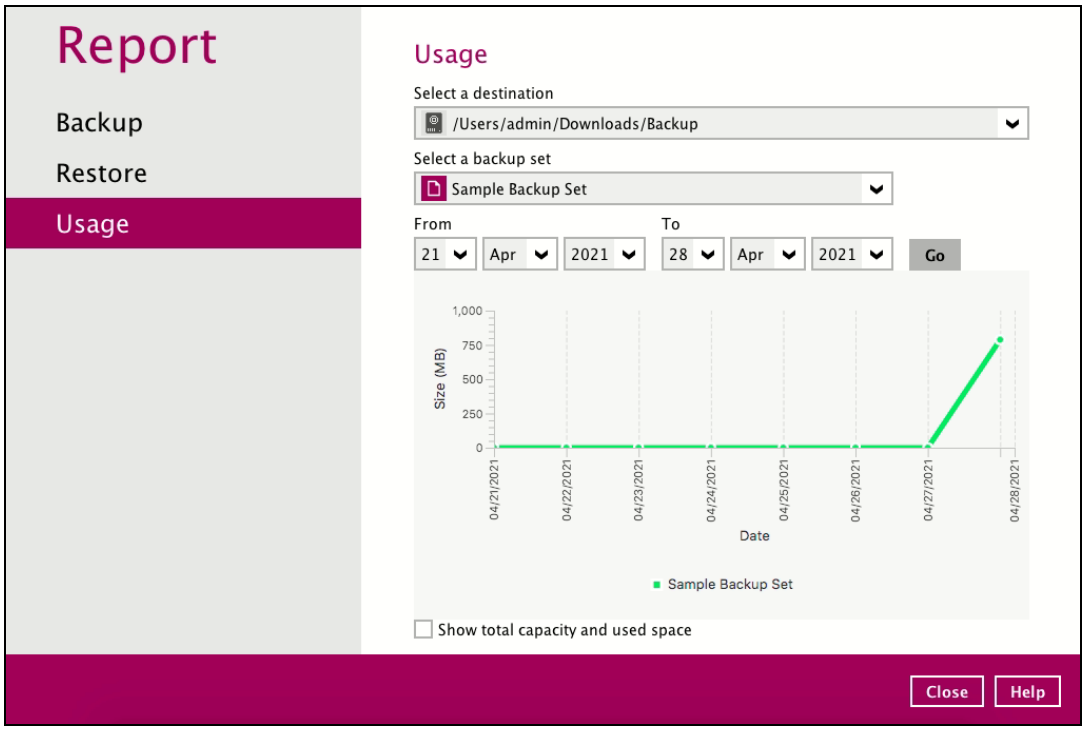
Destination

Status



7.5.3 Usage

This allows the user to view the storage and usage information in a graphical view for each backup set and backup destination by date.



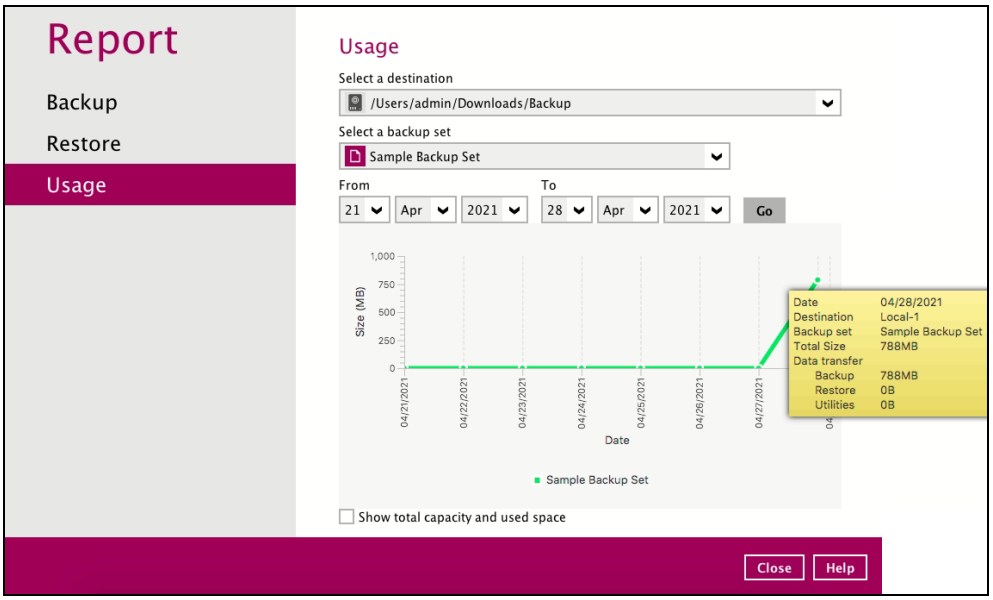
Storage Statistics

Total Size: Displays the total amount of backed up data on the backup destination.

The storage statistics of a backup set is updated every time the following functions are run:

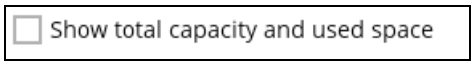
1. Backup job
2. Periodic Data Integrity Check (PDIC)
3. Data Integrity Check (DIC)
4. Space Freeing Up
5. Delete Backup Data

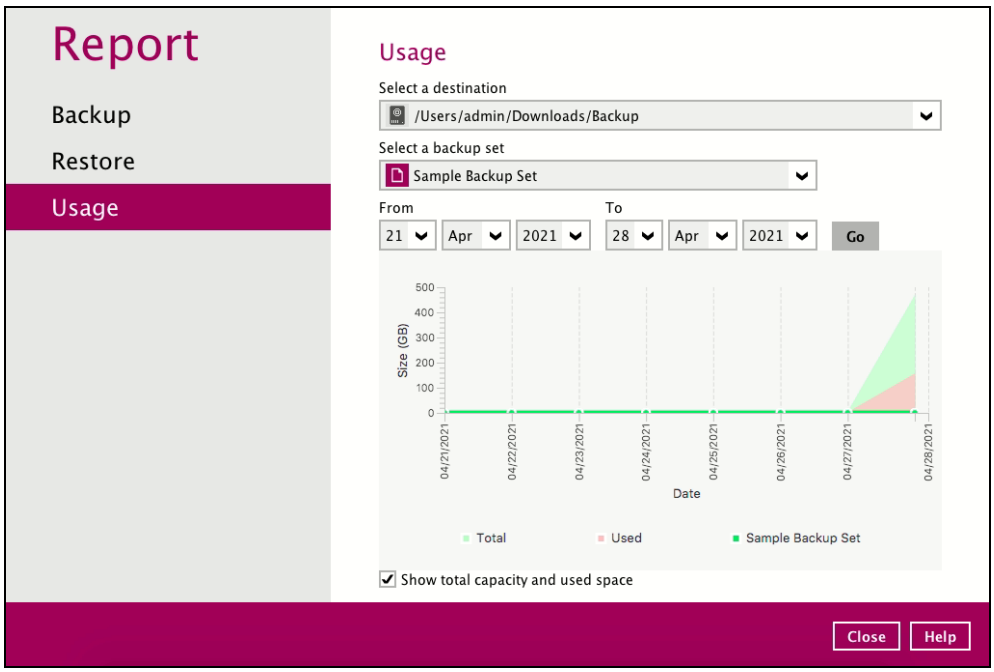
Example: The data transfer statistics will pop up when mouse pointer moves over a specific date.



- **Data Transfer Statistics**
  - **Backup:** displays the amount of data transferred to the backup destination for backups.
  - **Restore:** displays the amount of data transferred from the backup destination for restores.
  - **Utilities:** displays the amount of data transferred from the backup destination, when a Data Integrity Check (DIC) is run with the “Run Cyclic Redundancy Check (CRC) during data integrity check" option selected.

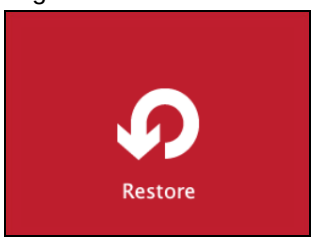
To check the total capacity and used space, tick the checkbox.



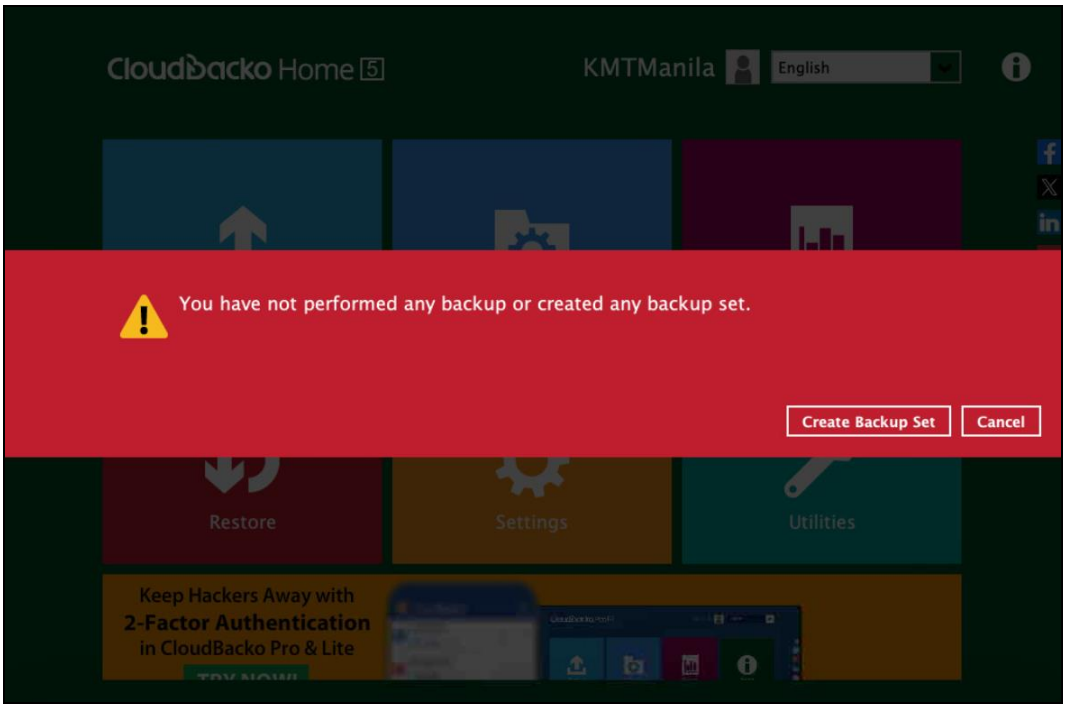


7.6 Restore

This feature is used to copy the backed up file(s) from the backup set and restoring it to its original location or new location.



If using CloudBacko Home for the first time, you will be asked to create a backup set and run a backup first. A restore cannot be performed unless you already run a backup.

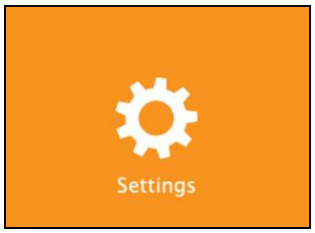


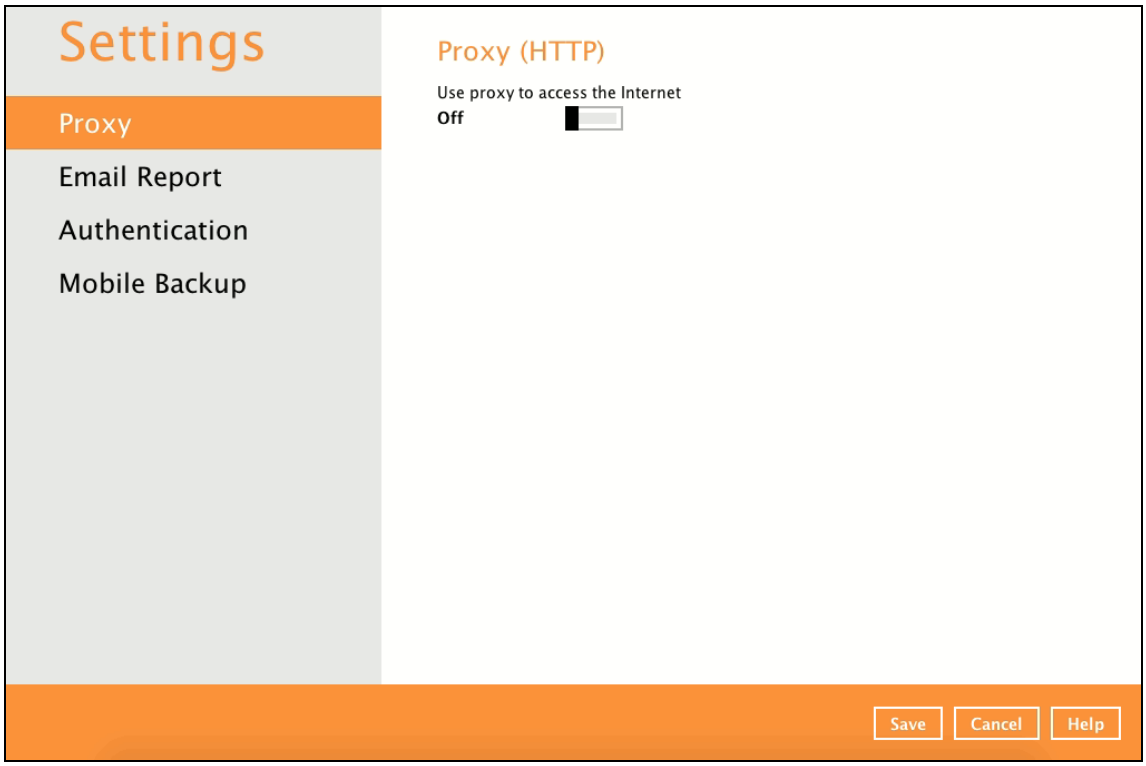
To restore backed up files, follow the instructions on Chapter 11.1 Restore Data.

7.7 Settings

Settings consist of four (4) sub modules:

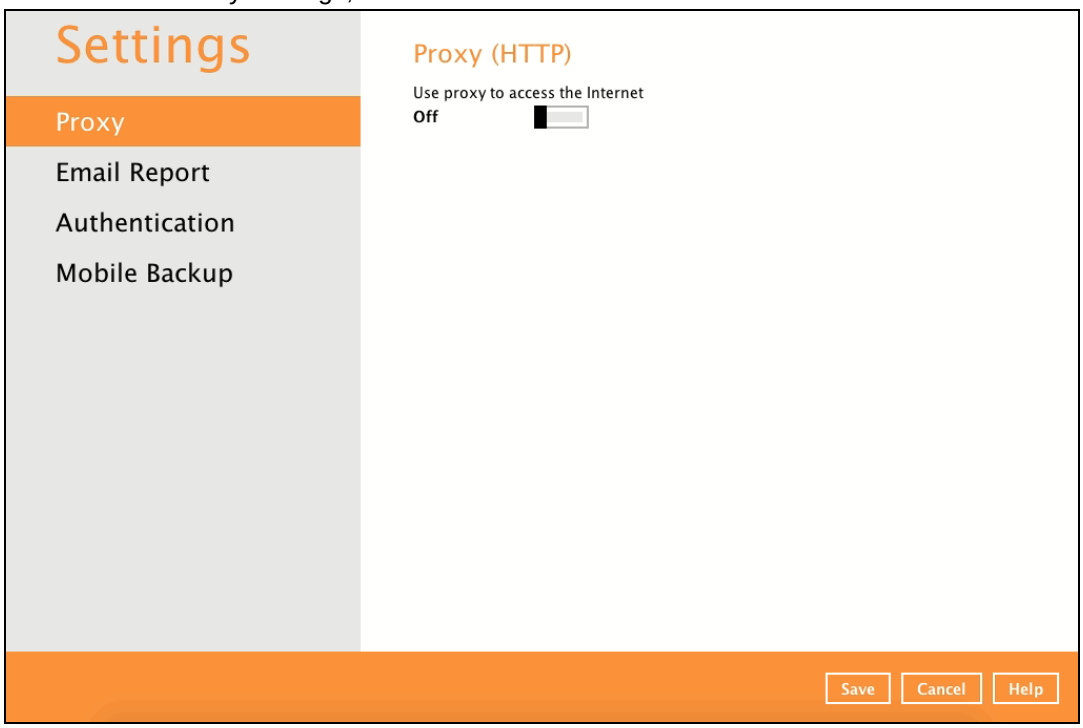
- Proxy
- Email Report
- Authentication
- Mobile Backup

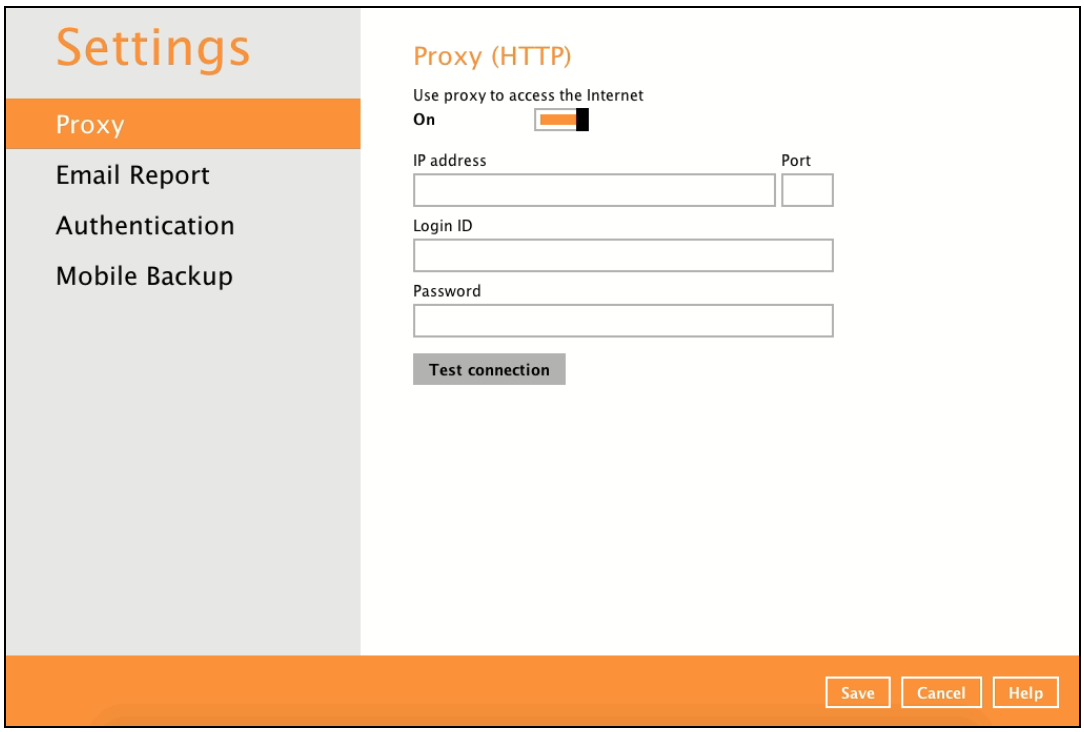




7.7.1 Proxy

To enable the Proxy Settings, follow the instructions below.





1. Complete the following fields:

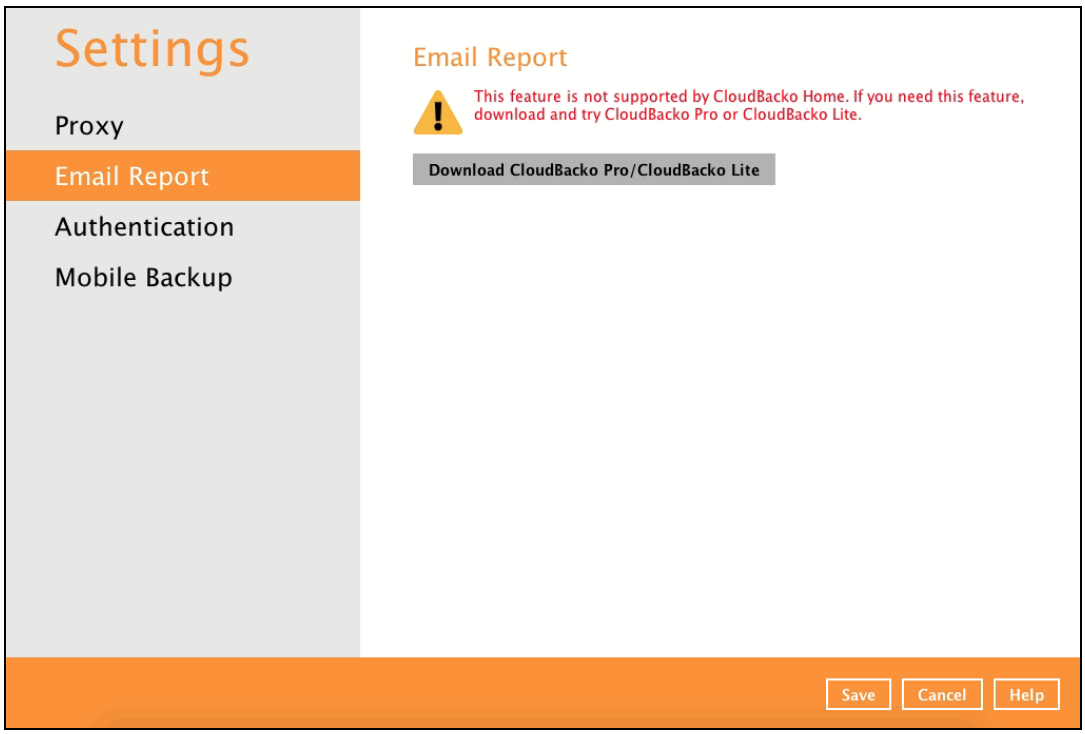
   IP address
   Port
   Login ID
   Password

2. Click **Test Connection** to validate the connection.
3. Click **Save** to store the settings.

7.7.2 Email Report

The Email Report feature is not supported for CloudBacko Home. This feature is only available for CloudBacko Pro or CloudBacko Lite.

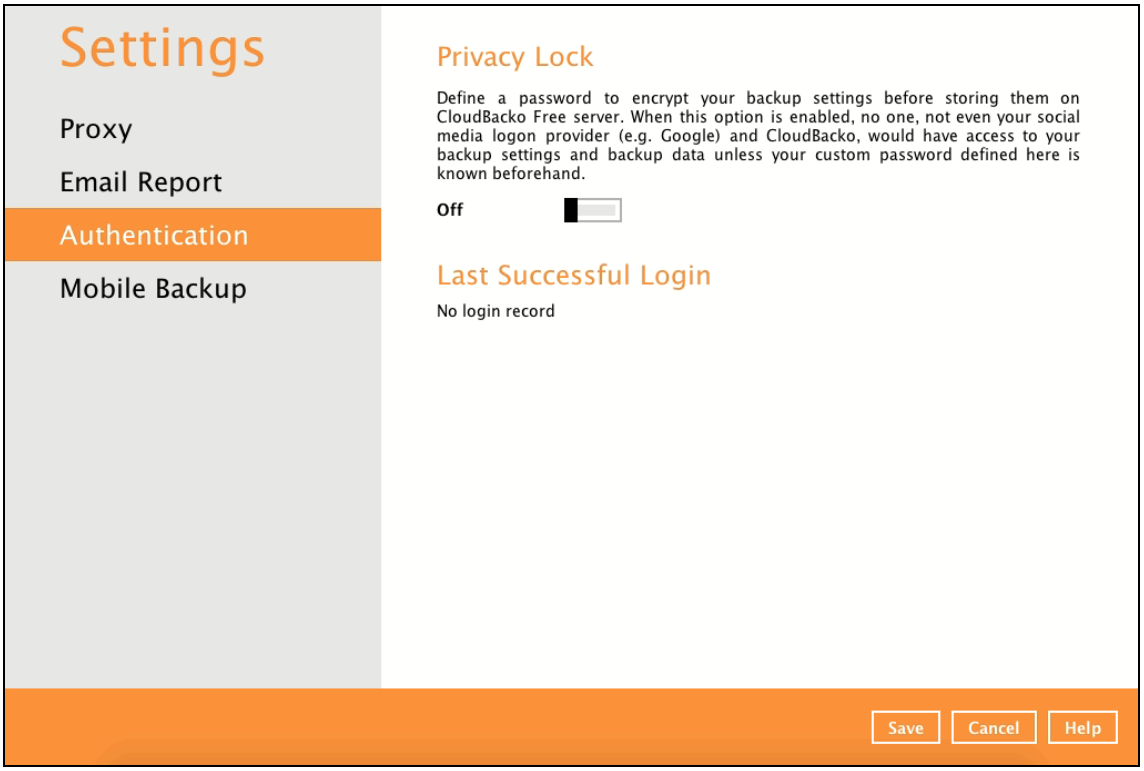
Click **Download CloudBacko Pro/CloudBacko Lite** for more details.



7.7.3 Authentication

You can use the Authentication function to:

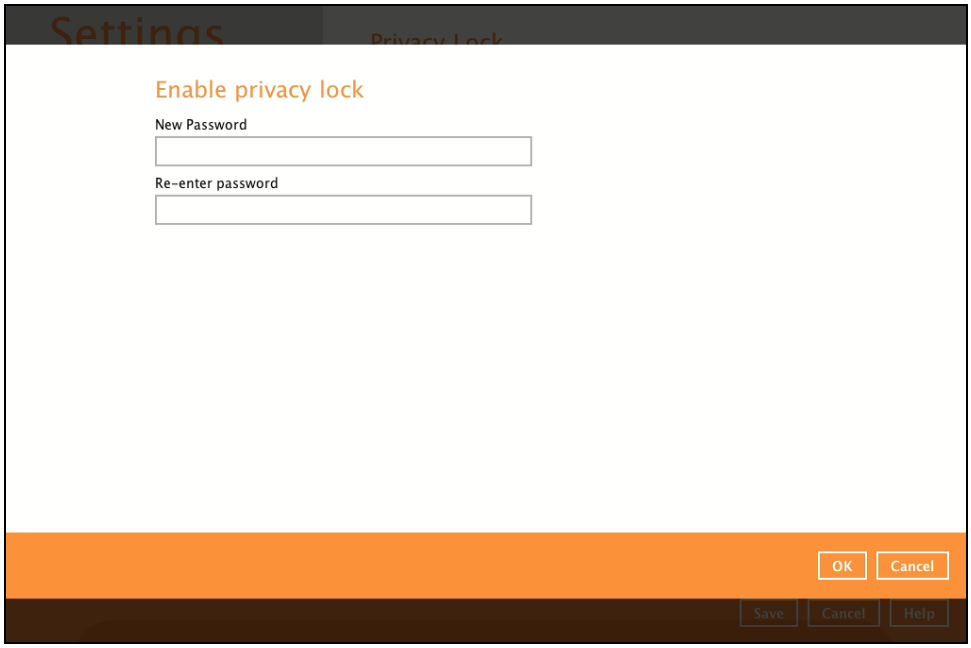
- Enable or disable the "Privacy Lock". Change the password of the "Privacy Lock".
- View details of the "Last Successful Login" for Privacy Lock.



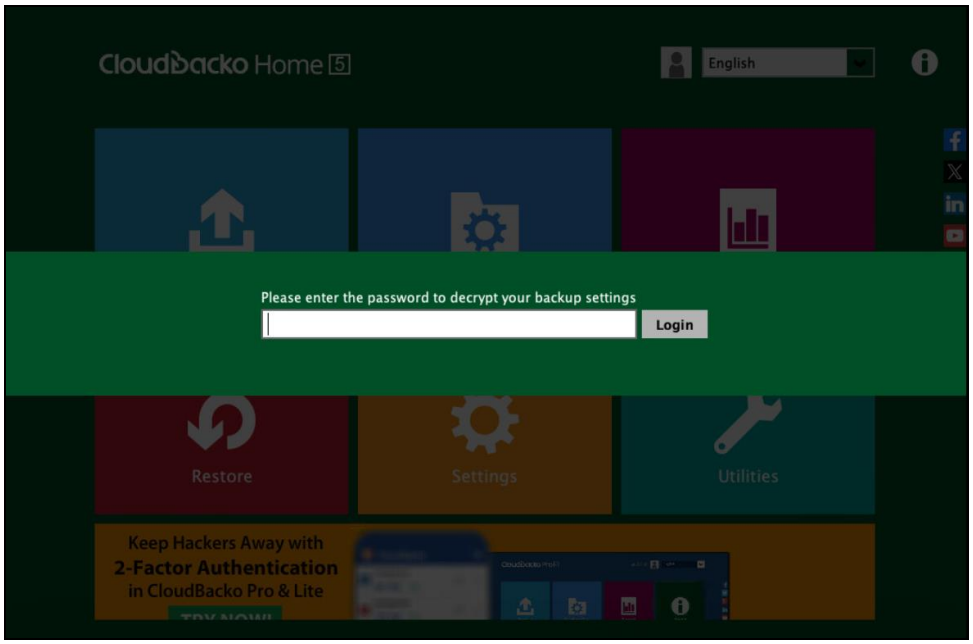
Privacy Lock

This feature allows the customer to define a password to encrypt the backup settings before storing the date to CloudBacko Free Server To enable the Privacy Lock feature, follow the instructions below:

1. Swipe the lever to the right to turn it on.
2. Enter the new password and re-enter it for authentication purposes.

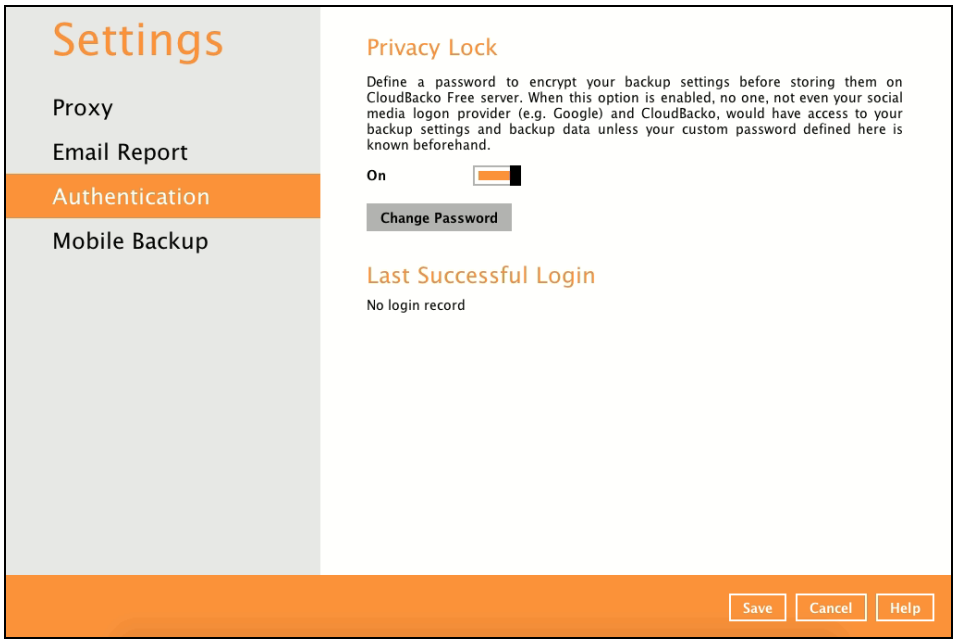


3. Click **OK** then click **Save** button to store the settings.
4. Upon launching the CloudBacko Home, it is required to enter the password to login.

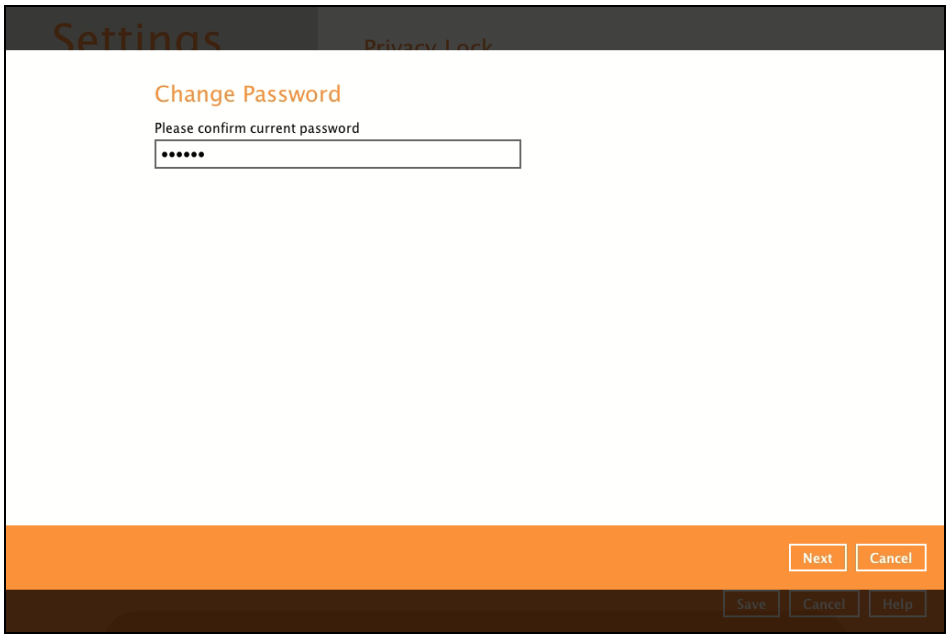


To change the password, follow the instructions below:

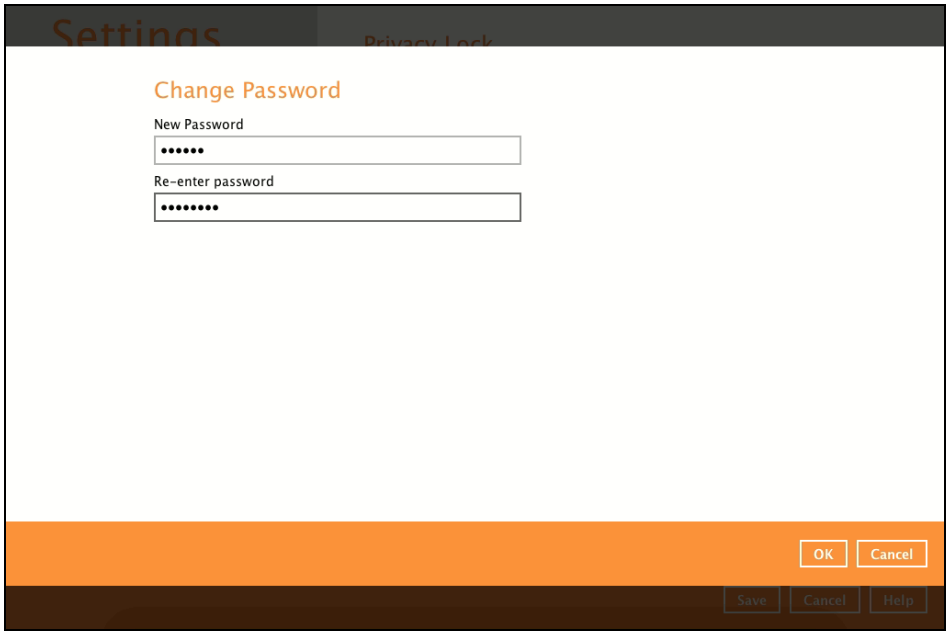
1. Click the **Change Password.**



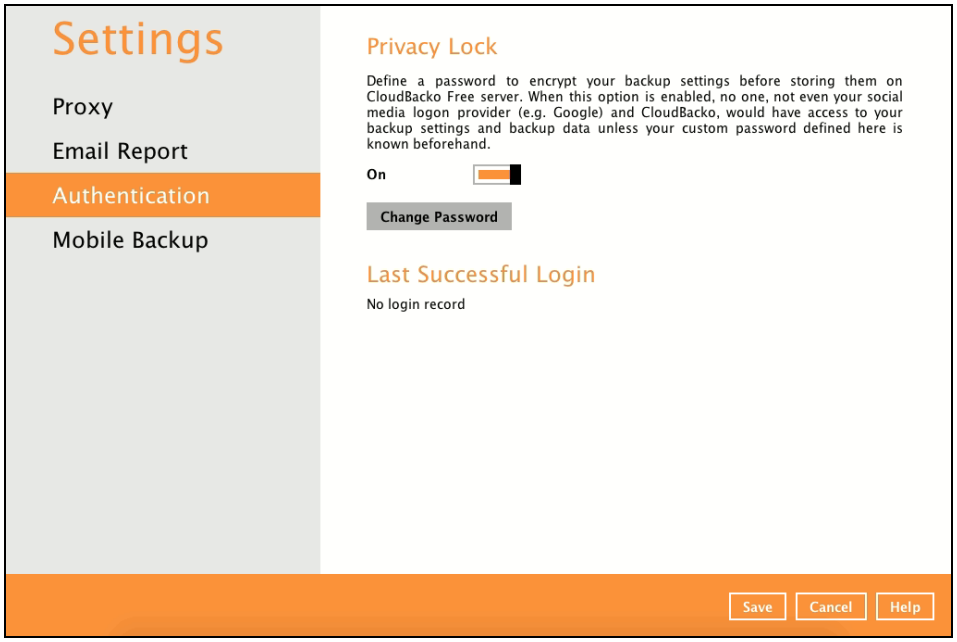
2. Enter the current password.



3. Enter the new password and re-enter it for authentication purposes. Click **OK** to return to main screen.

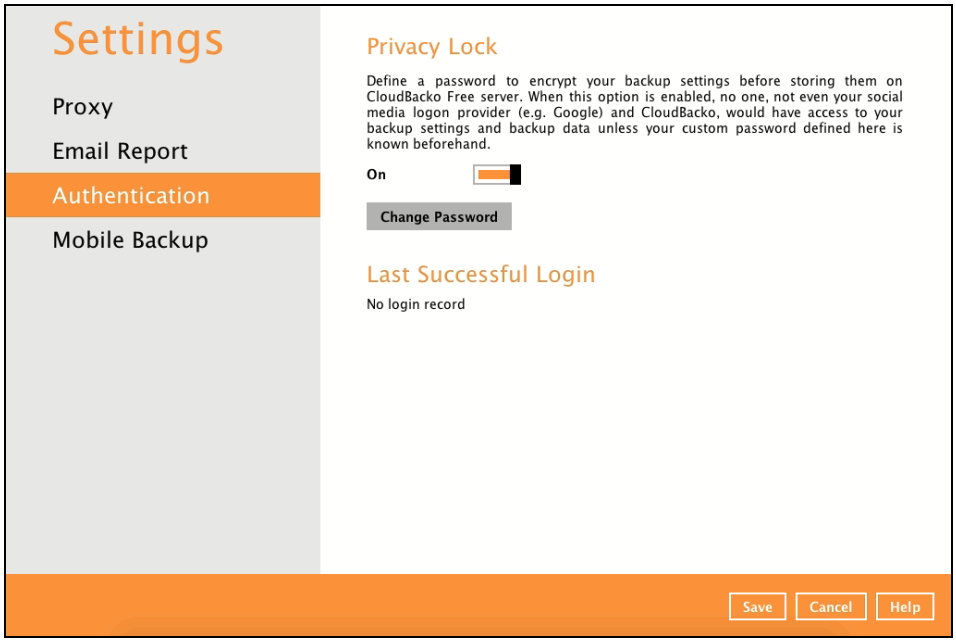


4. Click **Save** to store the settings.

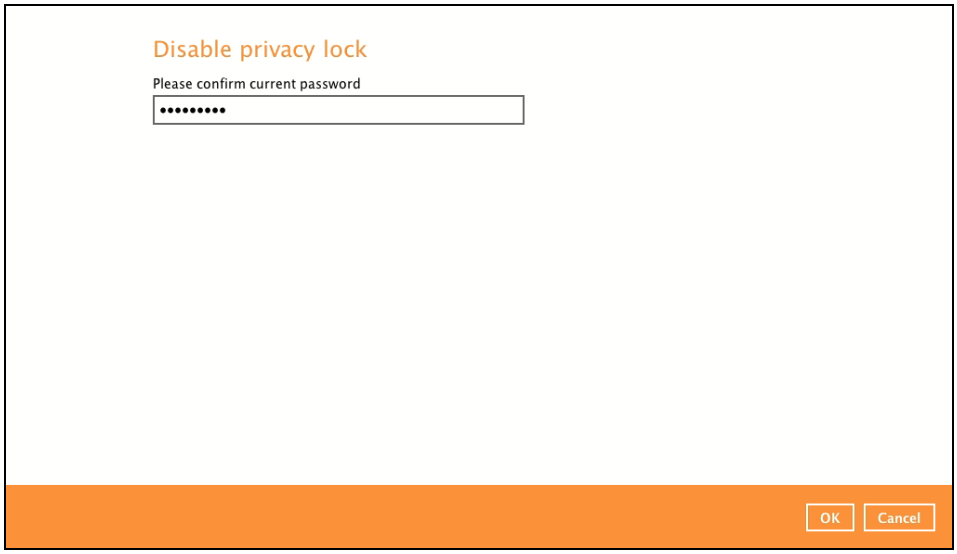


To disable the Privacy Lock feature, follow the instructions below:

1. Swipe the lever to the left to turn it off.



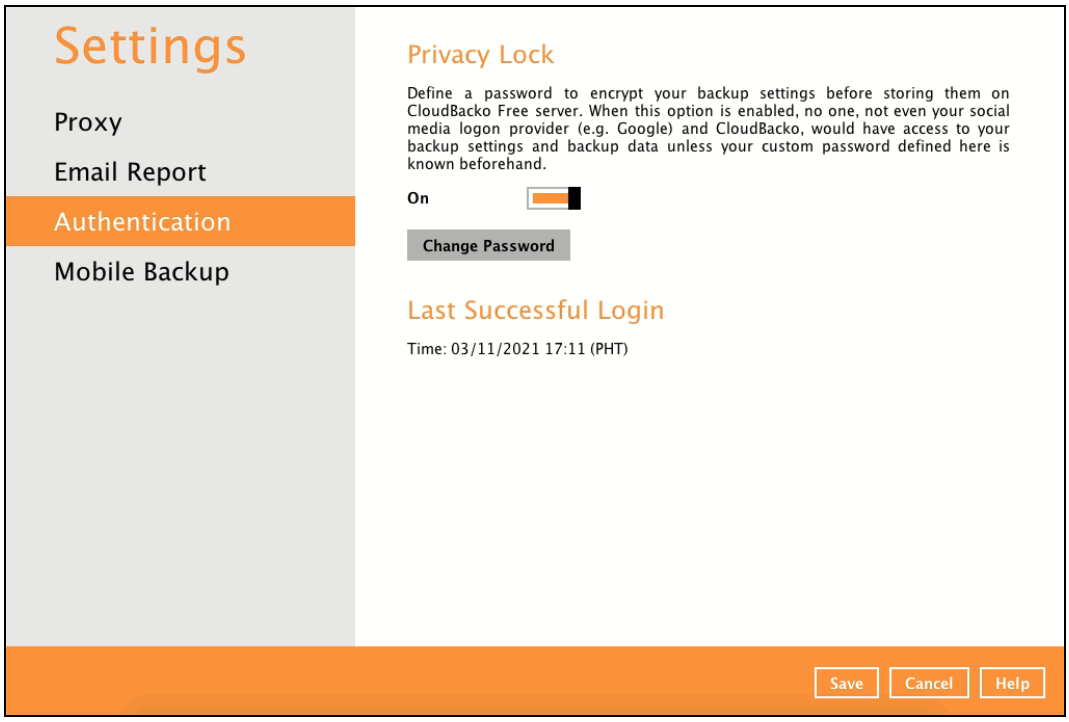
2. Enter the current password for authentication purposes.



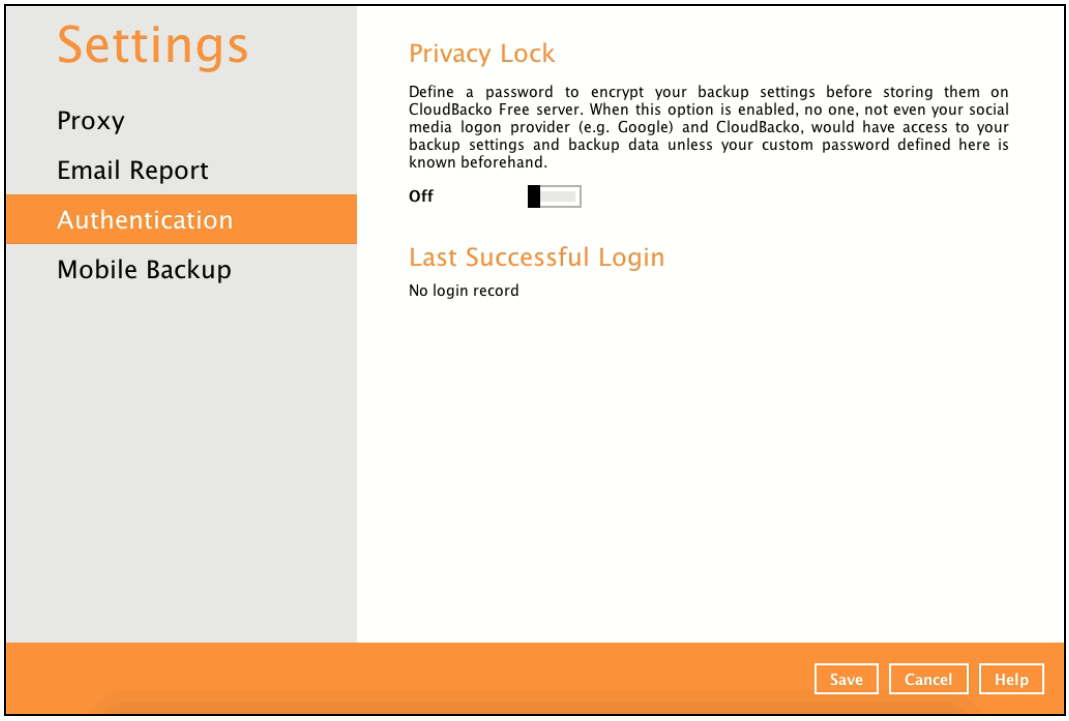
3. Click **OK** then click **Save** button to store the settings.

Last Successful Login

Displays the Date, Time, Timezone the user last logged in and the registered mobile device.



Below is the screenshot If there is no login record yet.



7.7.4 Mobile Backup

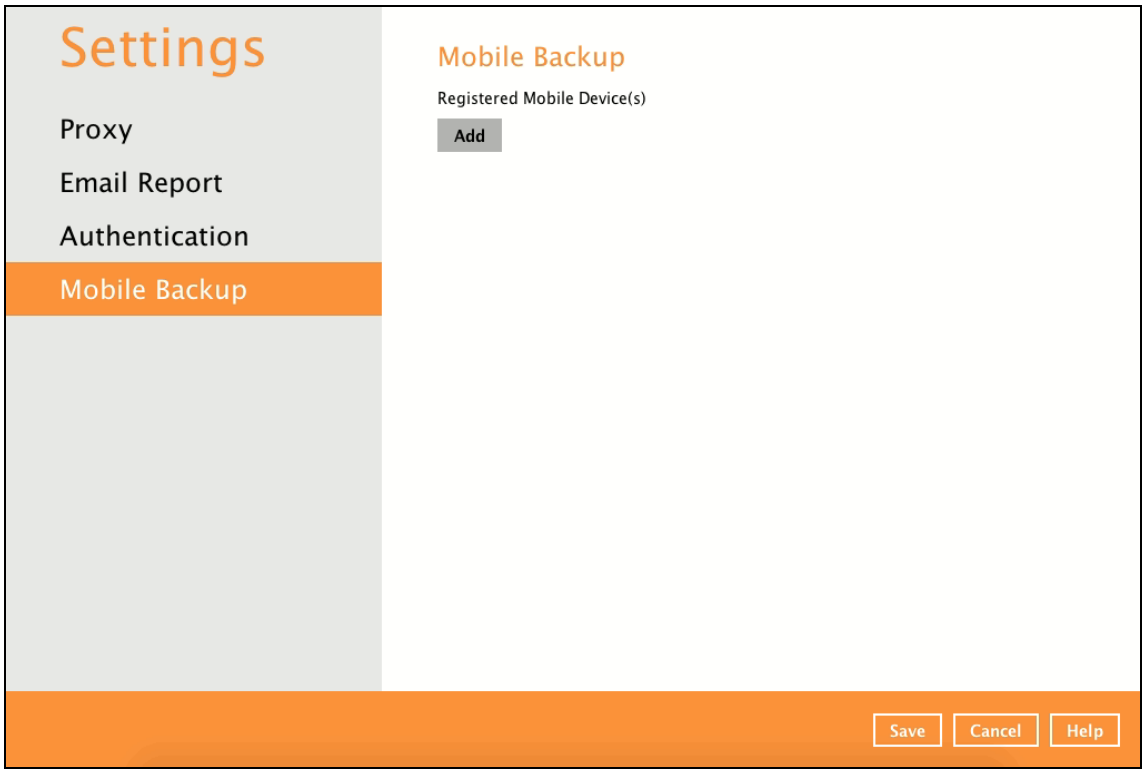
You can use the Mobile backup function to:

- Add one or more device(s) registered for Mobile Backup
- View backed up photos, videos and documents saved in the mobile backup destination.
- Change your mobile backup destination to:
  - new location in the same local machine
  - new machine
- Remove one or more device(s) registered for mobile backup.

NOTE

For the restore of photos, videos, documents and 2FA accounts to an alternate mobile device, the other mobile devices must be registered first for mobile backup on CloudBacko Home.

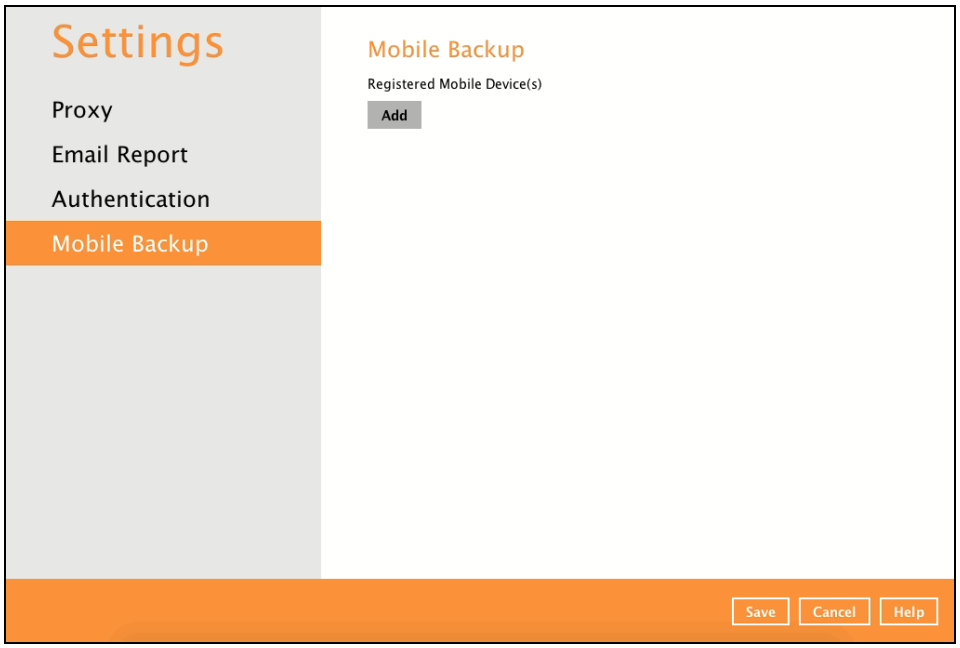
- Restore to a different mobile device on the same operating system.
- Restore to a different mobile device on another operating system, i.e., Android to iOS or iOS to Android.



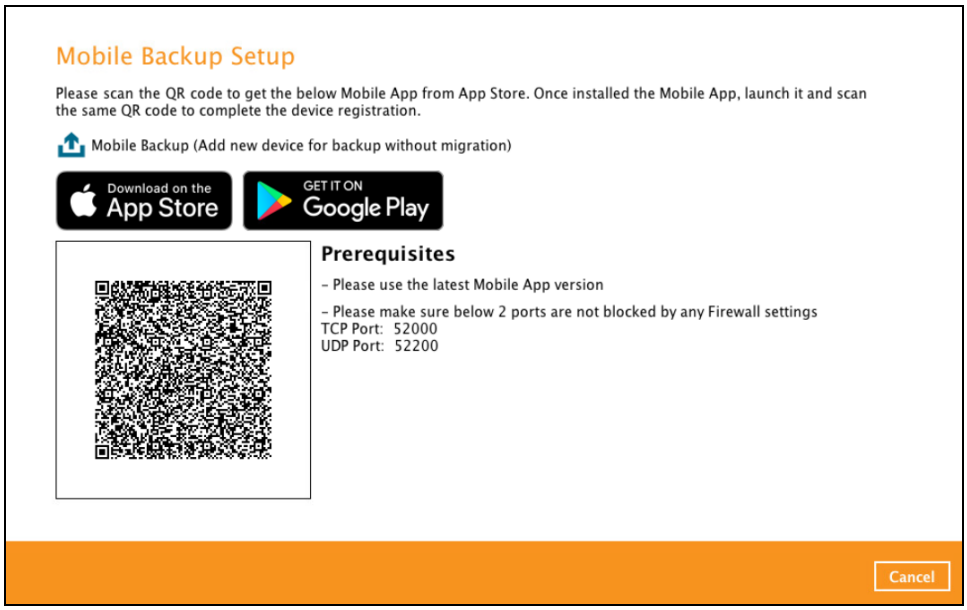
Add one or more device(s) registered for Mobile Backup

To add a mobile device, follow the instructions below:

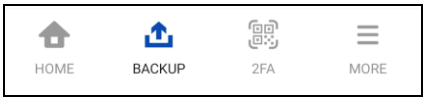
1. Go to **Settings** > **Mobile Backup** and click **Add**

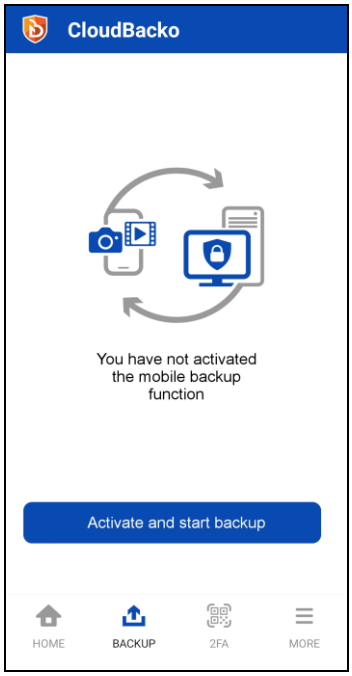


2. Download the CloudBacko app from Google Play Store for an Android device and from App Store for an iOS device and click **Next**.



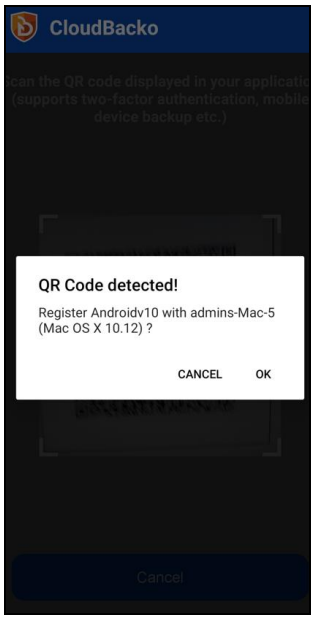
3. In the CloudBacko app, go to **Backup.** Tap **Activate and start backup** link to scan the QR Code on the CloudBacko Home.



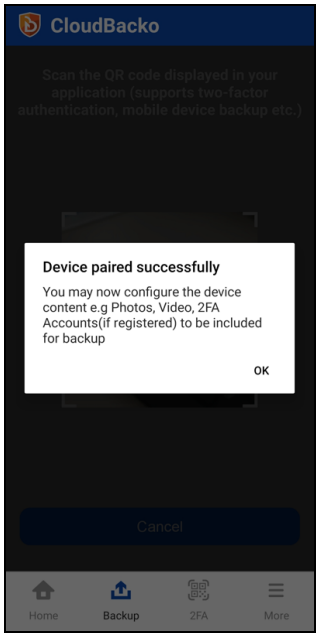


4. Scan the QR Code which can be found in CloudBacko Home. Otherwise, tap **Cancel** to return to previous screen.

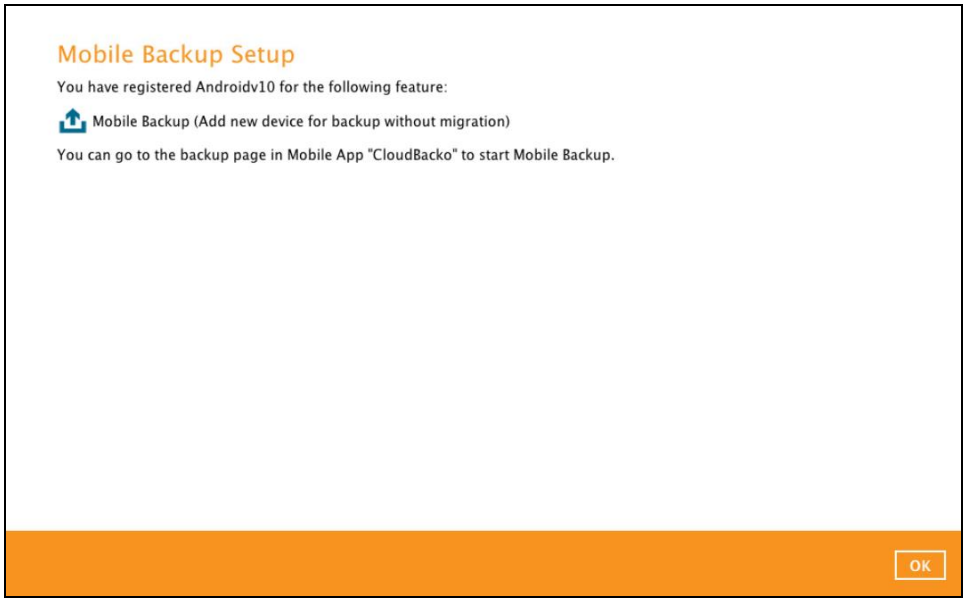
5. QR Code is detected, tap **OK** to proceed. Otherwise, tap **Cancel**.



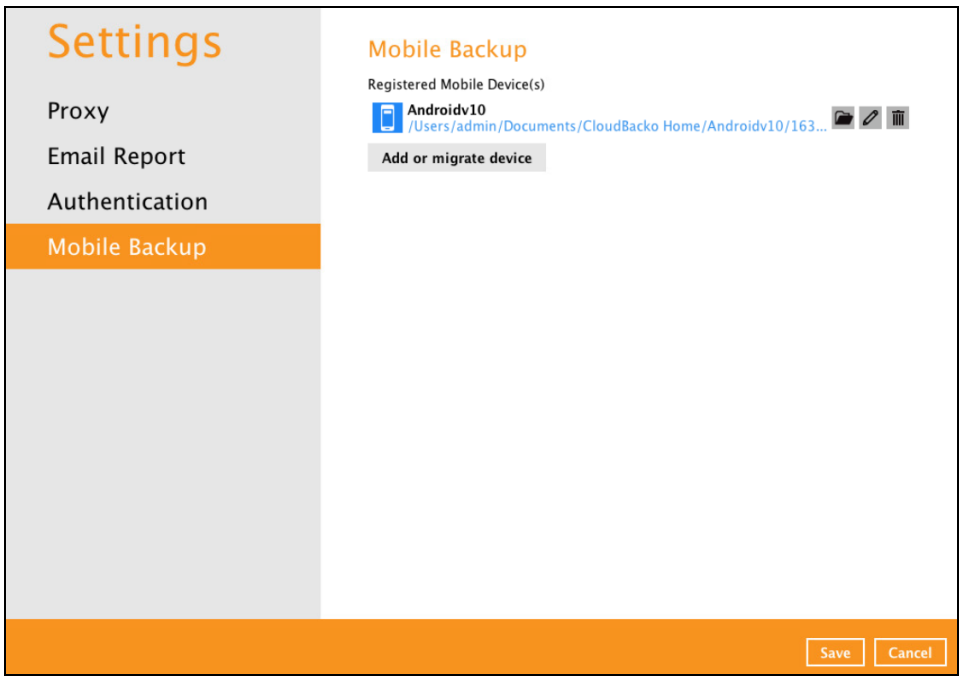
6. Mobile backup registration is successful. Tap **OK** to proceed.



Mobile backup registration is successful in CloudBacko Home. Click **OK** to finish the registration.



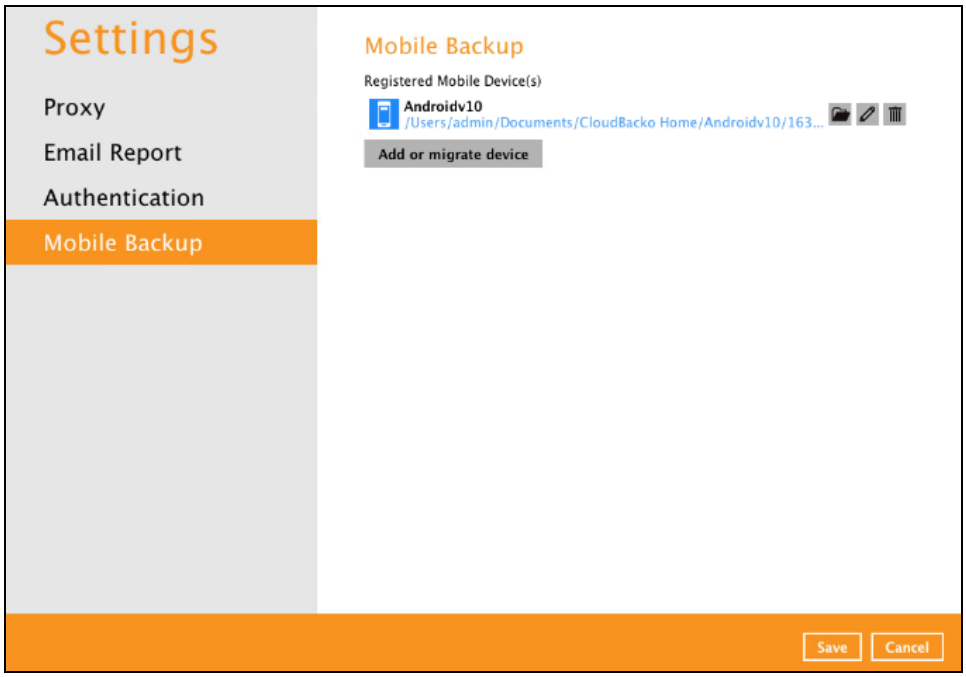
The registered mobile device will now be displayed.



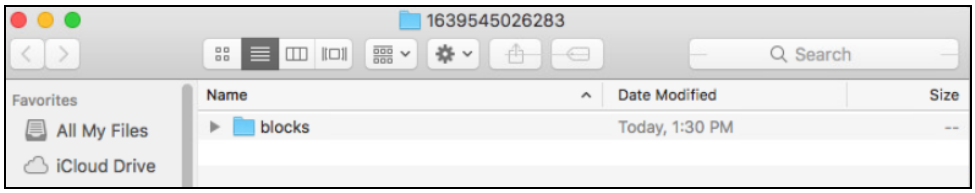
View backed up photos, videos and documents saved in the mobile backup destination

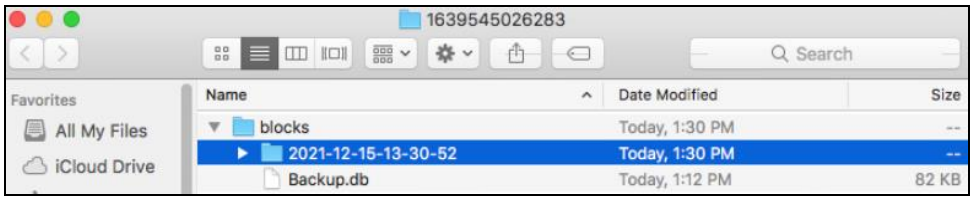
To view backed up photos, videos and documents saved in the mobile backup destination, follow the instructions below:

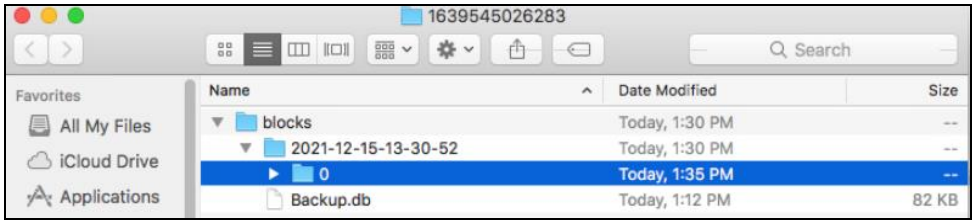
1. Click the **link** or the **Browse** icon on the right side of the registered mobile device.

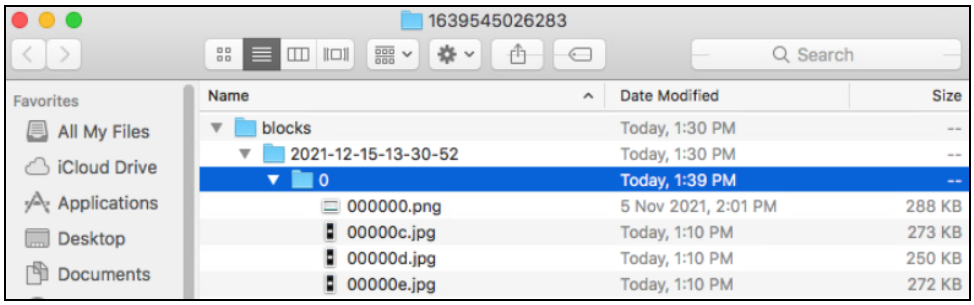


2. A new window will be displayed. Double-click the **blocks** folder, then double-click the folder named with the "YYYY-MM-DD-hh-mm-ss" format which is the date and time of the backup. This contains the folders where the photos, videos and documents are saved.









After viewing the backed up files, click the **X** button to exit.

Change mobile backup destination to new location in the same machine

These are scenarios upon changing the mobile backup destination to a new location in the same local machine:

- **Move to a new location in the same machine with enabled Free up space.**

  If Free up space is enabled on the CloudBacko Mobile app, it is required to copy the previously backed-up photos, videos, documents and 2FA accounts to the new location to prevent missing data upon restore.

  In case the previously backed up photos, videos, documents and 2FA accounts were not copied to the new location, even though the backup will re-upload all the photos, videos, documents and 2FA accounts again from the mobile device, this will not include the photos, videos, documents and 2FA accounts removed by the Free up space feature.

- **Move to a new location in the same machine with disabled Free up space.**

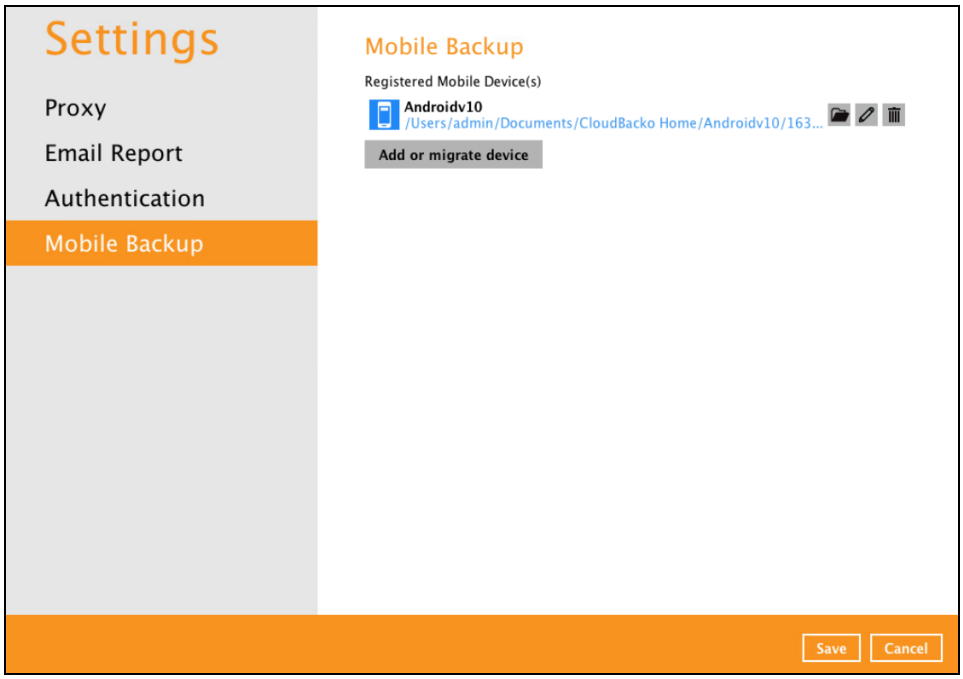
  If Free up space is disabled on the CloudBacko Mobile app, there are two (2) options available, copy the previously backed-up photos, videos, documents and 2FA accounts to the new location or continue to back up in the new location.

  In case the previously backed-up photos, videos, documents and 2FA accounts were not copied to the new location, the backup will re-upload all the photos, videos, documents and 2FA accounts again from the mobile device.

To change the mobile backup destination to another drive or folder on the CloudBacko machine, follow the instructions below:

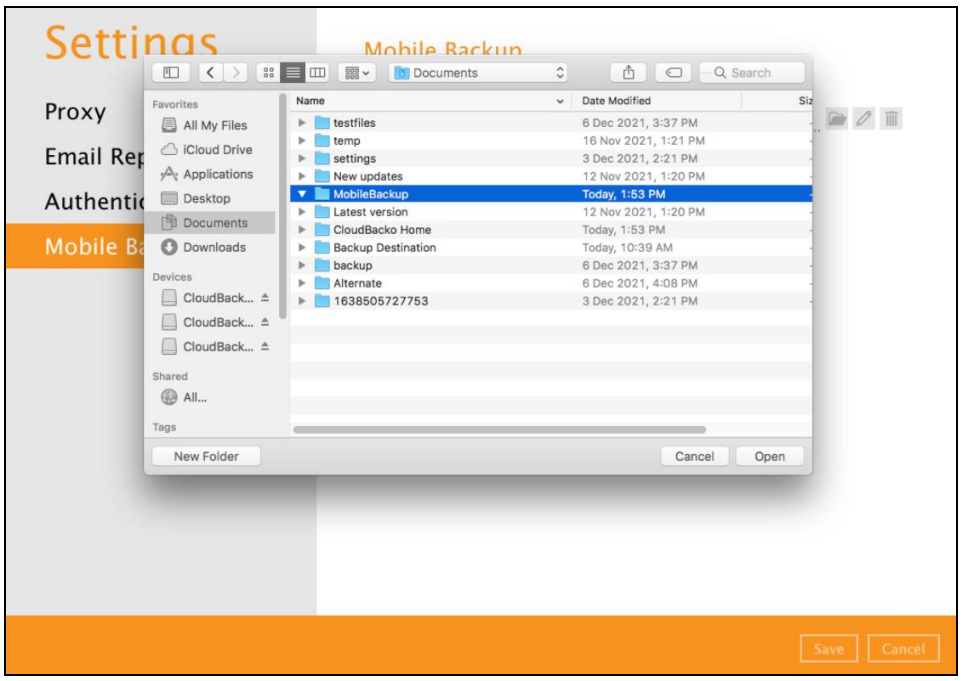
1. From the old location, secure a copy of the previously backed up photos, videos, documents and 2FA accounts. Skip this step if Free up space is disabled and proceed to Step 2.
2. Launch **CloudBacko Home**.

3. Go to **Settings** > **Mobile Backup**. Click the **Edit** icon on the right side of the registered mobile device.



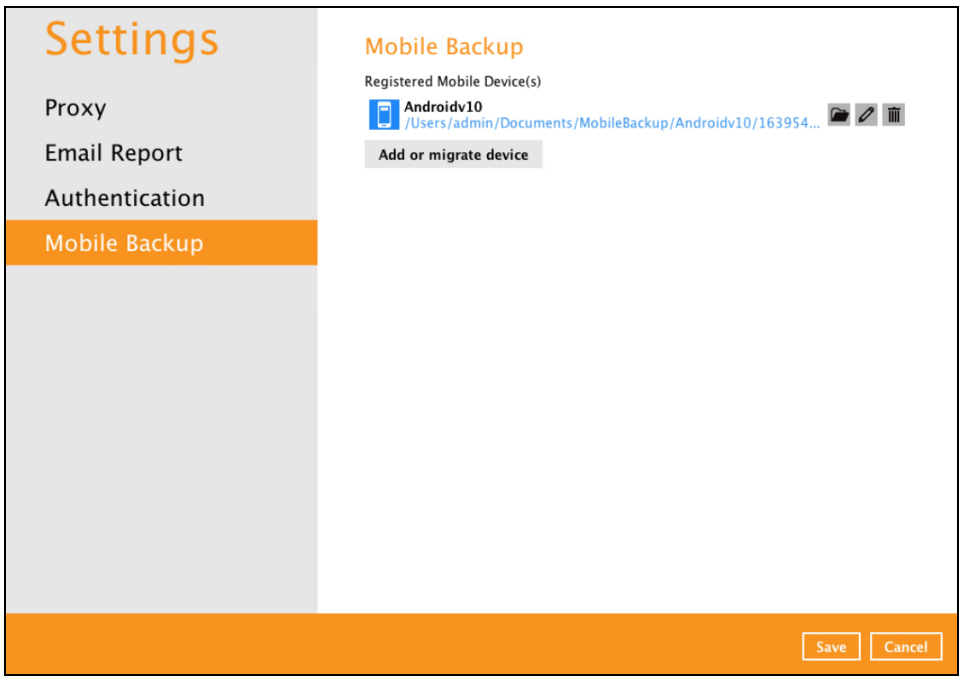
4. Select a new mobile backup destination then click **Open**.

   In this example, the new mobile backup destination will be **/Users/admin/Documents/MobileBackup**.



5. Click **Save** to store the change made. Otherwise, click **Cancel**.

   Mobile backup destination is successfully changed to **/Users/admin/Documents/MobileBackup**.



NOTE

The registered mobile device and backup set ID will be appended automatically to the new mobile backup destination.

6. Copy the previously backed up photos, videos, documents and 2FA accounts from the original location in the new mobile backup destination.

Change mobile backup destination to new machine

These are scenarios upon changing the mobile backup destination to a new machine:

- **Move to a new machine with enabled or disabled Free up space due to a broken, stolen, or lost machine.**

  If the machine is broken, stolen, or lost, the previously backed-up photos and videos are permanently gone. Also note that if Free up space is enabled on the CloudBacko Mobile app, all photos, videos, documents and 2FA accounts removed by the Free up space feature are permanently lost.

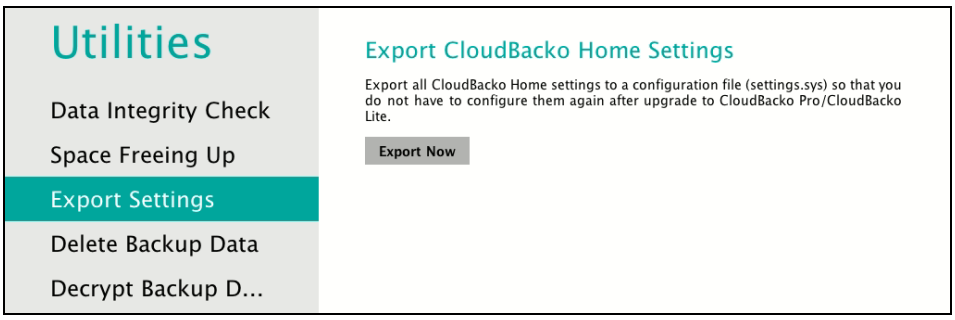
- **Move to a new machine with enabled or disabled Free up space due to upgrade.**

  If the machine needs upgrading, the previously backed-up photos and videos are still available. Also note that if Free up space is enabled on the CloudBacko Mobile app , it is required to copy the previously backed-up photos, videos, documents and 2FA accounts to the new machine to prevent missing data upon restore.

  Even if Free up space is disabled, it is recommended to copy the previously backed up photos, videos, documents and 2FA accounts to the new machine. Otherwise the photos, videos, documents and 2FA accounts on the mobile device will be backed up again from scratch.

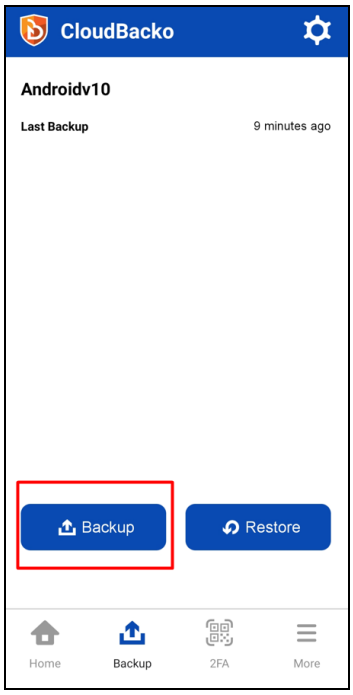
To change the mobile backup destination to a new machine, follow the instructions below:

1. From the old machine,
   - secure a copy of the previously backed up photos, videos, documents and 2FA accounts.
   - save a copy of the configuration file by going to **Utilities** > **Ex/Import** Setting then click **Export Now**. Select the destination where the file will be saved.

   Skip this step if the old machine is broken, stolen, or lost and proceed to Step 2.
2. On the new machine, install **CloudBacko Home**.
3. Login using the same social media account to retrieve the CloudBacko Home settings.
4. If the mobile backup destination needs to be updated, select a new destination. Otherwise, skip this step and proceed to step 5.
5. Copy the previously backed up photos, videos, documents and 2FA accounts from the old machine in the new mobile destination. Skip this step if the old machine is broken, stolen, or lost and proceed to Step 6.
6. Restart the **CloudBacko Home Services** on a newly installed CloudBacko Home to restart the MBS.

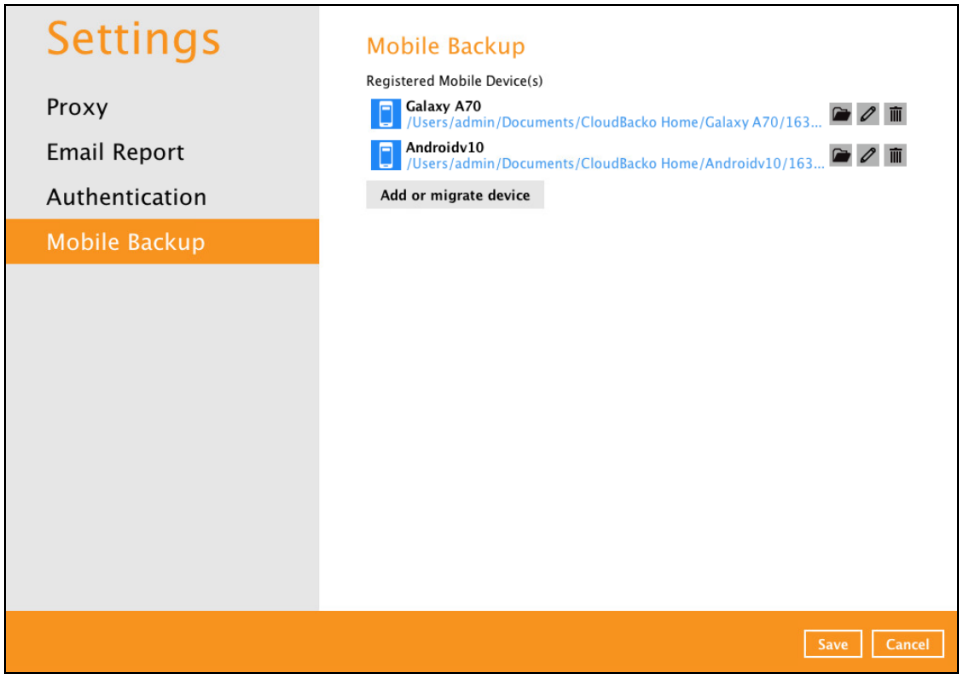
7. Start backup of photos, videos, documents and 2FA accounts.



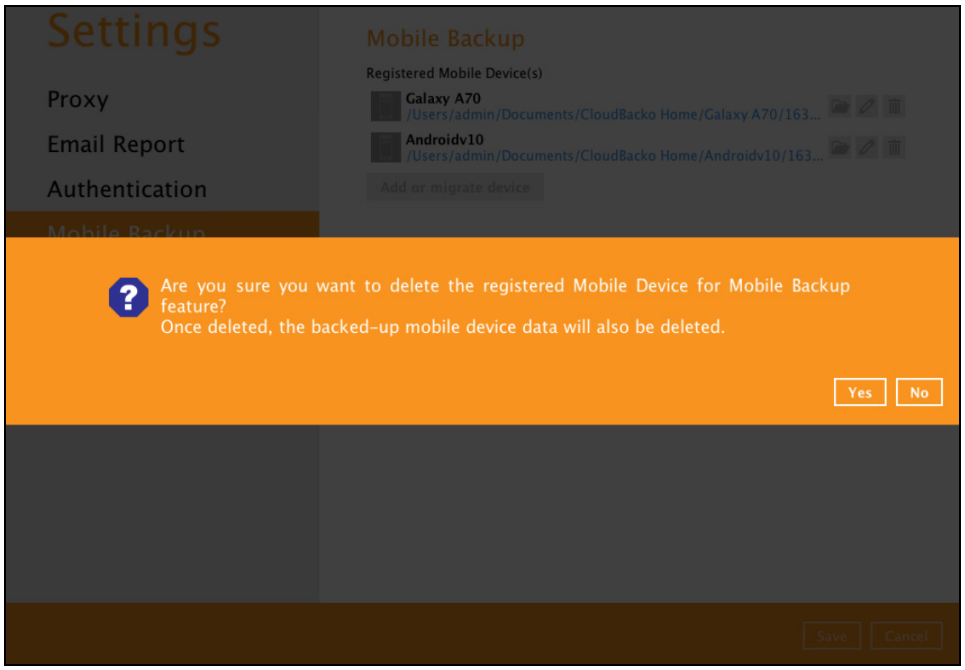
Remove one or more device(s) registered for Mobile Backup

To remove a mobile device, follow the instructions below:

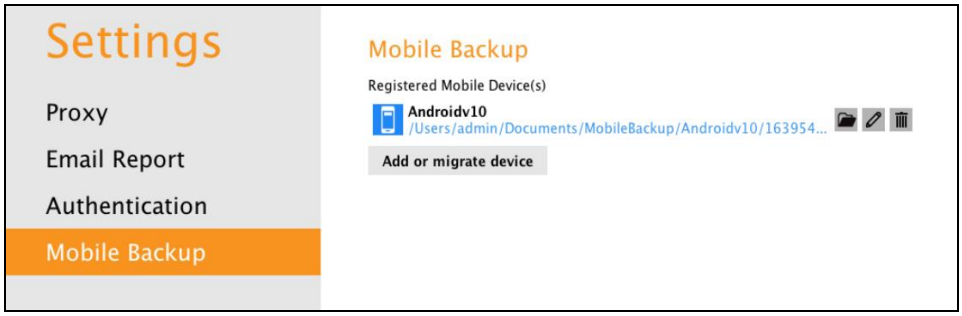
1. Click **Delete** icon on the left side of the registered mobile device.



2. A confirmation message will appear, click **Yes** to proceed. Otherwise, click **No**.

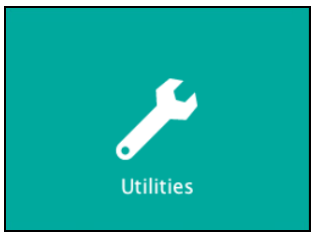


3. Mobile device is successfully removed along with any photos, videos, documents and 2FA accounts backed up in the mobile backup destination.



7.8 Utilities

This feature allows user to perform **quality check** of the index file and backed-up data, **free up storage space**, **delete,** and **decrypt** backed-up data.



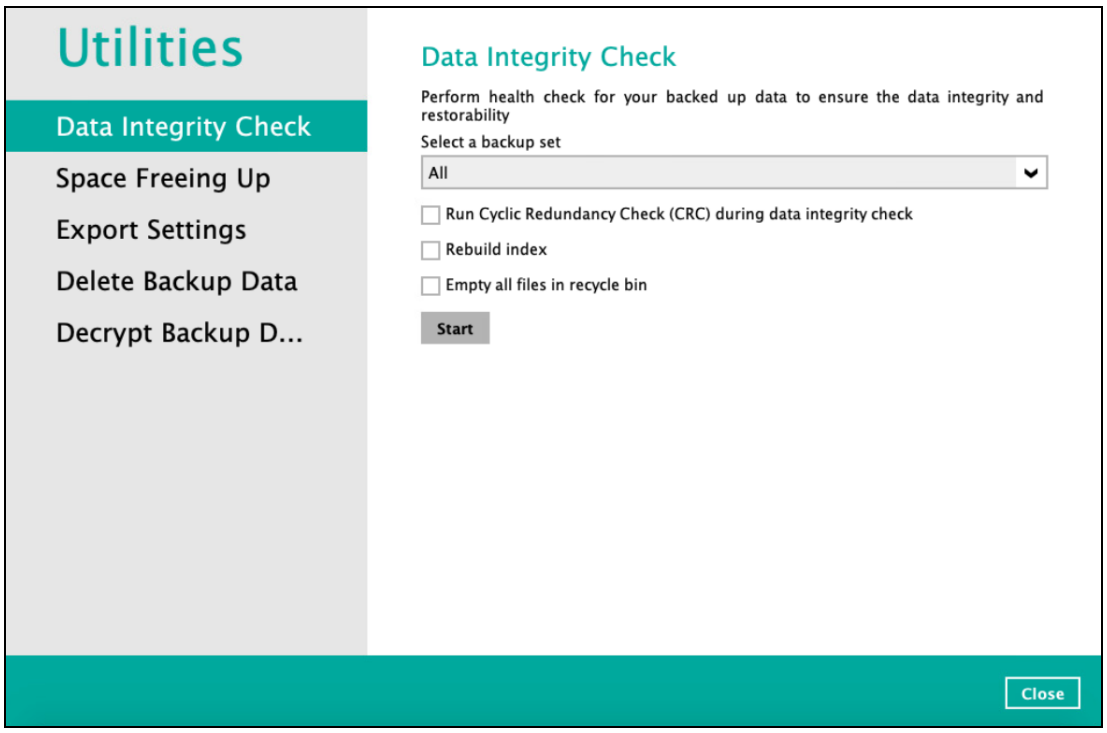
There are five (5) options available for this feature:

- Data Integrity Check
- Space Freeing Up
- Export Settings
- Delete Backup Data
- Decrypt Backup Data

7.8.1 Data Integrity Check

The Data Integrity Check (DIC) is used to identify the data in the backup set that has index-related issues, remove any corrupted file(s) from the backup destination(s) to ensure the integrity of the backup data and its restorability, and update the storage statistics.

For an efficient management of overall storage size of the backup destination(s), the data integrity check job will perform check for the backup destination(s) to remove old index files that are more than ninety (90) days old in the backup job folder(s).



NOTE

1. Data Integrity Check CANNOT fix or repair files that are already corrupted.
2. Data Integrity Check can only be started if there is NO active backup or restore job(s) running on the backup set selected for the DIC job. As the **backup**, **restore** and **data Integrity check** are using the same index for read and write operations. Otherwise, an error message will be displayed in the post-DIC to indicate the data integrity check is completed with error(s) and that the data integrity check had skipped a backup set with an active backup job.

- **Run Cyclic Redundancy Check (CRC)**

  When this option is enabled, the DIC will perform check on the integrity of the files on the backup destination(s) against the checksum file generated at the time of the backup job.

  If there is a discrepancy, this indicates that the files on the backup destination(s) are corrupted and will be removed from the backup destination(s). If these files still exist on the client machine on the next backup job, AhsayOBM will upload the latest copy of the files.

  However, if the corrupted files are in the Retention Area, they will not be backed up again as the source file has already been deleted from the client machine.

  The time required to complete a data integrity check depends on the number of factors such as:

  - number of files and/or folders in the backup set(s)
  - bandwidth available on the client computer
  - hardware specifications of the client computer such as, the disk I/O and CPU performance

  NOTE

  1. For user(s) with metered internet connection, additional data charges may be incurred if the Cyclic Redundancy Check (CRC) is enabled. As CRC data involves downloading the data from the backup destination(s) to the client machine in order to perform this check.
  2. To find out how much data is downloaded from the backup destination(s) for the CRC check, please refer the value for Utilities in the Data Transfer Statistics on Ch. 7.5.3.

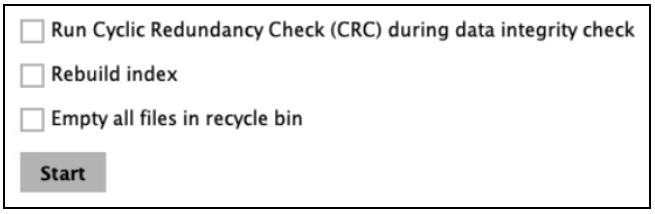
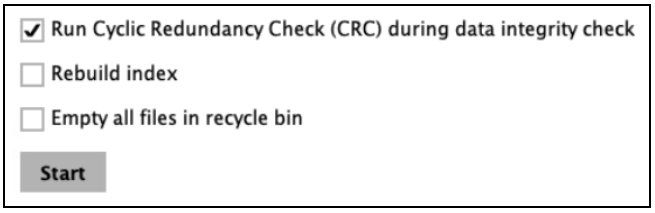
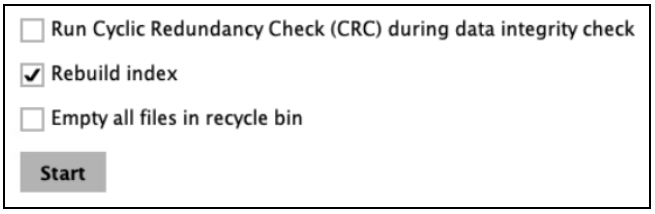
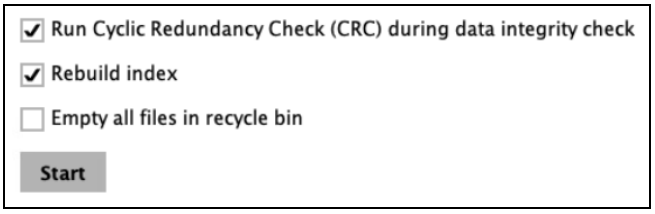
- **Rebuild Index**

  When this option is enabled, the data integrity check will start rebuilding corrupted index and/or broken data blocks if there are any.

- **Empty all files in recycle bin**

  When this option is enabled, all the files in the Recycle Bin will be deleted.

There are four (4) options in performing the Data Integrity Check:

Option 1 	For checking of index and data.
Option 2 	For checking of index and integrity of files against the checksum file generated at the time of the backup job.
Option 3 	For checking and rebuilding of index.
Option 4 	For checking of index, integrity of files against the checksum file generated at the time of the backup job and rebuilding of index.

The following diagrams show the detailed process of the Data Integrity Check (DIC) in four (4) modes:

- **Option 1**

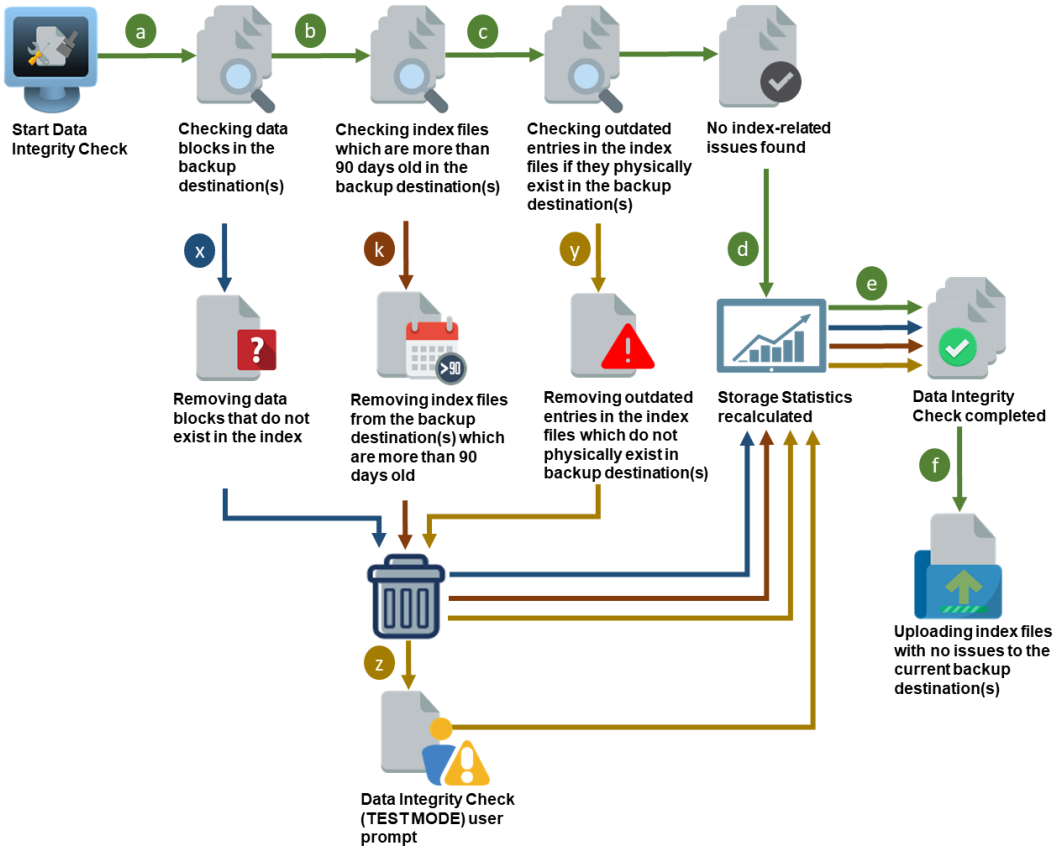
  Disabled Run Cyclic Redundancy Check (CRC) and Rebuild index (Default mode)
- **Option 2**

  Enabled Run Cyclic Redundancy Check (CRC) and Disabled Rebuild index
- **Option 3**

  Disabled Run Cyclic Redundancy Check (CRC) and Enabled Rebuild index
- **Option 4**

  Enabled Run Cyclic Redundancy Check (CRC) and Rebuild index

Option 1: Disabled Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Rebuild Index (Default mode)



a Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.
- ➔ If **YES**, proceed to b
- ➔ If **NO**, proceed to x

b Check the index files in the backup destination(s) to determine if they were more than 90 days old.
- ➔ If **YES**, proceed to k
- ➔ If **NO**, proceed to c

c Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).
- ➔ If **YES**, proceed to d
- ➔ If **NO**, proceed to y

d Storage Statistics for Data area and Retention area usage will be recalculated.

e Data integrity check is completed.

f Index files with no issues will be uploaded to the current backup destination(s).

x Data blocks (.bak files) that do not exist in the index and partially uploaded orphan files will be automatically removed from the backup destination(s).

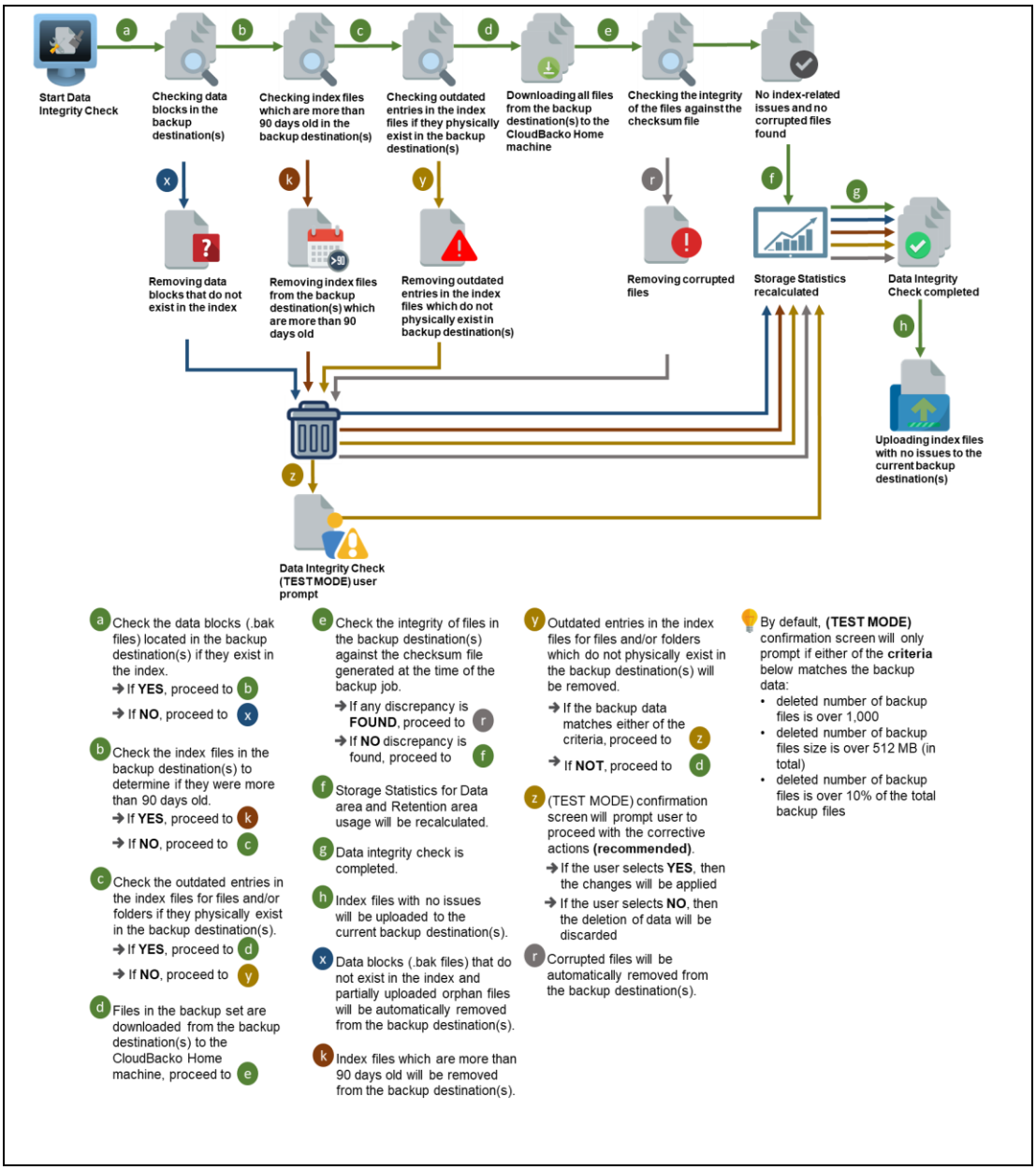
k Index files which are more than 90 days old will be removed from the backup destination(s).

y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.
- ➔ If the backup data matches either of the criteria, proceed to z
- ➔ If **NOT**, proceed to d

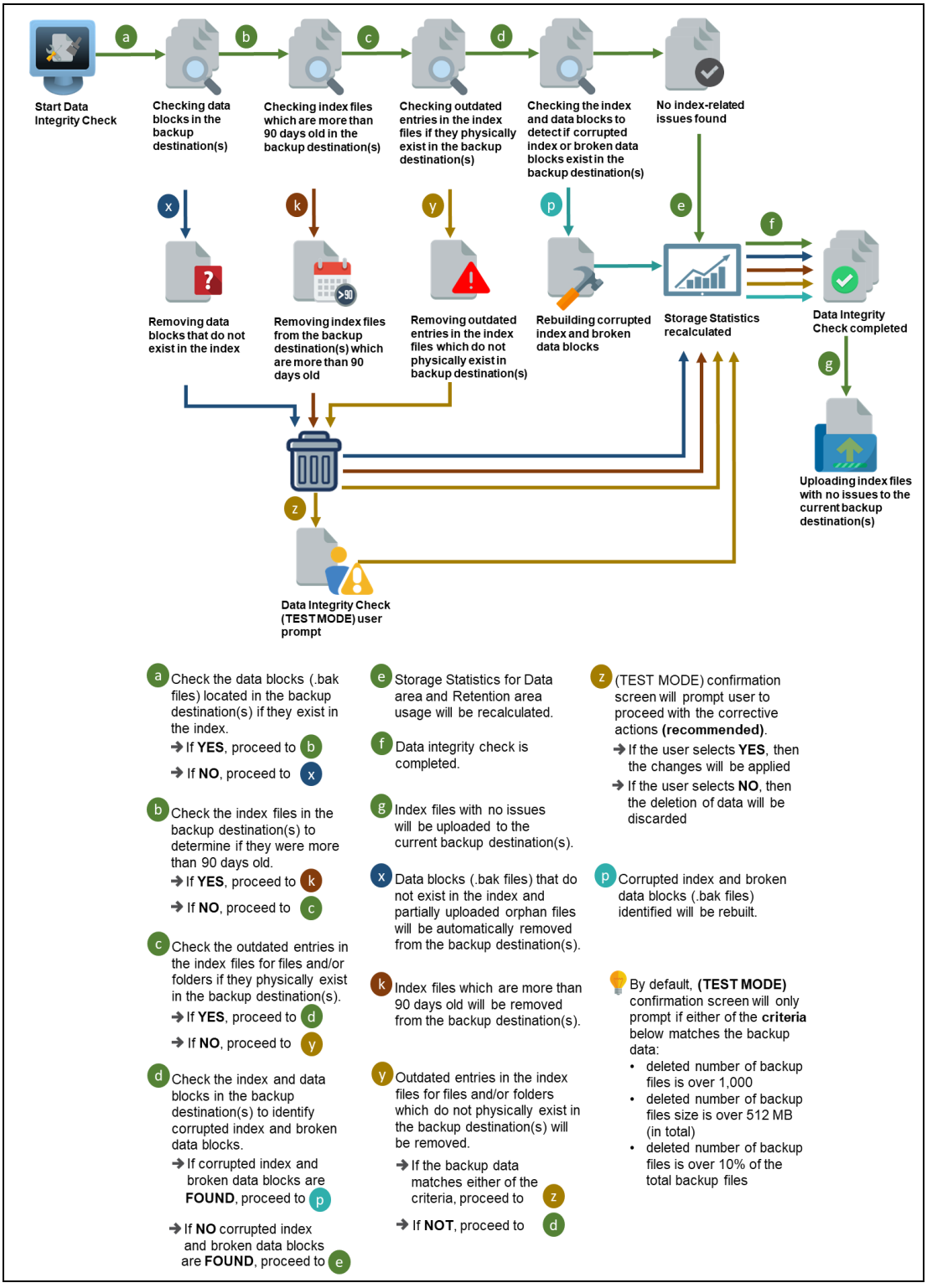
z (TEST MODE) confirmation screen will prompt user to proceed with the corrective actions **(recommended)**.
- ➔ If the user selects **YES**, then the changes will be applied
- ➔ If the user selects **NO**, then the deletion of data will be discarded

By default, **(TEST MODE)** confirmation screen will only prompt if either of the **criteria** below matches the backup data:
- deleted number of backup files is over 1,000
- deleted number of backup files size is over 512 MB (in total)
- deleted number of backup files is over 10% of the total backup files

Option 2: Enabled Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Disabled Rebuild Index



Option 3: Disabled Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Enabled Rebuild Index



a Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.
- → If **YES**, proceed to b
- → If **NO**, proceed to x

b Check the index files in the backup destination(s) to determine if they were more than 90 days old.
- → If **YES**, proceed to k
- → If **NO**, proceed to c

c Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).
- → If **YES**, proceed to d
- → If **NO**, proceed to y

d Check the index and data blocks in the backup destination(s) to identify corrupted index and broken data blocks.
- → If corrupted index and broken data blocks are **FOUND**, proceed to p
- → If **NO** corrupted index and broken data blocks are **FOUND**, proceed to e

e Storage Statistics for Data area and Retention area usage will be recalculated.

f Data integrity check is completed.

g Index files with no issues will be uploaded to the current backup destination(s).

x Data blocks (.bak files) that do not exist in the index and partially uploaded orphan files will be automatically removed from the backup destination(s).

k Index files which are more than 90 days old will be removed from the backup destination(s).

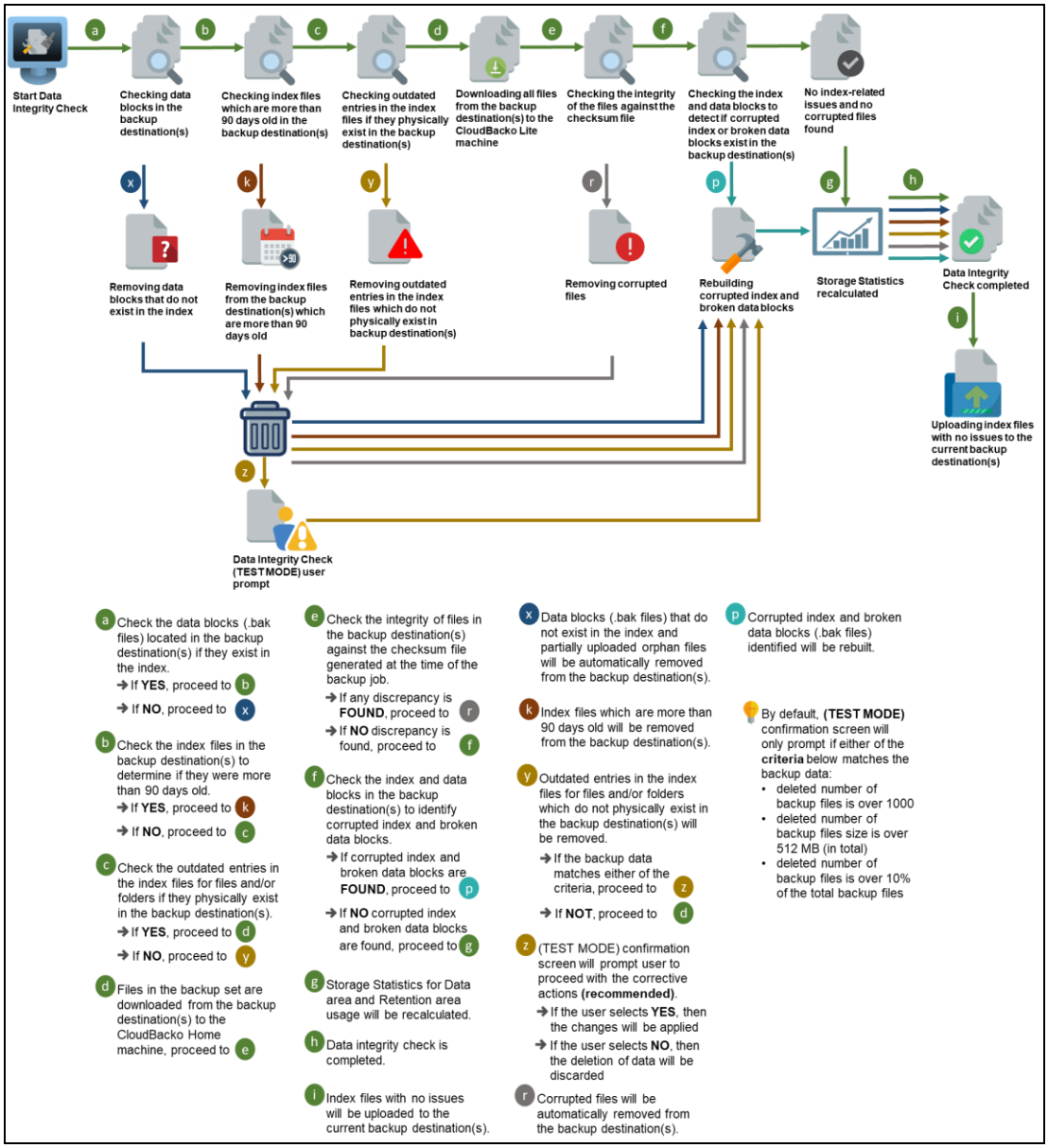
y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.
- → If the backup data matches either of the criteria, proceed to z
- → If **NOT**, proceed to d

z (TEST MODE) confirmation screen will prompt user to proceed with the corrective actions **(recommended)**.
- → If the user selects **YES**, then the changes will be applied
- → If the user selects **NO**, then the deletion of data will be discarded

p Corrupted index and broken data blocks (.bak files) identified will be rebuilt.

By default, **(TEST MODE)** confirmation screen will only prompt if either of the **criteria** below matches the backup data:
- deleted number of backup files is over 1,000
- deleted number of backup files size is over 512 MB (in total)
- deleted number of backup files is over 10% of the total backup files

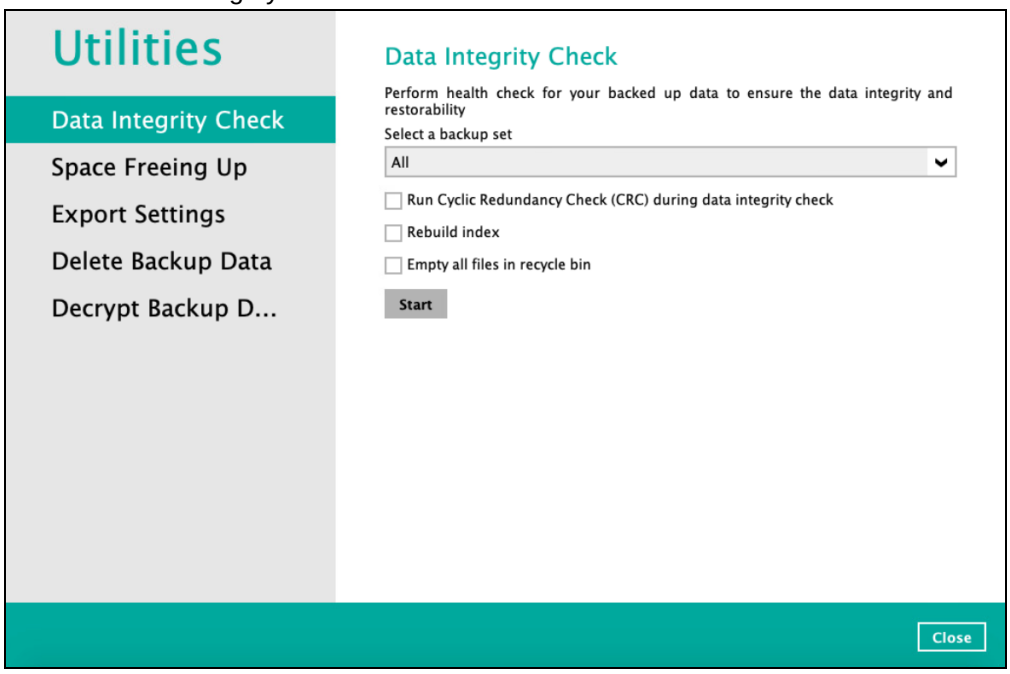
Option 4: Enabled Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Rebuild Index



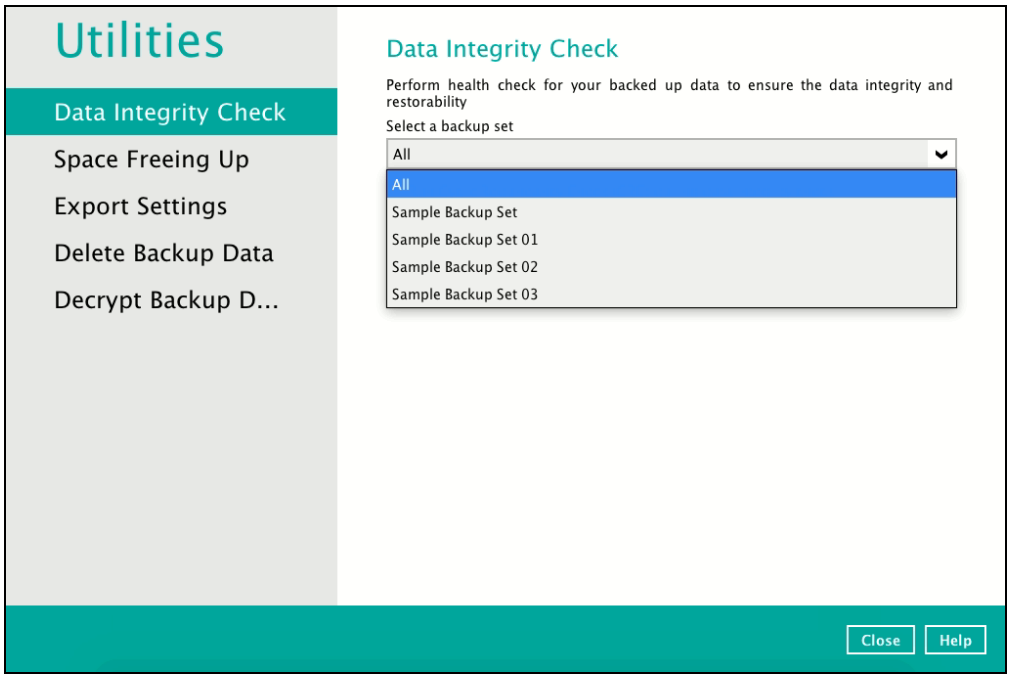
Perform a Data Integrity Check

To perform a Data Integrity Check, follow the instructions below:

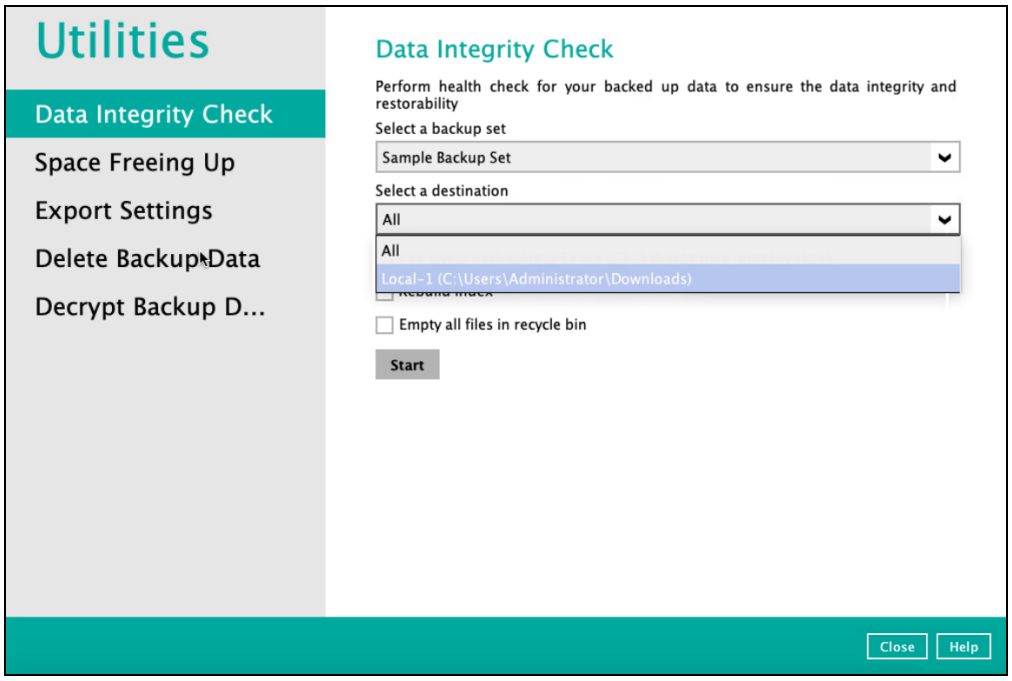
1. Go to the Data Integrity Check tab in the Utilities menu.



2. Click the drop-down button to select a backup set.

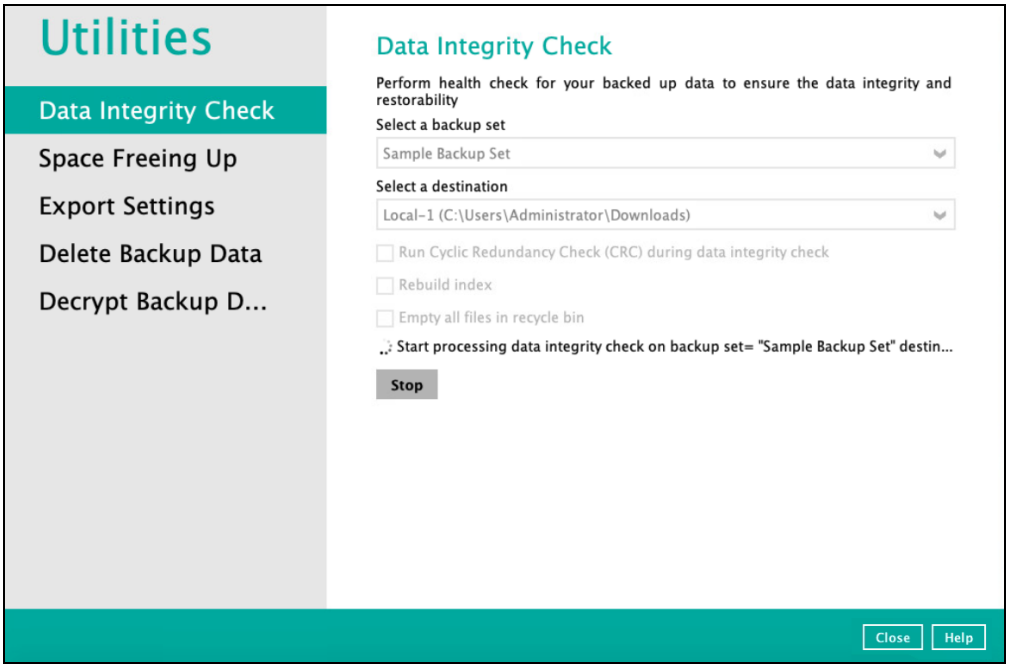


3. Click the drop-down button to select a backup destination.

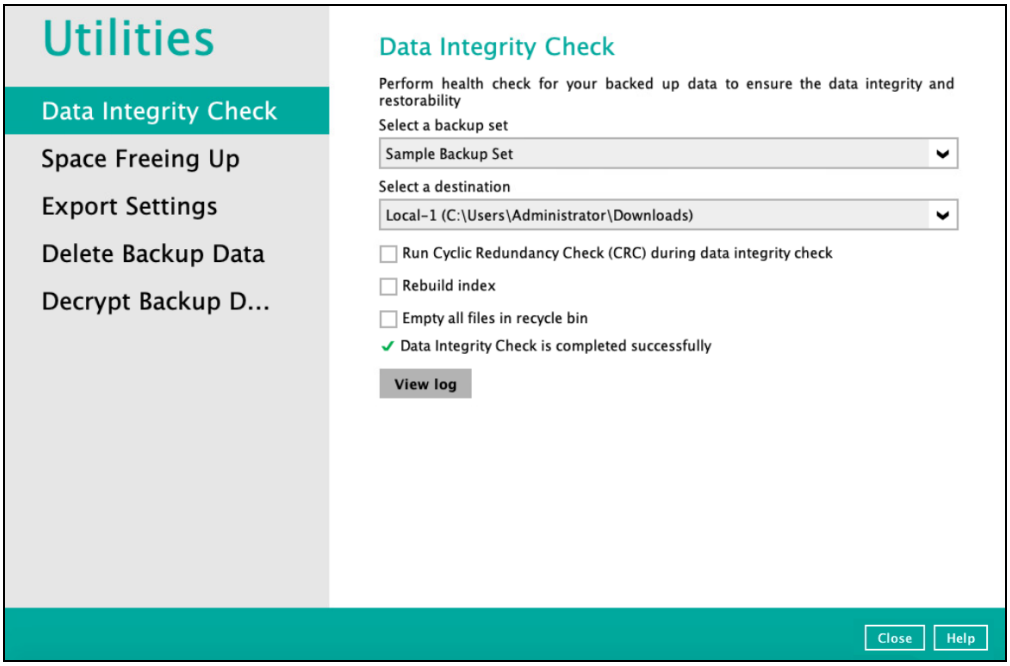


4. Click the Start button to begin the Data Integrity Check.

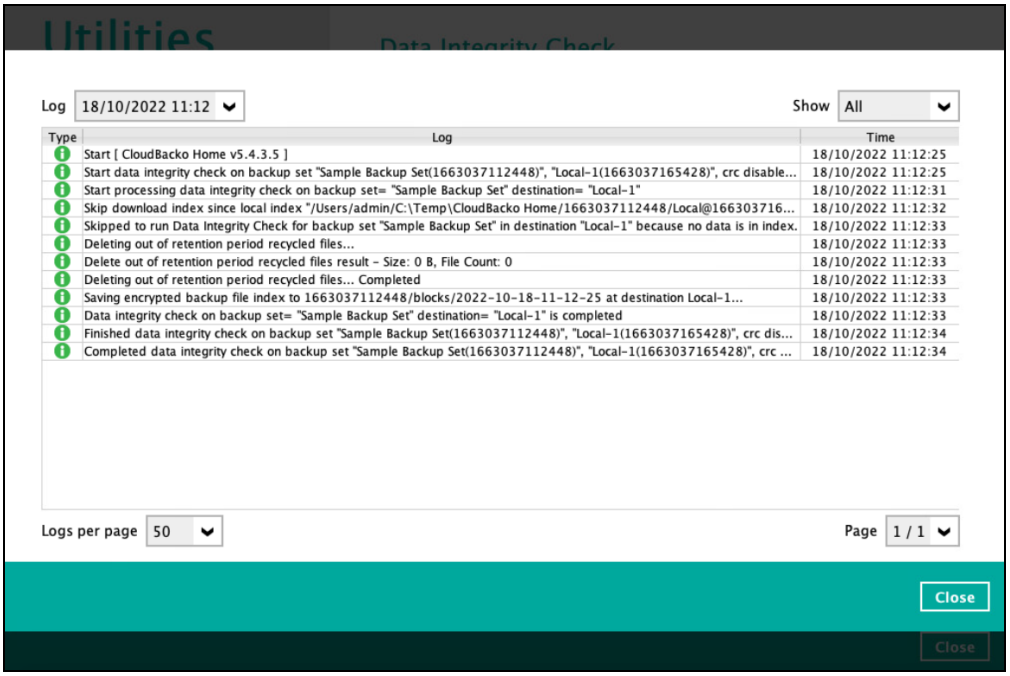
5. Data Integrity Check will start running on the selected backup set(s) and backup destination(s).



6. Once the DIC is complete, click the **View log** button to check the detailed process of the data integrity check.

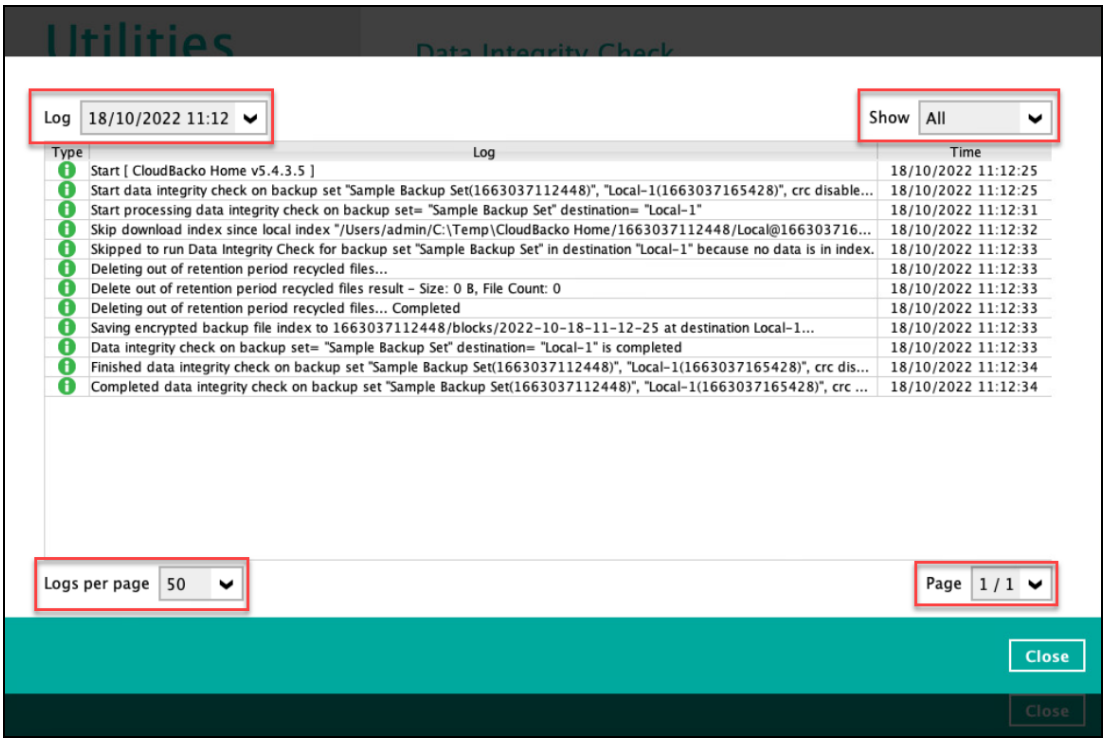


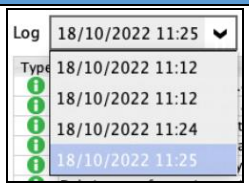
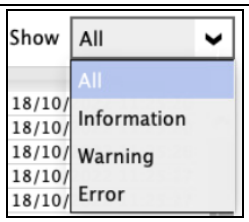
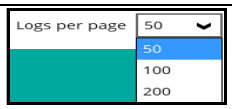
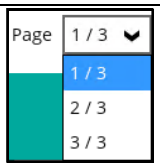
7. The detailed Data Integrity Check log will be displayed.



For further viewing of the detailed DIC log, there are four options that can be used:

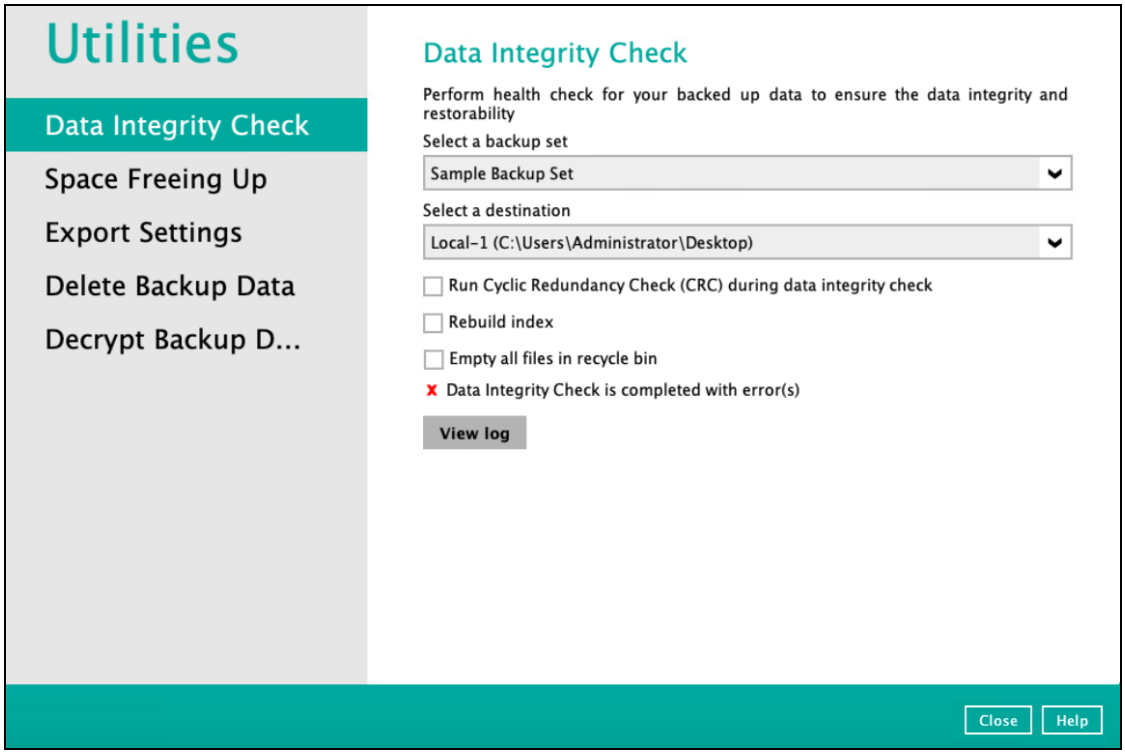
- Log filter
- Show filter
- Logs per page
- Page



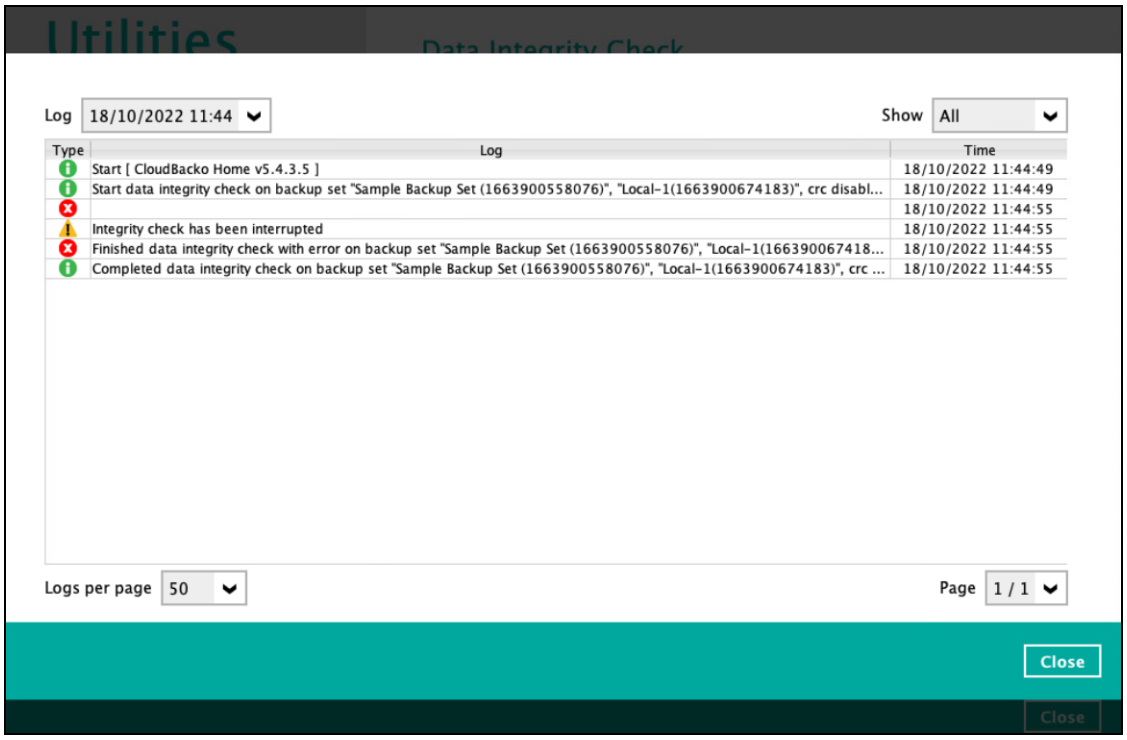
Control	Screenshot	Description
Log filter		This option can be used to display logs of the previous data integrity check jobs.
Show filter		This option can be used to sort the data integrity check log by its status (i.e. All, Information, Warning, and Error). With this filter, it will be easier to sort the DIC logs by its status especially for longer data integrity check logs.
Logs per page		This option allows user to control the displayed number of logs per page.
Page		This option allows user to navigate the logs to the next page(s).

7.8.1.1 Data Integrity Check Completed with Errors

The following screenshot is an example of a Data Integrity Check completed with error(s). A Data Integrity Check is run on a backup set with an active backup job running which resulted the Data Integrity Check to stop with error(s).



Clicking the **View log** button will display the details of the Data Integrity Check job error(s).

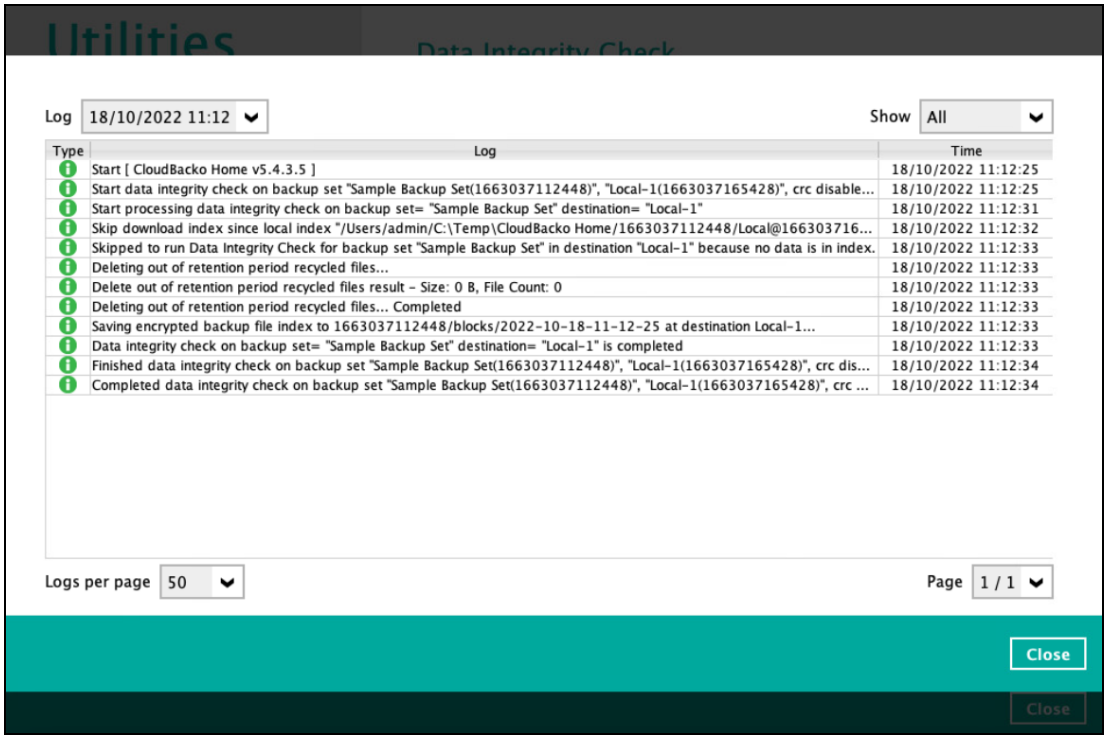


7.8.1.2 Data Integrity Check Result

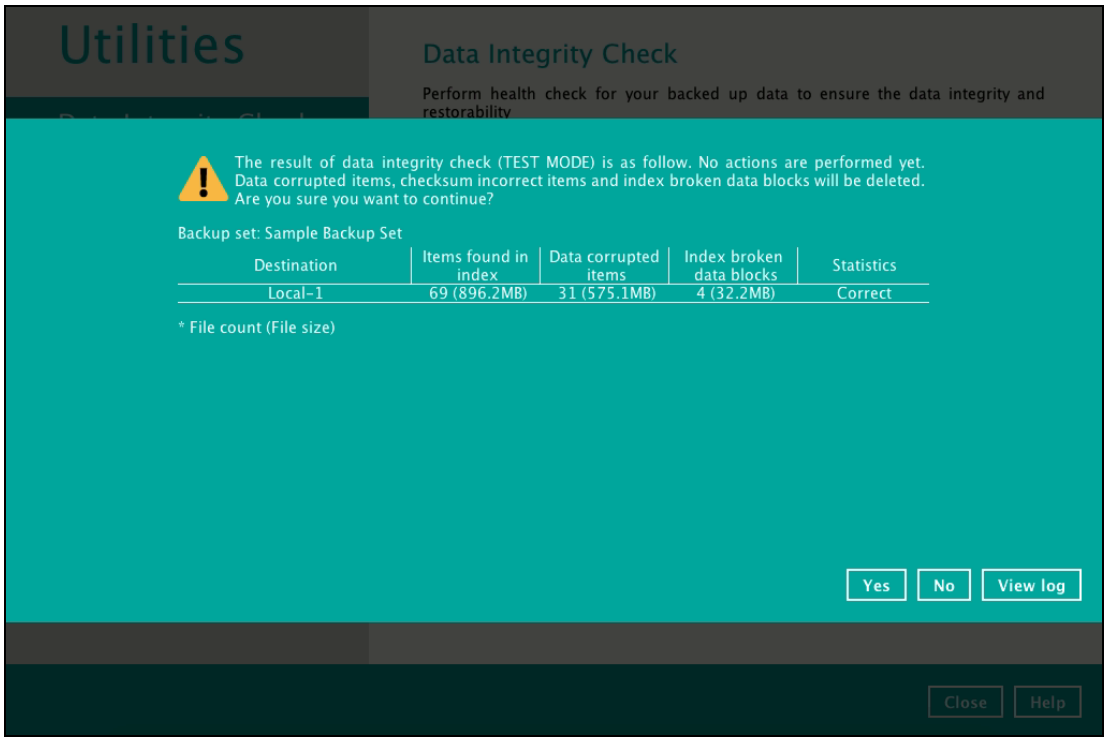
There are two possible outcomes after the completion of a data integrity check:

- Data Integrity Check is completed successfully with no data corruption/issues detected
- Corrupted data (e.g. index files, checksum files and/or broken data blocks) has been detected

The screenshot below shows an example of a data integrity check log with NO data corruption/issues detected.



If corrupted data is happened to be found, the (TEST MODE) confirmation screen will be displayed.



This is to inform the user of the following details:

- Backup set that contains an error
- Backup Destination
- Items found in index
- Data corrupted items
- Index broken data blocks
- Statistics (i.e. Correct or Incorrect)

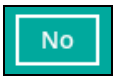
7.8.1.3 Test Mode Confirmation

The (TEST MODE) confirmation will ONLY prompt if either of the **criteria's** below matches the backup data during the data integrity check operation:

- deleted number of backup files is over 1,000
- deleted number of backup file size is over 512 MB (in total)
- deleted number of backup files is over 10% of total backup files

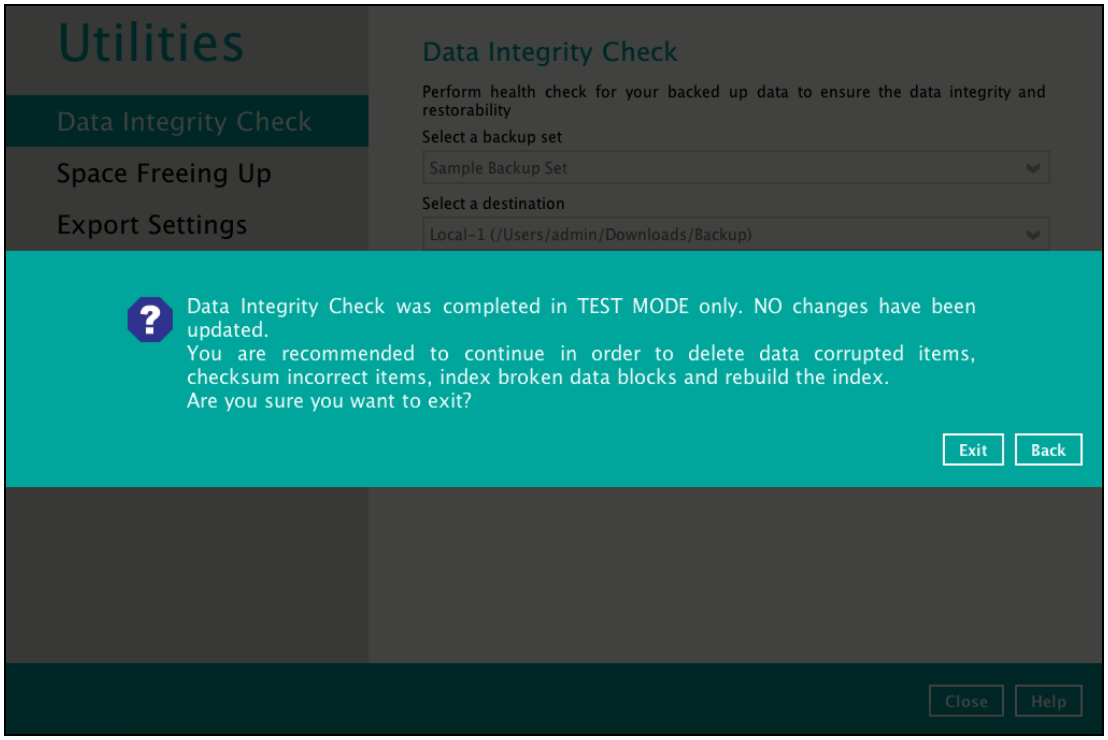
Otherwise, the Data Integrity Check job will **automatically** take corrective actions.

There are three options on the (TEST MODE) confirmation prompt:

Control	Screenshot	Description
Yes		Corrupted data (e.g. index files, checksum files and/or broken data blocks) will be deleted and statistics will be recalculated.
No		No action will be taken and a prompt message will be displayed.
View log		The detailed process of the data integrity check will be displayed.

Clicking **No** will display the following screen:

- If the **Exit** button is clicked, the data integrity check result will be discarded.
- If the **Back** button is clicked, it will go back to the (TEST MODE) confirmation screen.

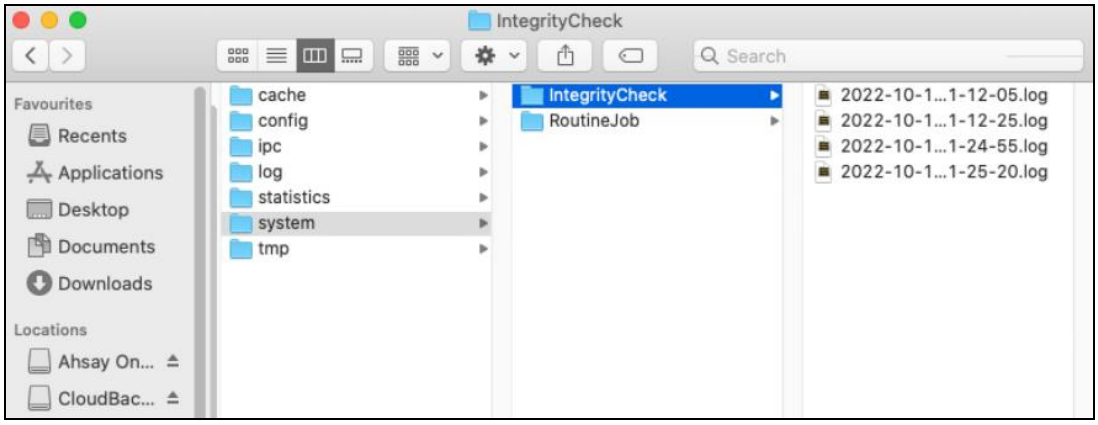


NOTES

1. It is strongly recommended to apply corrective actions when the (TEST MODE) confirmation screen pops up (clicking the **Yes** button). This is to ensure that the remaining corrupted file(s) will be removed from the backup destination(s), so on the next backup job, these files are backed up again if they are still present on the client machine. However, if the corrupted files are in Retention Area, then they will not be backed up again as the source file has already been deleted from the client machine.
2. If the DIC detects data blocks (.bak files) in the backup destination(s) that does not have related index entries, then these physical data blocks will be **automatically** removed from the backup destination(s) without the (TEST MODE) confirmation prompt.

Besides viewing the Data Integrity Check logs directly on the CloudBacko Home, they can be viewed on the file system of the CloudBacko Home machine. For CloudBacko Home Mac, the DIC logs are located in:

%UserProfile%/./cbh/system/IntegrityCheck

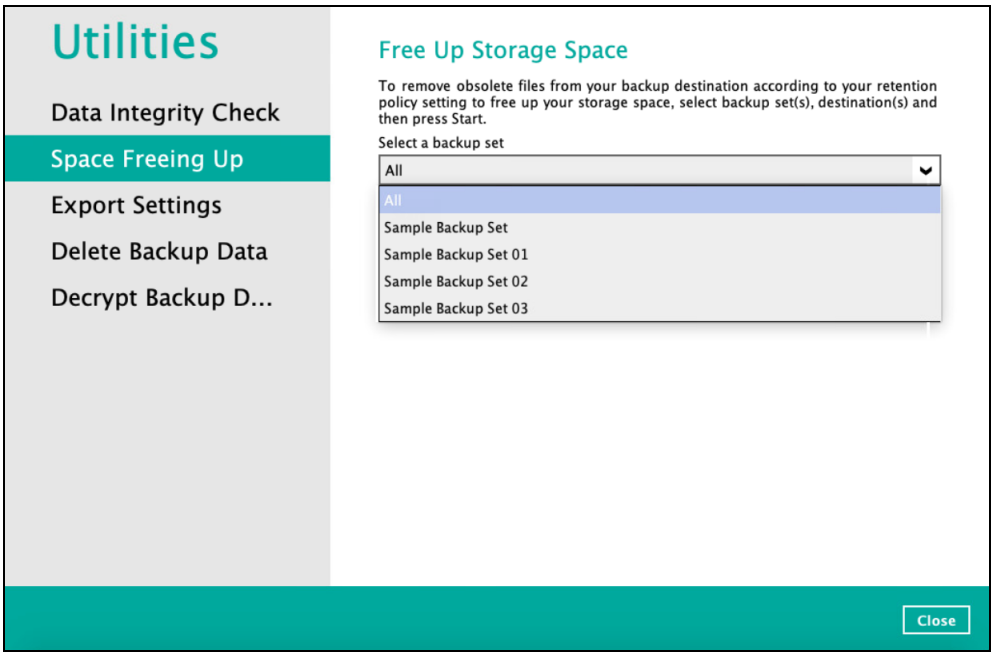


7.8.2 Space Freeing Up

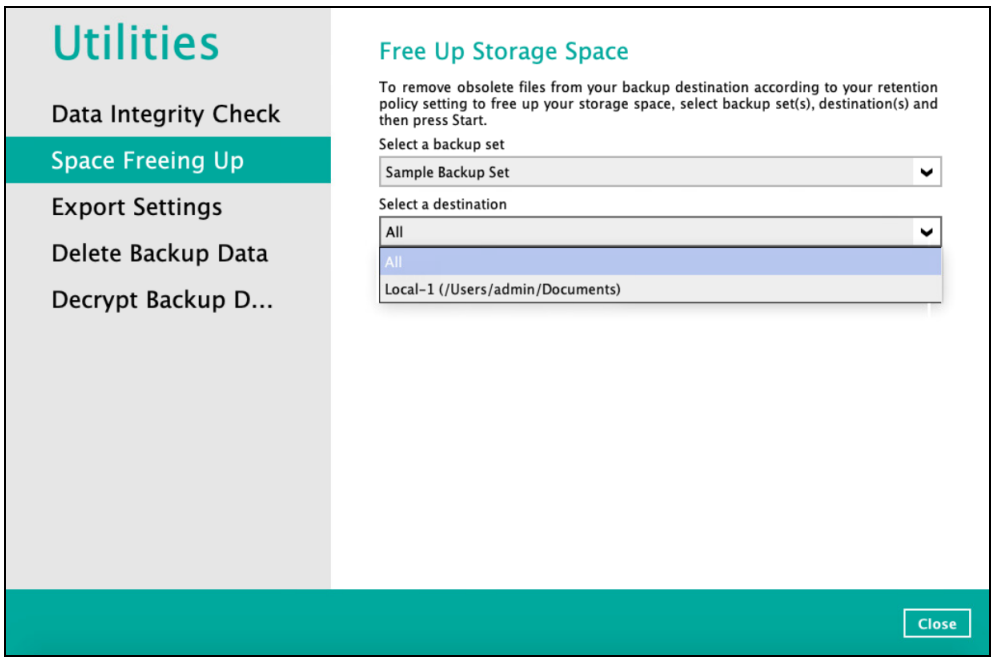
This feature is used to remove obsolete file(s) from your selected backup set and destination (manually start Retention Policy). After the Space Freeing Up job is completed, the storage statistics of the backup set(s) are updated.

To perform deletion of backup data, follow the instructions below:

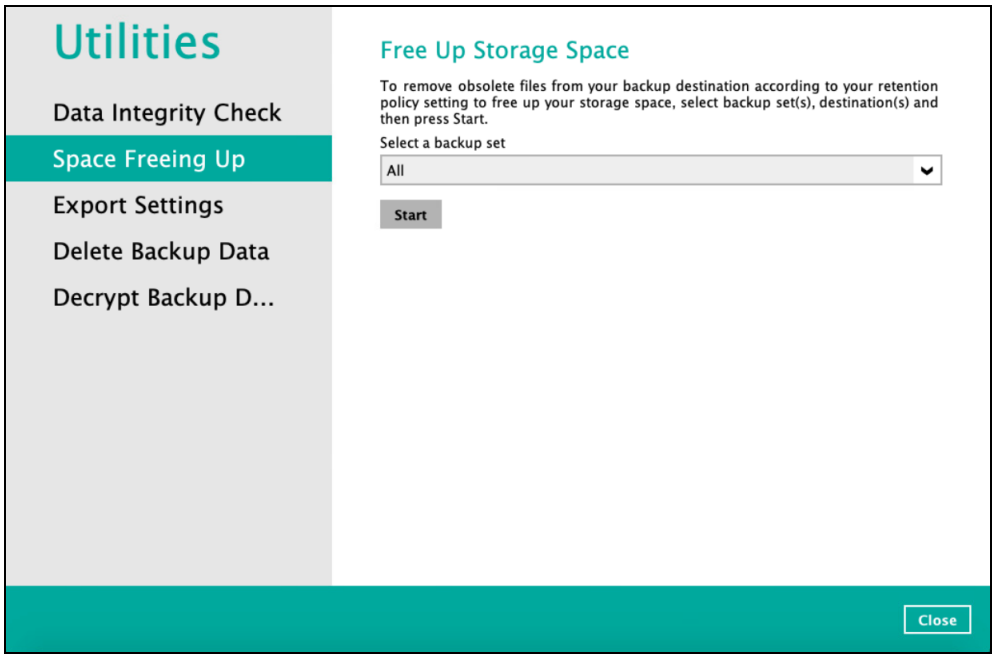
1. Select a backup set from the drop-down list.



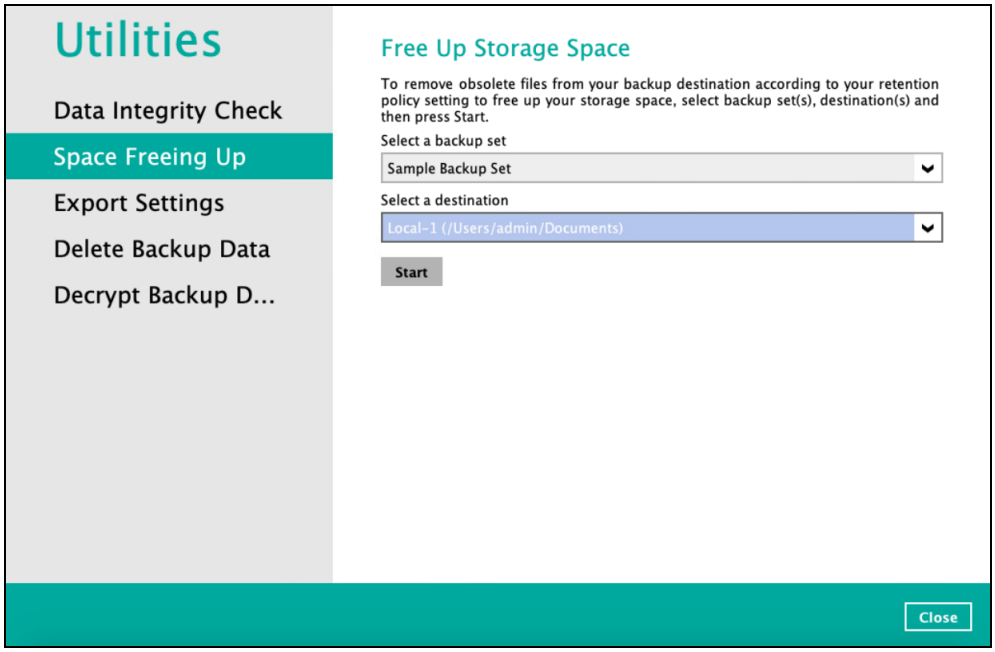
If you select a specific backup set, you will also have to choose a specific or **ALL** destination. Separate

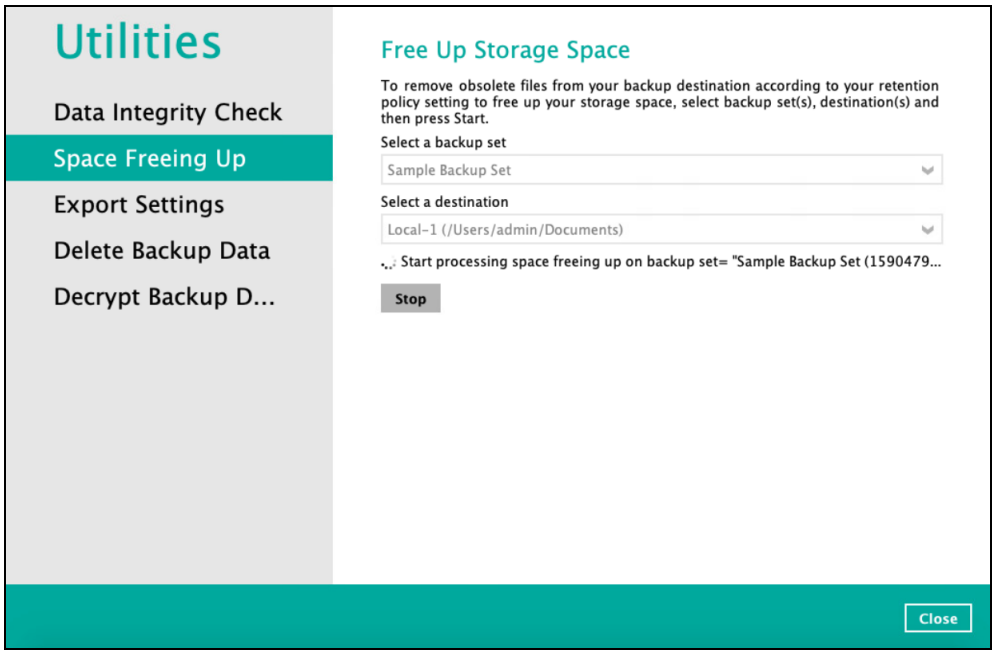


If you select **ALL** backup sets, you will not have to choose a destination.

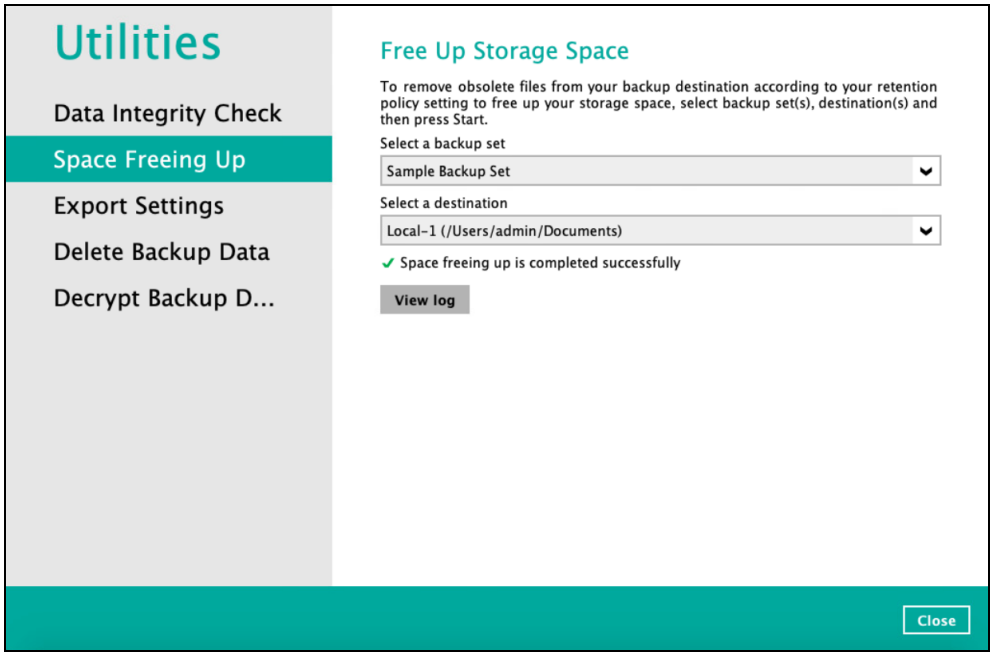


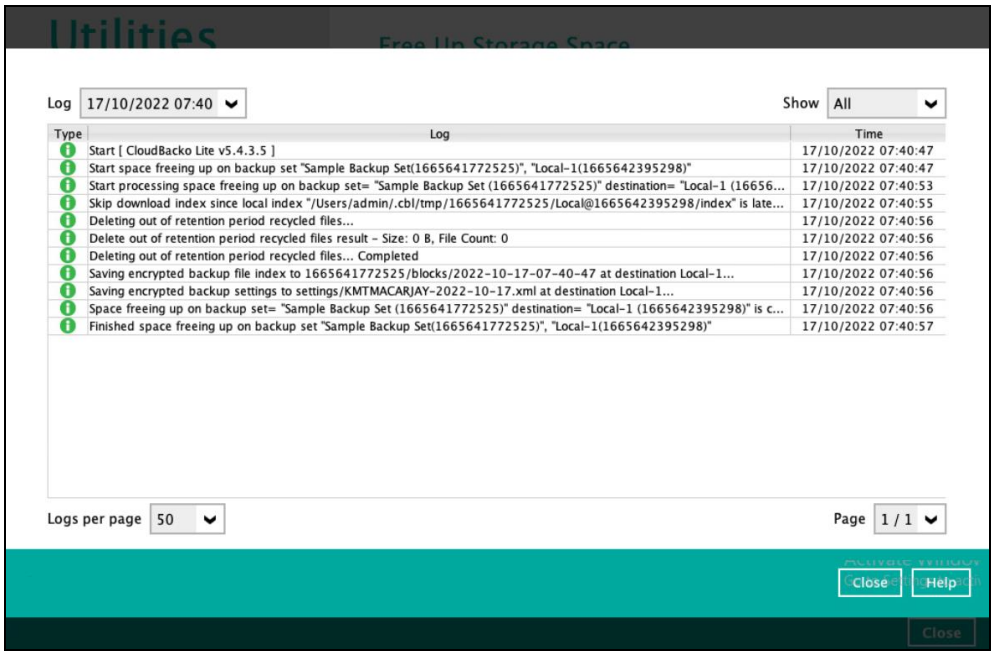
2. Once a backup set and destination have been selected, click start to perform space free up.





Once the space freeing up is completed, click **view log** to see more details.




Utilities
Free Up Storage Space
Log 17/10/2022 07:40
Show All
Type
Log
Time
Start [CloudBacko Lite v5.4.3.5] 17/10/2022 07:40:47
Start space freeing up on backup set "Sample Backup Set(1665641772525)", "Local-1(1665642395298)" 17/10/2022 07:40:47
Start processing space freeing up on backup set= "Sample Backup Set (1665641772525)" destination= "Local-1 (16656... 17/10/2022 07:40:53
Skip download index since local index "/Users/admin/.cbl/tmp/1665641772525/Local@1665642395298/index" is late... 17/10/2022 07:40:55
Deleting out of retention period recycled files... 17/10/2022 07:40:56
Delete out of retention period recycled files result - Size: 0 B, File Count: 0 17/10/2022 07:40:56
Deleting out of retention period recycled files... Completed 17/10/2022 07:40:56
Saving encrypted backup file index to 1665641772525/blocks/2022-10-17-07-40-47 at destination Local-1... 17/10/2022 07:40:56
Saving encrypted backup settings to settings/KMTMACARJAY-2022-10-17.xml at destination Local-1... 17/10/2022 07:40:56
Space freeing up on backup set= "Sample Backup Set (1665641772525)" destination= "Local-1 (1665642395298)" is c... 17/10/2022 07:40:56
Finished space freeing up on backup set "Sample Backup Set(1665641772525)", "Local-1(1665642395298)" 17/10/2022 07:40:57
Logs per page 50
Page 1 / 1
Close
Help
Close

7.8.3 Export Settings

This feature is used to export and import CloudBacko Home Settings to the **settings.sys** file, this includes information on:

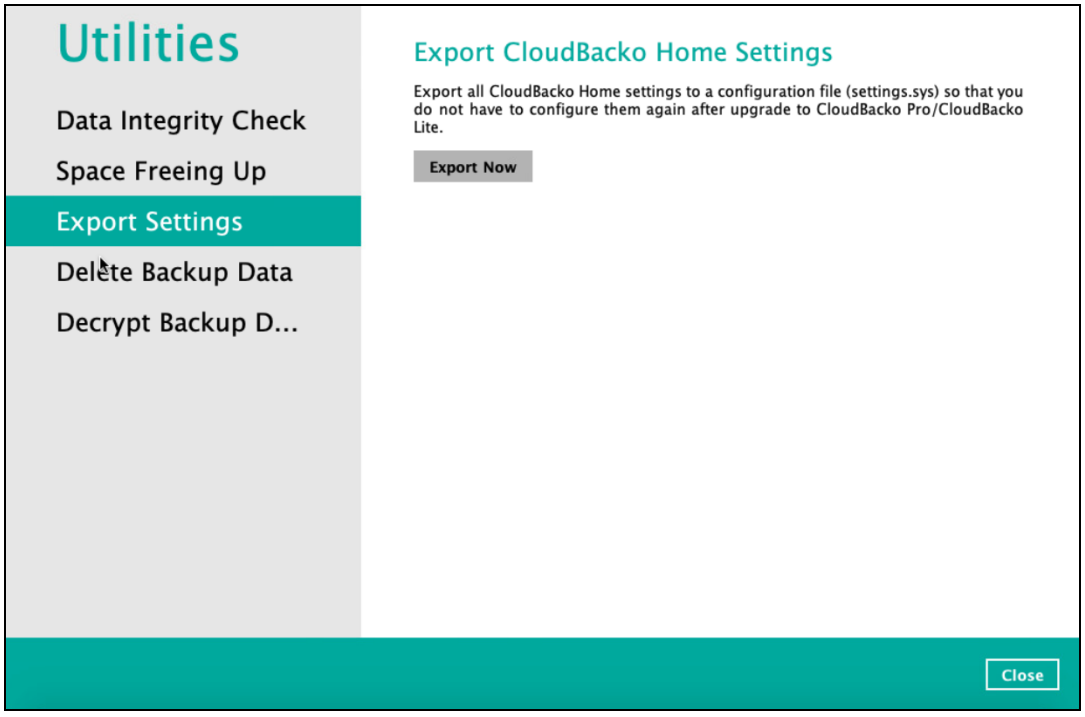
- Proxy Settings
- Email Report Settings
- Software Update Settings
- Windows Event log Settings (Windows Platform Only)
- Backup Set Settings

It is strongly recommended to export a copy of the configuration file (settings.sys) whenever there are general settings changes to CloudBacko Home, new backup sets added, or updates to existing backup sets.

WARNING!

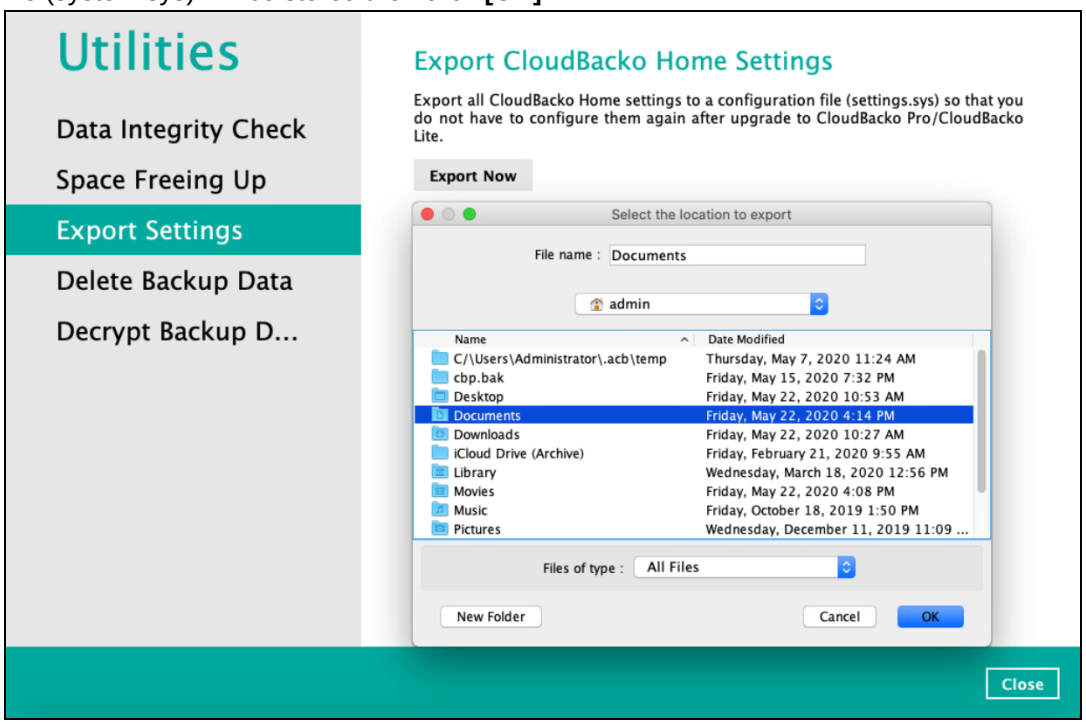
A separate copy of the settings.sys file should be saved in another location for safe keeping.

Otherwise, If the machine where the CloudBacko Home is installed on suffers a disk or hardware failure or is stolen and a copy of the settings.sys file is not available, it will not be possible to access and recover any data backed up by CloudBacko Home.

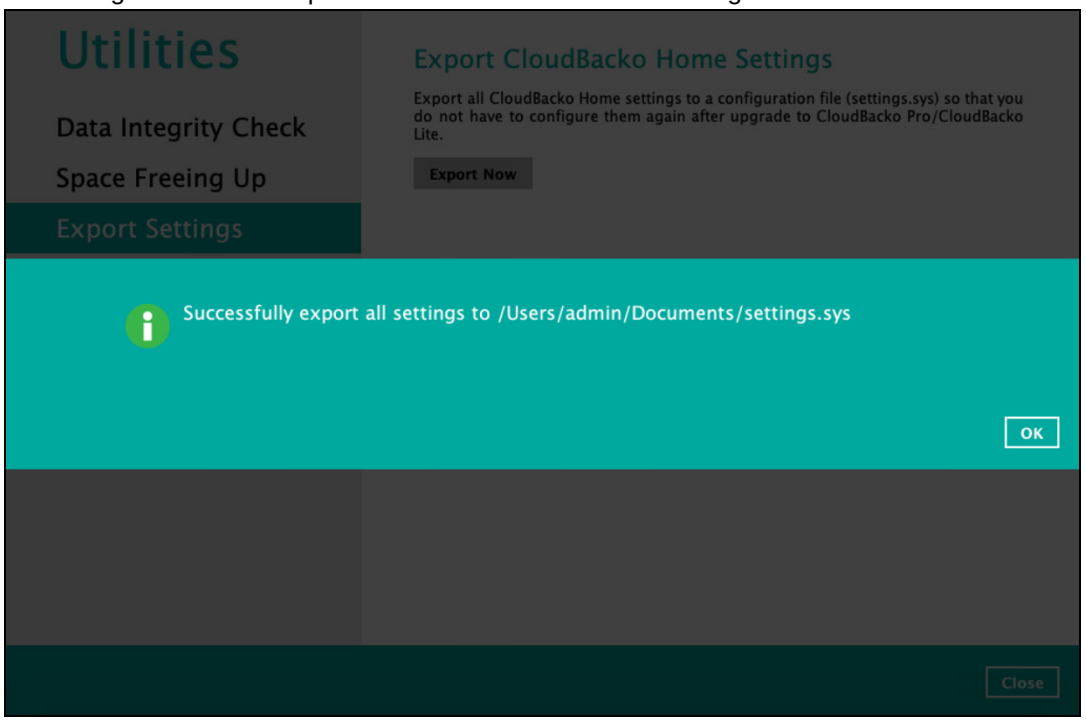


Export CloudBacko Home Settings

To export, click the **[Export Now]** button. Select a path where the CloudBacko Home configuration file (system.sys) will be stored then click **[OK]**.



If the system.sys file is successfully exported to the preferred path, it will display a message containing the status and path of the CloudBacko Home configuration file.

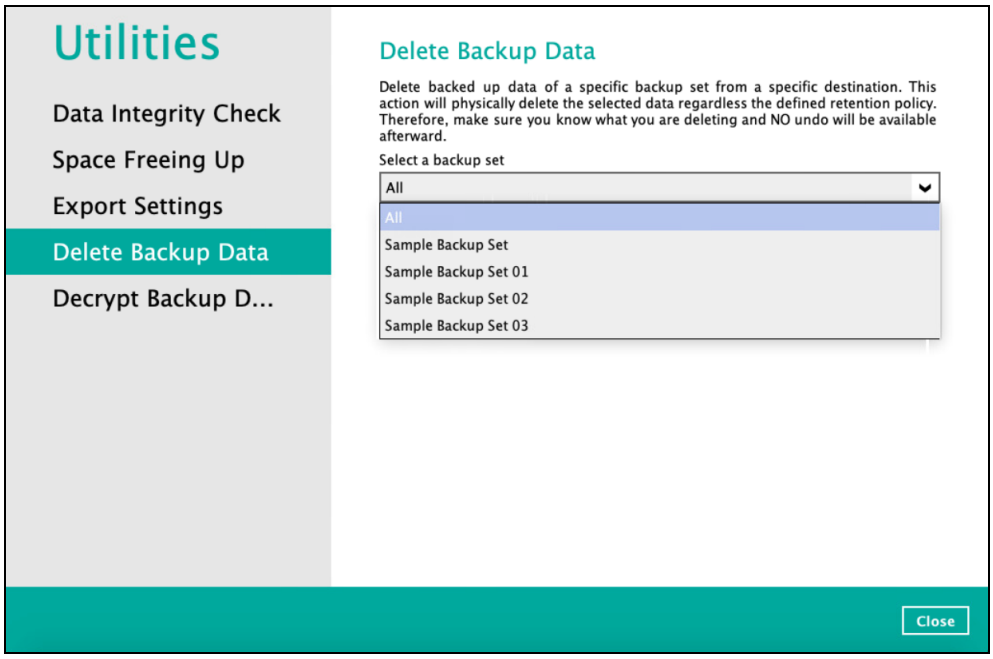


7.8.4 Delete Backup Data

This feature is used to permanently delete backed up data from a backup set(s), destination(s), backup job, or delete all backed-up data. After the data is deleted, the storage statistics of the backup set(s) are updated.

To perform deletion of backup data, follow the instructions below:

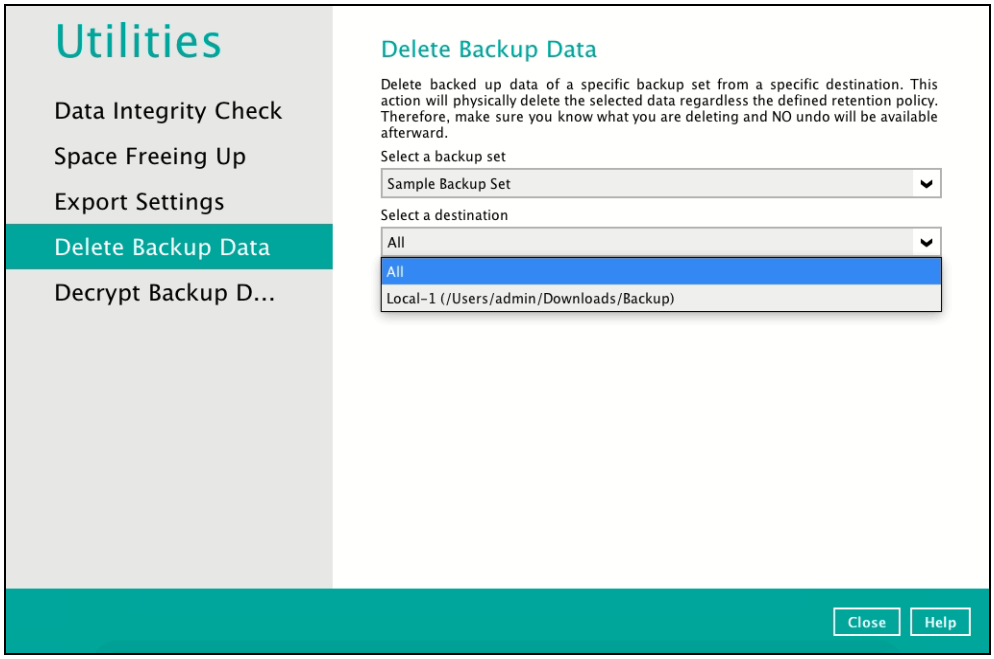
1. Select a backup set to delete from.



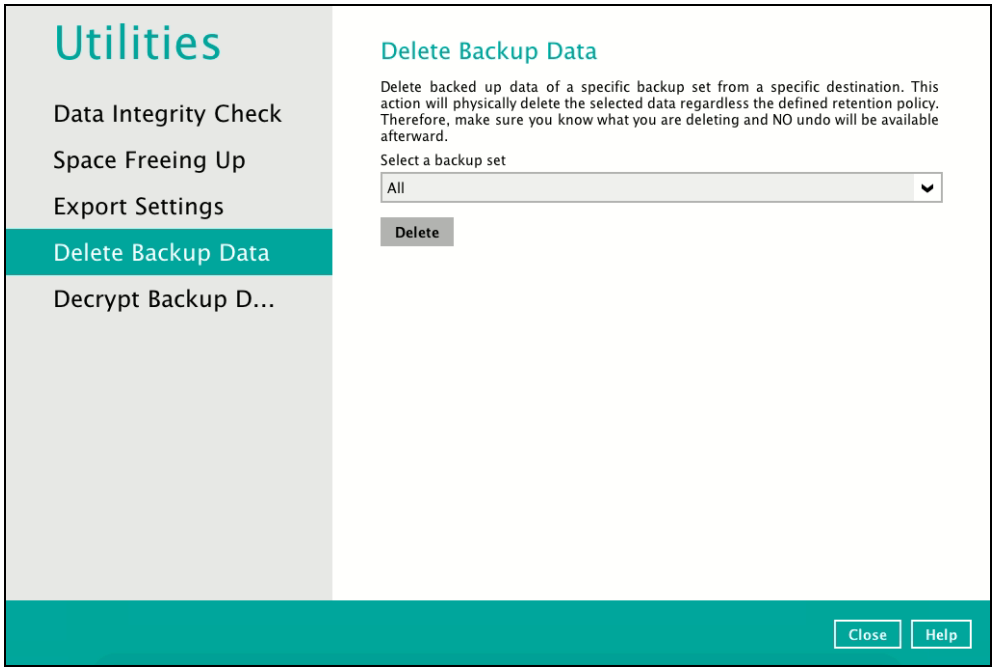
NOTE

This will only delete the backed up files in a backup set(s) and destination(s), but the backup set and destination will remain.

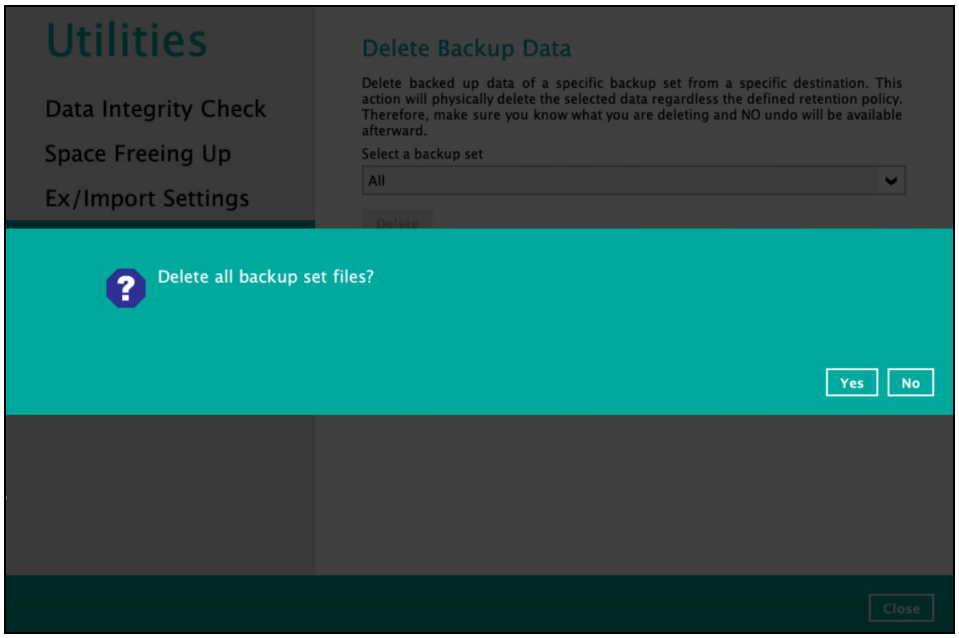
If you select a specific backup set, you will also have to choose a specific or **ALL** destination.



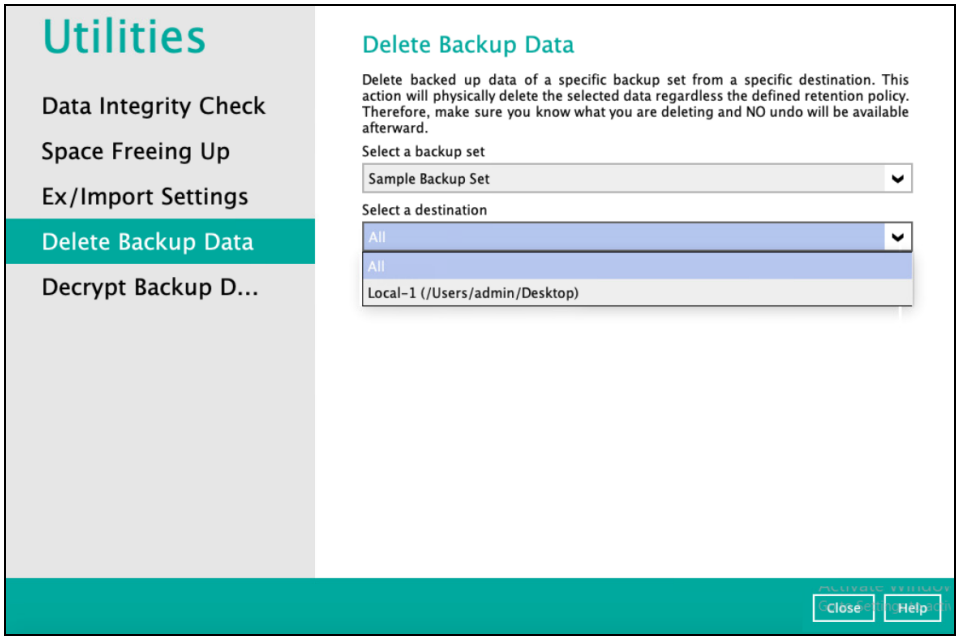
If you select **All** backup sets, then there is no need to select a destination.



2. If you choose to delete **All** backup set(s), the following message will be displayed. By clicking **Yes**, all backed up files from the selected backup set(s) and destination(s) will be deleted.



If you select a specific backup set, you will have an option to choose a destination.

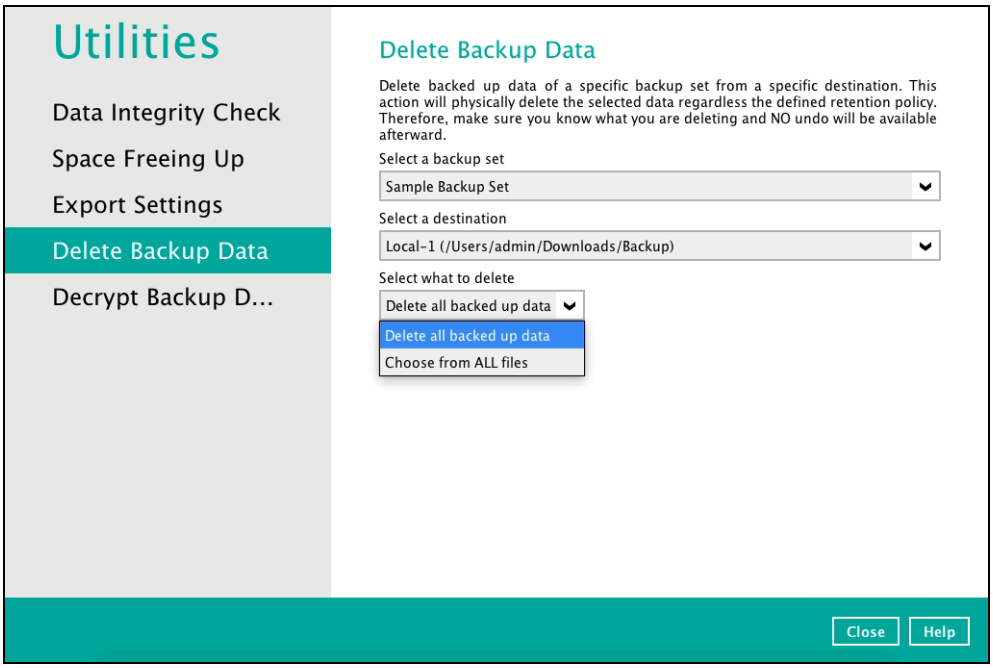


If you select **ALL** backup sets, you will not have to choose a specific destination.

There are two (2) options from the type of file(s) to delete if you select a specific backup set and a specific destination:

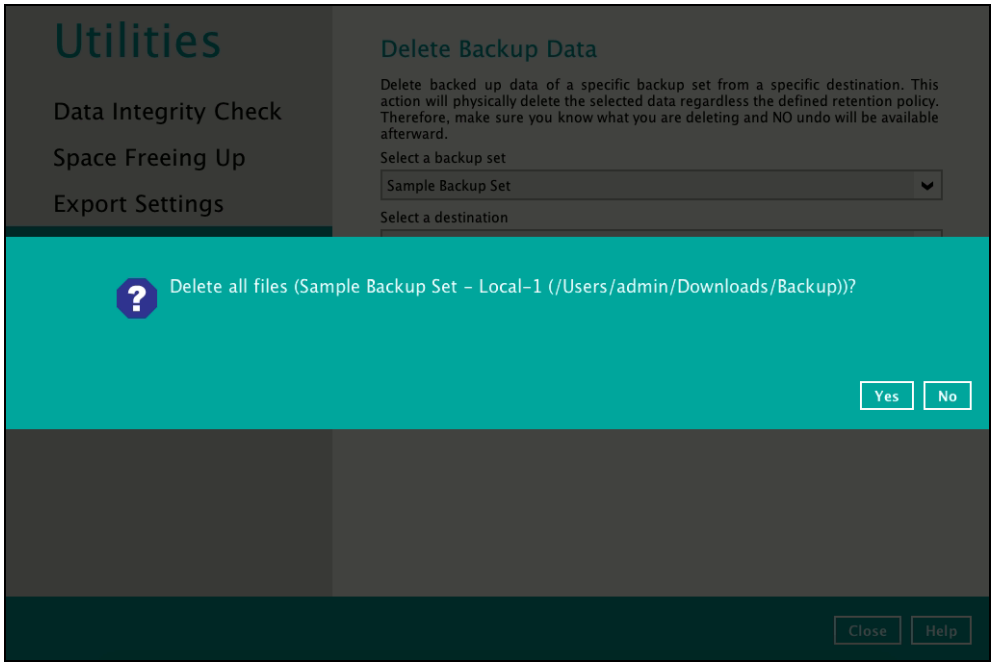
Delete all backup data

Choose from ALL files



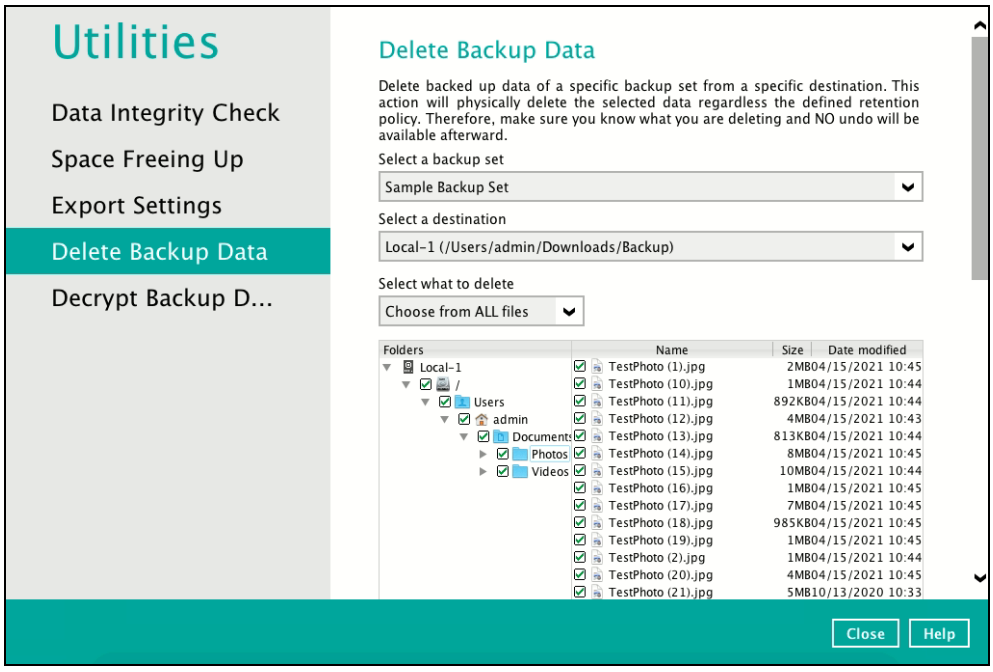
Delete all backed up data

If you choose this option, the following message will be displayed. By clicking **Yes**, all backed up data from the selected backup set(s) and destination(s) will be deleted.

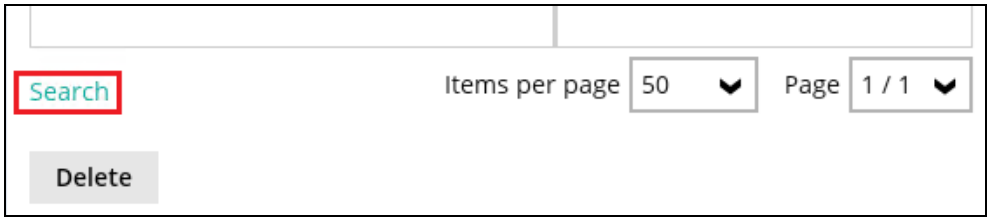


Choose from ALL files

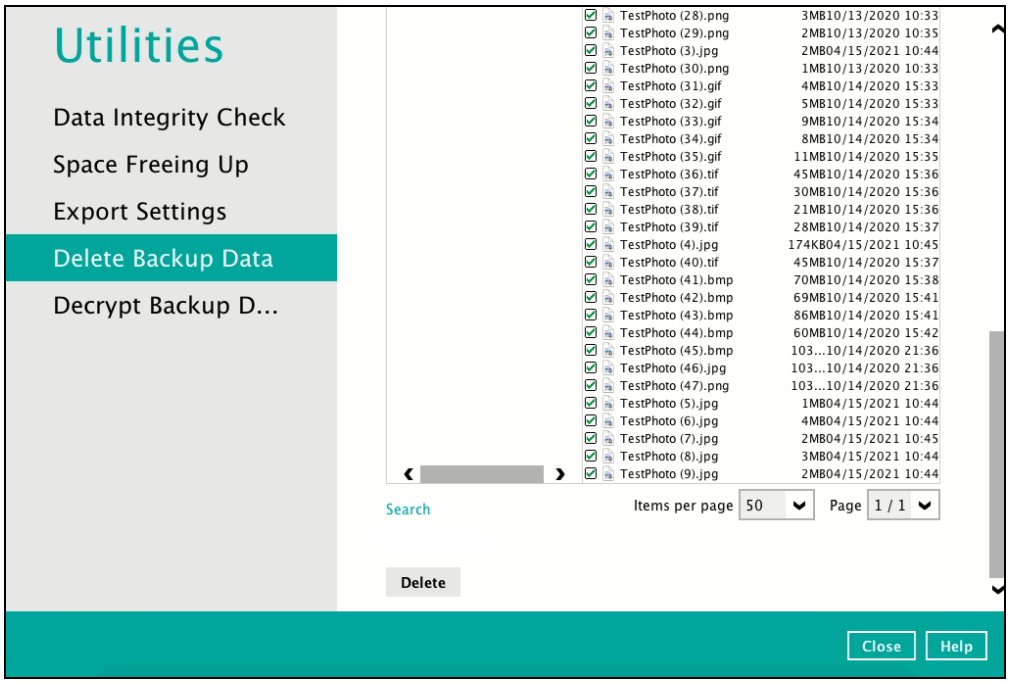
If you select "**Choose from ALL files**", you can select any file(s) in the backup set.

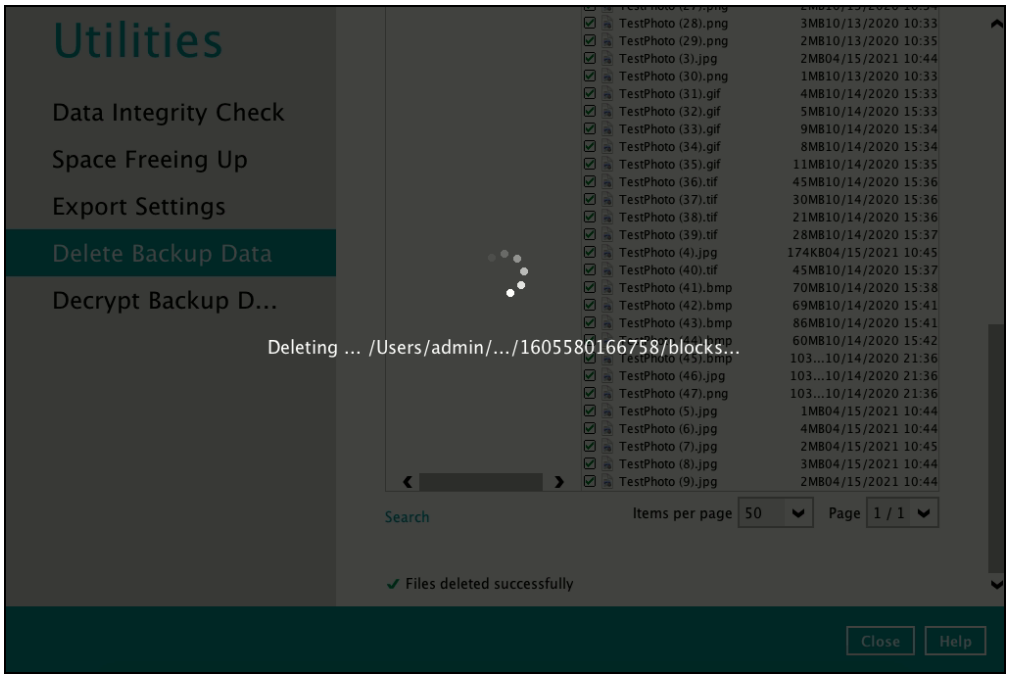


You also have the option to click the **Search** link to do an advance search.

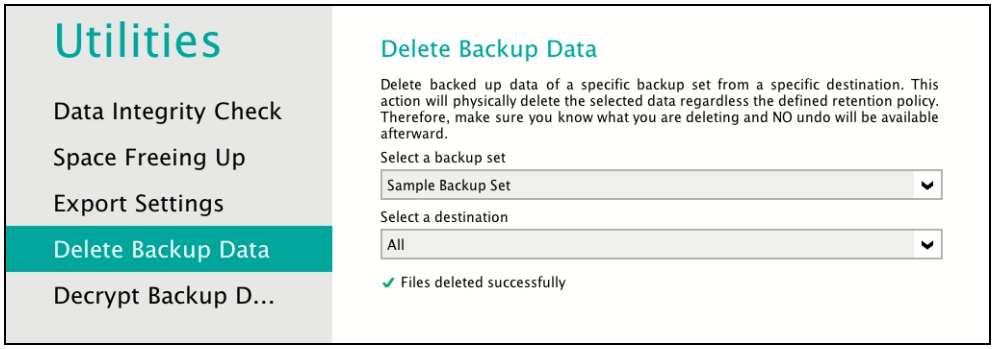


3. Click **delete** to start the deletion of file(s).





4. Files deleted successfully.

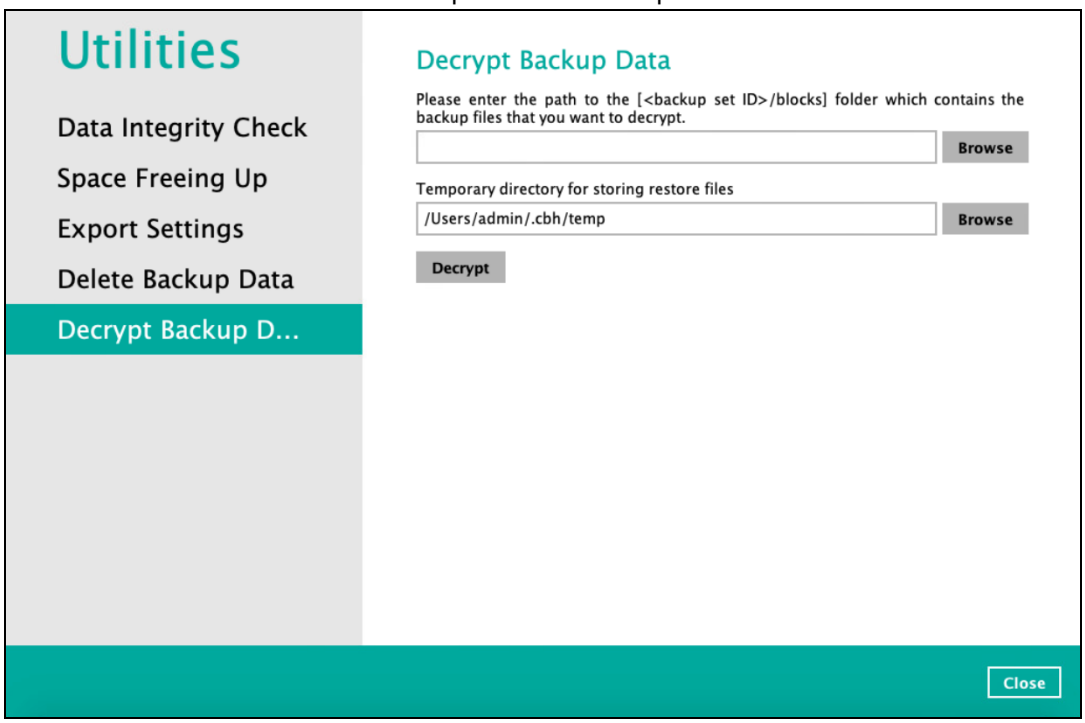


7.8.5 Decrypt Backup Data

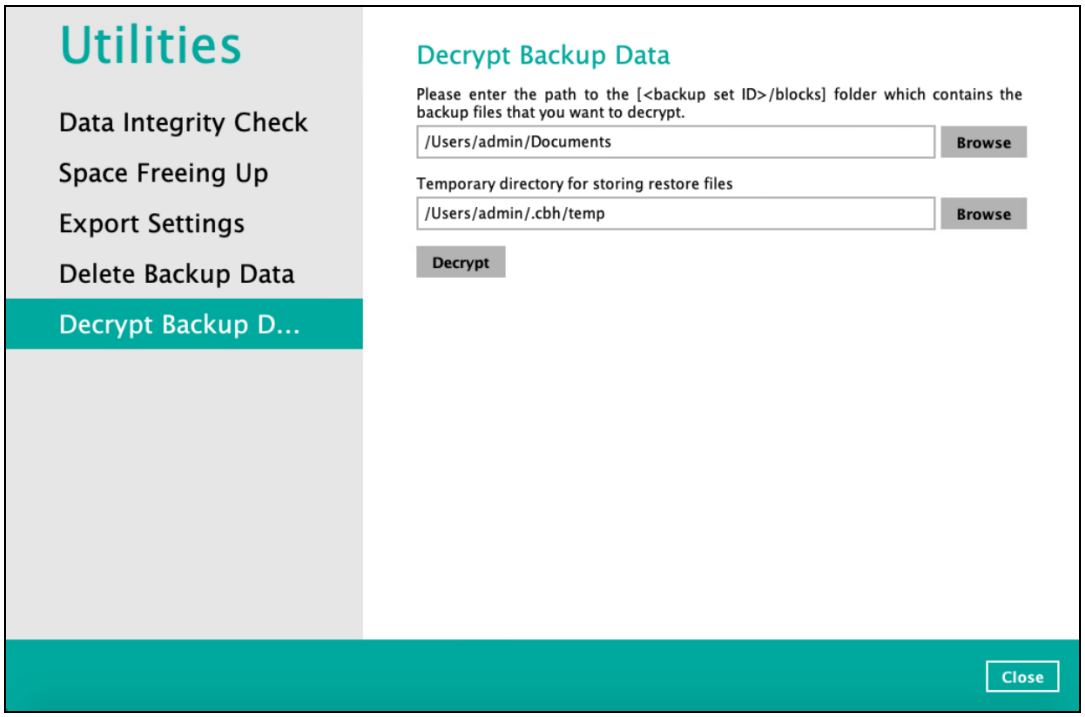
This feature is used to restore raw data by using the **data encryption key** that was set for the backup set.

To perform decryption of backup data, follow the instructions below:

1. Click the **Browse** button to locate the path of the backup set ID / blocks folder.



2. Click the **Browse** button to re-select the temporary folder for the decrypt process. Then click the **Decrypt** button to begin.



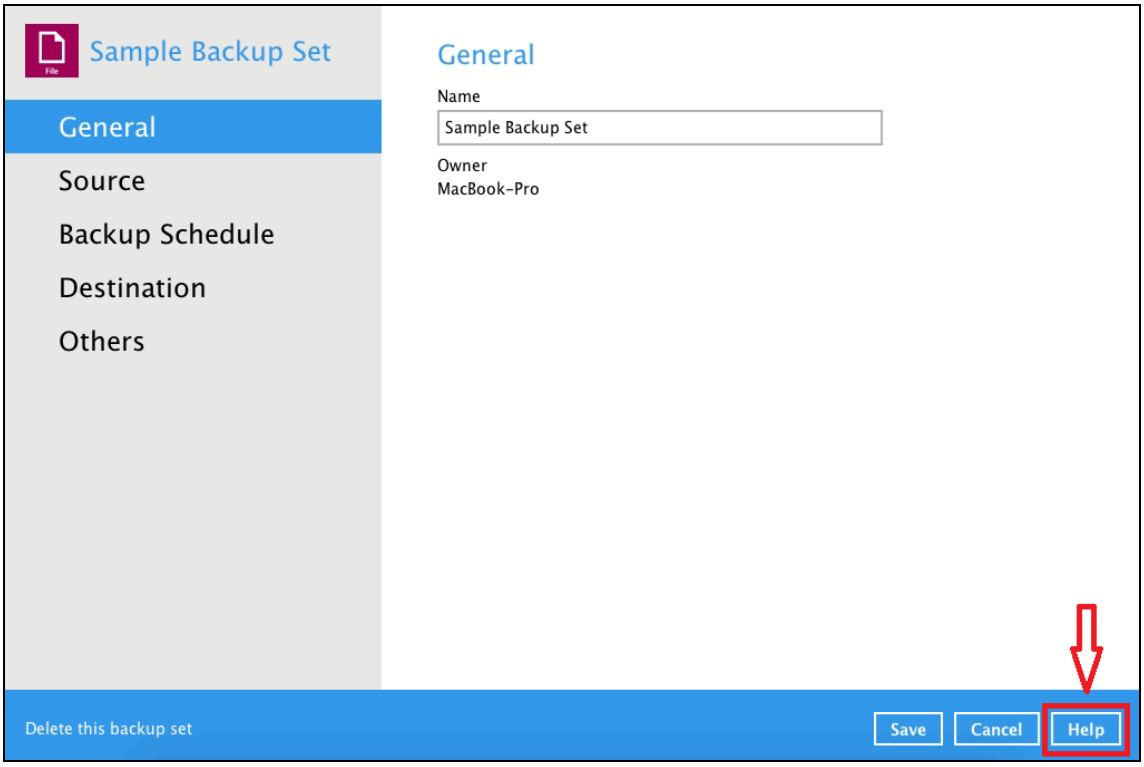
7.9 Social Media Icons

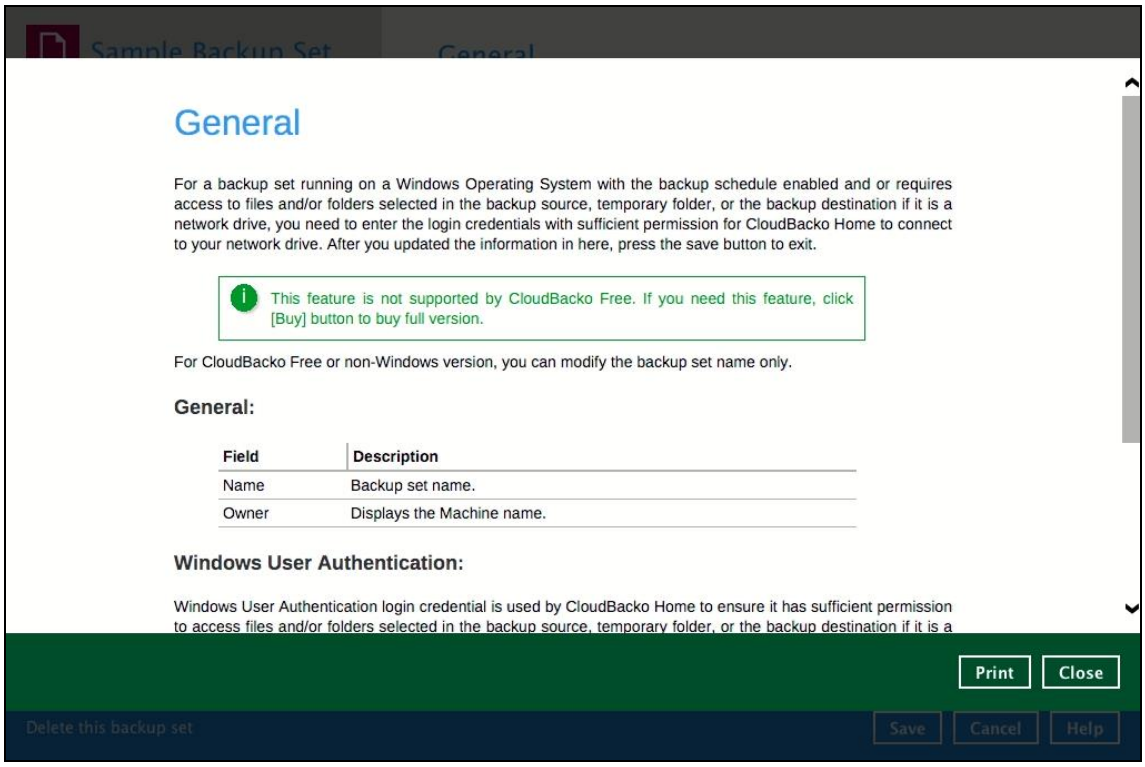
These are the social media accounts of CloudBacko. Each icon links to the CloudBacko page or channel.

Facebook	https://www.facebook.com/cloud.backo
Twitter	https://twitter.com/CloudBacko
LinkedIn	https://www.linkedin.com/company/cloudbacko-corporation
YouTube	https://www.youtube.com/user/CloudBacko

7.10 Online Help

This allows the user to view the summary of information and instructions of each available features in CloudBacko Home.

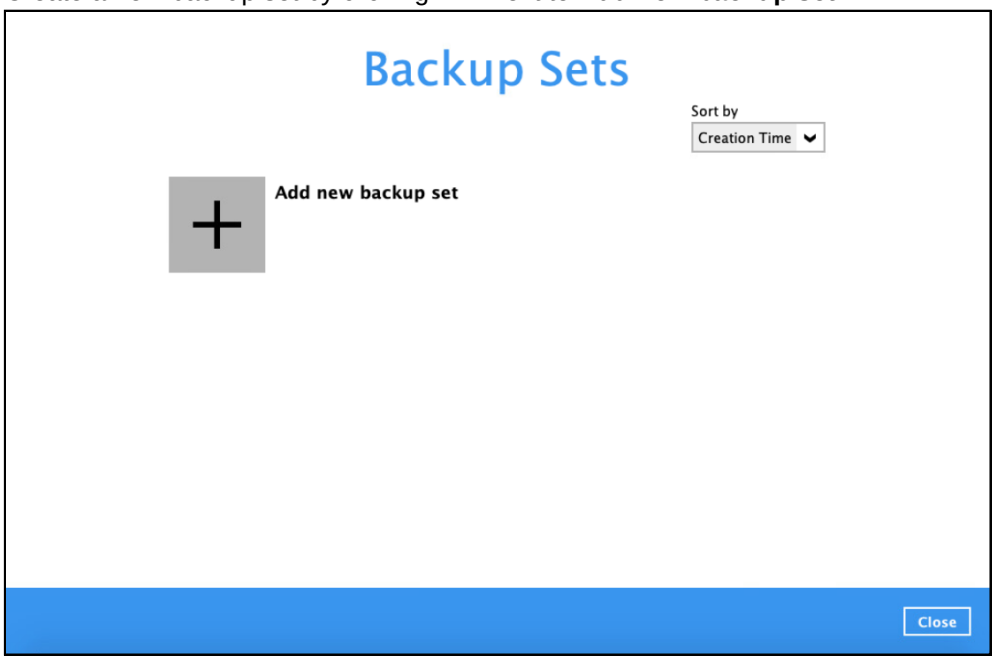



Sample Backup Set
General
General
For a backup set running on a Windows Operating System with the backup schedule enabled and or requires access to files and/or folders selected in the backup source, temporary folder, or the backup destination if it is a network drive, you need to enter the login credentials with sufficient permission for CloudBacko Home to connect to your network drive. After you updated the information in here, press the save button to exit.
This feature is not supported by CloudBacko Free. If you need this feature, click [Buy] button to buy full version.
For CloudBacko Free or non-Windows version, you can modify the backup set name only.
General:
Field
Description
Name
Backup set name.
Owner
Displays the Machine name.
Windows User Authentication:
Windows User Authentication login credential is used by CloudBacko Home to ensure it has sufficient permission to access files and/or folders selected in the backup source, temporary folder, or the backup destination if it is a
Print
Close
Delete this backup set
Save
Cancel
Help

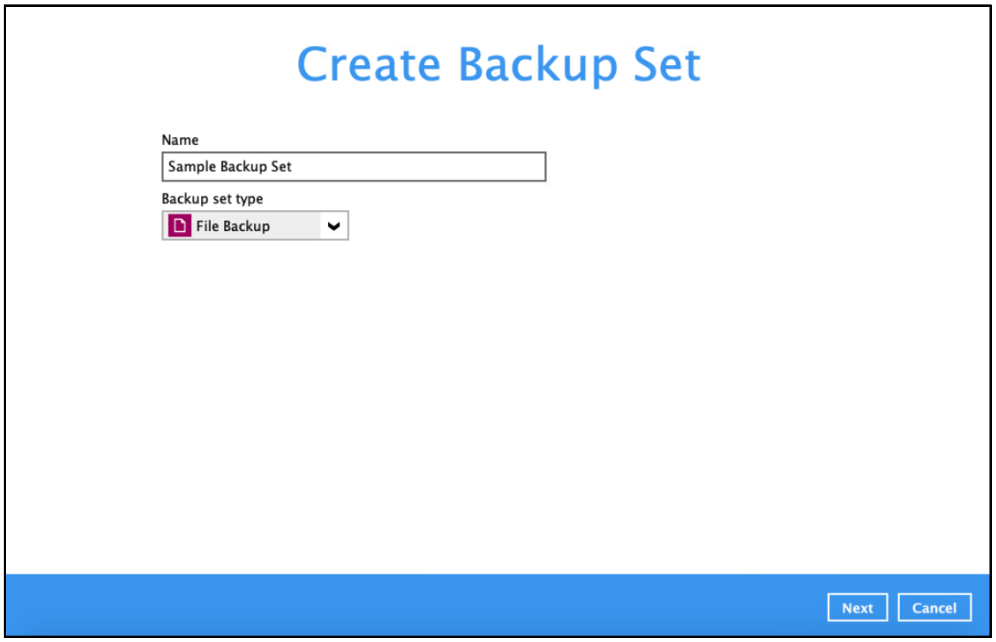
8 Create a Backup Set

1. Click the **Backup Sets** icon on the main interface of CloudBacko Home.

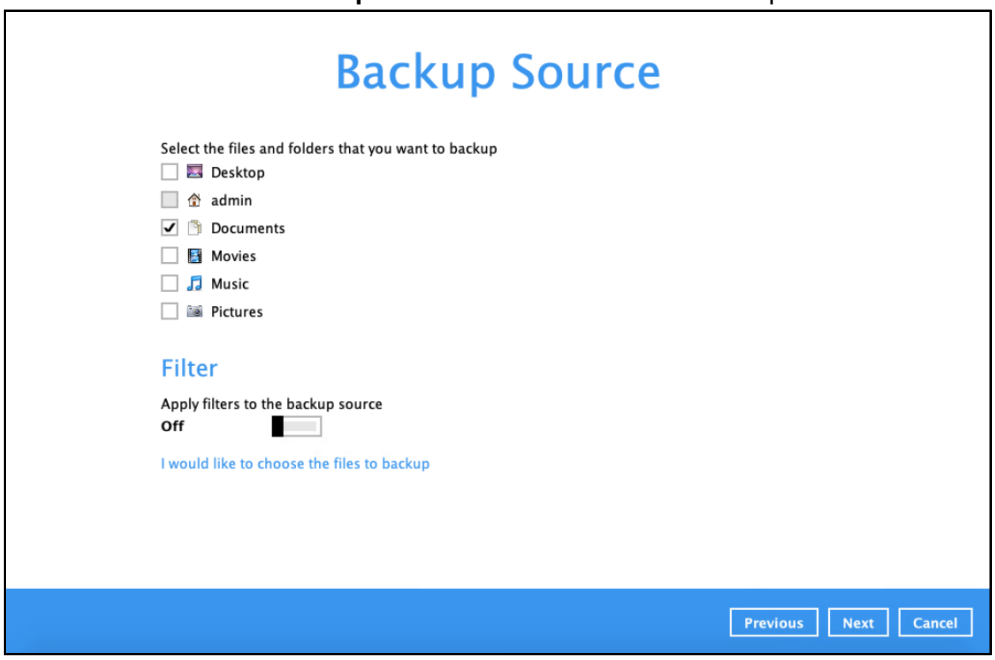
2. Create a new backup set by clicking next to **Add new backup set**.



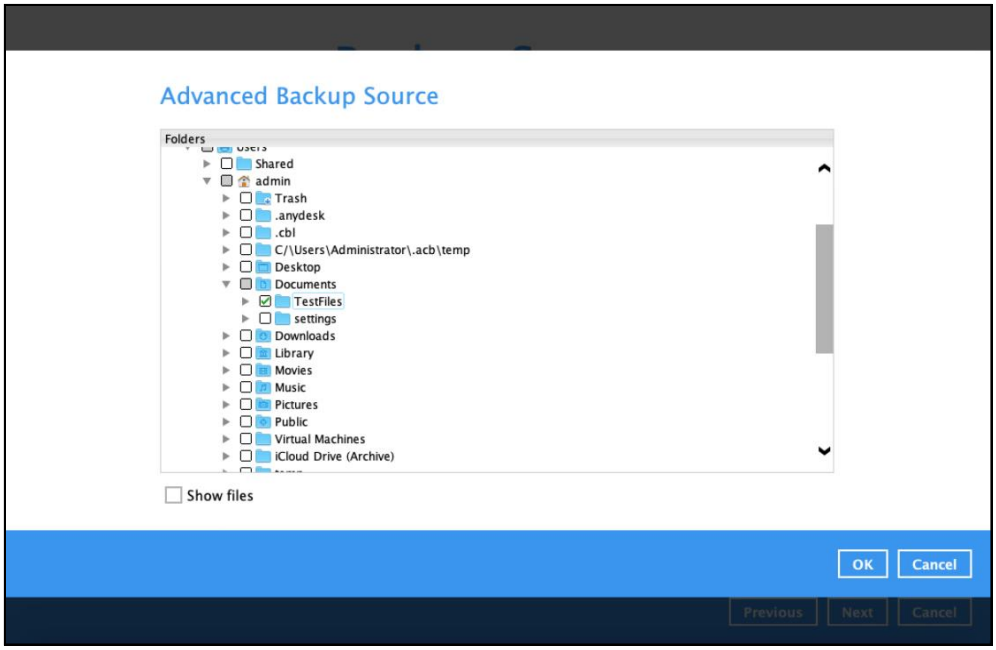
3. When the Create Backup Set window appears, name your new backup set, and select the **Backup set type**. Then, click **Next** to proceed.



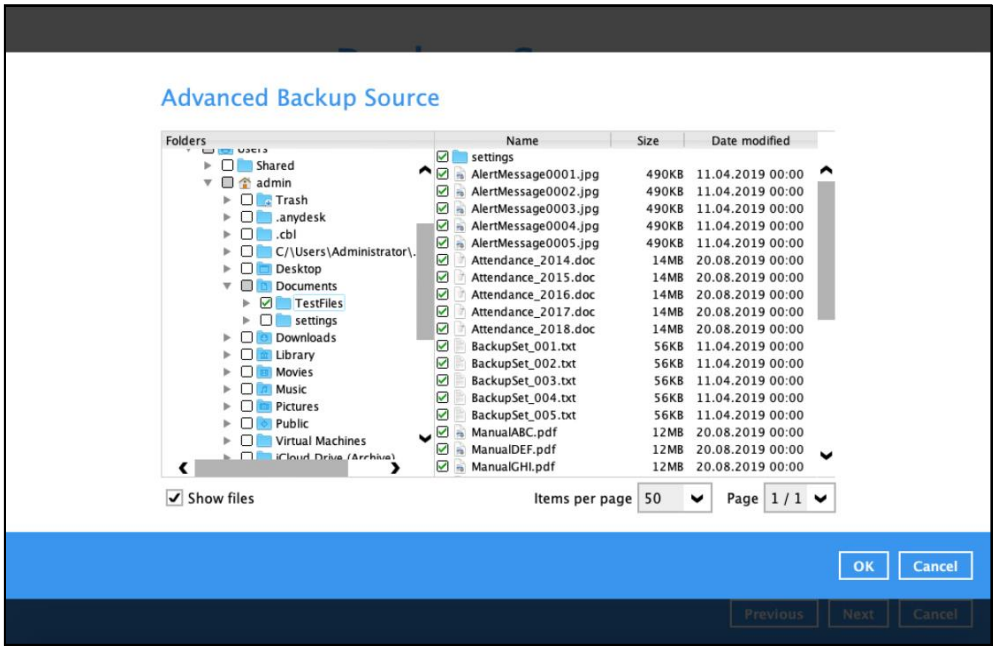
4. In the Backup Source window, select the source files and folders for backup. Click **I would like to choose the files to backup** to select individual files for backup.



5. In the **Advanced Backup Source** window, select folder(s) to back up all files in the folder(s).



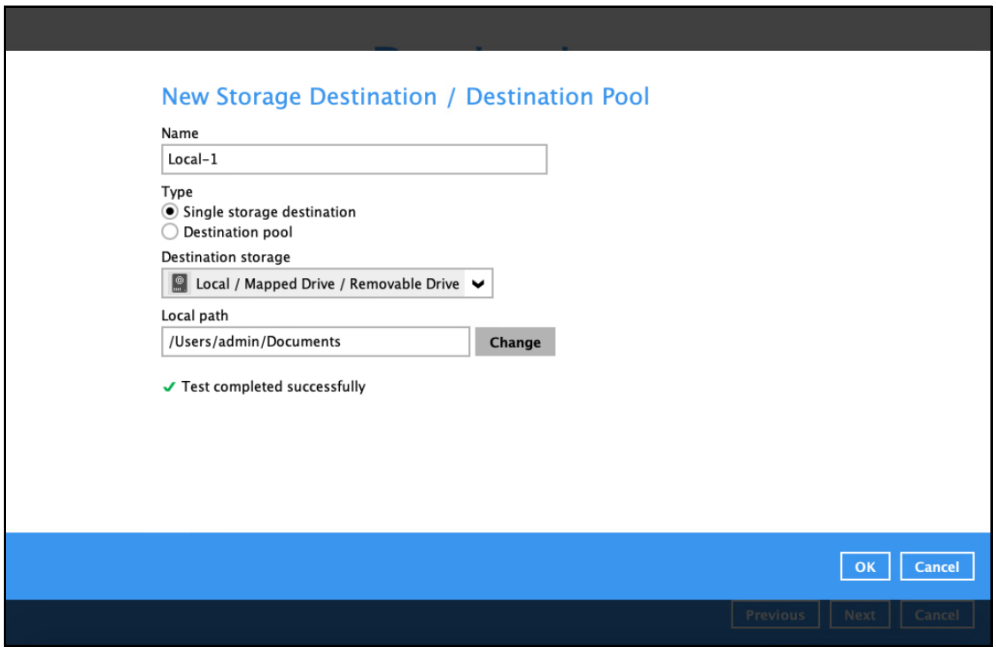
6. Alternatively, if you want to back up only specific files instead of all files in your selected folder(s), select the **Show files** checkbox at the bottom of the screen. A list of files will appear on the right-hand side. Select the checkbox(es) next to the file(s) to back up. Then, click **OK** to save your selections and close the Advanced Backup Source window.



7. In the Backup Source window, click **Next** to proceed. The **Destination** window will appear.

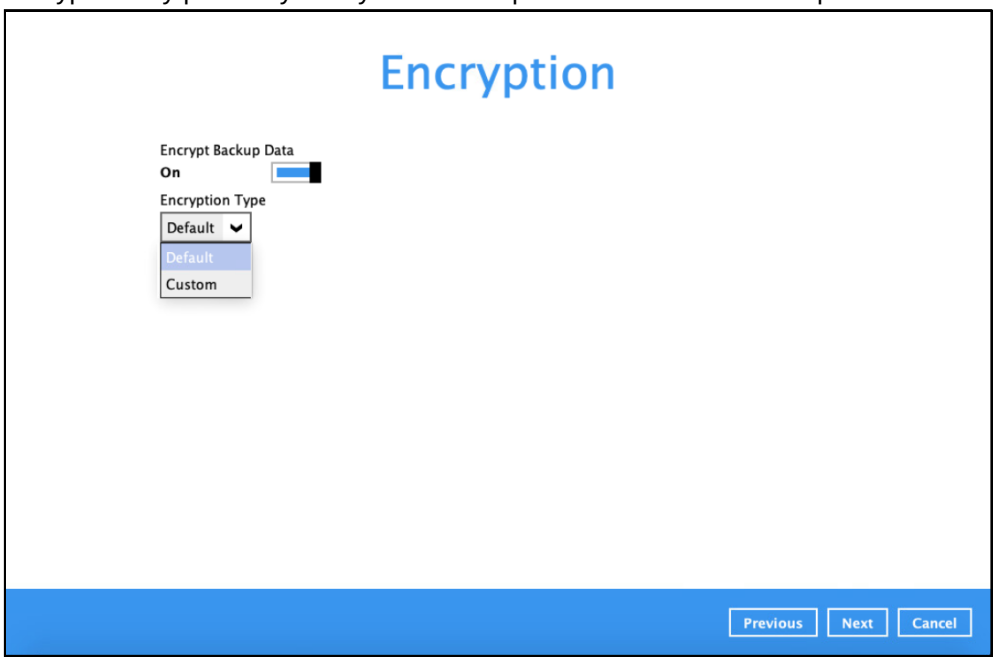
To select a backup destination for the backup data storage, click + next to **Add new storage destination / destination pool**.

8. In the New Storage Destination / Destination Pool window, select the destination type and destination storage. Then, click **OK** to confirm your selection.



9. In the Destination window, your selected storage destination will be shown. Click **Next** to proceed.

10. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.

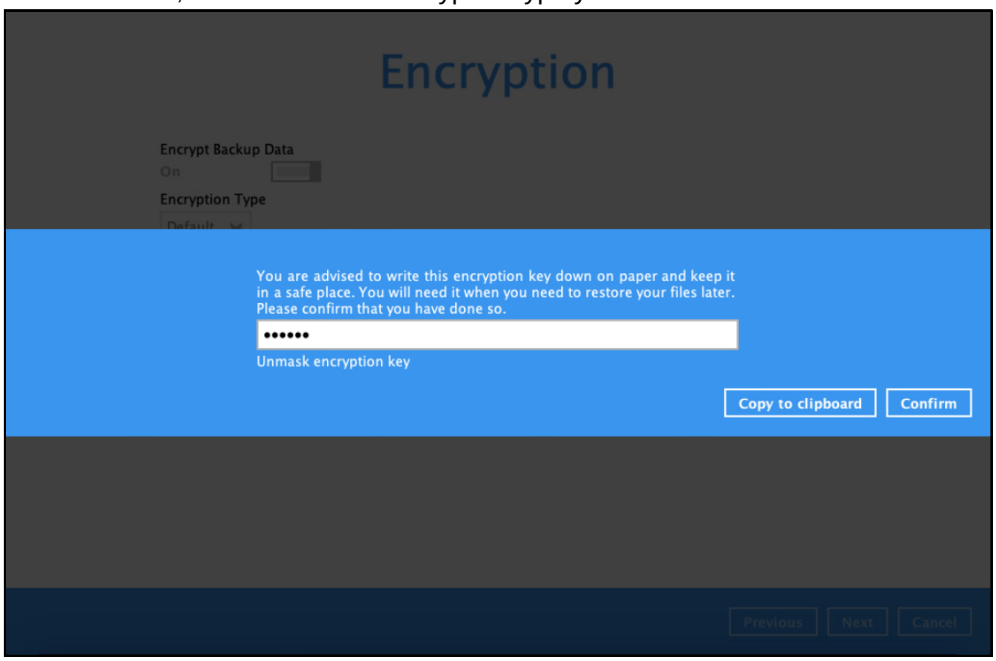


You can choose from one of the following three Encryption Type options:

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method, and key length.

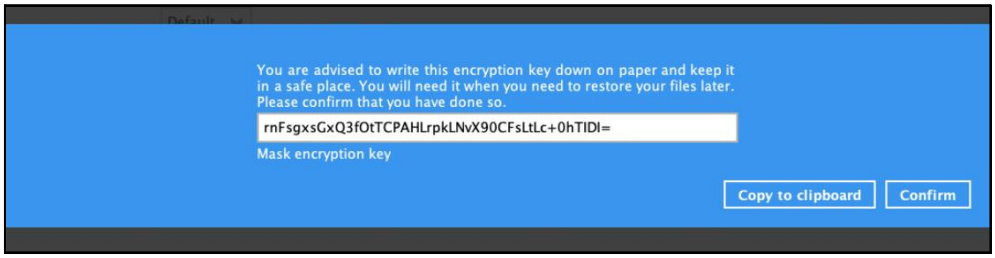
Click **Next** when you are done setting.

11. If you have enabled the Encryption Key feature in the previous step, the following pop-up window shows, no matter which encryption type you have selected.



The pop-up window has the following three options to choose from:

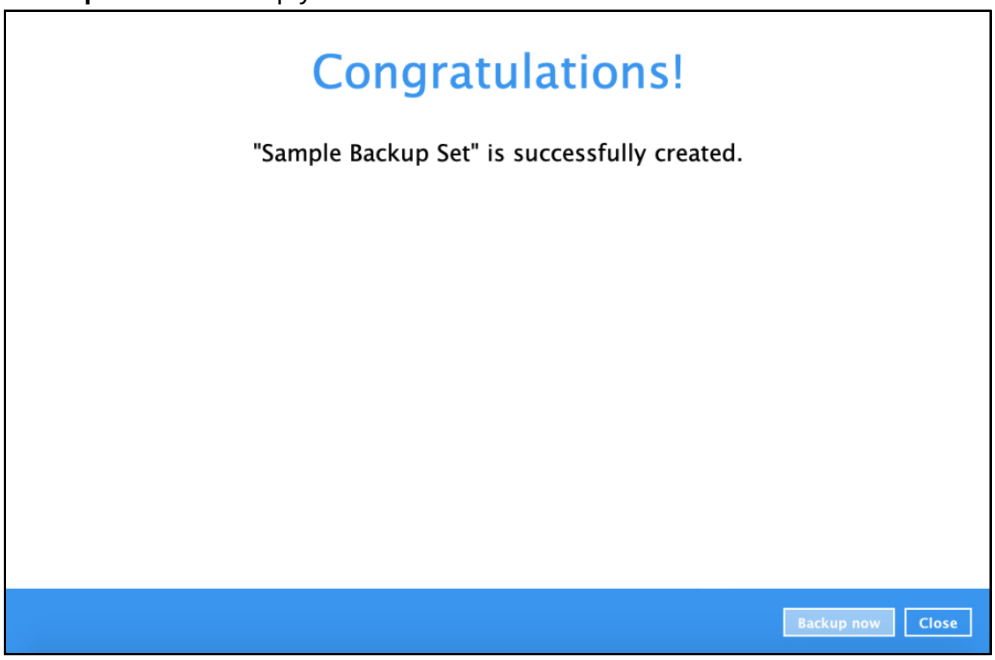
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.

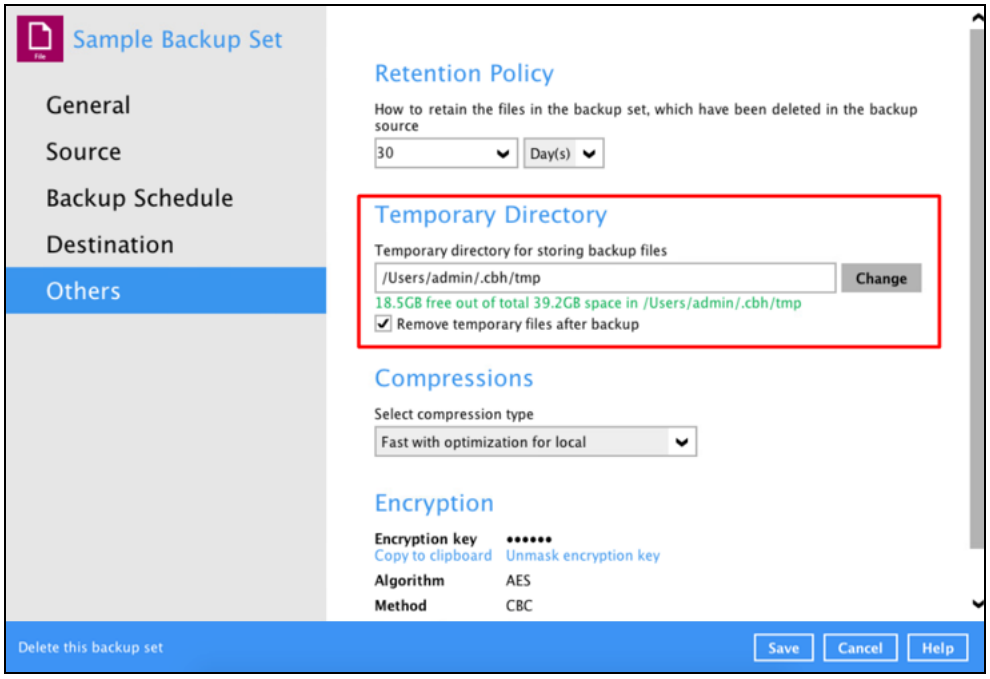
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

12. Upon successful creation of the backup set, the following screen will appear. You can click **Backup now** to back up your data or click **Close** to exit.



13. It is highly recommended to change the Temporary Directory. Select another location with sufficient free disk space other than **/Users/admin/.cbh/tmp**.

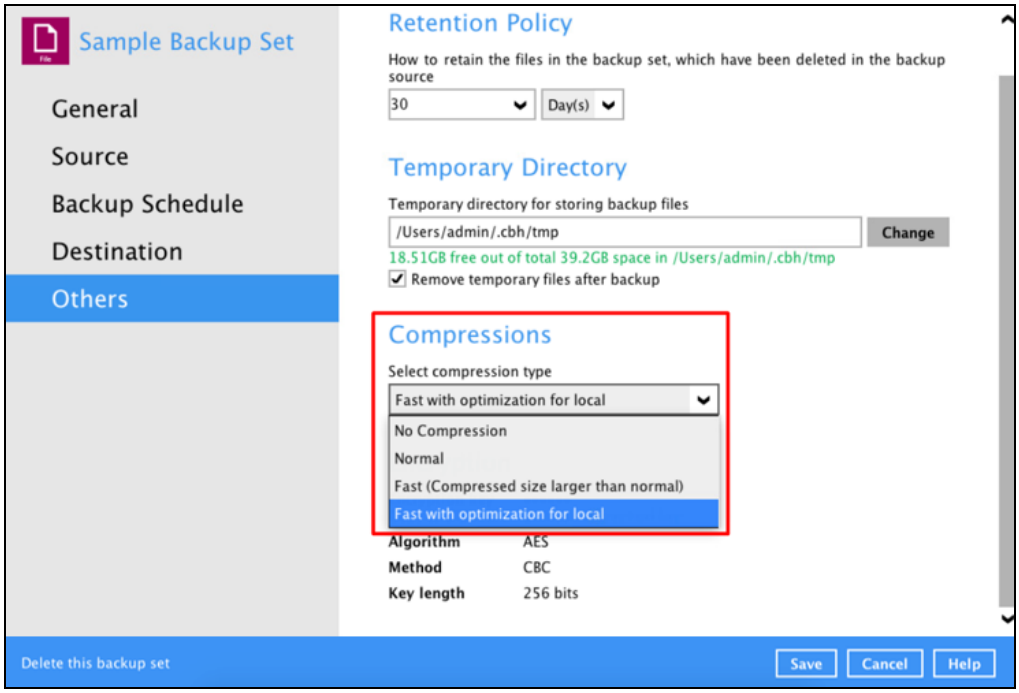
    Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



14. Optional: Select your preferred **Compression** type. By default, the compression is set to Fast with optimization for local.

    Go to **Others** > **Compressions**. Select from the following:

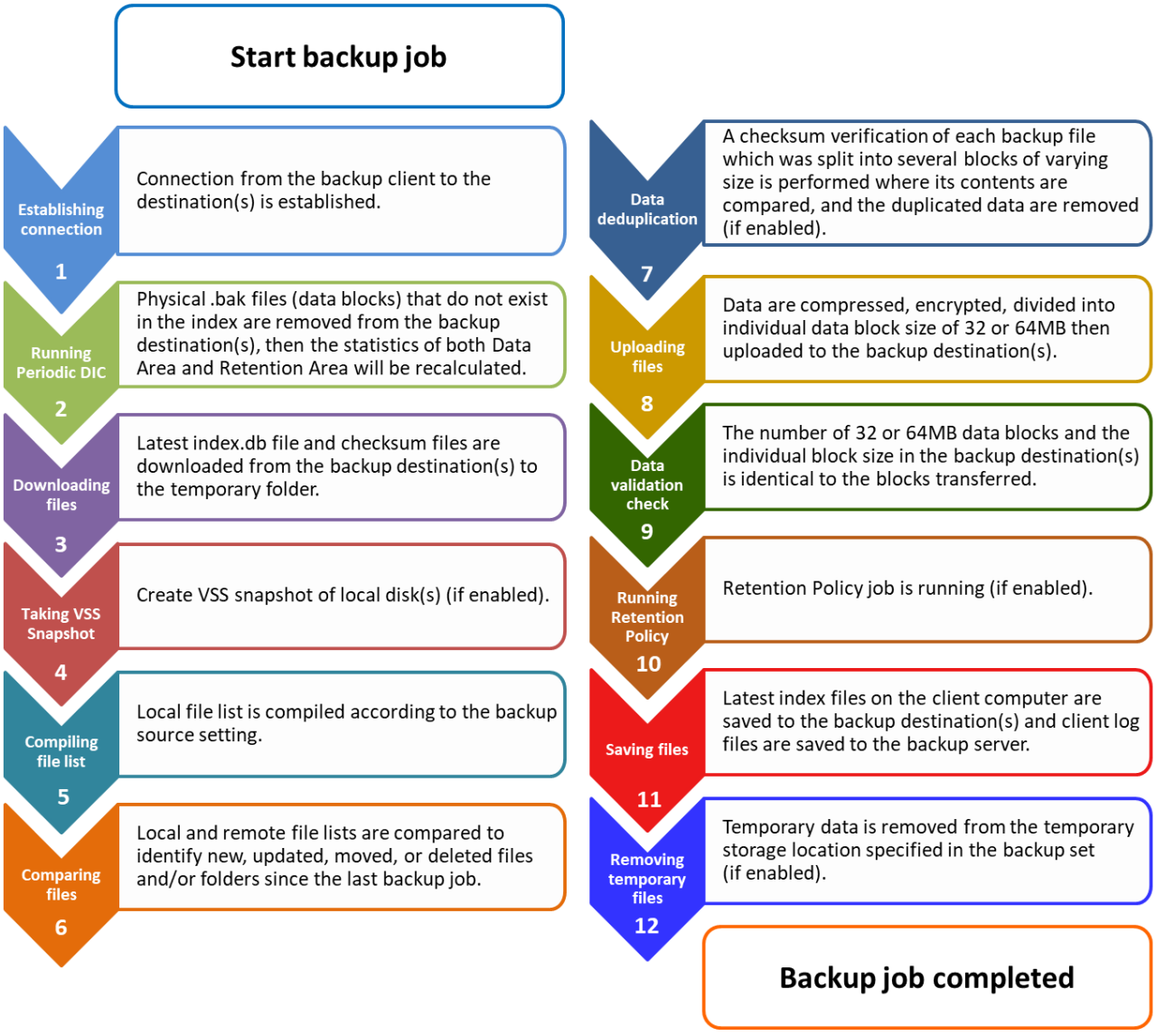
    - No Compression - file will not be compressed before backup.
    - Normal - compression is comparable to gzip Normal compression ratio.
    - Fast (Compressed size larger than normal) - (Compressed size larger than normal) – compression will be faster but with less compression and lower CPU usage compared to Normal.
    - Fast with optimization for local - uses Snappy compression library when backing up to local destination only, otherwise setting will default to gzip if backing up to other destinations. Has the lowest CPU usage, very high speed and reasonable compression but compressed file size may be larger than Fast.



9 Overview on Backup Process

The following steps are performed during a backup job. For an overview of the detailed process for Steps **2**, **3, 9,** and **11**, refer to the following chapters:

- Periodic Data Integrity Check (PDIC) Process **(Step 2)**
- Backup Set Index Handling Process
  - Start Backup Job **(Step 3)**
  - Completed Backup Job **(Step 11)**
- Data Validation Check Process **(Step 9)**



9.1 Periodic Data Integrity Check (PDIC) Process

For CloudBacko Home v4.5.0.0 (or above), the PDIC will run on the first backup job that falls on the corresponding day of the week from **Monday to Friday**.

To minimize the impact of the potential load of large number of PDIC jobs running, the schedule of a PDIC job for each backup set is automatically determined by the result of the following formula:

PDIC schedule = ***%BackupSetID% modulo 5***
or
%BackupSetID% mod 5

The calculated **result** will map to the corresponding day of the week (i.e., from Monday to Friday).

0	**Monday**
1	**Tuesday**
2	**Wednesday**
3	**Thursday**
4	**Friday**

NOTE
The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

Calculation: 1594627447932 mod 5 = ***2***

2	**Wednesday**

In this example:

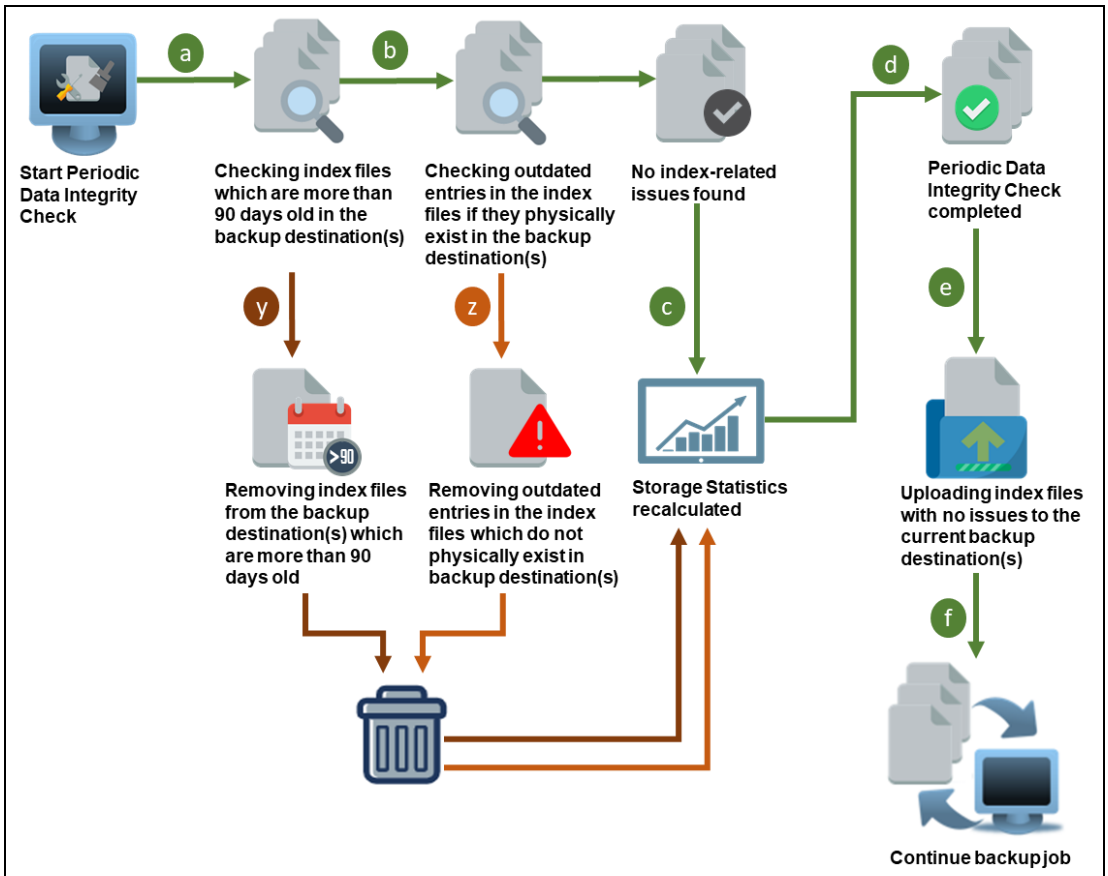
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

Although according to the PDIC formula for determining the schedule is ***%BackupSetID% mod 5***, this schedule only applies if the previous PDIC job was actually run more than 7 days prior.

Under certain conditions, the PDIC may not run strictly according to this formula. For example:

1. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it detects that the previous PDIC job was run more than 7 days ago.
2. Every time a data integrity check (DIC) is run, the latest PDIC run date is reset, the next PDIC job will run after 7 days.
3. The PDIC job will not run if there are no files in both the data and Retention Areas. For example: a newly created backup set with no backup job history or a backup set where all the data has been deleted using the Delete Backup Data feature.



a Check the index files in the backup destination(s) to determine if they were more than 90 days old.
- ➜ If **YES**, proceed to y
- ➜ If **NO**, proceed to b

b Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).
- ➜ If **YES**, proceed to c
- ➜ If **NO**, proceed to z

c Storage Statistics for Data area and Retention area usage will be recalculated.

d Periodic Data Integrity check is completed.

e Index files with no issues will be uploaded to the current backup destination(s).

f The backup job process will continue.

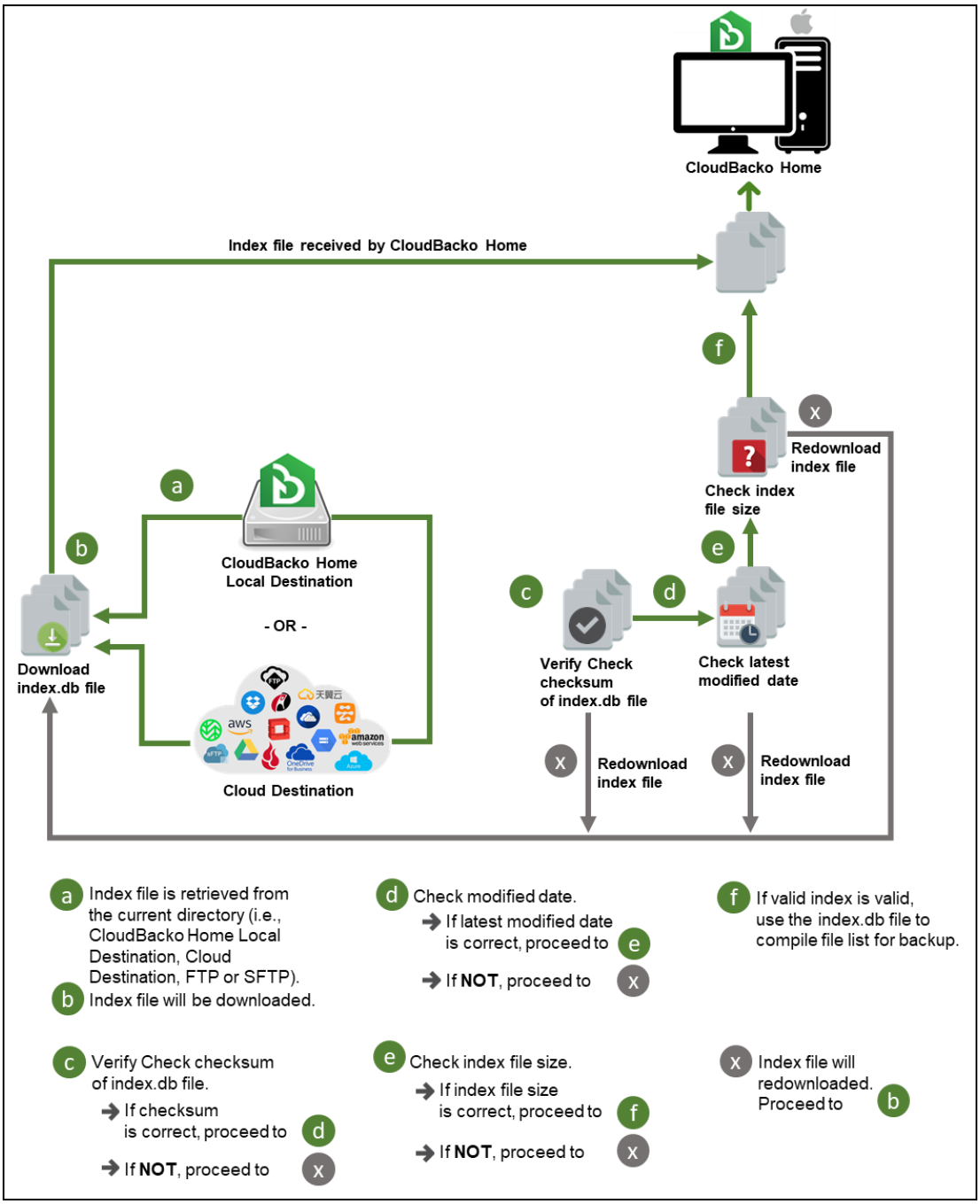
y Index files which are more than 90 days old will be removed from the backup destination(s).

z Outdated entries in the index files for files and/folders which do not physically exist in backup destination(s) will be removed.

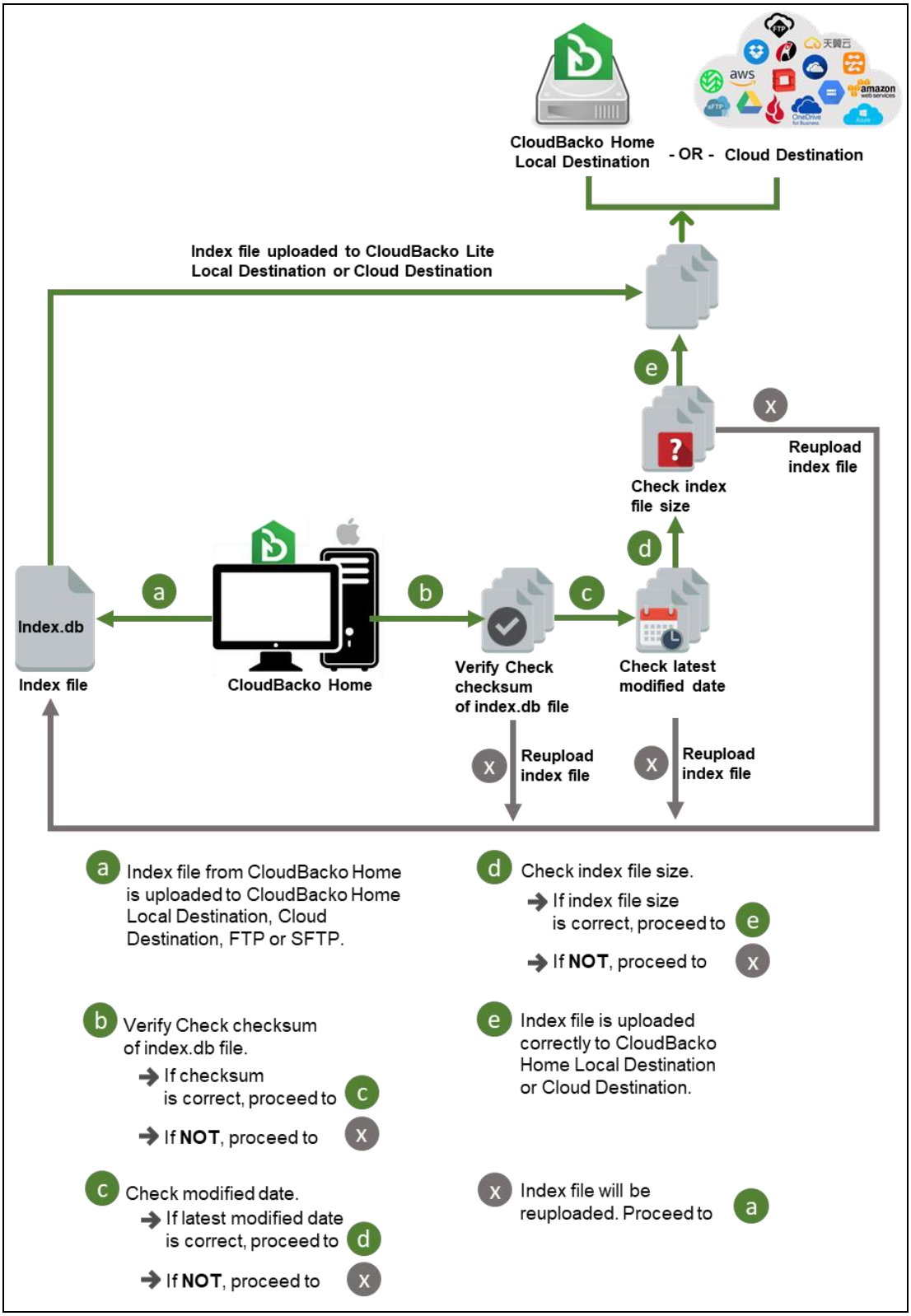
9.2 Backup Set Index Handling Process

To minimize the possibility of index related issues affecting backups, each time index files are downloaded from and uploaded to backup destination(s); the file size, last modified date, and checksum is verified to ensure index file integrity.

9.2.1 Start Backup Job

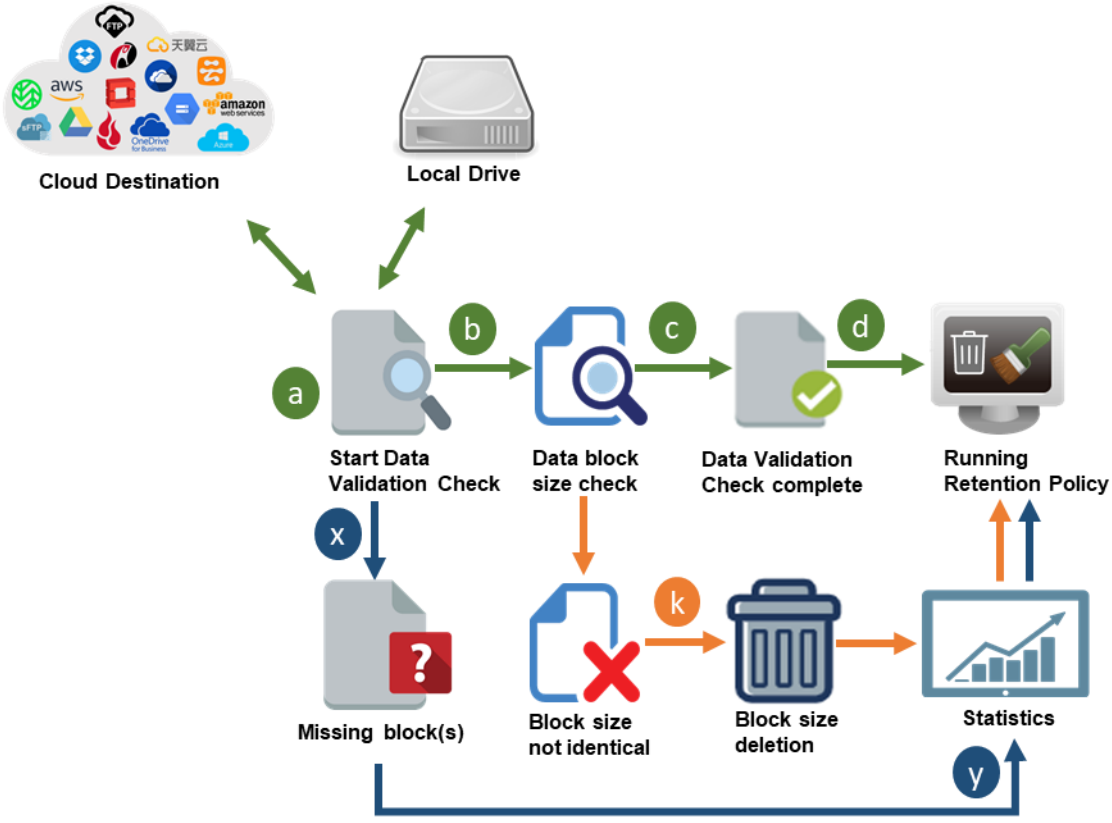


9.2.2 Completed Backup Job



9.3 Data Validation Check Process

As an additional measure to ensure that all files transferred to the backup destination(s) are received and saved correctly, both the number of 16 or 32 MB data block files and the size of each block file are checked again after the files are transferred.



a Check the number of 32 or 64MB data blocks in the backup destination(s) is identical to the number of blocks transferred.

→ If YES, proceed to b

→ If NO, proceed to x

b Check the individual sizes of each data block in the backup destination(s) is identical to the sizes of each block transferred.

→ If YES, proceed to c

→ If NO, proceed to k

c Data validation check is complete.

d Retention policy will run (if enabled).

x Files in the missing block(s) will be removed from the index.db file.

y Statistics will be updated according to the files removed.

Proceed to d

k Block size that are not identical will be removed from the backup destination(s).

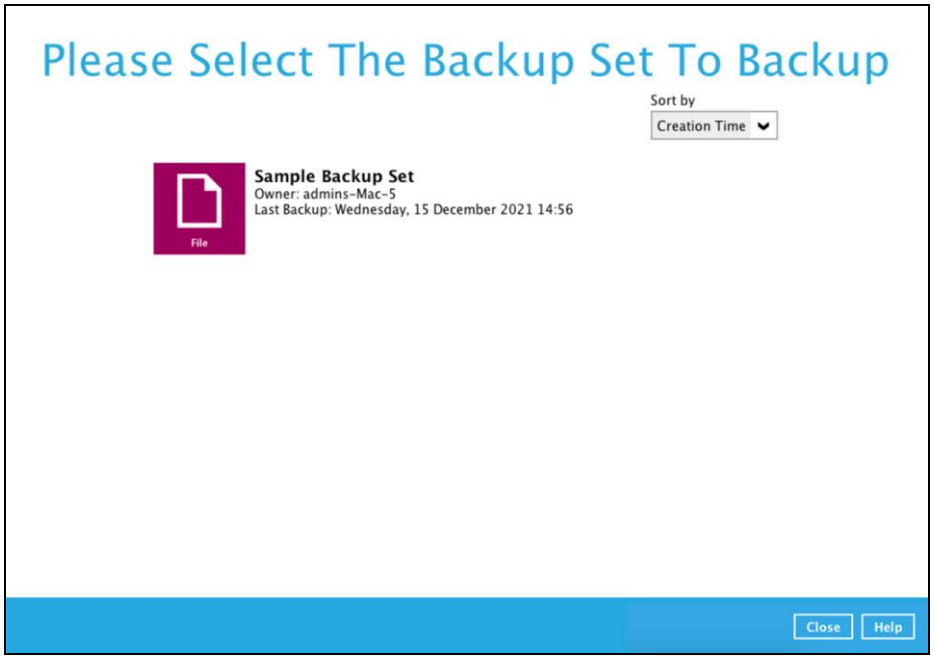
Proceed to y then

Proceed to d

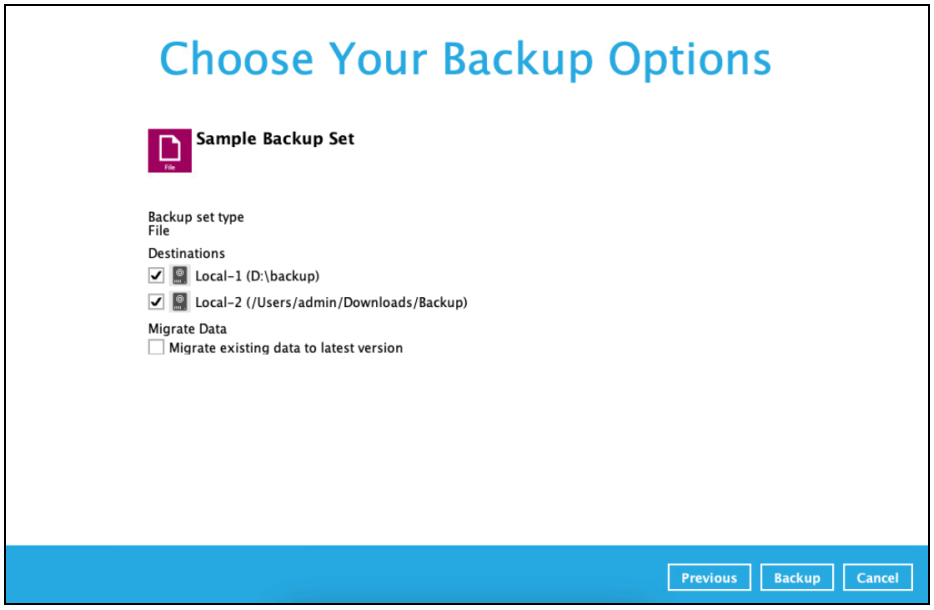
10 Run Backup Jobs

1. Click **Backup** on the main interface of CloudBacko Home

2. Select the backup set that you would like to start a backup job for.



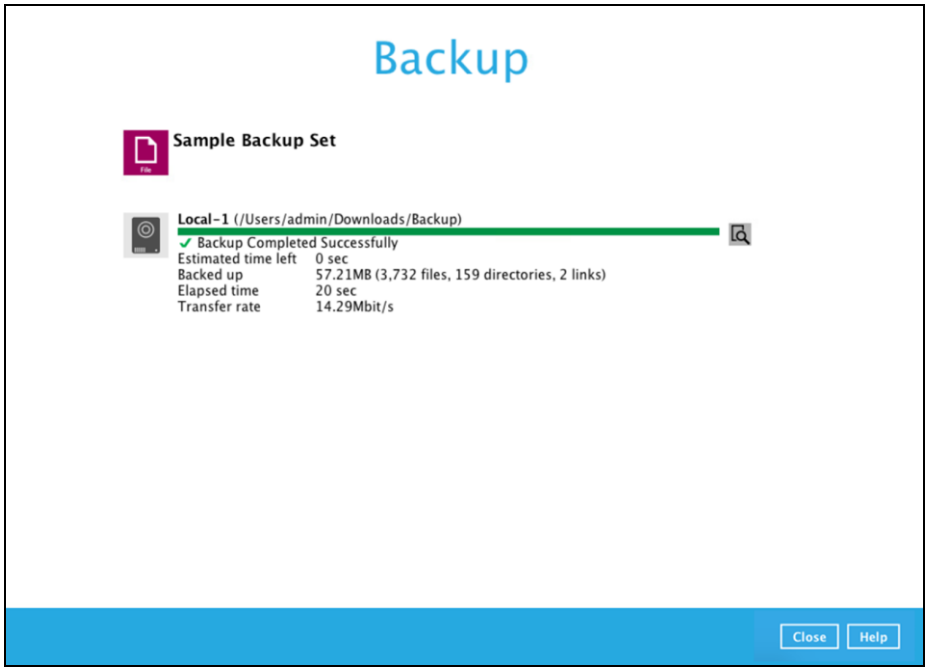
3. You can change the Destinations and Migrate Data options. Once done with the settings, click the **Backup** button to start the backup job.



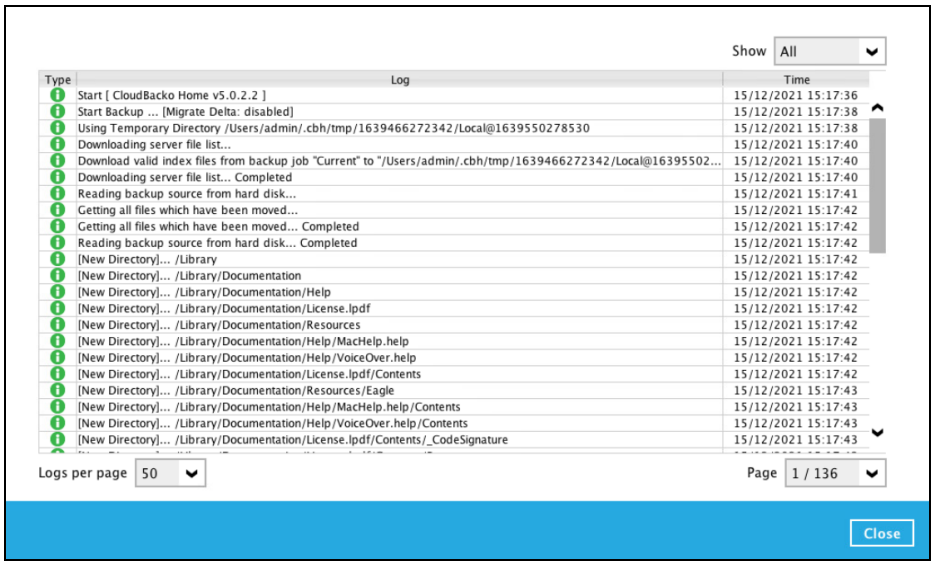
NOTE

Backup job(s) for backup sets with Migrate Data enabled may take longer to finish.

5. The following screen will be displayed to indicate that the backup job is successfully completed. You may click the button to check for the backup log.



6. Once you are done with checking the backup log, click the **Close** button to return to the previous screen.



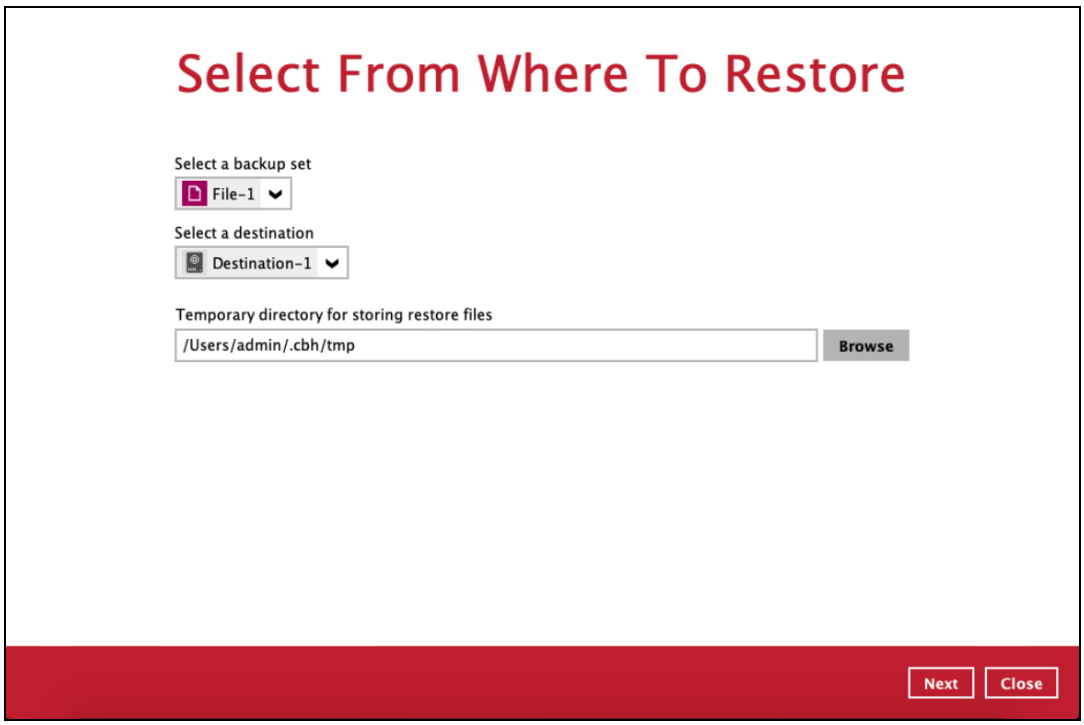
11 Restore Data

11.1 Restore Data

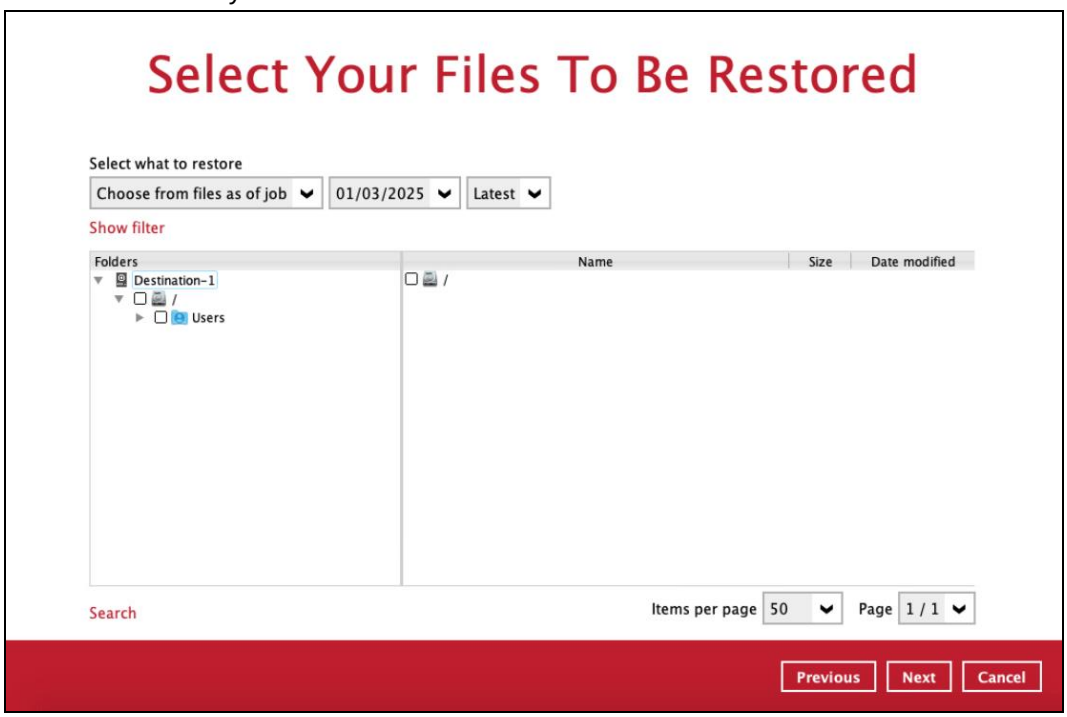
1. Log in to the Cloudbacko Home application according to the instructions in the section Chapter 6 Start CloudBacko Home.
2. Click the **Restore** icon on the main interface of CloudBacko Home.

3. In the next page, you will have several options to select. On this page, you may select the **Backup Set** to restore, as well as the **Destination** to which the data will be restored to.

   You may also choose the temporary directory for restoring files by selecting a destination beneath **Temporary directory for storing restore files**.

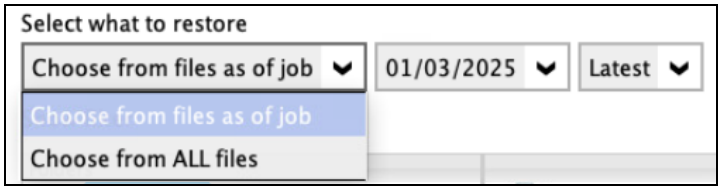


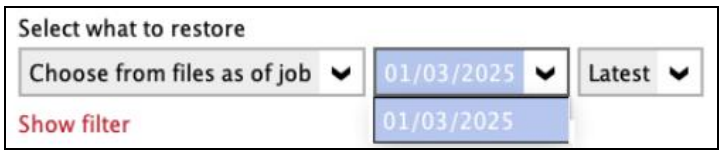
4. Select to restore files from a specific backup job, or from all files available. Then, select the files or folders that you would like to restore.



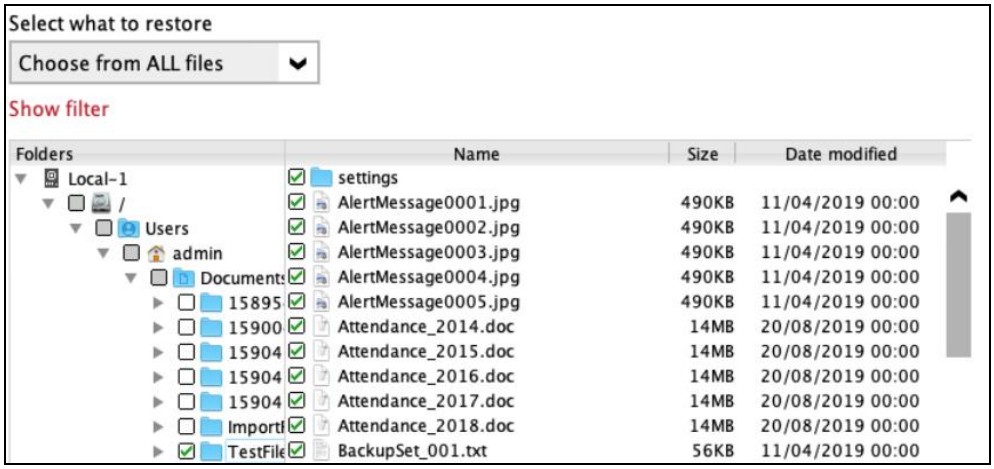
There are two options from the **Select what to restore** dropdown menu:

Choose from files as of job – This option allows you to select a backup version from a specific date and time to restore.





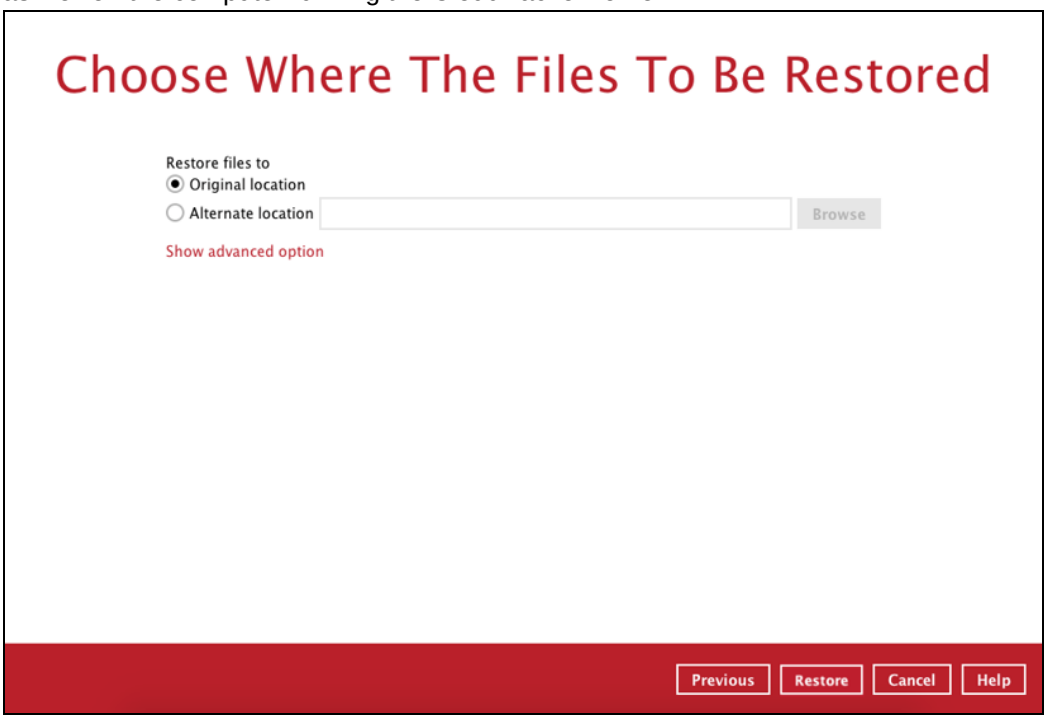
Choose from ALL files – This option allows you to restore all the available backup versions for this backup set. Among all the available backup versions, you can even select only some of the backup versions of a file to restore. Click the **Show files** checkbox to select individual files for restoration.



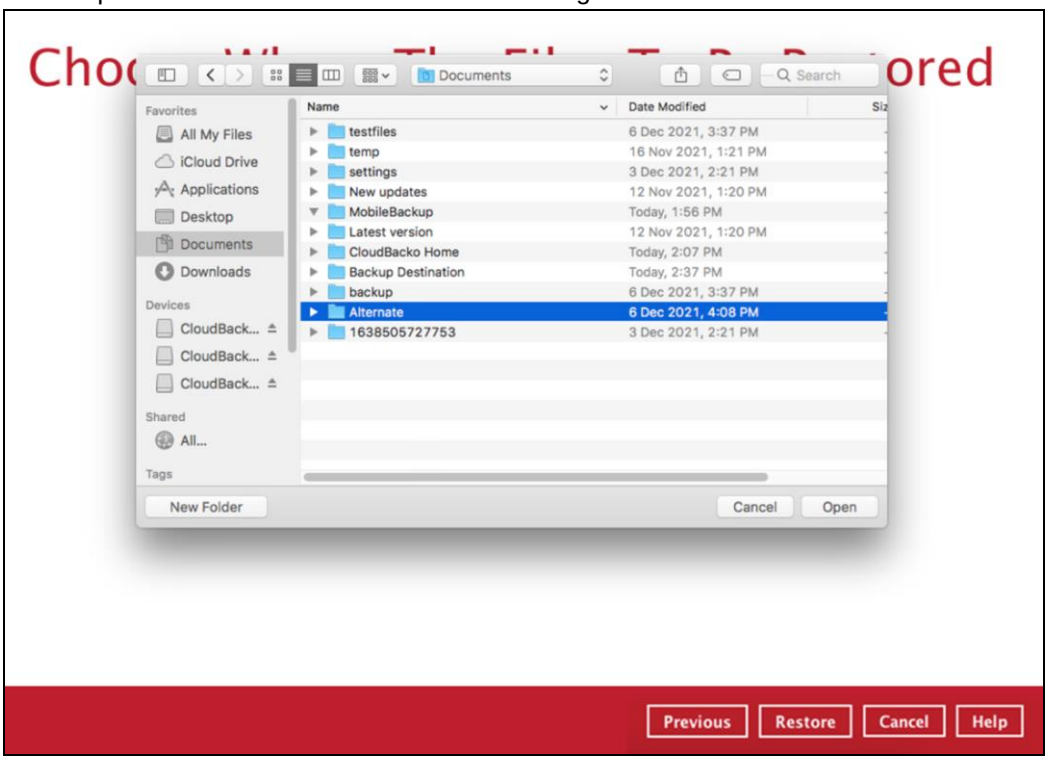
5. Click **Next** to proceed when you are done with the selections.
6. Select to restore the files to their **Original location**, or to an **Alternate location**. Then, click **Next** to proceed.

   Original location – the backed-up data will be restored to the computer running the CloudBacko Home under the same directory path as on the machine storing the backup source.

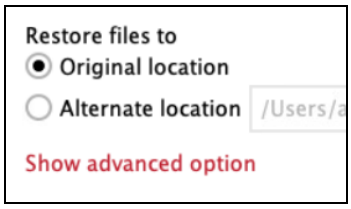
   For example, if the backup source files are stored under **Users/[User's Name]/Downloads** folder, the data will be restored to **Users/[User's Name]/Downloads** as well on the computer running the CloudBacko Home.

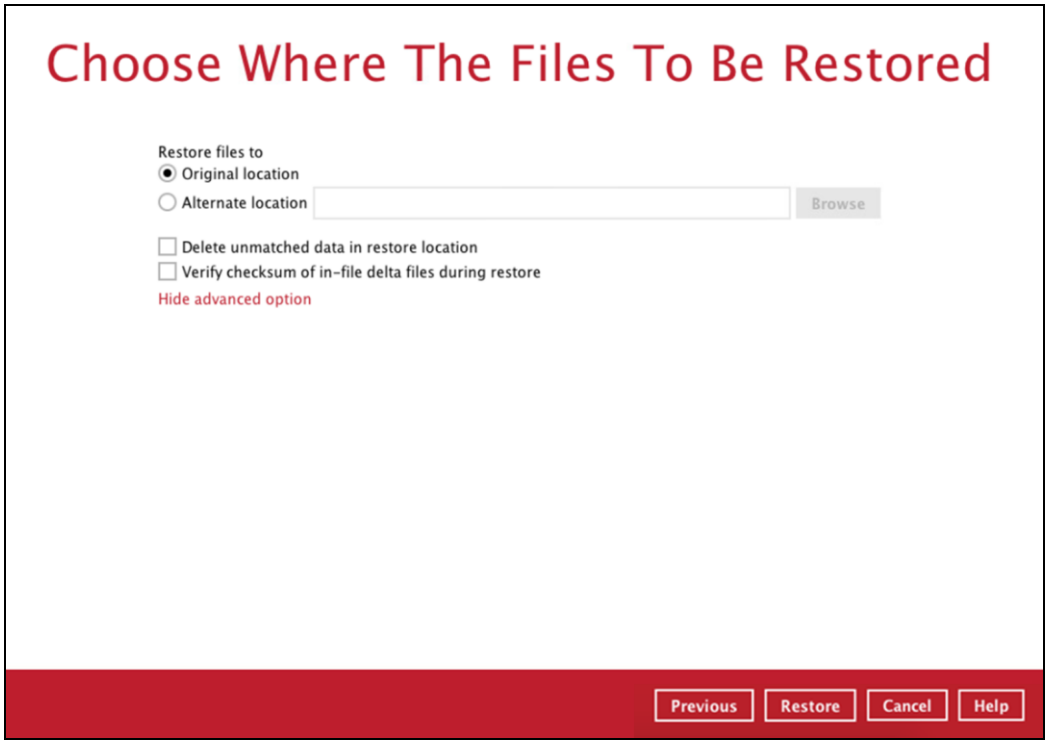


Alternate location – you can choose to restore the data to a location of your choice on the computer where CloudBacko Home is running.



7. Click **Show advanced option** to configure other restore settings:





Delete unmatched data in restore location

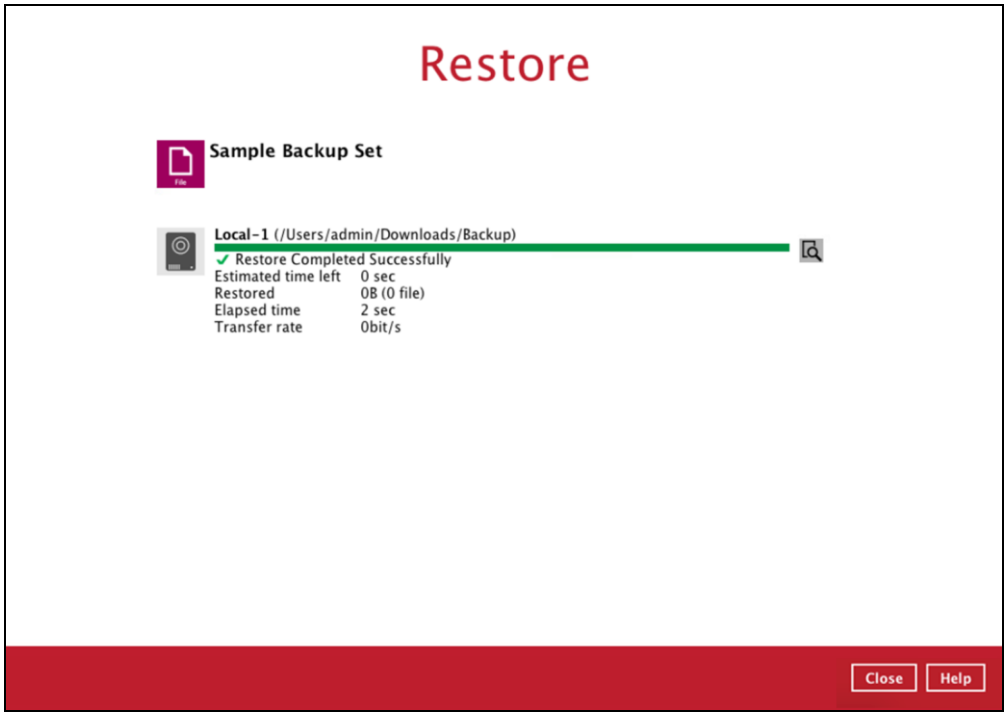
By enabling this option, the restore process will attempt to synchronize the selected restore source with the restore destination, making sure the data in the restore destination is the same as the restore source. Any data created after backup will be treated as “unmatched data” and will be deleted from the restore source if this feature is enabled.

Verify checksum of in-file delta files during restore

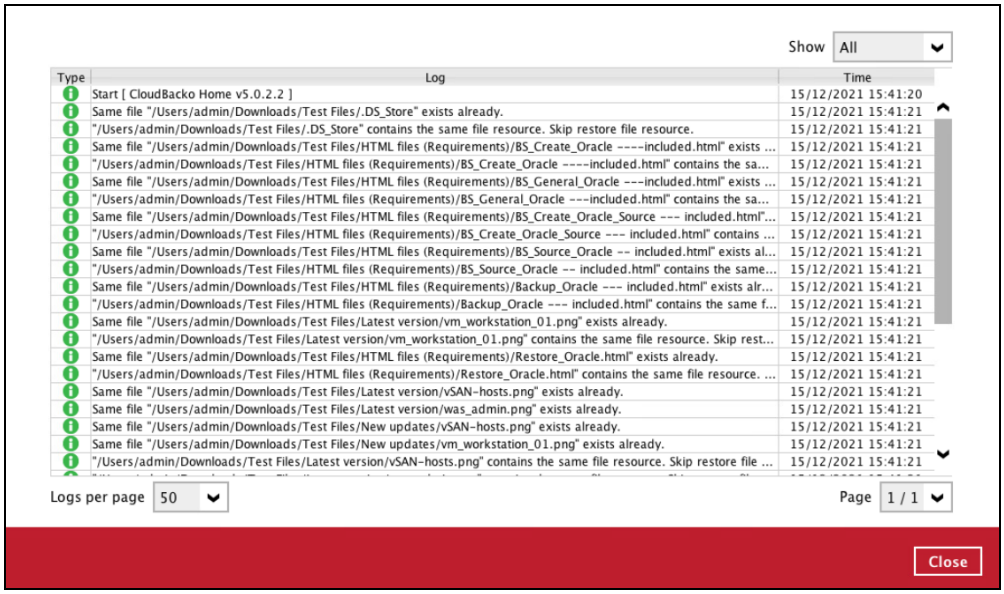
Verify checksum of in-file delta files during restore is disabled by default. When enabled, the checksum of in-file delta files will be verified. As the feature will make the restore process time longer, it is recommended to enable the feature only if you want to verify whether the merged files were correct.

Click **Restore** to start the restore process.

8. The following screen will be displayed to indicate that the restore job is successfully completed. You may click the button to check for the restore log.



9. Once you are done with checking the backup log, click the **Close** button to return to the previous screen.



10. In the Restore window, click **Close** to exit the Restore window.

11. To exit CloudBacko Home, click the "**x**" button on the top left corner. A confirmation message will appear. Click **Yes** to close the application.

11.2 Restore Filter

This search feature allows you to search directories, files, and folders.

To make it more flexible, the search feature offers filtering. You can add additional pattern upon searching. Pattern includes the following criteria:

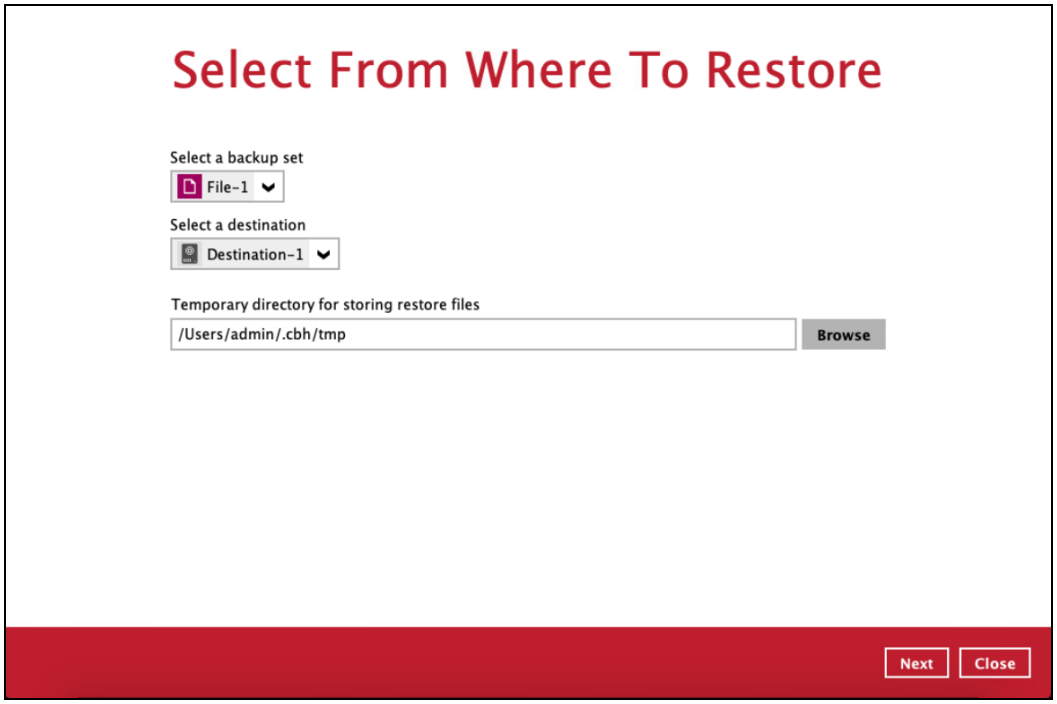
- **Contains**
  These are Directories, Files, and Folders with the name **containing** the specific letter or word.
- **Exact**
  These are Directories, Files, and Folders with the **exact** or **accurate** name.
- **Start With**
  These are Directories, Files, and Folders with the name **starting** with a specific letter or word.
- **Ends With**
  These are Directories, Files, and Folders with the name **ending** with a specific letter or word.

It also has the **Match Case** function, which serves as an additional accuracy when searching for any specific directories, files, folders, and mails.

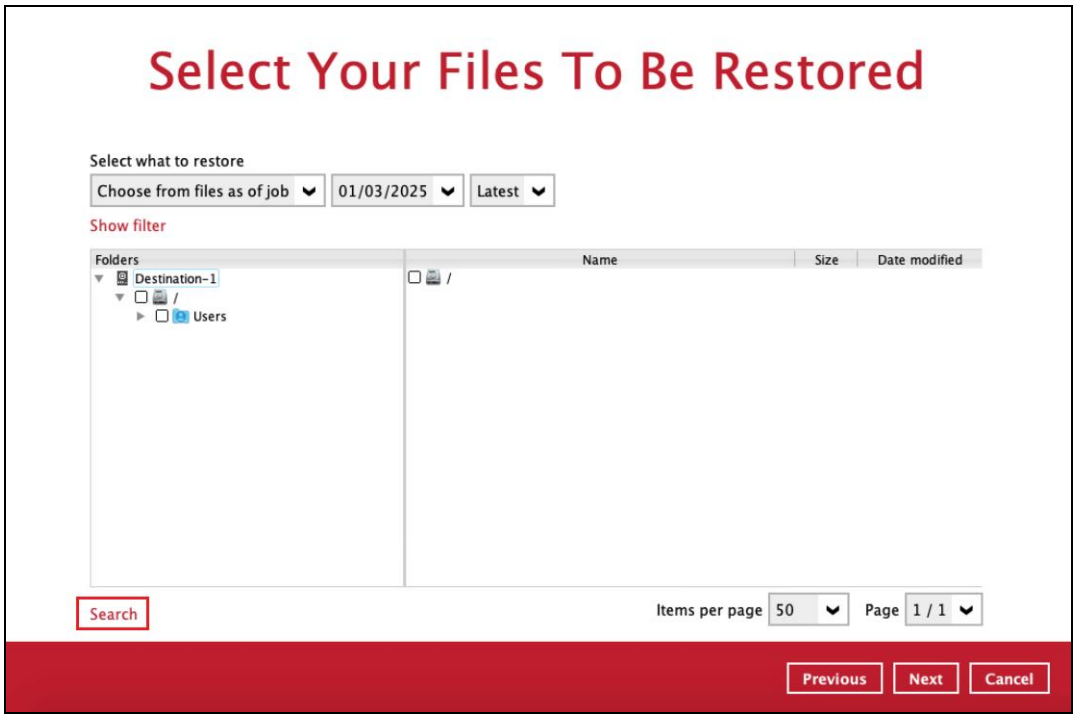
For more detailed examples using the restore filter on CloudBacko Home, refer to Appendix B: Example Scenarios for Restore Filter.

1. Log in to the Cloudbacko Home application according to the instructions in the section Chapter 6 Start CloudBacko Home.
2. Click the **Restore** icon on the main interface of CloudBacko Home.
3. In the next page, you will have several options to select. On this page, you may select the **Backup Set** to restore, as well as the **Destination** to which the data will be restored to.

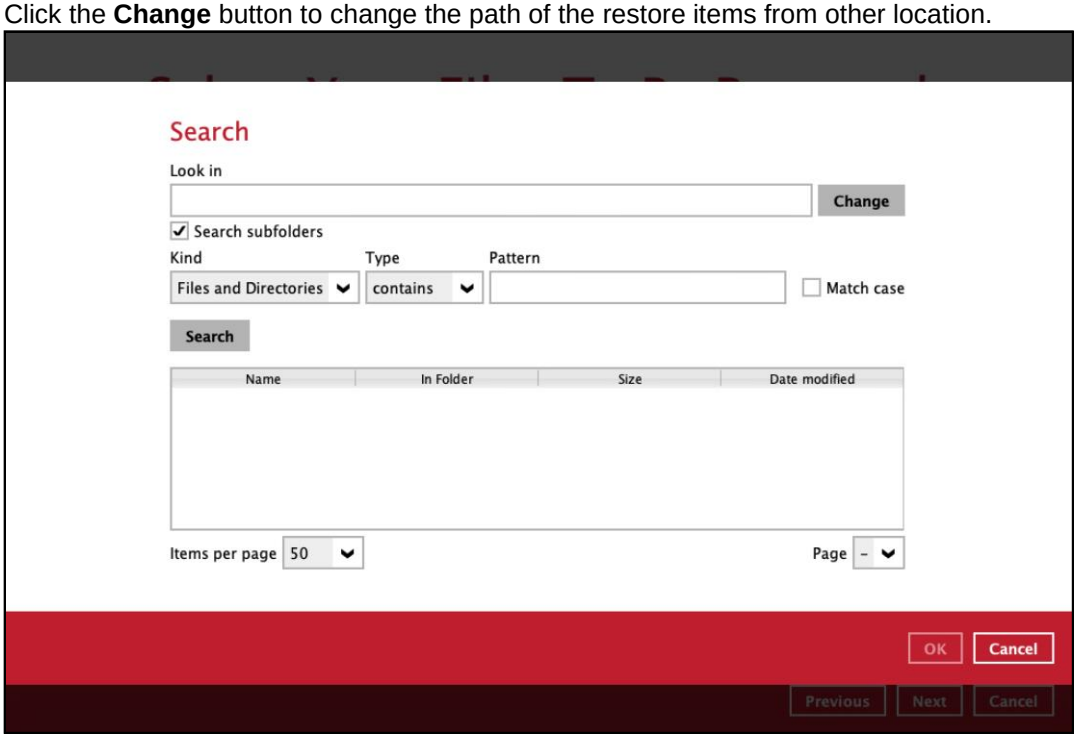
   You may also choose the temporary directory for restoring files by selecting a destination beneath **Temporary directory for storing restore files**.

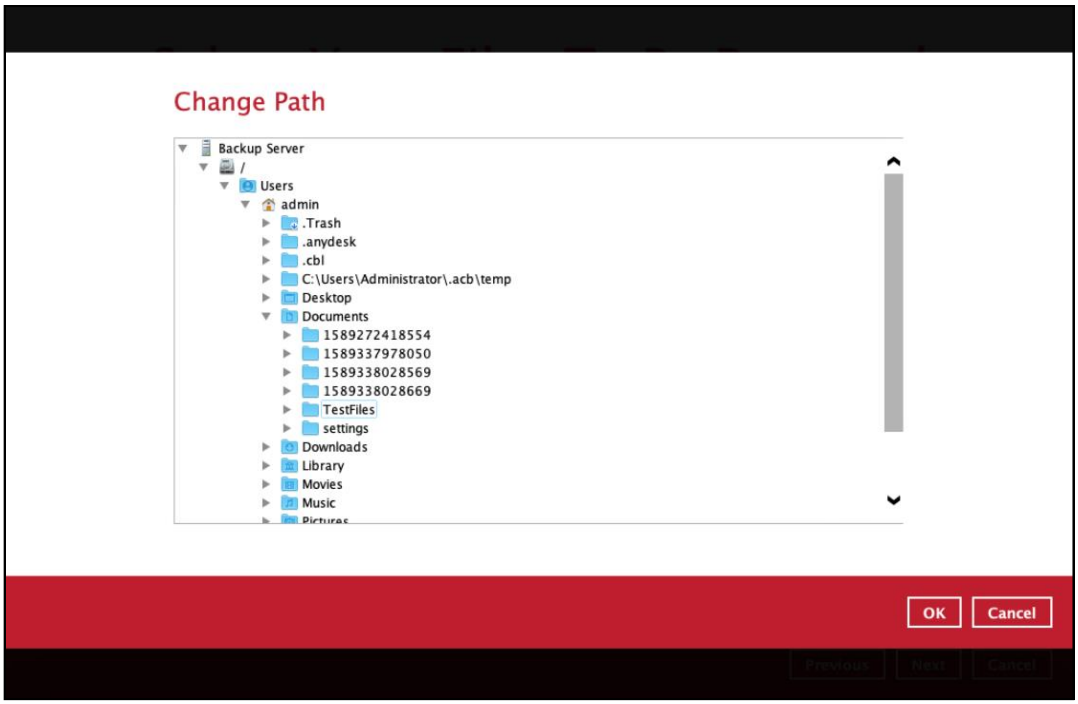


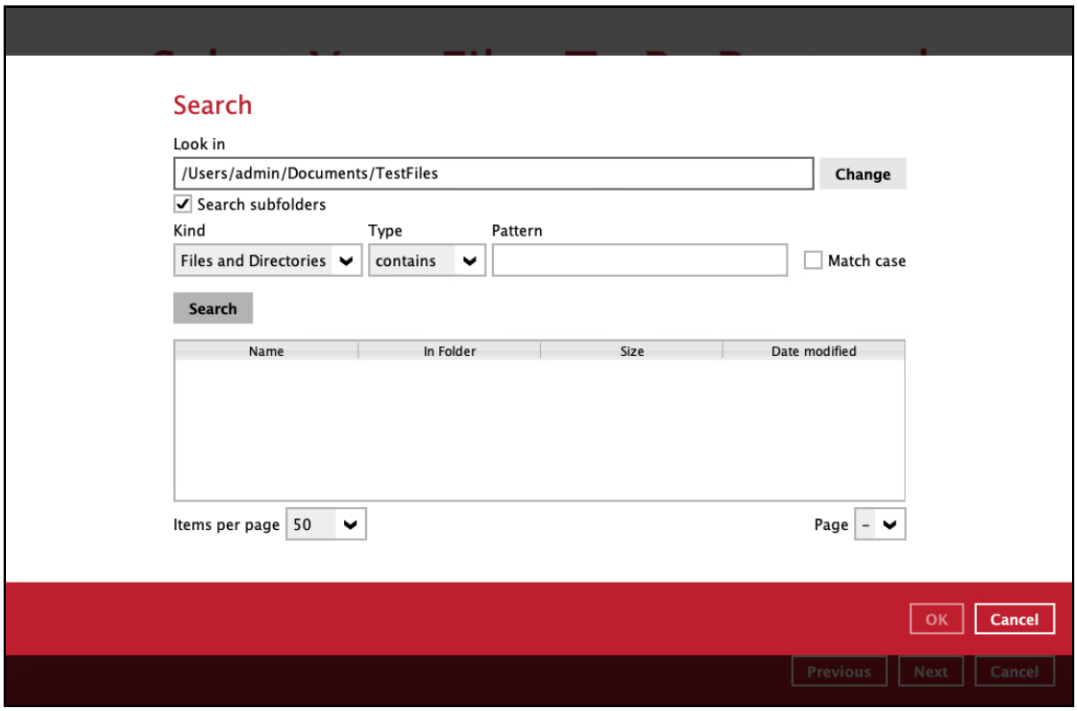
4. Click **Search** located on the lower left side of the screen.



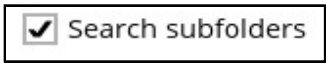
5. Click the **Change** button to change the path of the restore items from other location.







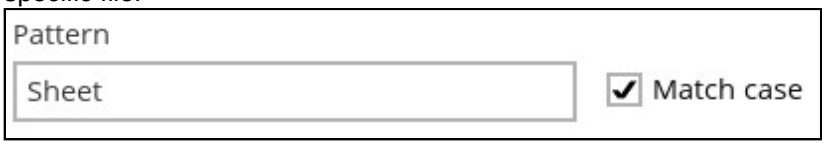
6. Tick **Search subfolders** to include available subfolders upon searching.



7. Select from the following Kind of files you want to search.
    - Files and Directories
    - Files only
    - Directories

8. Select from the following Type of filtering you want to search.
    - Contains
    - Exact
    - Starts With
    - Ends With

9. Enter a pattern you want and tick the **Match case** checkbox if you want to accurately search for a specific file.



10. Click the **Search** button and the result will be displayed.

11. Check all the items or check a specific item that you want and click the **OK** button to proceed and return to the restore main screen.

12 Mobile Backup and Restore to Cloud

To perform mobile backup and restore to Cloud, follow the steps below:

1. Back up photos, videos, documents and 2FA accounts from CloudBacko app to CloudBacko Home local destination. For more detailed information, refer to CloudBacko App User Guide for Android and iOS.
2. Create a File backup set according to the instructions in Chapter 8 Create a Backup Set with the following setup:
   - The backup source should be the photos, videos, documents and/or 2FA account(s) backed up in the CloudBacko Home local destination.

     Example: **Users/admin/Documents/MobileBackup1**
   - The backup destination should be a Cloud destination (e.g., Google Drive, OneDrive, Wasabi, etc.).
3. Run a backup job according to the instructions in Chapter 10 Run Backup Jobs.
4. Restore data according to the instructions in Chapter 11.1 Restore Data. This can be from Original or Alternate Location.

   There are two (2) options to restore data from Cloud storage to the mobile device, Original location, and Alternate location.

   - **Original location** - data will be restored on the original location which is the **backup destination for your mobile device**.

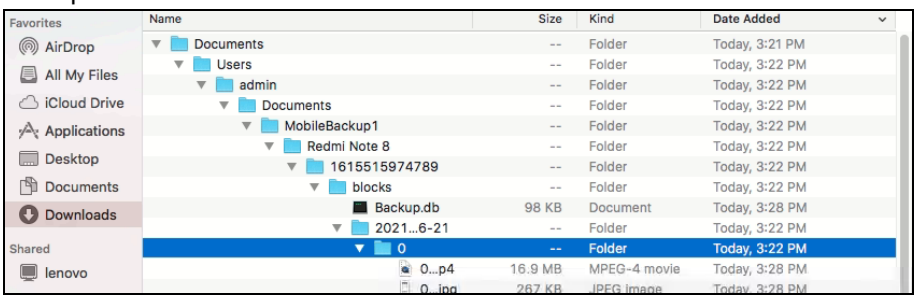
     Using this option, you can perform seamless restore to your mobile device as the location is the same with the mobile backup destination.
   - **Alternate location** - data will be restored on an alternate location which can be setup anywhere in the CloudBacko Home local machine. If you choose this option, then restoring to your mobile device will have to be manually done. There are two (2) options available.

     NOTE: Restore to alternate location is not supported on another CloudBacko Home machine. Options 1 and 2 must be on the original machine where the backups were performed.

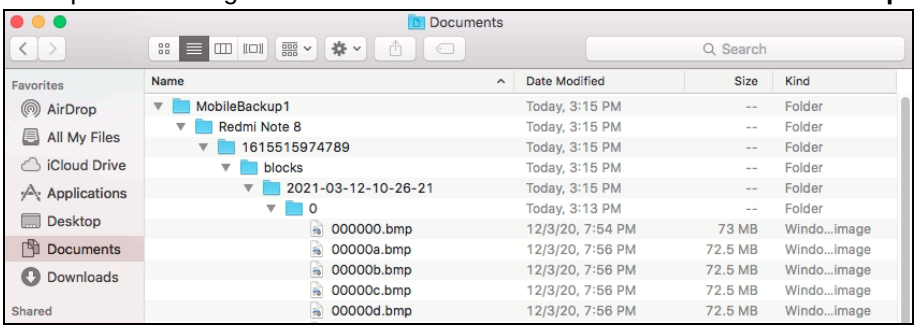
     In case the original machine is no longer available, CloudBacko Home will be able to restore the photos, videos, documents and 2FA accounts from the Cloud destination to the mobile backup destination folder. However, as the mobile device was not originally paired with the new installation or machine, the mobile device will not be able to restore the photos, videos, documents and 2FA accounts from the CloudBacko Home.

     Option 1: Copy the restored data from alternate location to original location which is the **backup destination for your mobile device**. You can now use the CloudBacko app to restore the photos, videos, documents and 2FA accounts back to your mobile device.

Example of the Alternate location: **/Users/admin/Downloads/Documents**



Example of the Original location: **/Users/admin/Documents/MobileBackup1**



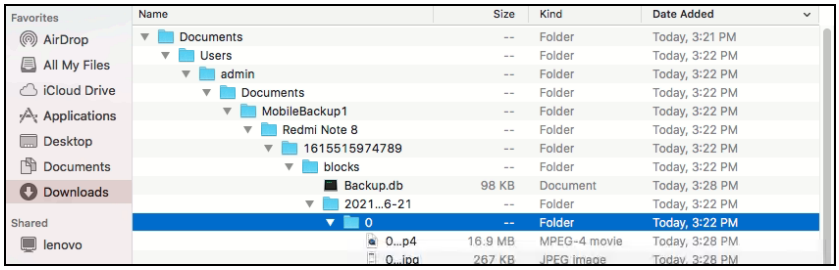
You can now use the CloudBacko app to restore the photos, videos, documents and 2FA accounts back to your mobile device.

Option 2: Copy the restored data from the alternate location to your Android or iOS mobile device.

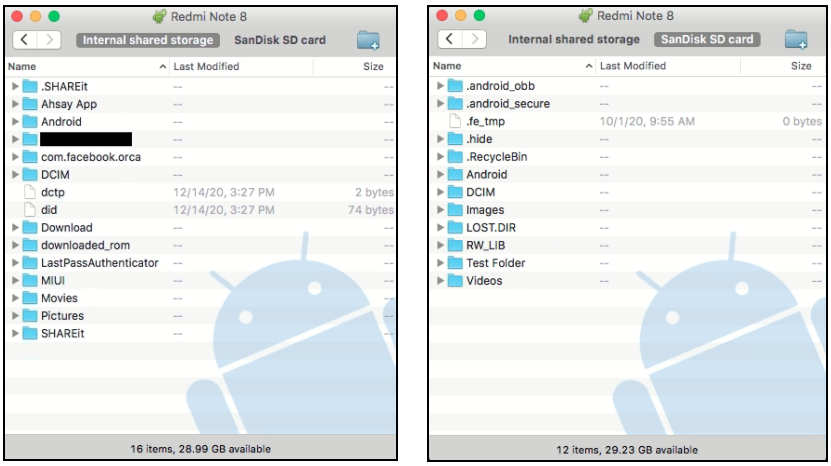
Instructions:

- For an Android device, you need to plug your cable and transfer the restored data from the alternate location to your mobile device storage.

  Alternate location: **/Users/admin/Downloads/Documents**

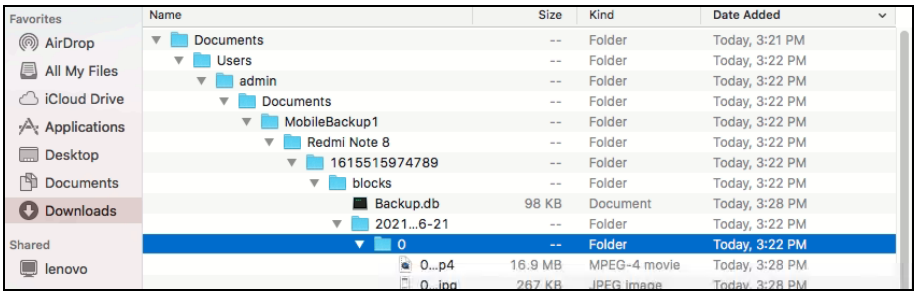


Android device Internal storage and SD Card

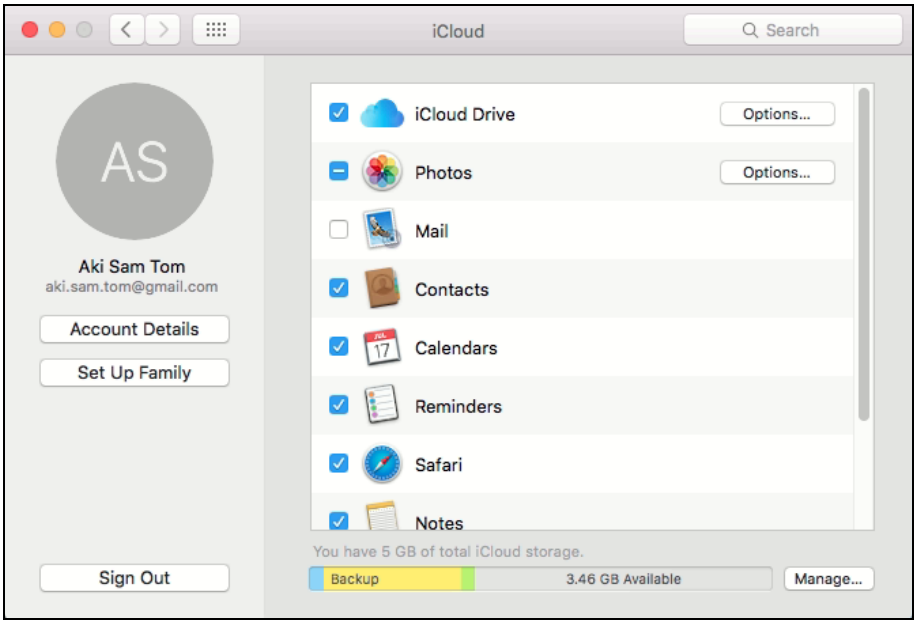


- For an iOS device, you need to transfer the restored data from the alternate location to iCloud.

  Alternate location: **/Users/admin/Downloads/Documents**



  Upload to iCloud.



13 Contact CloudBacko

Technical Assistance

To contact CloudBacko support representatives for technical assistance, please visit the Contact Us page to submit a support ticket:

https://www.cloudbacko.com/support

Use the CloudBacko Wiki for resource such as Hardware Compatibility List, Software Compatibility List, and other product information. To also check available documentations and hotfix please visit the Support page.

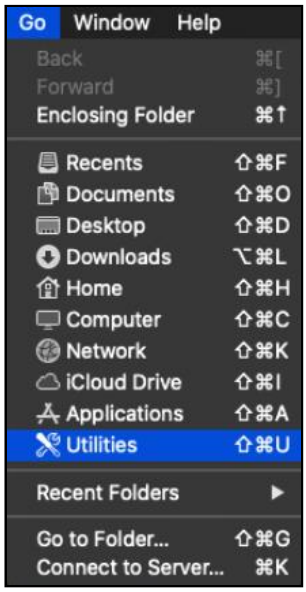
Appendix

Appendix A: Uninstall CloudBacko Home

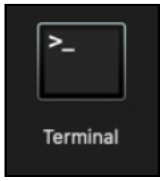
Before you uninstall CloudBacko Home it is recommended that you make a backup of your current CloudBacko settings, using the **[Utilities] -> [Export Settings] -> [Export Now]** feature to get a copy of the latest **settings.sys** file. For more information, please check Chapter 7.8.3 Export Settings.

Otherwise, if you intend to re-install CloudBacko Home either on the same machine or a new machine, you will lose your current settings and access to any backed-up data.

1. Click **Go** at the top menu bar and then select **Utilities**.



2. Double-click the Terminal.app icon.



3. Use the command highlighted in red to enter the Applications folder.

```
#cd /Applications

#[user]-Mac-mini:Applications [user]$
```

4. Use the command highlighted in red to enter the CloudBacko Home folder.

```
#[user]-Mac-mini:Applications [user]$ cd CloudBacko\
Home.app/bin

#[user]-Mac-mini:bin [user]$
```

5. Use the command highlighted in red to execute the uninstallation. Enter the password for logging in to your Mac when prompted.

```
#[user]-Mac-mini:bin [user]$sudo sh uninstall.sh
#Password:
```

6. The following scripts show when the uninstallation is completed.

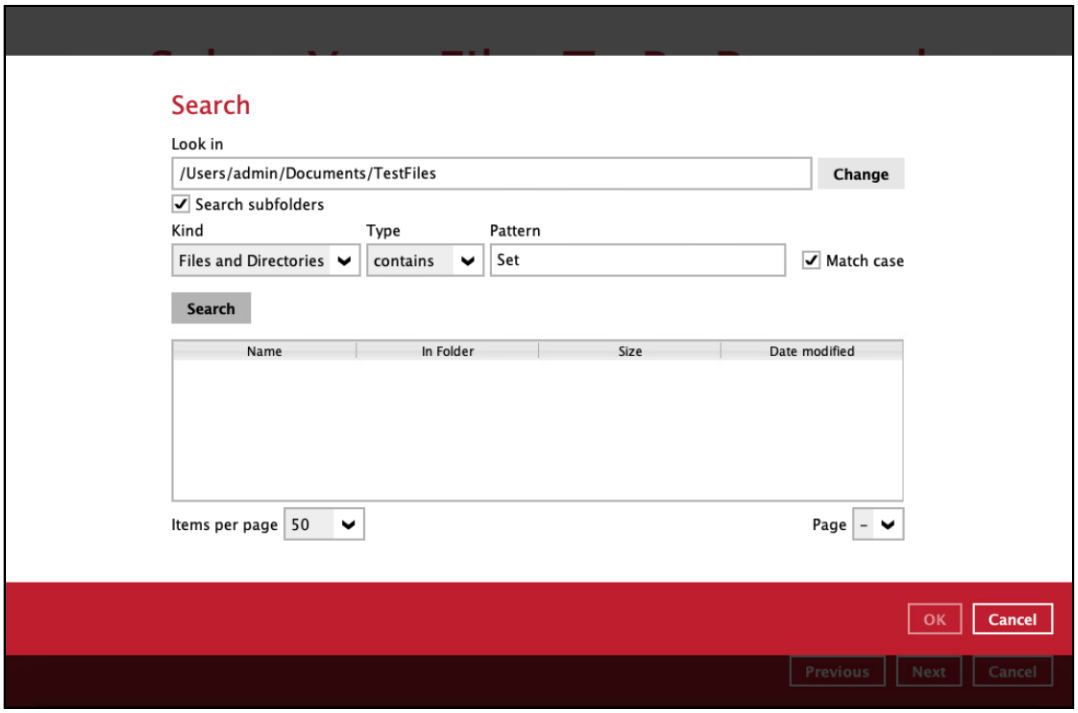
```
#Shutdown Scheduler for CloudBacko Home

#Wait 5 seconds before Scheduler exits

#Kill Process by Image Name:/Applications/CloudBacko
Home.app/jvm/bin/bJW

#Ignore Process by Image Name:

#Kill Process by Image Name: /Applications/ CloudBacko Home.app
/jvm/bin/bschJW

#Ignore Process by Image Name:

#Kill Process by Image Name: /Applications/ CloudBacko Home.app
/jvm/bin/java

#Ignore Process by Image Name:

#Remove LaunchDaemons for com.CloudBackoHome.scheduler from
service

#Remove CloudBacko Home from Your Mac OS X

#[user]-Mac-mini:bin [user]$
```

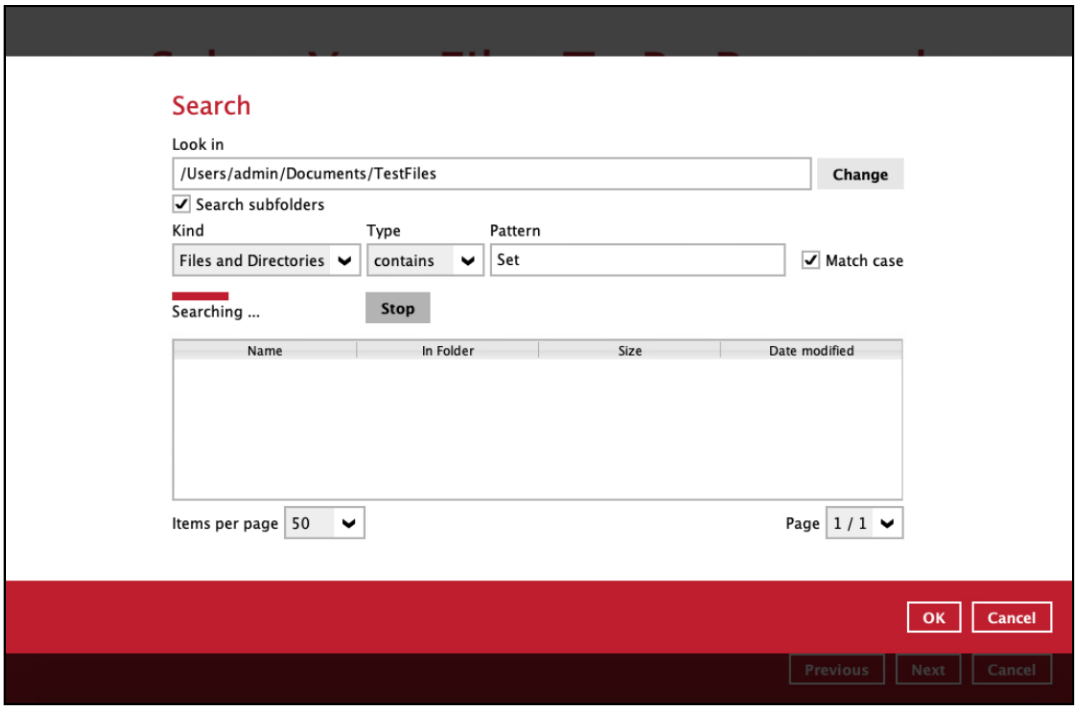
Appendix B: Example Scenarios for Restore Filter

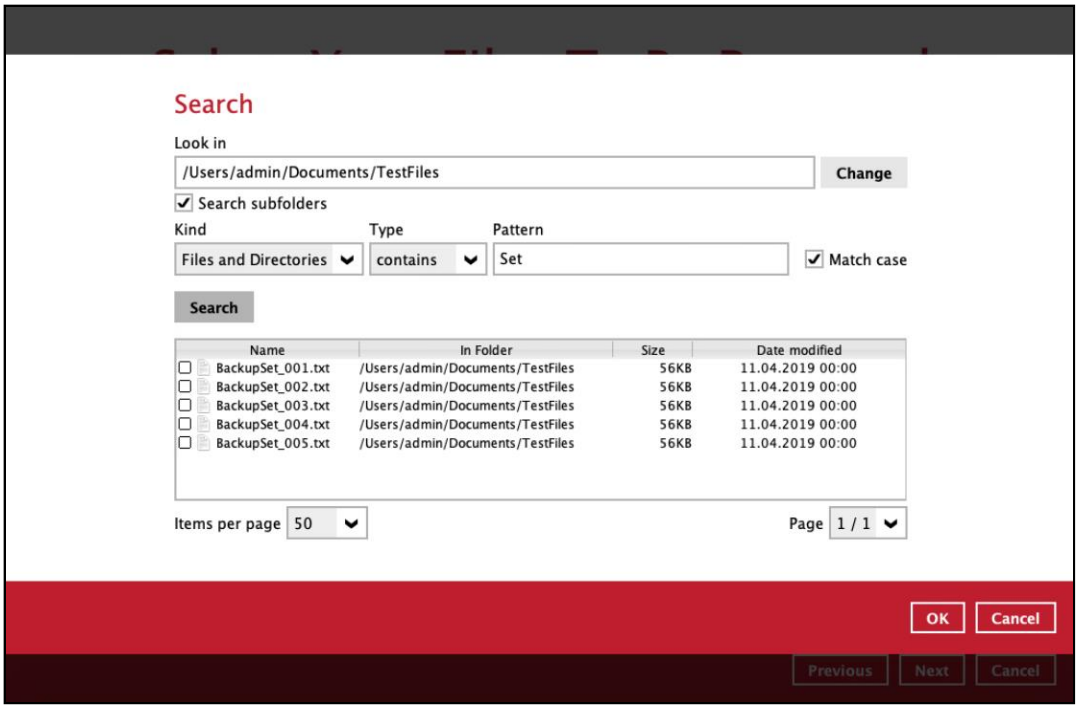
Example No.1: Restore filter setting from /Users/admin/Documents/TestFiles with filter type Contains

Location:	/Users/admin/Documents/TestFiles
Search subfolders:	True
Kind:	Files and Directories
Type:	Contains
Pattern:	Set
Match Case:	True

Follow the step-by-step procedure indicated on Restore Filter.







Explanation:

All files and directories under /Users/admin/Documents/TestFiles that has the pattern that contains with ‘Set’ with match case set to true will be included upon performing search.

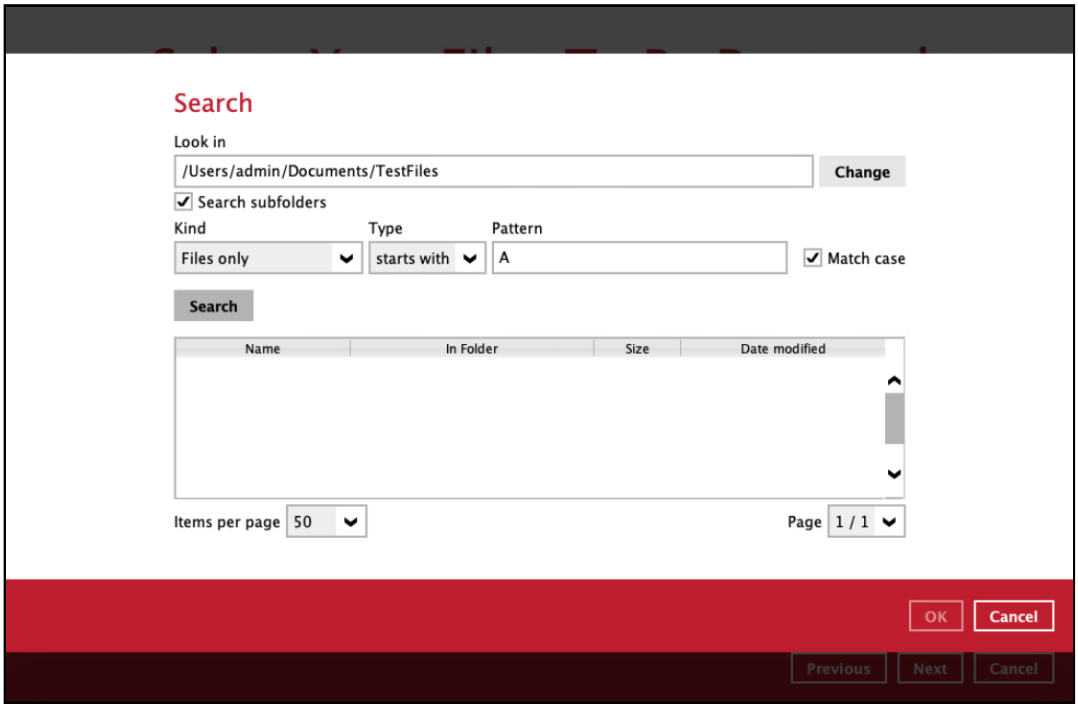
As you can see on the screen shot above, the result panel contains the Name of the file or directory, Directory which are indicated In-Folder column, Size, and Date Modified.

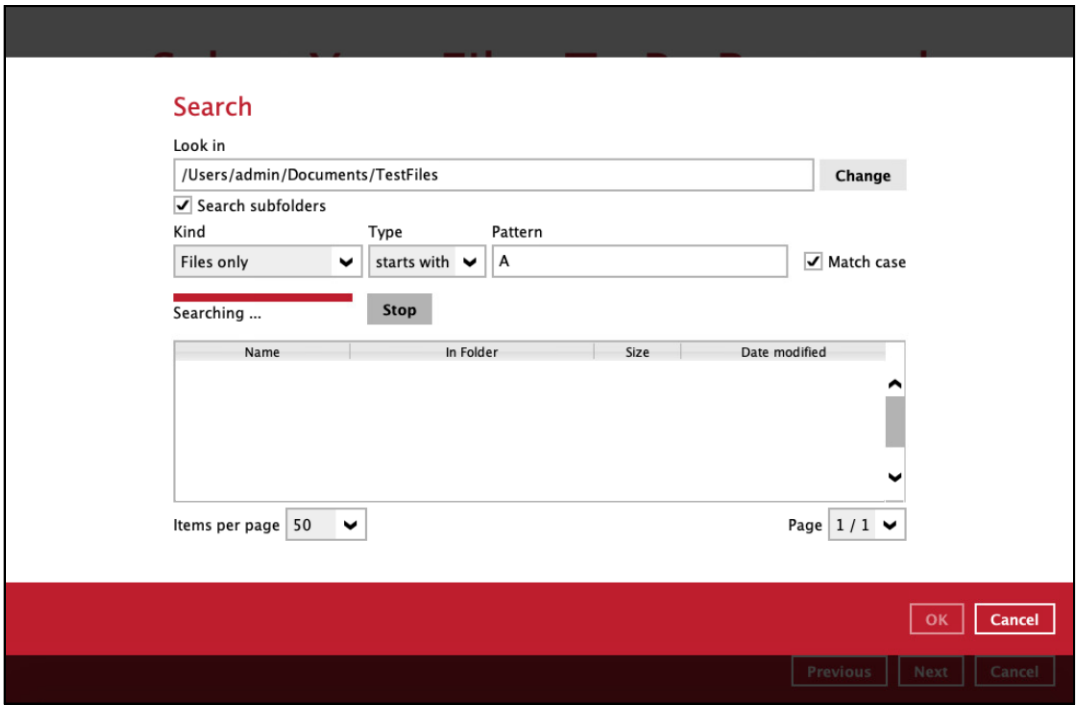
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in \TestFiles upon searching. And it will strictly search only the specified pattern and case which starts with ‘Set’.

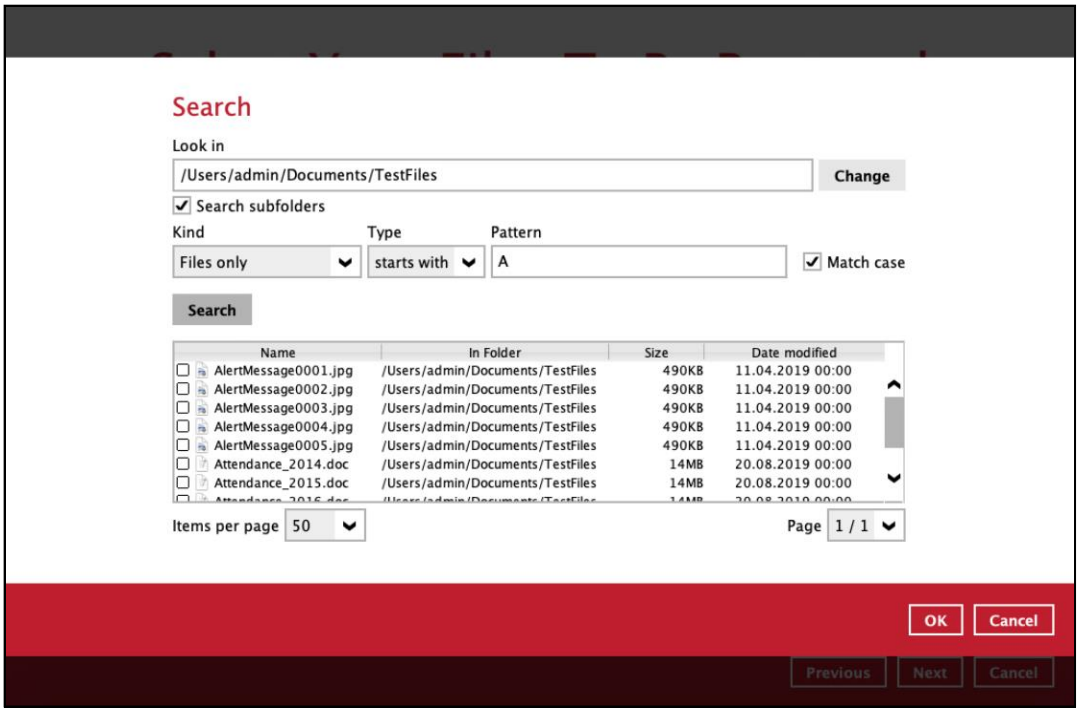
Example No.2: Restore filter setting from /Users/admin/Documents/TestFiles with filter type Starts With

Location:	/Users/admin/Documents/TestFiles
Search subfolders:	True
Kind:	Files
Type:	Starts With
Pattern:	A
Match Case:	True

Follow the step-by-step procedure indicated on Restore Filter.







Explanation:

All files and directories under /Users/admin/Documents/TestFiles that has the pattern that starts with ‘A’ with match case set to true will be included upon performing search.

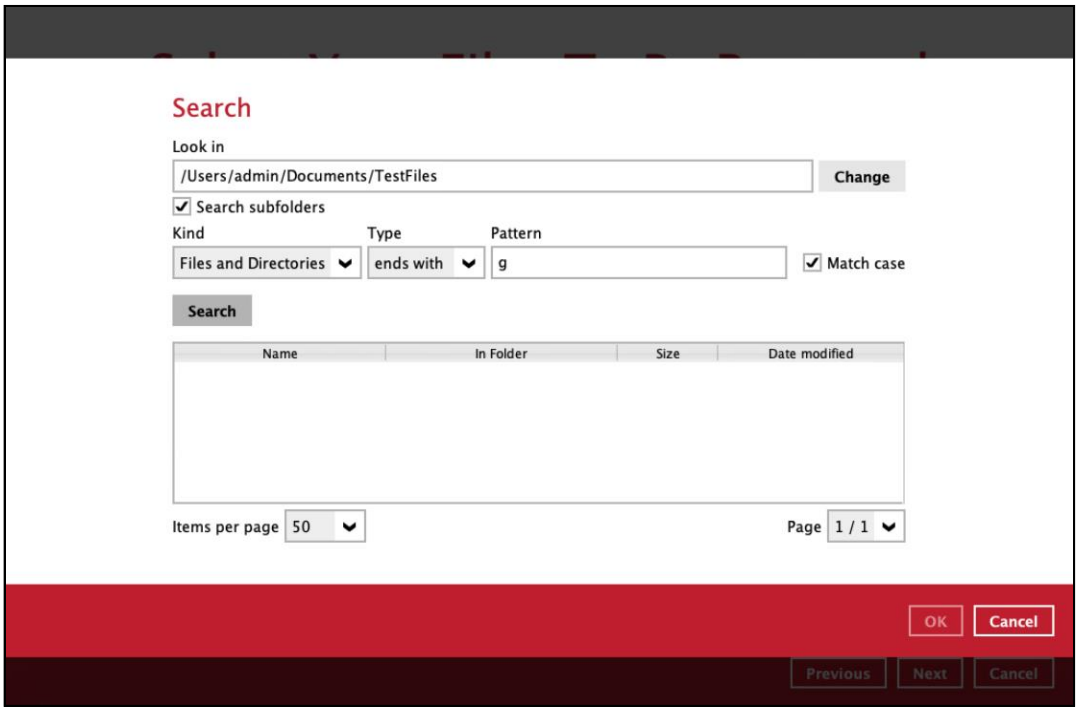
As you can see on the screen shot above, the result panel contains the Name of the file, Directory which are indicated In-Folder column, Size, and Date Modified.

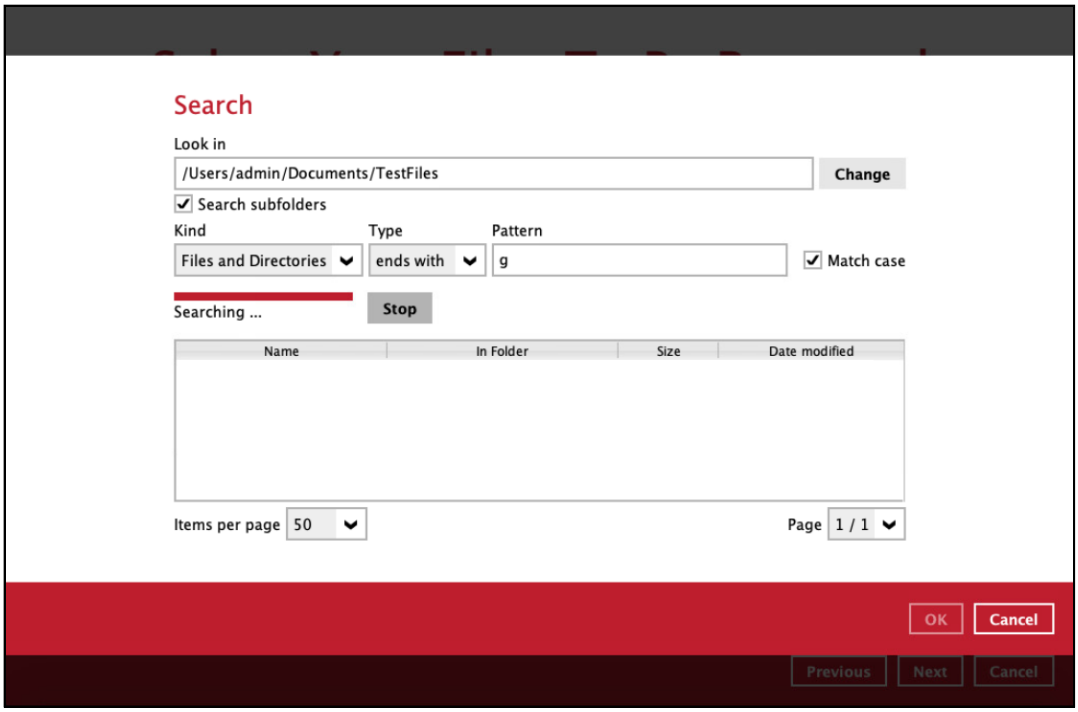
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in \TestFiles upon searching. And it will strictly search only the specified pattern and case which starts with ‘A’.

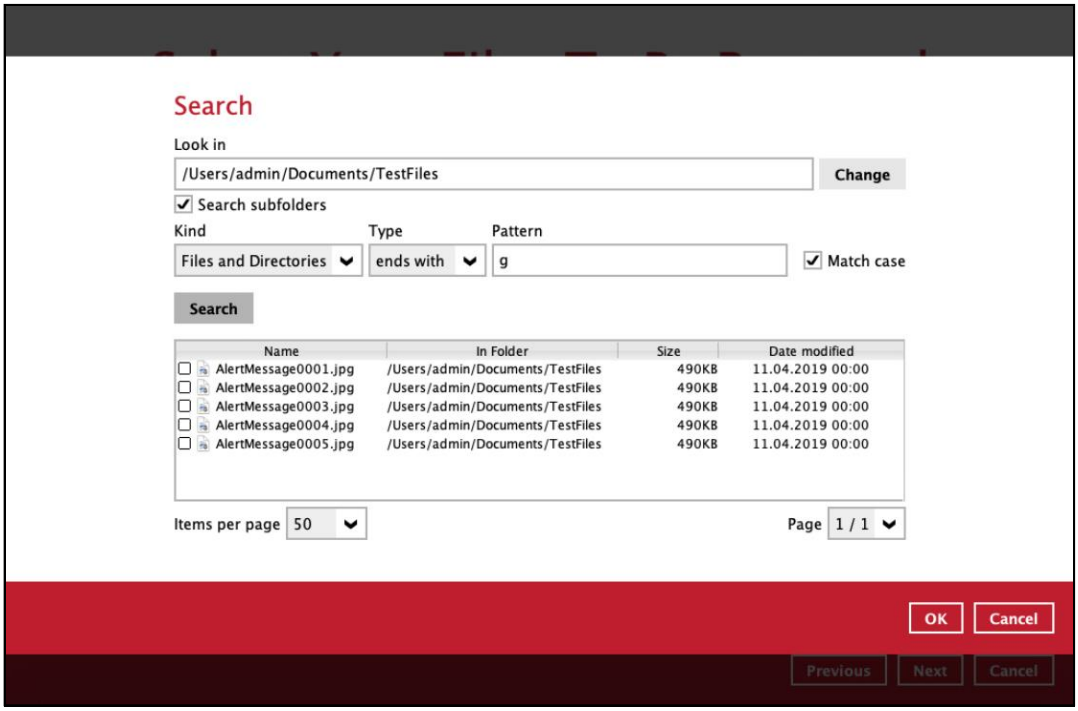
Example No.3: Restore filter setting from /Users/admin/Documents/TestFiles with filter type Ends With

Location:	/Users/admin/Documents/TestFiles
Search subfolders:	True
Kind:	Files and Directories
Type:	Ends With
Pattern:	g
Match Case:	True

Follow the step-by-step procedure indicated on Restore Filter.







Explanation:

All files and directories under /Users/admin/Documents/TestFiles that has the pattern that ends with ‘g’ with match case set to true will be included upon performing search.

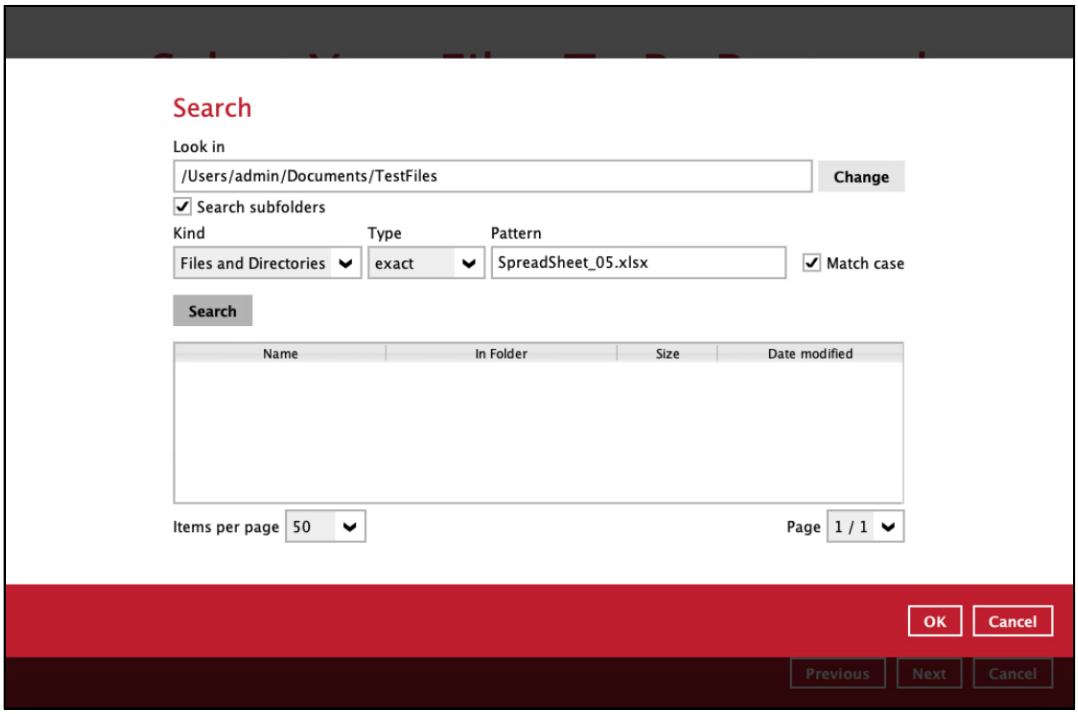
As you can see on the screen shot above, the result panel contains the Name of the files and directories, Directory which are indicated In-Folder column, Size, and Date Modified.

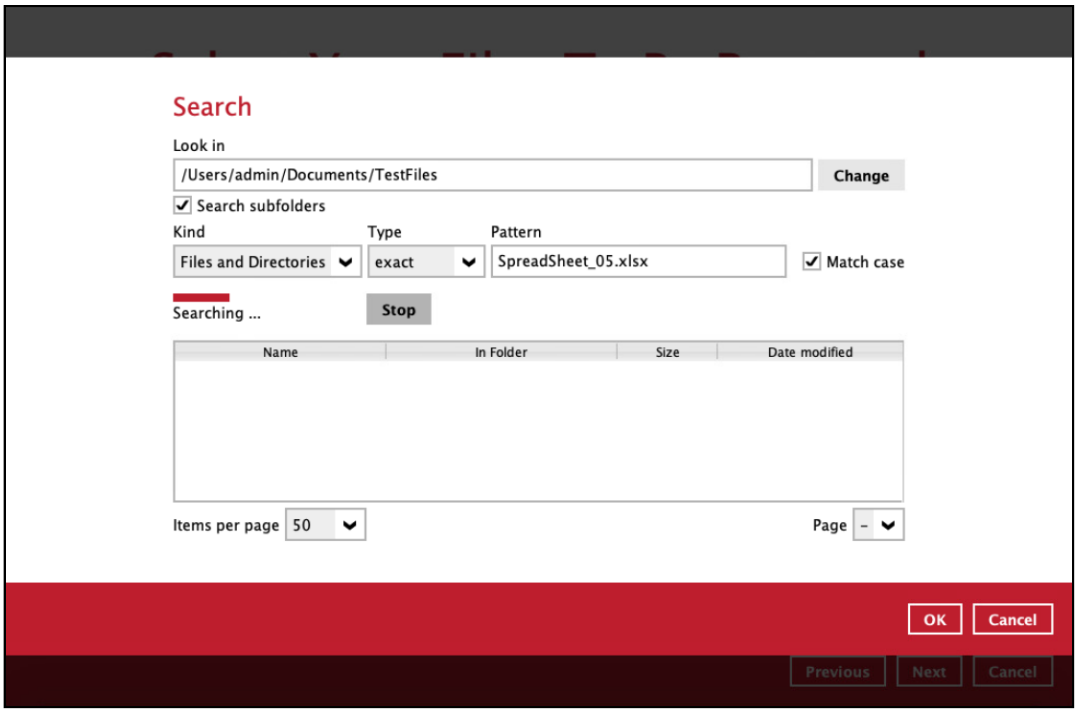
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in \TestFiles upon searching. And it will strictly search only the specified pattern and case which starts with ‘g’.

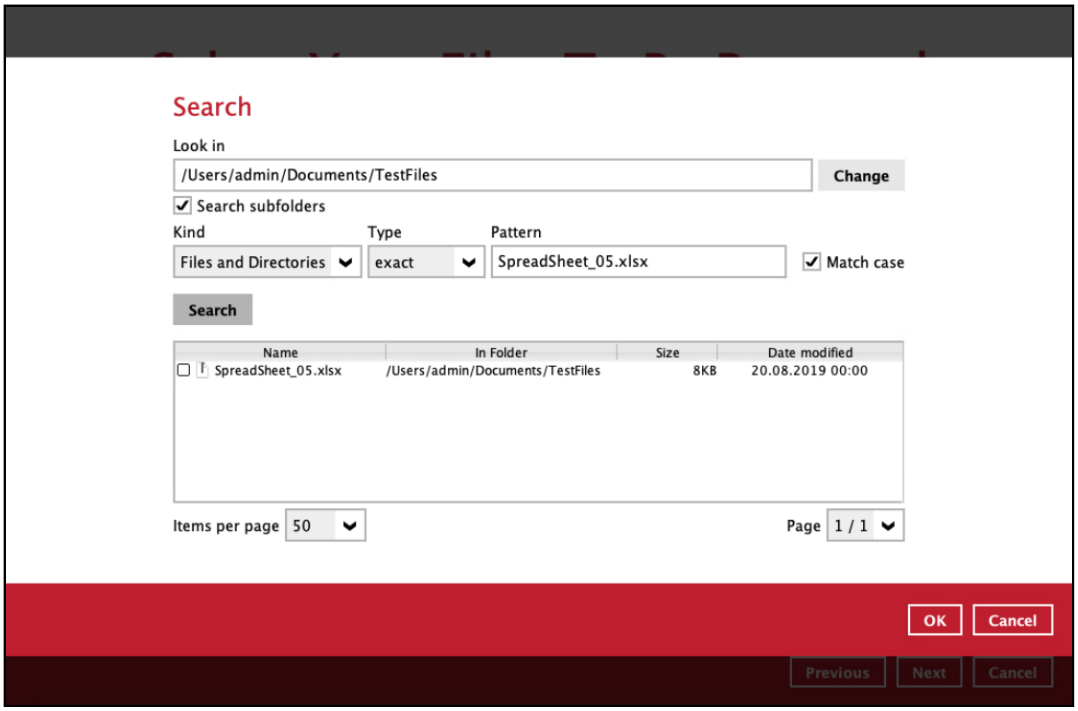
Example No.4: Restore filter setting from /Users/admin/Documents/TestFiles with filter type Exact

Location:	/Users/admin/Documents/TestFiles
Search subfolders:	True
Kind:	Files and Directories
Type:	Exact
Pattern:	SpreadSheet_05.xlsx
Match Case:	True

Follow the step-by-step procedure indicated on Restore Filter.







Explanation:

All files and directories under /Users/admin/Documents/TestFiles that has the pattern that has the exact pattern 'SpreadSheet_05.xlsx' with match case set to true will be included upon performing search.

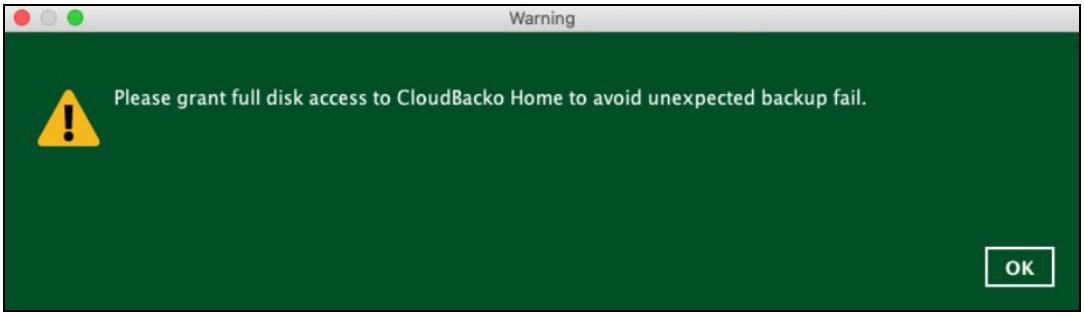
As you can see on the screen shot above, the result panel contains the Name of the files and directories, Directory which are indicated In-Folder column, Size, and Date Modified.

The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in \TestFiles upon searching. And it will strictly search only the specified pattern and case which starts with 'SpreadSheet_05.xlsx'.

Appendix C: Setting up Full Disk Access Permission

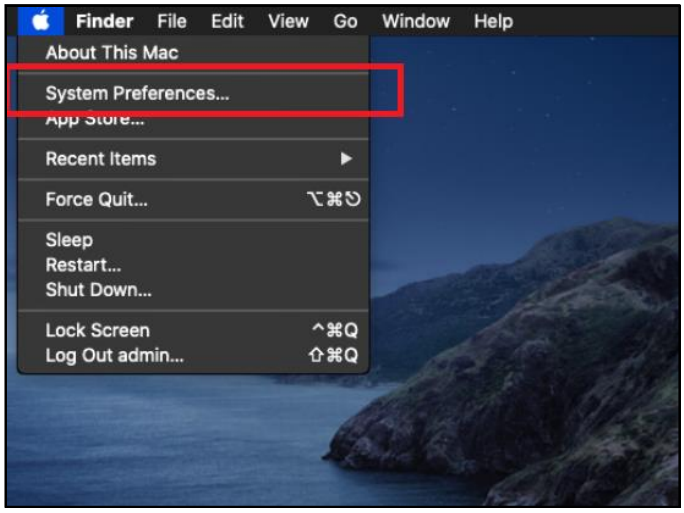
What is Full Disk Access? Full Disk Access is a new security feature in macOS 10.15 or higher that requires some applications to be given full permission to access your protected files and have certain administrative settings available.

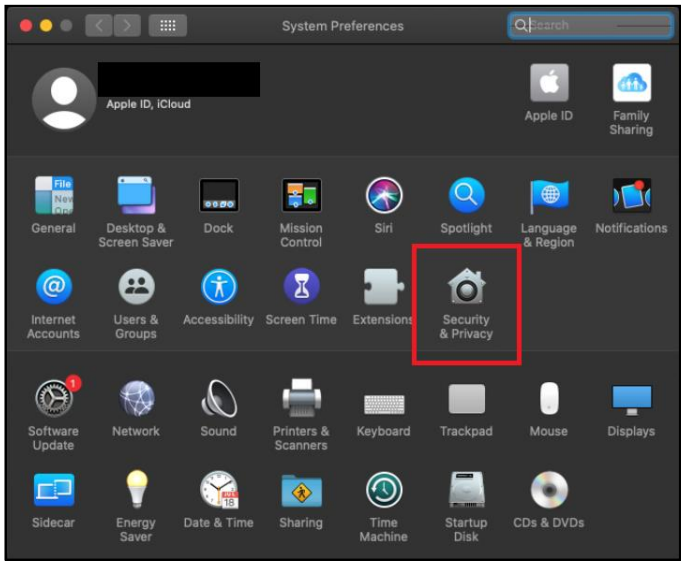
If CloudBacko Home was launched without granting a full disk access, this warning message will appear. It is advisable to setup the permission before launching the CloudBacko Home to avoid any unexpected backup and restore failure.



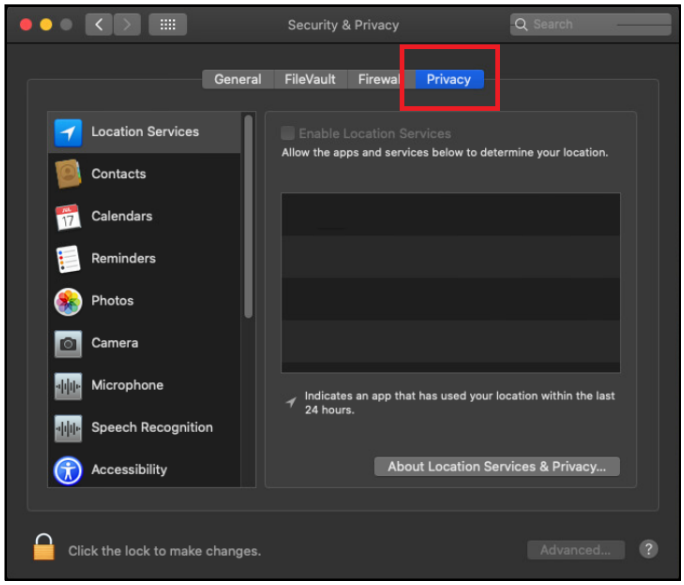
Here are the steps on how to setup and grant CloudBacko Home a Full Disk Access:

1. Open **System Preferences** > **Security & Privacy**.

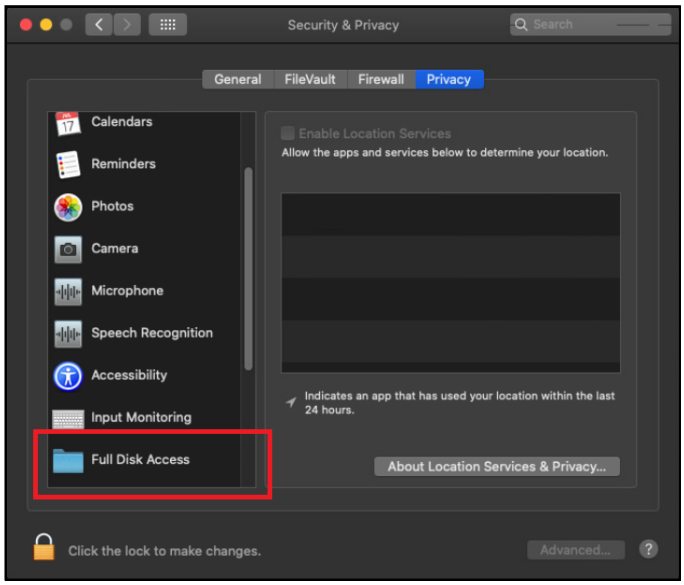


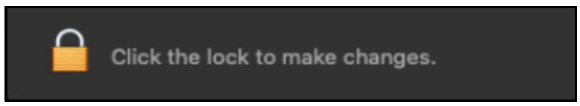


2. Select the **Privacy** tab.

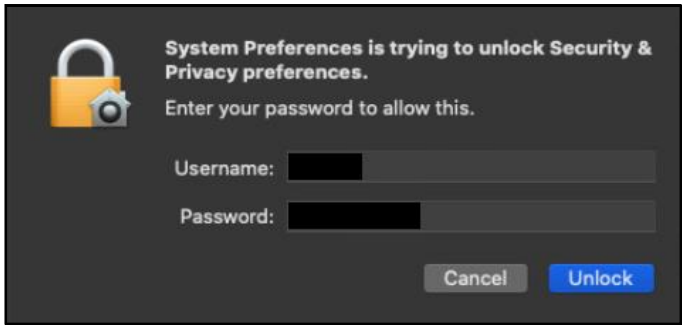


3. Select **Full Disk Access**, then click the lock icon.

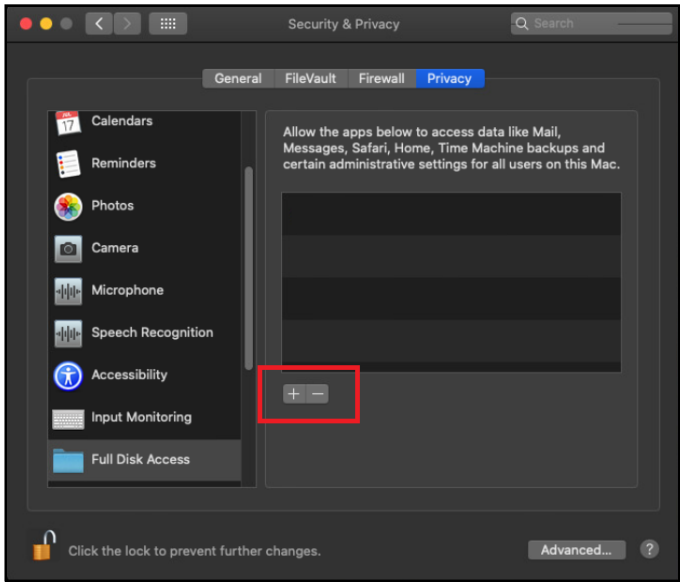




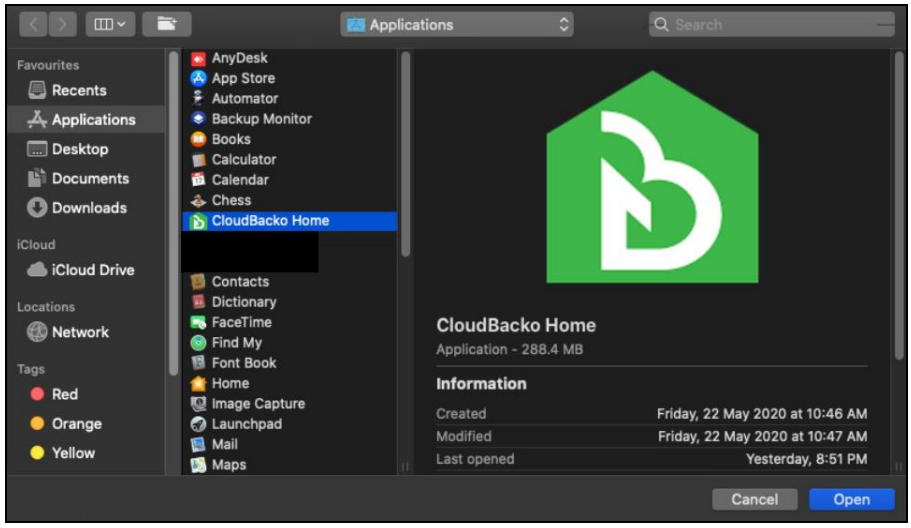
4. Enter the System Administrator credentials and click the **Unlock**.



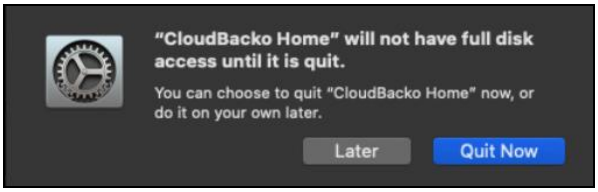
5. Click the plus icon.



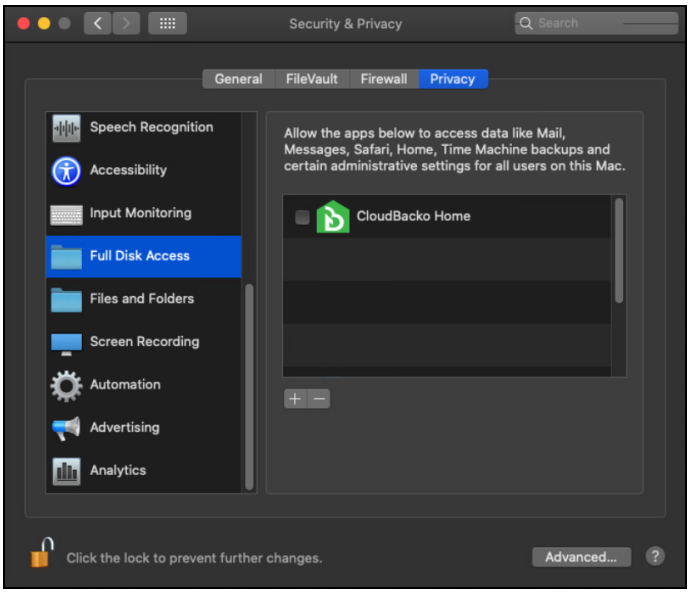
6. Click the **Applications**, then select **CloudBacko Home**, and click **Open**.



This message will appear if you have the CloudBacko Home open. Click **Quit Now** to proceed.



7. CloudBacko Home has now Full Disk Access.



Appendix D: Exclude Filter System Files

If home for admin is selected, all files and/or folders located in **/Users/admin/** is recommended to include these folders to exclude from the backup source using the Exclude Filter.

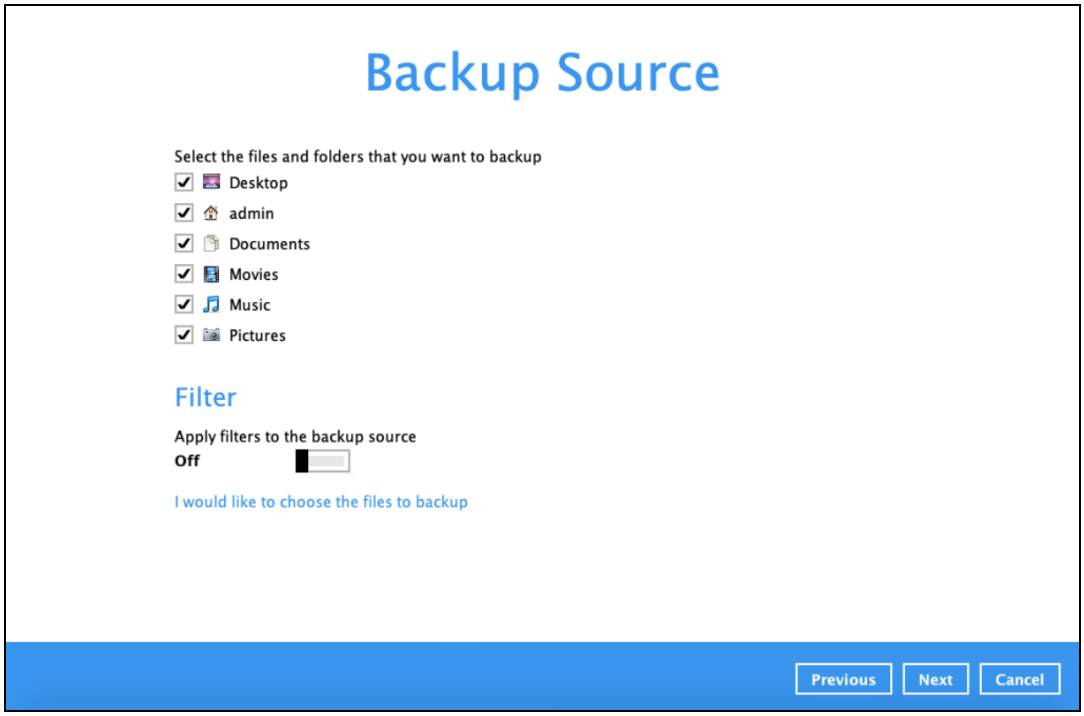
/Users/admin/Library

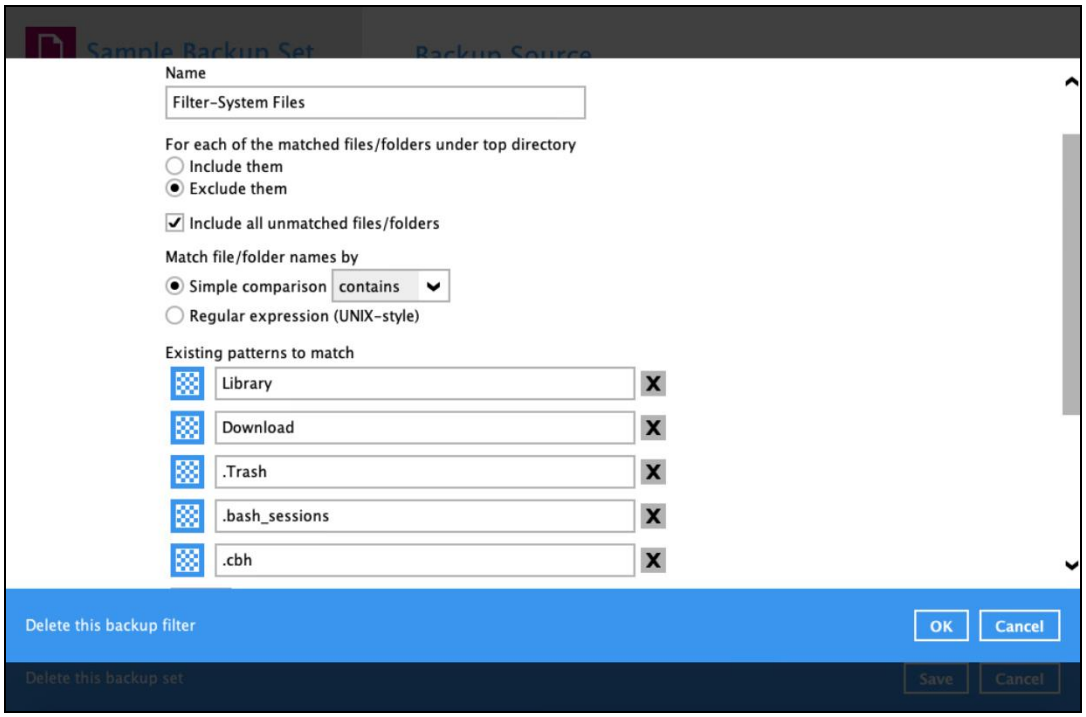
/Users/admin/Download

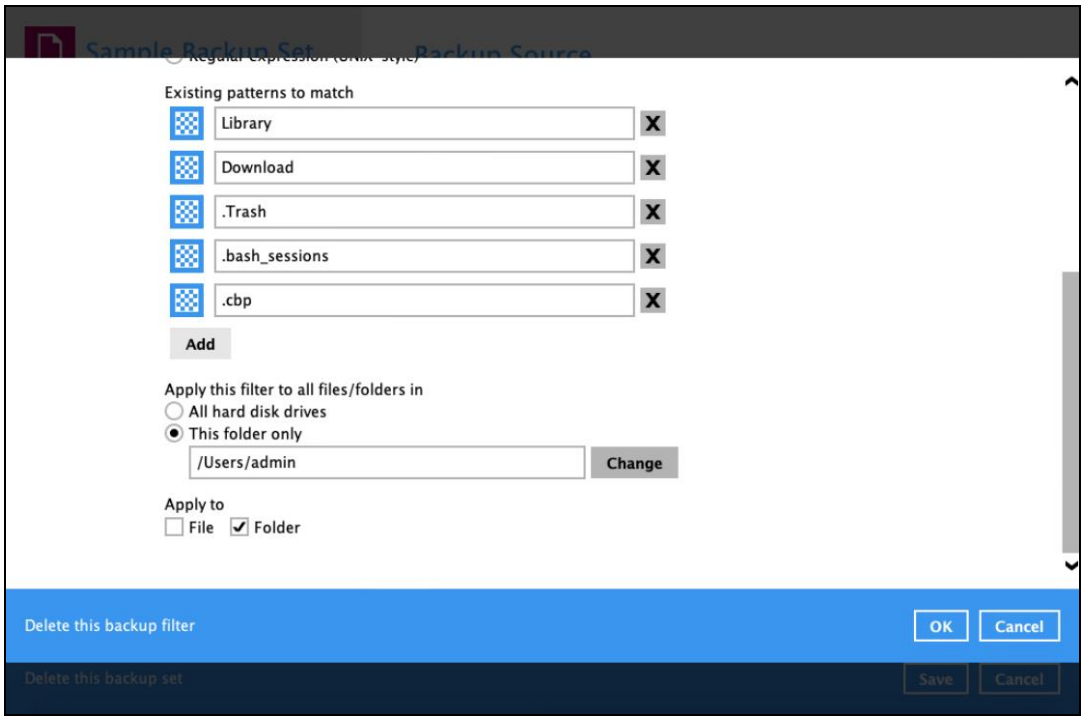
/Users/admin/.Trash

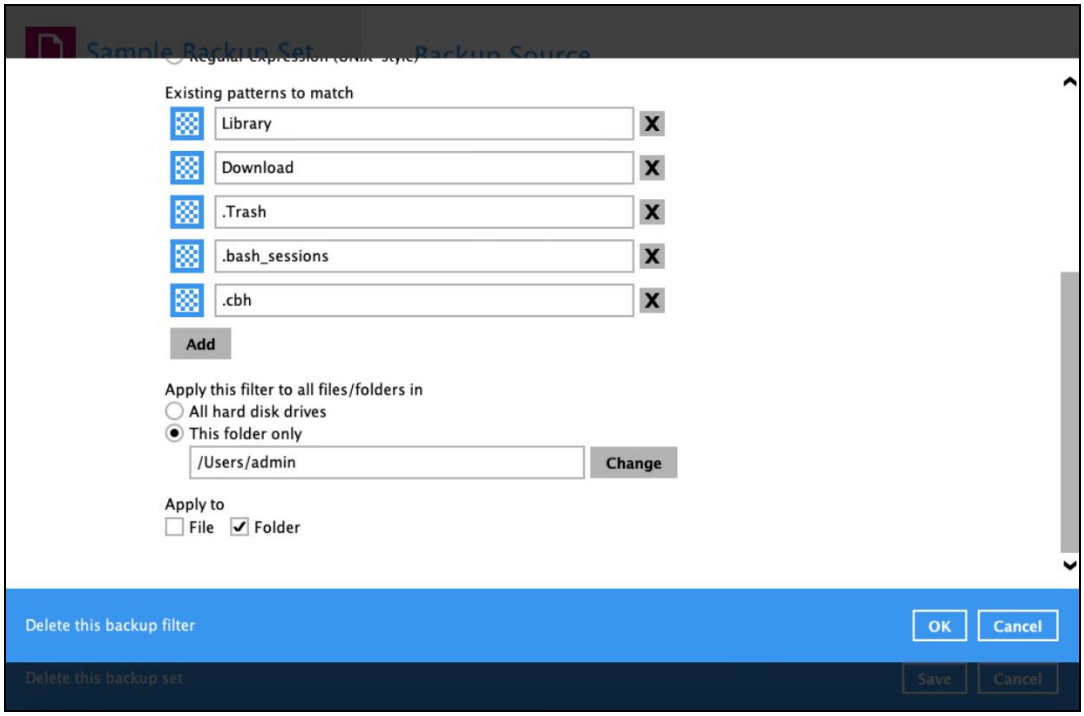
/Users/admin/.bash_sessions

/Users/admin/.cbh






Existing patterns to match
Library
Download
.Trash
.bash_sessions
.cbp
Add
Apply this filter to all files/folders in
All hard disk drives
This folder only
/Users/admin
Change
Apply to
File
Folder
Delete this backup filter
OK
Cancel
Delete this backup set
Save
Cancel


Existing patterns to match
Library
Download
.Trash
.bash_sessions
.cbh
Add
Apply this filter to all files/folders in
All hard disk drives
This folder only
/Users/admin
Change
Apply to
File
Folder
Delete this backup filter
OK
Cancel
Delete this backup set
Save
Cancel