CloudBacko Pro

Quick Start Guide for Linux

CloudBacko Corporation

6 January 2025

Copyright Notice

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	▪ Added Tibero Trademark ▪ Ch. 1.1 – updated list of backup set types ▪ Ch. 7.4 – updated module list ▪ Ch. 7.8 – updated Data Integrity Check ▪ Ch. 10 – updated backup instructions ▪ Ch. 12.3 – updated restore instructions ▪ Updated images	5.9.14.0
2 September 2024	▪ Ch. 7.4.1.3 – updated screenshots ▪ Ch. 7.4.1.5 – updated screenshots ▪ Ch. 7.4.1.6 – updated screenshots and instructions ▪ Ch. 11.1 – updated scrrenshots	5.11
6 January 2025	▪ Ch. 7.4.1.9 – Removed OpenDirect, updated screenshots ▪ Ch. 7.7.4 – Added PostgreSQL and Linux Bare Metal Modules ▪ Ch. 8 – Removed OpenDirect ▪ Ch. 11 – Updated Restore steps ▪ Ch. 11.2 – Updated Restore Filter instructions	5.13

Contents

1 Overview

1.1 What is this software?

CloudBacko brings you specialized client backup software, namely CloudBacko Pro, to provide a comprehensive backup solution for protecting the following applications and databases:

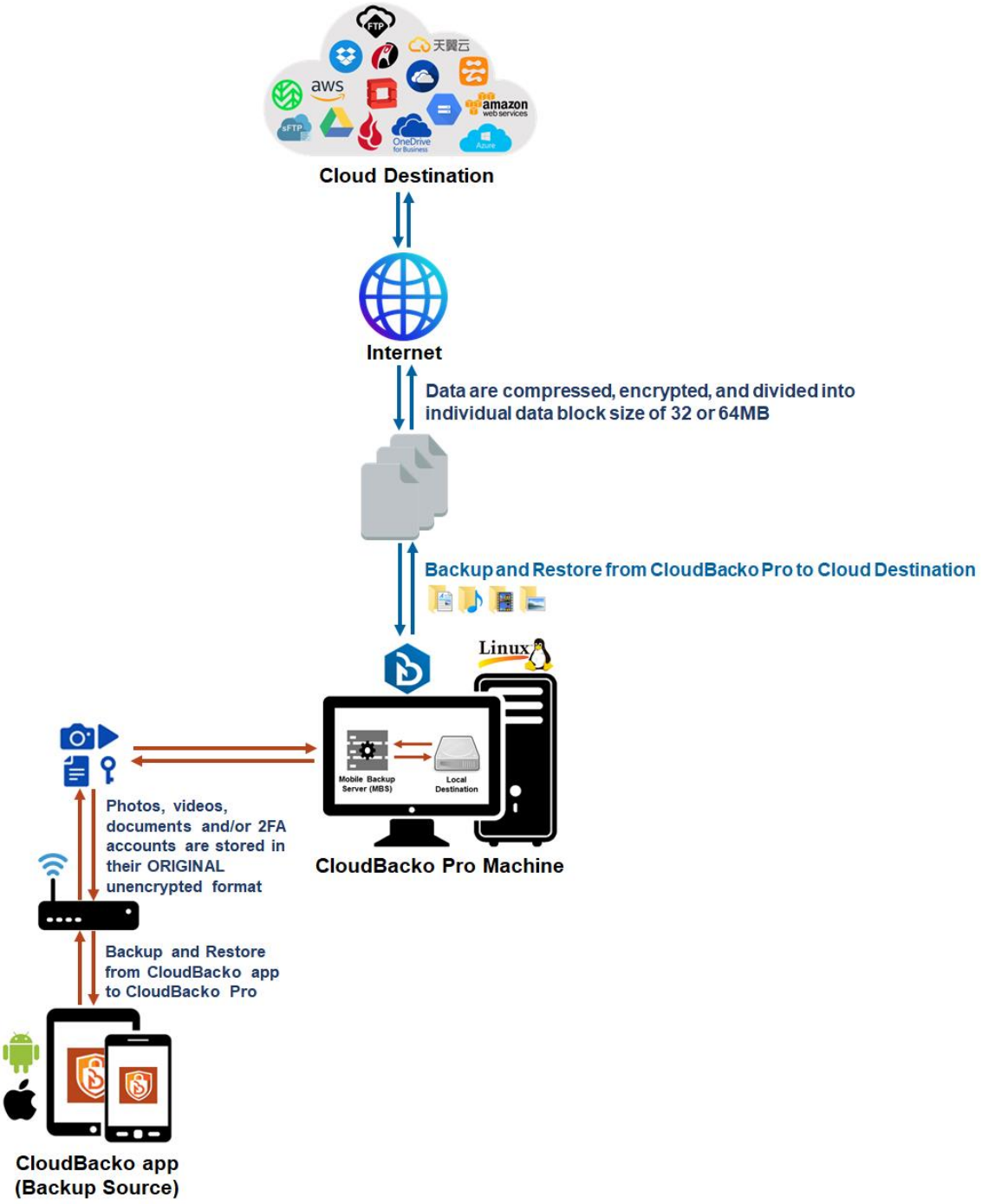
- File
- Cloud File
- Microsoft 365
- MariaDB
- MySQL
- Oracle Database
- VMware
- Tibero Database Server

It also supports a wide variety of backup destinations, which are the following:

- Local hard drive / USB drive / Network share
- 1&1 IONOS
- Alibaba Cloud (Aliyun)
- Amazon S3
- S3-Compatible Cloud Storage
- BackBlaze B2
- CenturyLink
- CTYun
- DreamHost's DreamObjects
- Dropbox
- IBM Cloud Object Storage
- Google Cloud Storage
- Google Drive
- Microsoft Azure
- Microsoft OneDrive
- Microsoft OneDrive for Business
- OpenStack
- Rackspace Cloud File
- S3ForMe
- Scality
- Wasabi
- Zadara
- FTP
- SFTP

1.2 System Architecture

Below is the system architecture diagram illustrating the major elements involved in the backup process among the backup machine CloudBacko Pro and CloudBacko app (mobile client).



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 Pro, which is located in the “mbs” folder inside the CloudBacko Pro folder.

System Diagram

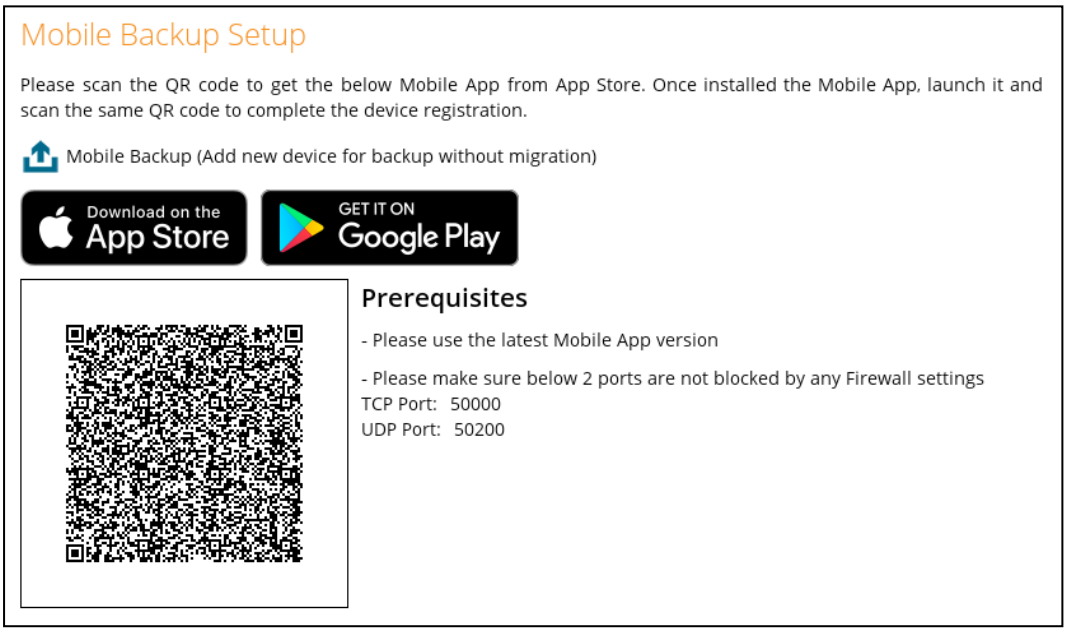
The Mobile Backup Server (MBS) will be activated automatically when a mobile device installed with the CloudBacko app is successfully registered for mobile backup with CloudBacko Pro. Afterwards, it will be automatically restarted whenever the CloudBacko pro services is restarted or when the CloudBacko Pro 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 Pro services is restarted.

The MBS will use the following port ranges for the request of CloudBacko app:

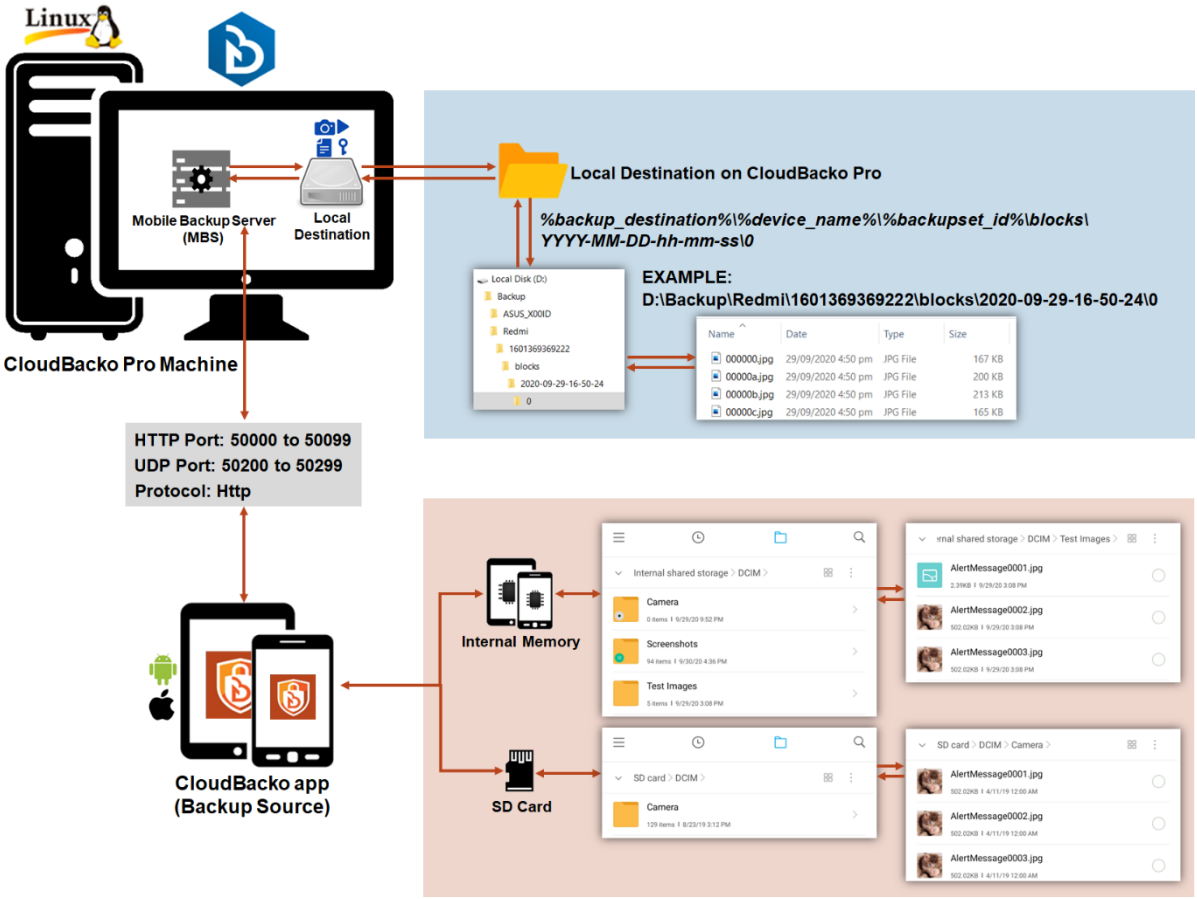
- **TCP Port:** 50000 to 50099
- **UDP Port:** 50200 to 50299
- Protocol: Http

The default TCP and UDP ports are 50000 and 50200, 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 Pro when pairing a mobile device for mobile backup.



Photos, videos, documents and 2FA accounts are stored either in the 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 a CloudBacko machine, that can be a Hard Drive, Flash Drive, and/or Network Drive in their ORIGINAL format unencrypted. For Android, photos and videos will retain all EXIF. While for iOS, photos and videos will retain most of the EXIF including capture date, location, and lens.

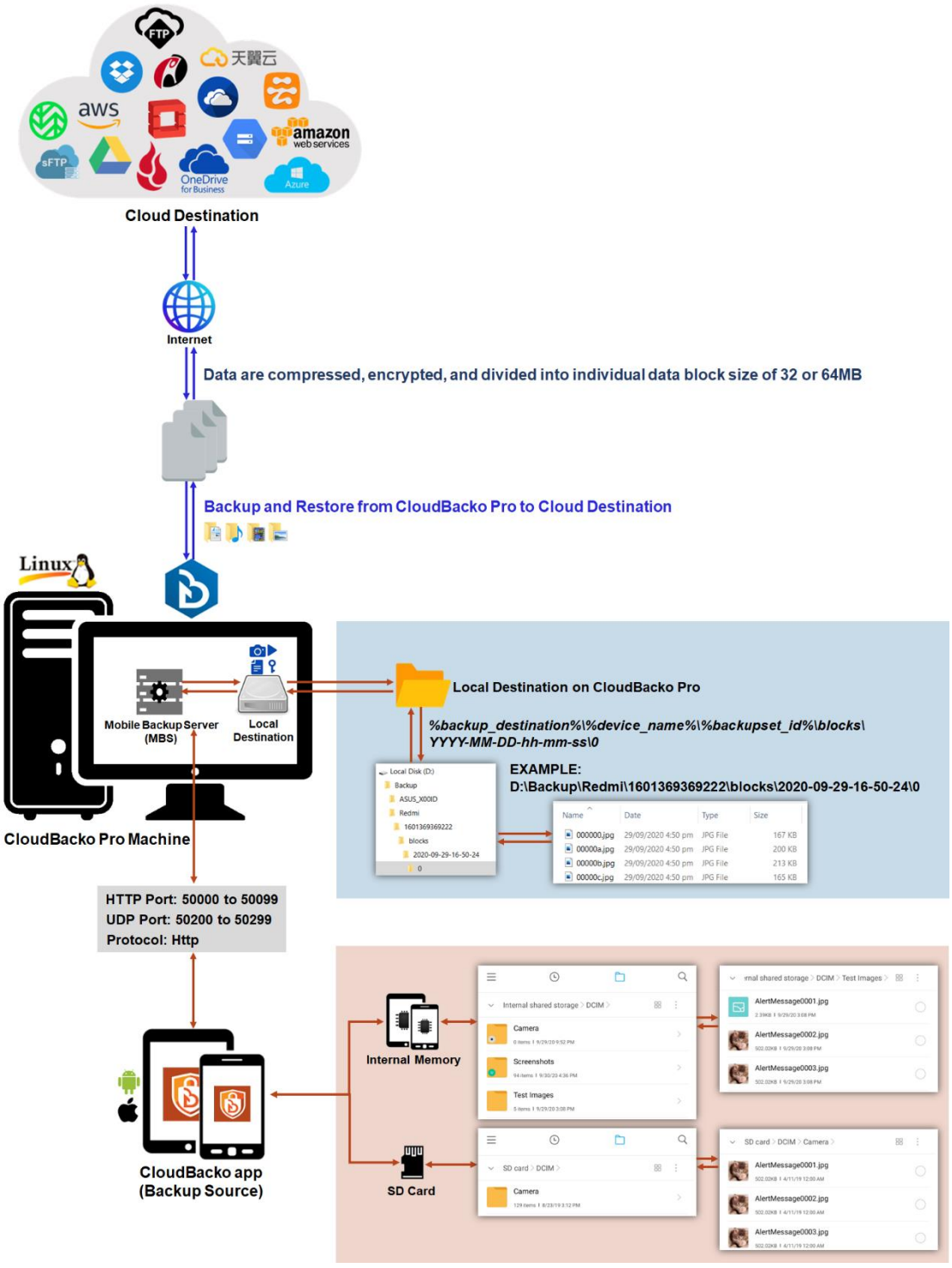


If storage of photos, videos, documents and 2FA accounts to a cloud destination is required, then this can be done using CloudBacko Pro to perform a secondary backup and restore of the photos, videos, documents and 2FA accounts on the local drive to the cloud.

To backup and restore photos, videos, documents and 2FA accounts from CloudBacko app to CloudBacko Pro and cloud, is a two-step process.

1st: Backup of photos, videos, documents and/or 2FA accounts from CloudBacko app to CloudBacko Pro local destination.

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

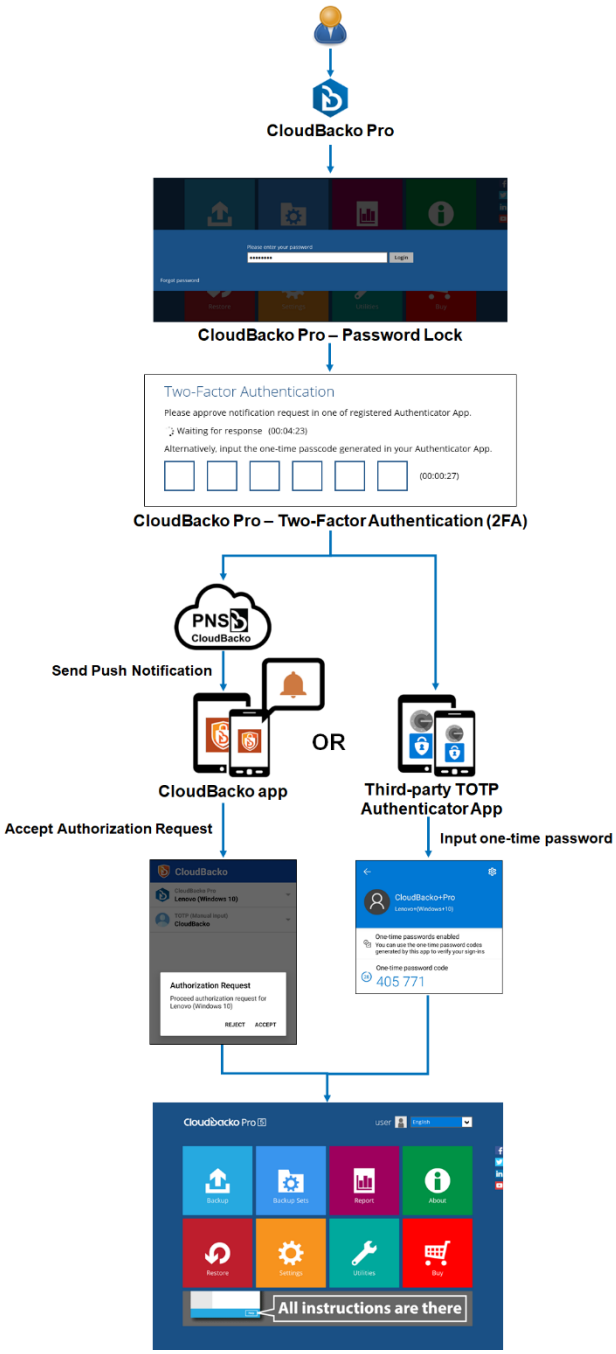


1.4 Two-Factor Authentication

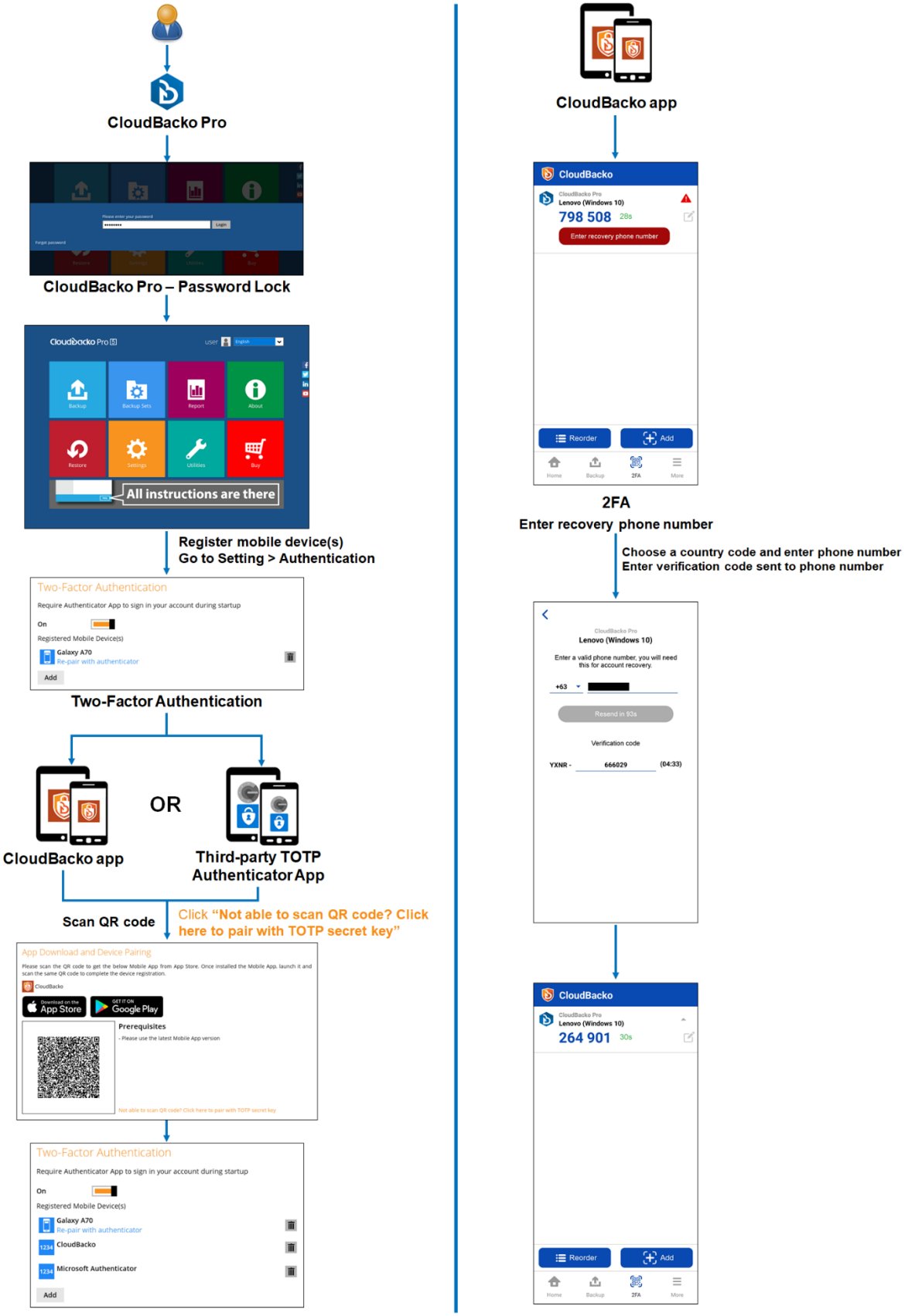
The two-factor authentication implemented on CloudBacko Pro include support for TOTP (Time-based One-time Password) and Push notification authentication using the CloudBacko app to provide additional security for the user login process.

Upon initial login, you will have an option to setup your two-factor authentication feature. You may skip the setup and do it later. If you continue the setup of two-factor authentication, it will be automatically enabled for future CloudBacko sign in process. If you like, you may register your CloudBacko Pro with multiple mobile devices for two-factor authentication.

For log ins with two-factor authentication enabled CloudBacko Pro, the 2FA method will depend on the authenticator app registered. You will either accept the login request via push notification in the CloudBacko app or enter a one-time password generated in the third-party authenticator app such as Authy, Duo, Google Authenticator, Microsoft Authenticator, LastPass etc.



This illustrates the registration of mobile devices for Two-Factor Authentication.



2 Requirements for CloudBacko app

2.1 Backup Software Version Requirement

- Download and install the latest version of CloudBacko Pro.
- 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 Pro. 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 System Requirements

3.1 Hardware Requirements

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

CloudBacko Pro: Hardware Requirement

3.2 Supported Platforms

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

CloudBacko Pro: Supported Operating Systems

3.3 Internet Connection

CloudBacko machine must have a fixed internet connection

3.4 SMTP Server

- CloudBacko Pro supports SMTP server using TLS v1.0, v1.1 or v1.2.
- CloudBacko Pro supports SMTP server with or without authentication.

3.5 Supported Applications

Refer to the link below for the details of the applications supported by CloudBacko Pro.

CloudBacko Pro: Supported Applications

3.6 Supported Microsoft 365 Services and Items

Refer to the link below for the details of the supported Microsoft 365 Services and Items for CloudBacko Pro.

CloudBacko Pro: Supported Microsoft 365 Services and Items Microsoft 365 Backup

3.7 Java Heap Size

The default maximum Java heap size setting is 2048M. This value is usually sufficient for most types backups, however for backup sets with large number of files and or very large files the value may need to be increased.

Refer to the link below for the details on how to increase Java Heap Size for CloudBacko Pro.

CloudBacko Pro: How to increase Java Heap Size

3.8 Two-Factor Authentication Requirements

Please refer to the CloudBacko App v1 User Guide for Android and iOS – Chapter 2.4 for details of the minimum and recommended requirements for using Two-Factor Authentication on CloudBacko app.

3.9 Mobile Device Requirements

Refer to the CloudBacko App v1 User Guide for Android and iOS – Chapter 2.5 for details of the minimum and recommended requirements for installing the CloudBacko app.

3.10 GUI Desktop Environment

The Linux machine must be installed with a GUI desktop environment, i.e. GNOME, KDE, Cinnamon etc.

3.11 Date, Time, and Timezone for 2FA (TOTP only)

Make sure to check the date, time, and time zone are synced between the CloudBacko Pro machine and mobile device installed with CloudBacko app before pairing the device for 2FA

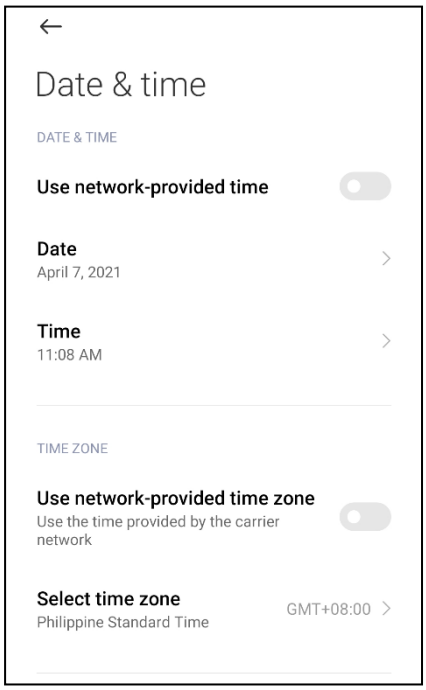
(TOTP only) to avoid unsuccessful pairing of devices and/or TOTP authentication failures. This also applies to third-party TOTP Authenticators.

To check the date, time, and time zone, follow the instructions below. For a different date, time, and time zone and how to change it, refer to Appendix K: Different Date, Time, and Time zone with CloudBacko Pro machine and mobile device

Same Date, Time, and Time zone with CloudBacko Pro machine and mobile device

1. Check the date, time and timezone in CloudBacko app.

   Example: Time zone settings of a mobile device used in the Philippines (time zone GMT+08:00).



2. Check the date, time, and timezone in CloudBacko Pro machine.

   Example: Time zone setting of a Linux machine used in the Philippines (time zone GMT+08:00).

```
[root@centos73 ~]# timedatectl
      Local time: Wed 2021-04-07 11:10:15 +08
  Universal time: Wed 2021-04-07 03:10:15 UTC
        RTC time: Wed 2021-04-07 03:10:28
       Time zone: Asia/Manila (+08, +0800)
     NTP enabled: no
NTP synchronized: no RTC in local TZ: no
      DST active: n/a
```

3.12 Limitations

3.12.1 OpenDirect

OpenDirect is only supported on Windows platform.

3.12.2 Continuous Backup

Continuous Backup is only supported on Windows platform.

3.12.3 File Permissions

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

3.12.4 Follow Link

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

3.13 Best Practices and Recommendations

Periodic Backup Schedule

The periodic backup schedule should be reviewed regularly to ensure the interval is sufficient to handle the data volume on the machine. Over the time, data usage pattern may change on a production server, i.e. the number of new files created, the number of files which are updated/delete, new users may be added etc.

When using periodic backup schedules with small backup intervals such as backup every 1 minute, 2 minutes, 3 minutes etc. although the increased backup frequently does ensure that changes to files are captured regularly which allows greater flexibility in recovery to a point in time.

Consider the following key points to efficiently handle backup sets with periodic backup schedule.

- **Hardware** – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine's appropriate hardware specifications to accommodate frequency of backups,
    - so that the data is always backed up within the periodic backup interval
    - so that the backup frequency does not affect the performance of the production server
- **Network** – make sure to have enough network bandwidth to accommodate the volume of data within the backup interval.
- **Storage** – ensure you have enough storage quota allocated based on the amount of new data and changed data you will backup.
- **Retention Policy** – also make sure to take into account the retention policy settings and retention area storage management which can grow because of the changes in the backup data for each backup job.

3.14 Linux Packages

The following packages have to be present on the Linux machine in order for CloudBacko Pro be installed.

- tar https://www.gnu.org/software/tar

  The ‘tar’ command is used by both the CloudBacko Pro sh script, gz, and rpm installer to un-compress and extract installation files or components downloaded onto the Linux machine.

- rpm http://rpm.org

  The ‘rpm’ package must be installed to use the CloudBacko Pro rpm installation method.

- dpkg https://packages.ubuntu.com/bionic/dpkg-dev

  The ‘dpkg’ package must be installed to use the CloudBacko Pro deb installation method on supported Ubuntu Linux platforms.

- psmisc http://psmisc.sourceforge.net/

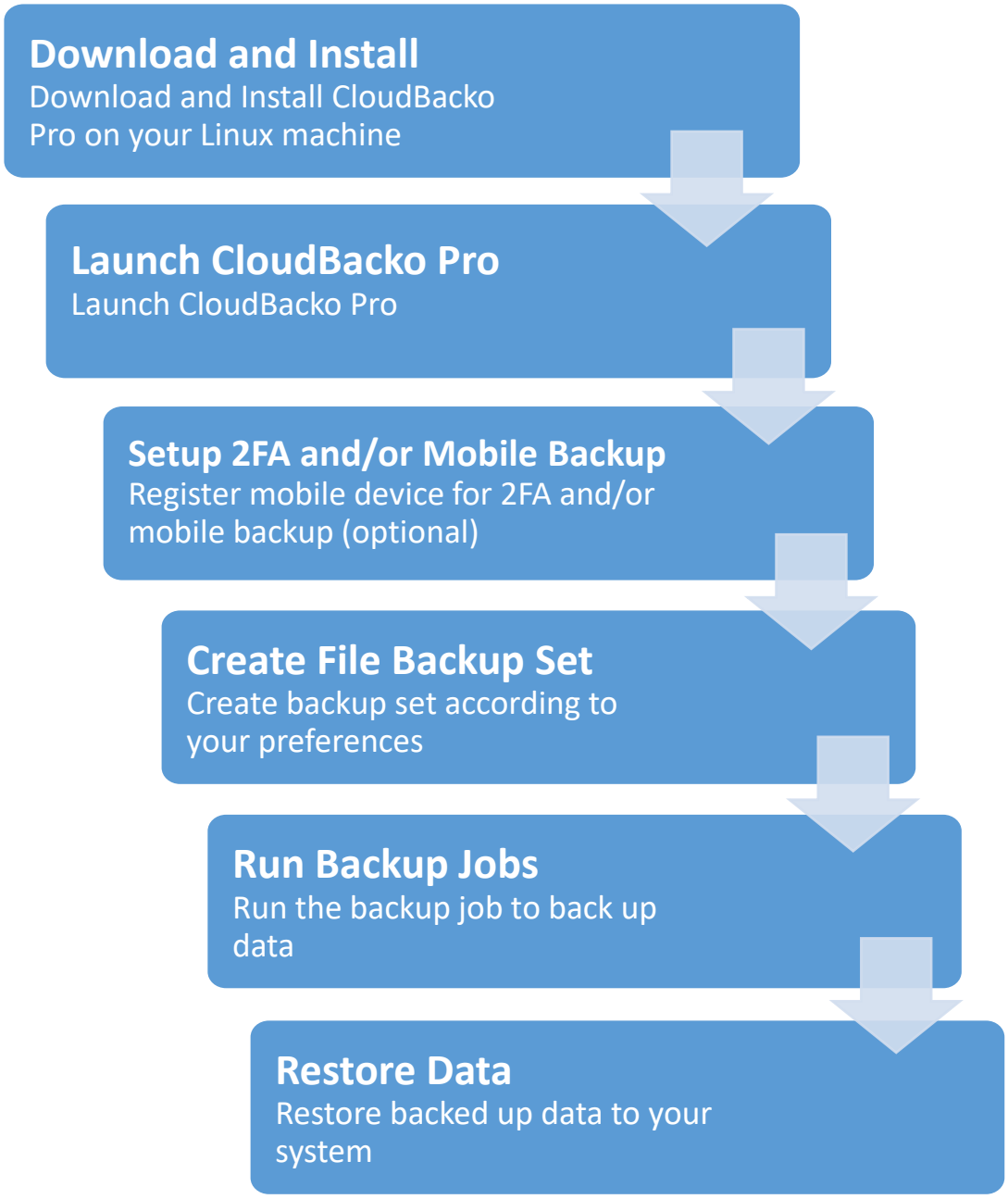
  The ‘psmisc’ package which contains the ‘fuser’ components must be installed for CloudBacko Pro on Linux, for the software update to work properly.

- GNU LIBC 2.14 https://www.gnu.org/software/libc/

  GNU LIBC version must at least be 2.14 to support OpenJDK 8 which is used by CloudBacko Pro.

4 Getting Started

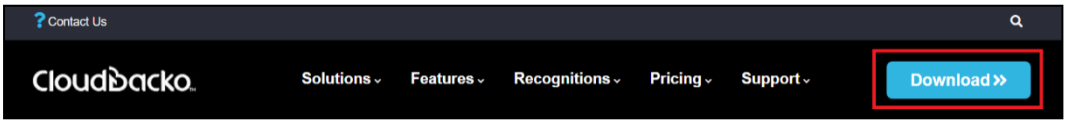
This quick start guide will walk you through the following six (6) major parts to get you started with using CloudBacko Pro.



5 Download and Install CloudBacko Pro

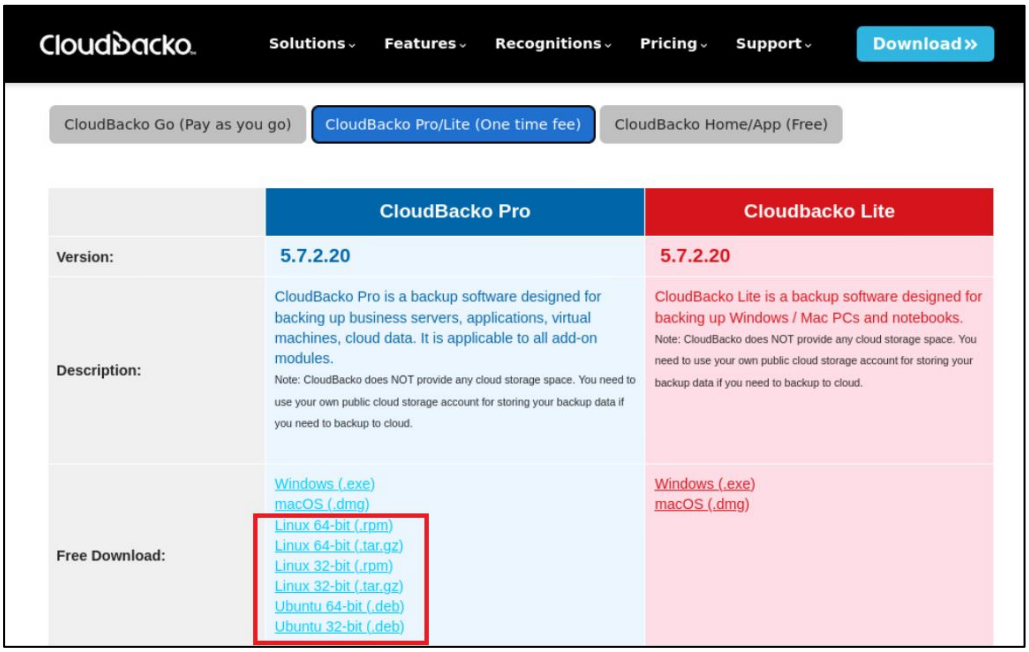
5.1 Download CloudBacko Pro

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 Pro/Lite (One time fee).** You can choose the CloudBacko Pro installer by operating system and click the corresponding link to start downloading.



5.2 Install CloudBacko Pro

CloudBacko Pro on Linux GUI supports three (3) types of installation methods:

- Red Hat Package Manager (rpm)
- Linux Script (sh)
- Debian Software Package (deb)

5.2.1 Red Hat Package Manager (rpm)

1. Login as root on the Linux machine using the GUI.

2. Download the CloudBacko Pro

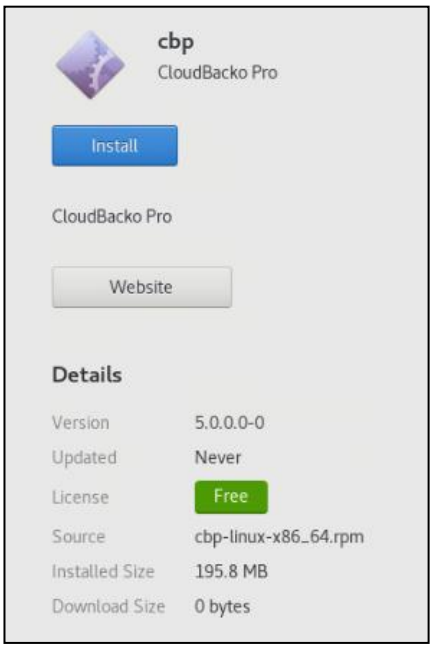
   For instructions please refer to Chapter 5.1 Download CloudBacko Pro.

   There are two (2) types of rpm installer, Linux 32-Bit(.rpm) and Linux 64-Bit(.rpm). Choose the appropriate installer for your machine.

3. Double-click the installation package you have downloaded.

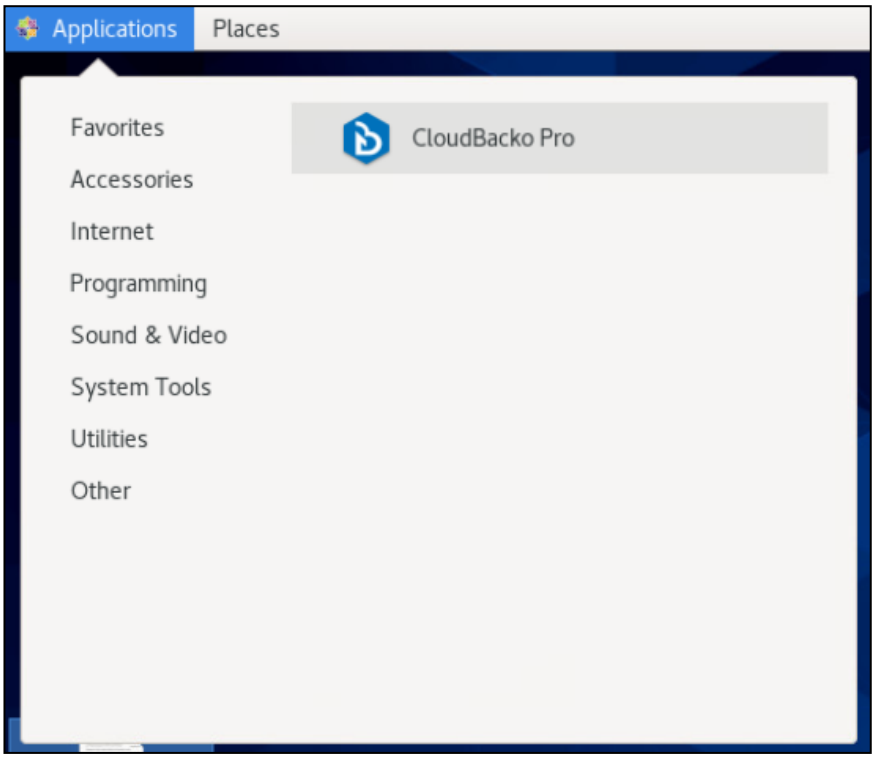
4. When the notification message **"Application Installer"** appears, click the **Software** tab to proceed.

5. Click **Install** to start the installation.



6. Upon successful installation, the **CloudBacko Pro** icon will be added to the desktop as a shortcut.

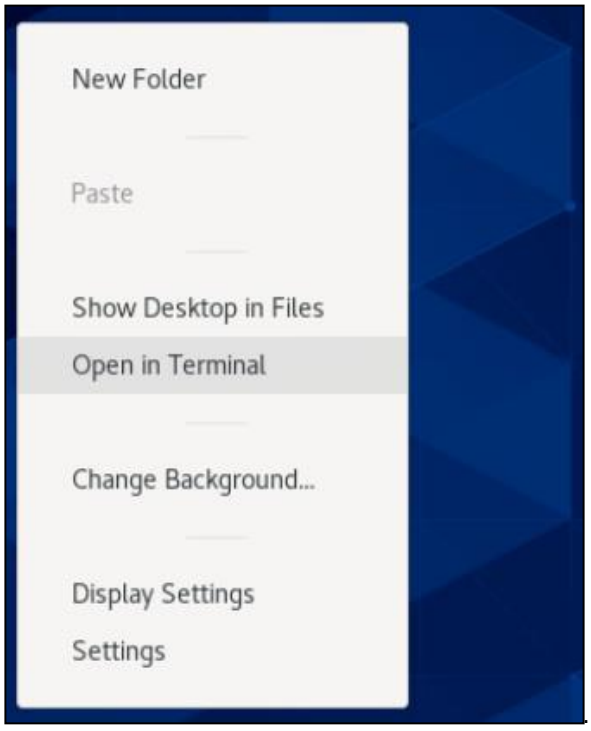
Alternatively, you can also click the **Applications** menu bar and then select **Other** to see the **CloudBacko Pro**.



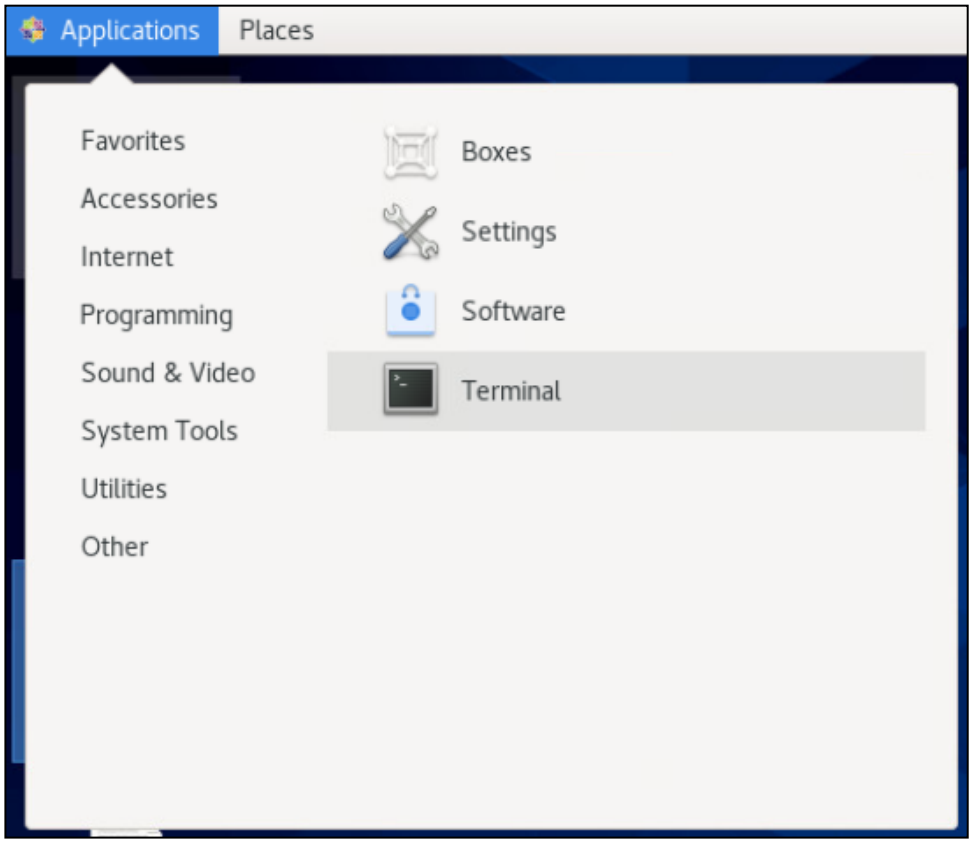
5.2.2 Linux script (sh)

1. Login as root on the Linux machine using the GUI.

2. Right-click on the desktop and select **Open in Terminal**.



Alternatively go **to Application**s > **System Tools** > **Terminal** to launch the application.



3. Create a new directory `# mkdir -p /usr/local/cbp` for the installation of CloudBacko Pro. Then, go to the new directory `# cd /usr/local/cbp`.

```
# mkdir -p /usr/local/cbp
# cd /usr/local/cbp
```

4. Download the CloudBacko Pro.

   For instructions, please refer to Chapter 5.1 Download CloudBacko Pro.

   There are two (2) types of tar installer packages, Linux 32-Bit(.tar.gz) and Linux 64-Bit(.tar.gz). Choose the appropriate installer for your machine and save it in the new directory you just created.

5. Untar the gz file `# tar xvfz cbp-linux-x86_64.tar.gz`.

NOTE

The following example is for CloudBacko Pro installation on 64-bit Linux machine.

```
# tar xvfz cbp-linux-x86_64.tar.gz

app.pkg/jre-std-linux-amd64.tar.gz
app.pkg/util-nix-cbp.tar.gz
app.pkg/app-common.tar.gz
app.pkg/app-inst-nix-cbp.tar.gz
app.pkg/util-common.tar.gz
app.pkg/aua-inst-nix-cbp.tar.gz
app.pkg/app-nix-cbp.tar.gz
app.pkg/aua-nix-cbp.tar.gz
app.pkg/properties-common.tar.gz
installer.sh
app.pkg/app-native-nix-x64.tar.gz
app.pkg/aua-common.tar.gz
```

```
app.pkg/aua-native-nix-x64.tar.gz
```

6. Execute the CloudBacko Pro install script `# sh installer.sh`.

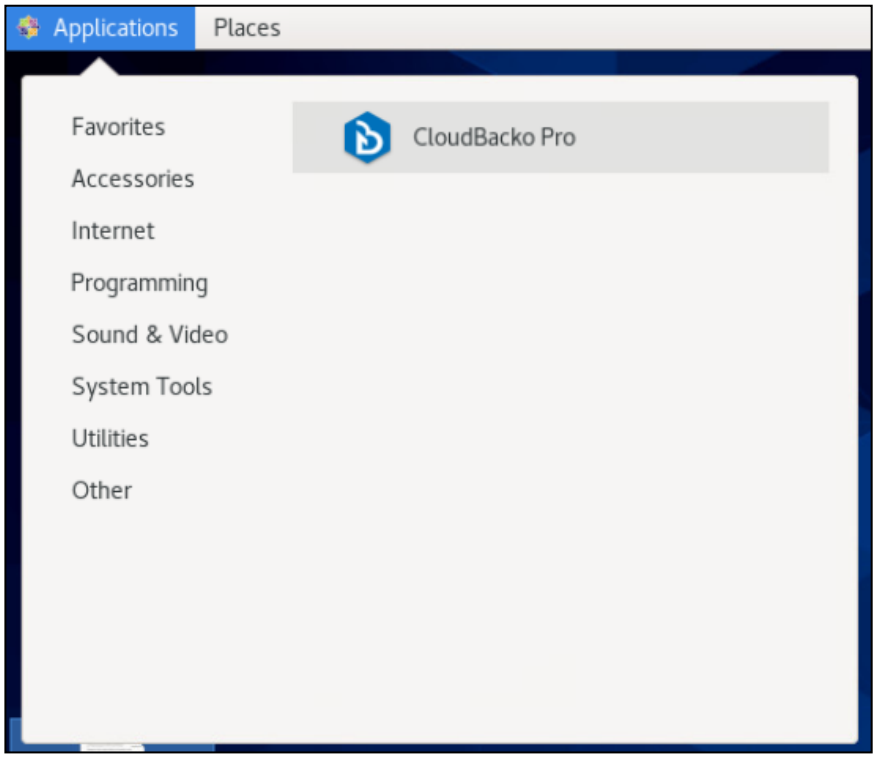
```
# sh installer.sh
```

7. The installation is completed when **Done** shows at the end of the script.

```
# sh installer.sh

Log Time: Thu Dec 9 10:06:20 HKT 2021
Untar jre-std-linux-amd64.tar.gz to
/tmp/_cbp.200518115551/jvm
Untar app-common.tar.gz to /tmp/_cbp.200518115551
Untar app-native-nix-x64.tar.gz to /tmp/_cbp.200518115551
Untar app-nix-cbp.tar.gz to /tmp/_cbp.200518115551
Untar aua-common.tar.gz to /tmp/_cbp.200518115551
Untar aua-native-nix-x64.tar.gz to /tmp/_cbp.200518115551
Untar aua-nix-cbp.tar.gz to /tmp/_cbp.200518115551
Untar util-common.tar.gz to /tmp/_cbp.200518115551
Untar util-nix-cbp.tar.gz to /tmp/_cbp.200518115551
Untar properties-common.tar.gz to /tmp/_cbp.200518115551
Untar app-inst-nix-cbp.tar.gz to /tmp/_cbp.200518115551
Untar aua-inst-nix-cbp.tar.gz to /tmp/_cbp.200518115551
  No old application found, begin fresh install
Install Application Path: /usr/local/cbp
Done
```

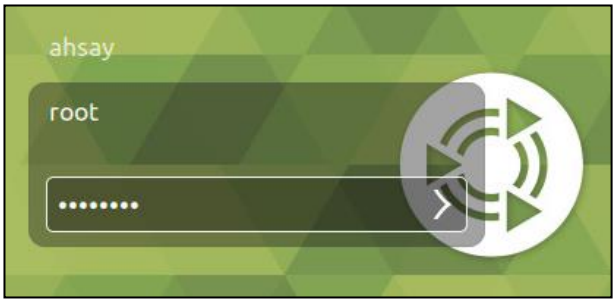
8. Upon successful installation, the CloudBacko Pro icon will be added in the desktop.

Alternatively, it can also be accessed from **Applications** > **Other**.



5.2.3 Debian Software Package (deb)

1. Login as root to the Ubuntu Linux machine using the GUI.



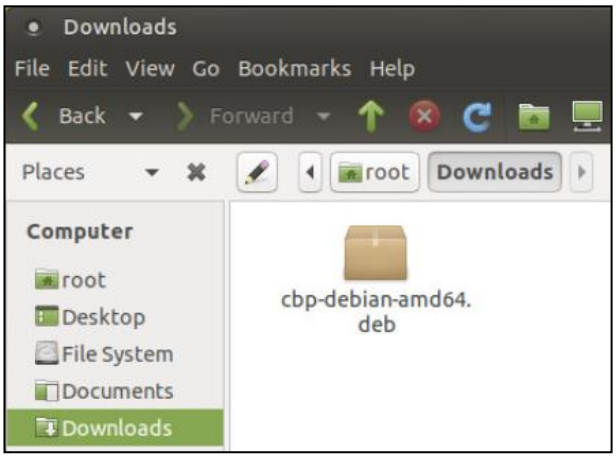
2. Download the CloudBacko Pro.

   For instructions please refer to Chapter 5.1 Download CloudBacko Pro.

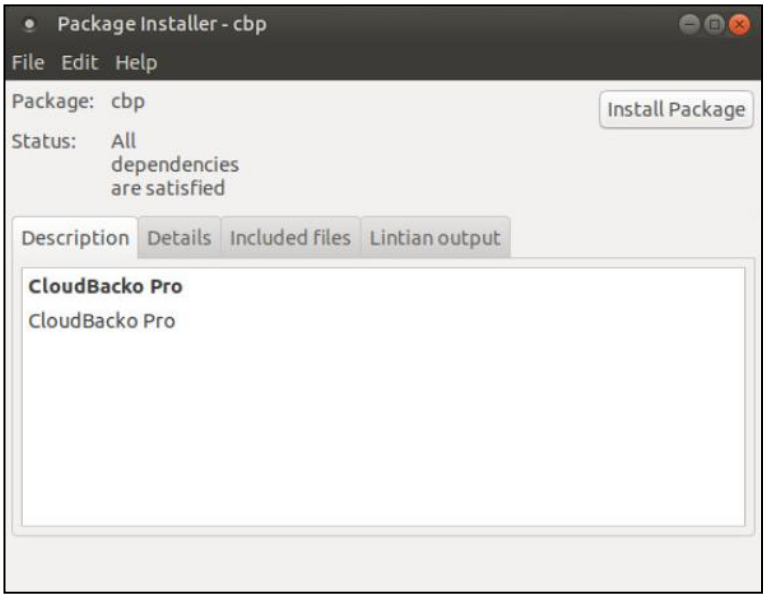
   There are two (2) types of deb installer packages, Ubuntu 32-Bit(.deb) and Ubuntu 64-Bit(.deb). Choose the appropriate installer for your machine.

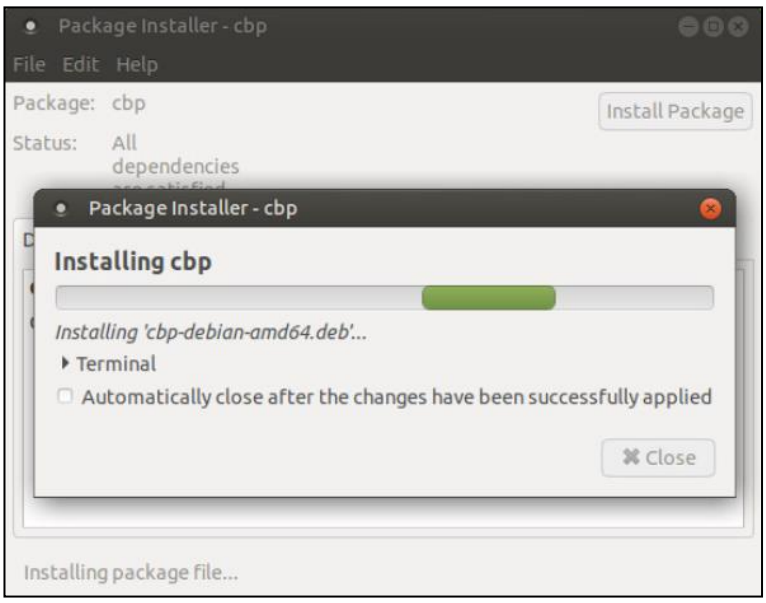
3. Go to **Downloads** folder and double click on the file you just downloaded.

   Option: If there are problem with the installation, it is advisable to do the Pre-installation Check to verify there is a pre-existing version of CloudBacko Pro or if a previous version was not cleanly uninstalled.

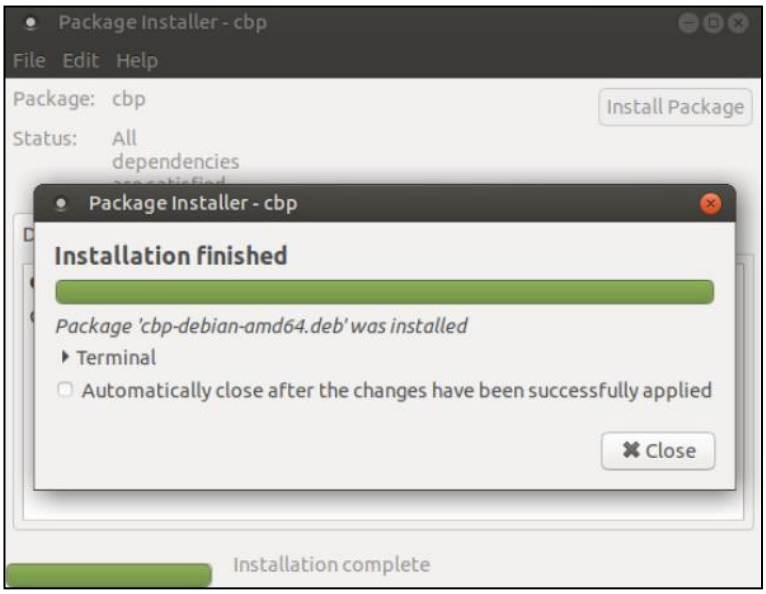


4. Click **Install Package** to start the installation.





5. After installation is done **Installation finished** message will be shown.



6. Upon successful installation, CloudBacko Pro will be added to the menu under **Other**.

6 Start CloudBacko Pro

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

- Launch CloudBacko Pro without 2FA
- Launch CloudBacko Pro with 2FA

6.1 Launch CloudBacko Pro without 2FA

To launch to CloudBacko Pro without two-factor authentication follow the steps below:

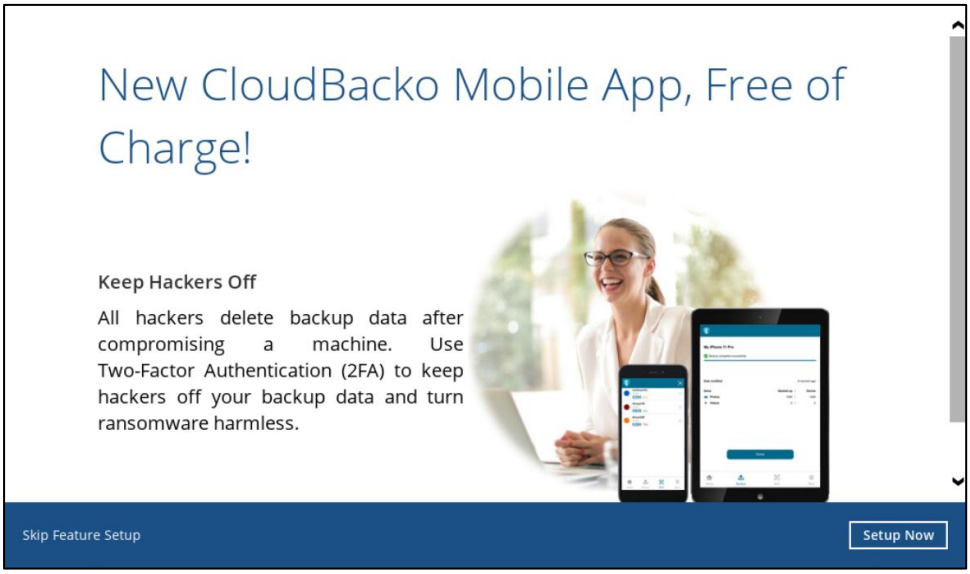
- Initial launch skipping two-factor authentication and mobile backup features setup
- Subsequent logins without 2FA but with password lock
- Subsequent login without 2FA and password lock

6.1.1 Initial launch skipping two-factor authentication and mobile backup features setup

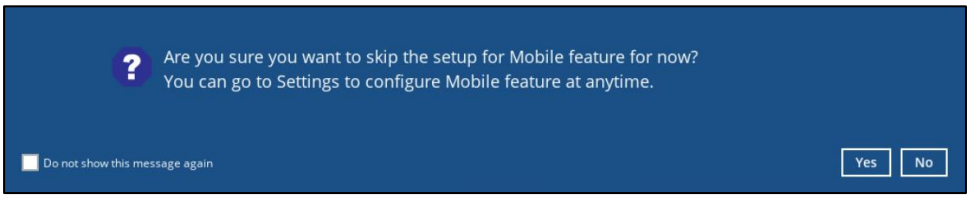
When launching the CloudBacko Pro for the first time and skipping the two-factor authentication and mobile backup features setup, please follow the steps below:

1. A shortcut icon of CloudBacko Pro will be available on your desktop after installation. Double-click the icon to launch the application.

2. The following screen will be displayed. Click **Skip Feature Setup**.



3. Click **Yes** in the pop-up message that will be displayed.



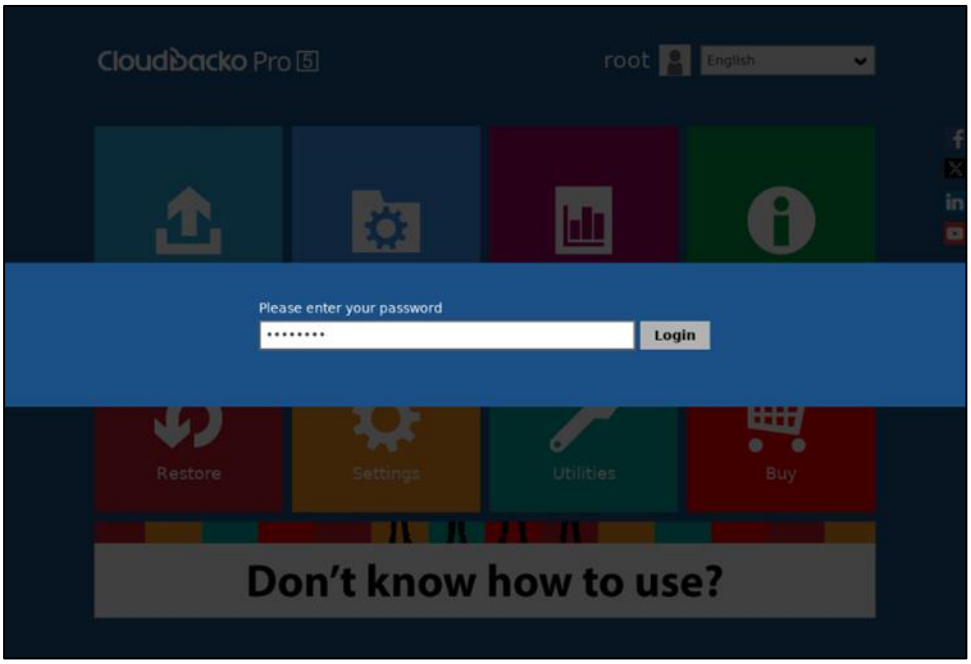
4. CloudBacko Pro main screen will appear.

6.1.2 Subsequent logins without 2FA but with password lock

For succeeding logins to CloudBacko Pro without two-factor authentication, please follow the steps below:

1. A shortcut icon of CloudBacko Pro will be available on your desktop after installation. Double click the icon to launch the application.

2. Enter password.



3. CloudBacko Pro main screen will appear.

6.1.3 Subsequent logins without 2FA and password lock

For succeeding logins to CloudBacko Pro without two-factor authentication and password lock, please follow the steps below:

1. A shortcut icon of CloudBacko Pro will be available on your desktop after installation. Double click the icon to launch the application.

2. CloudBacko Pro main screen will appear.

6.2 Launch CloudBacko Pro with 2FA using Android or iOS mobile device

There are two types of authenticator that can be used for 2FA:

- CloudBacko app Authenticator
  - Supports two types of authentication:
    - Push Notification
    - TOTP
  - Can be configured to support two 2FA modes:
    - Push Notification and TOTP (default mode) or,
    - TOTP only
- Third-party TOTP Authenticator

  (e.g. Authy, Duo, Google Authenticator)

To launch to CloudBacko Pro with two-factor authentication follow the steps below:

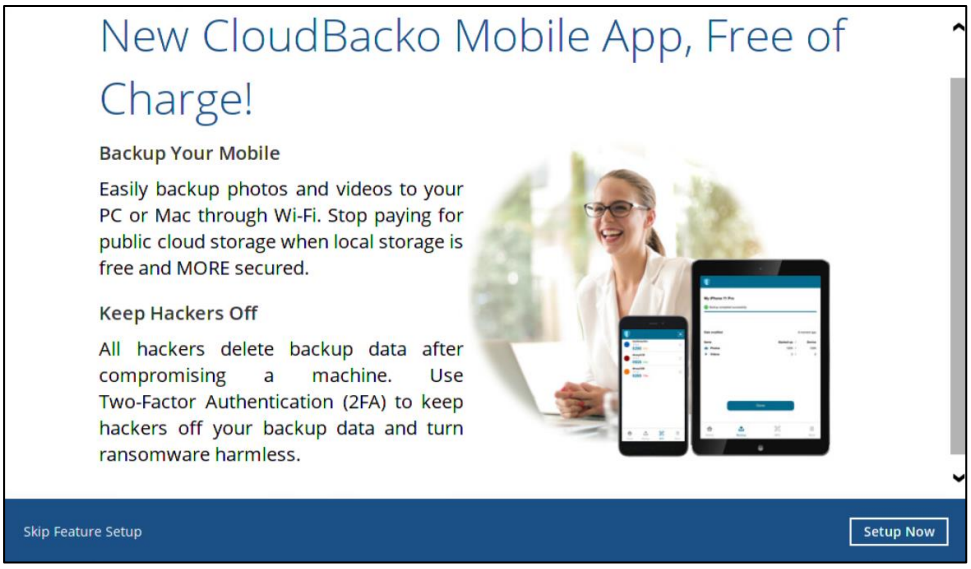
- Initial launch setting up two-factor authentication and mobile backup features
- Subsequent logins with 2FA
- Subsequent logins with 2FA and password lock

6.2.1 Initial launch setting up two-factor authentication and mobile backup features

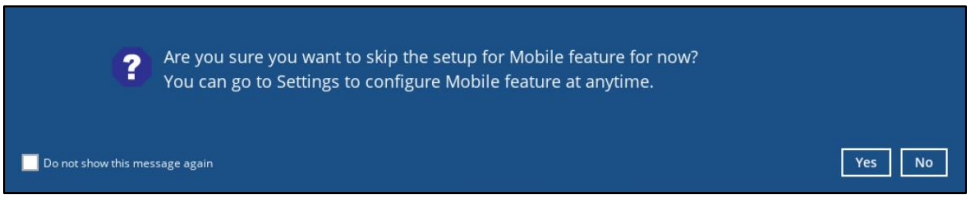
When launching the CloudBacko Pro for the first time and setting up the two-factor authentication feature, please follow the steps below:

1. A shortcut icon of CloudBacko Pro will be available on your desktop after installation. Double click the icon to launch the application.

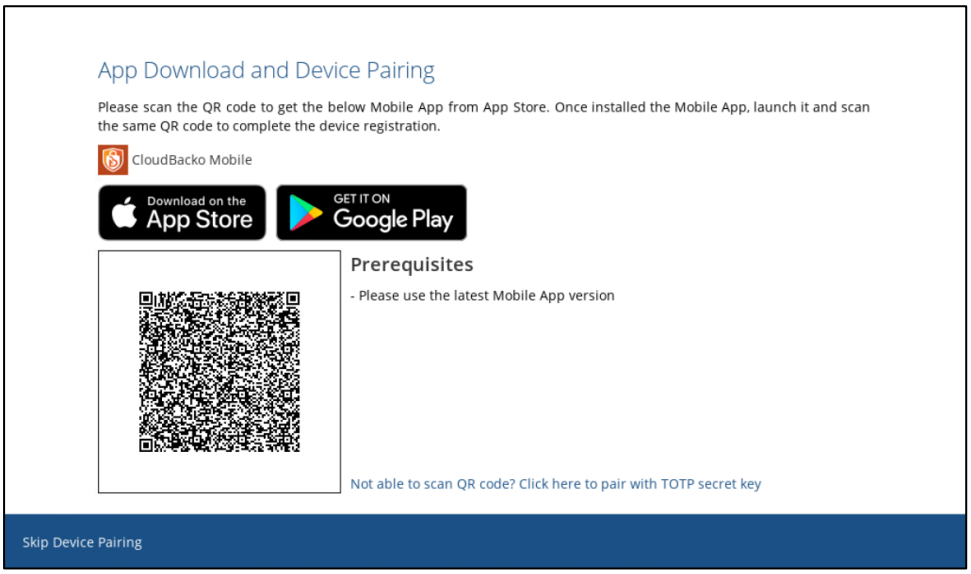
2. You will have the option to set up your mobile backup. Click **Setup Now**.



If you do not want to set up the mobile feature, click the **Skip Feature Setup** link. Click **Yes** in the pop-up message that will be displayed. Otherwise, click **No** to continue with the set-up of mobile feature.



3. Download the CloudBacko app from Google Play for an Android device and from App Store for an iOS device.

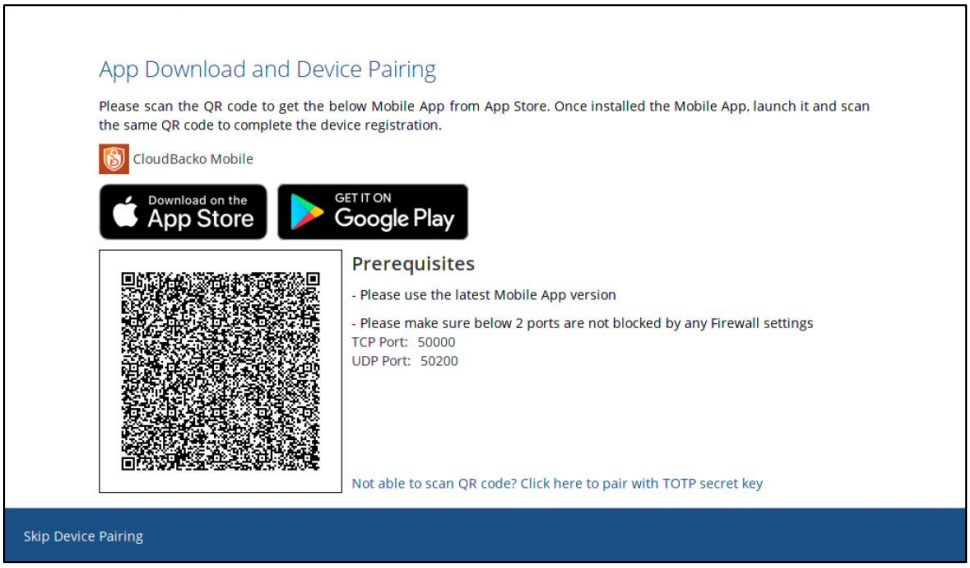


4. CloudBacko app supports two types of authentication method:
   - Push Notification
   - TOTP

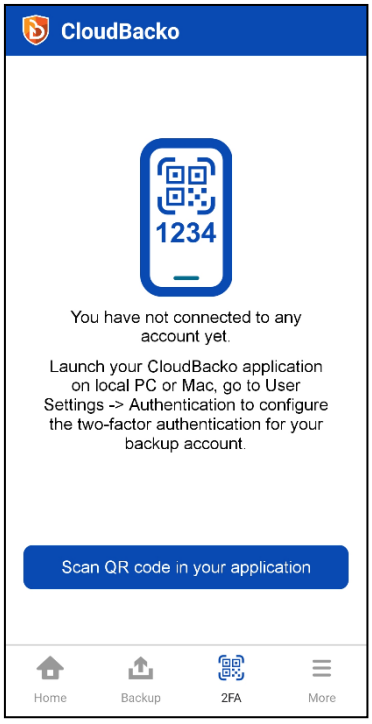
   CloudBacko app can be configured to support two 2FA modes:
   - Push Notification and TOTP (default mode) or,
   - TOTP only

Push Notification and TOTP

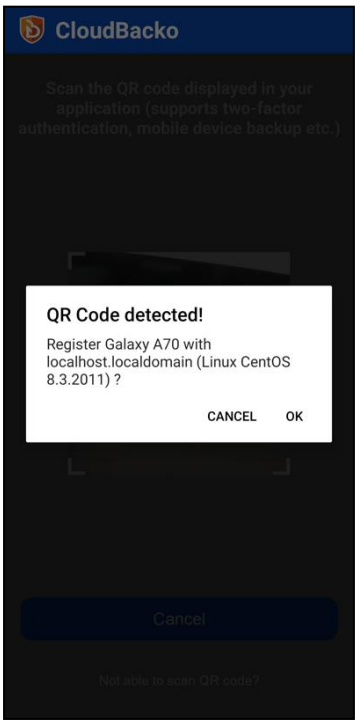
a. Scan the QR code to complete the device registration for two-factor authentication (Push Notification and TOTP) feature.



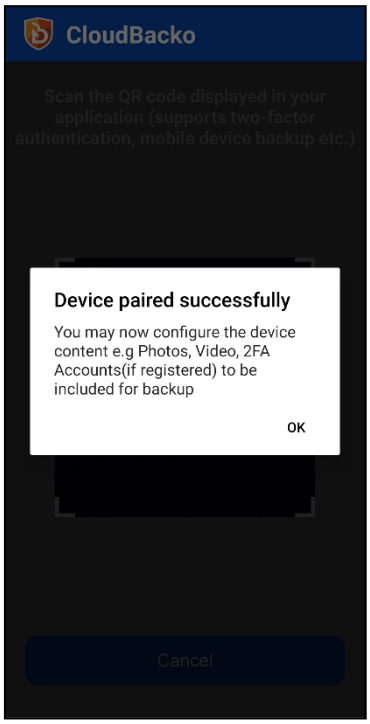
b. In the CloudBacko app, go to **2FA**. Tap the **Scan QR code in your application** link to scan the QR Code on the CloudBacko Pro.



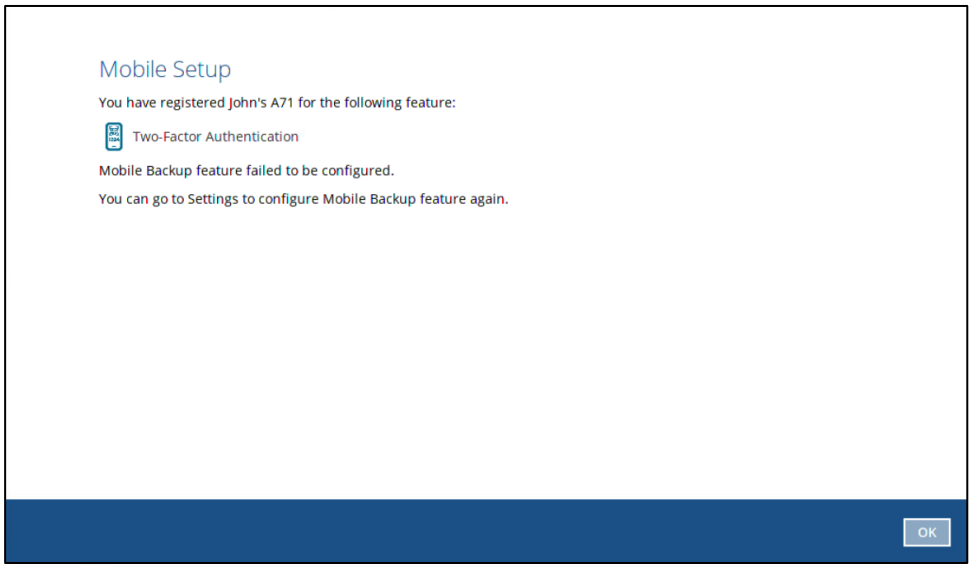
c. QR Code is detected, tap **OK** to proceed.



Device paired successfully.

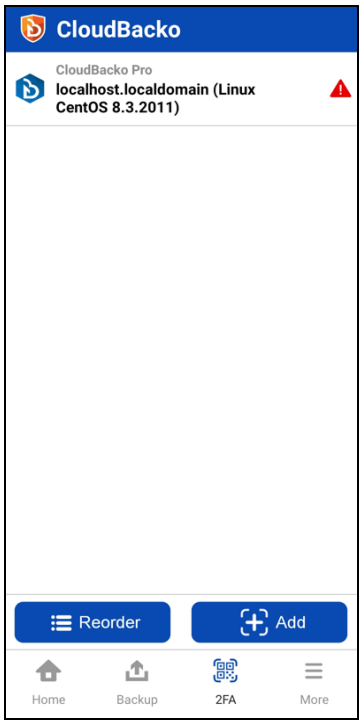


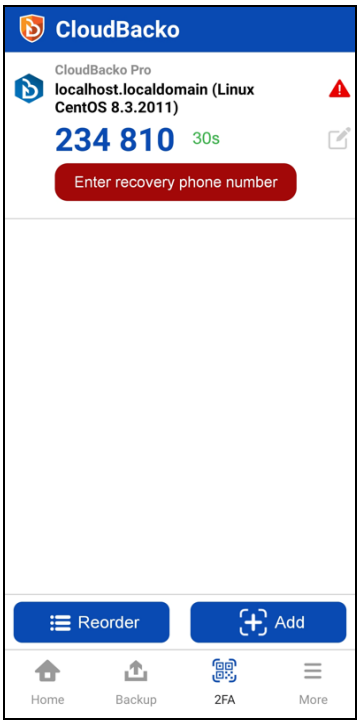
d. Once the registration is successful, the following screen will be displayed. You have now registered your device for two-factor authentication then click **OK.**



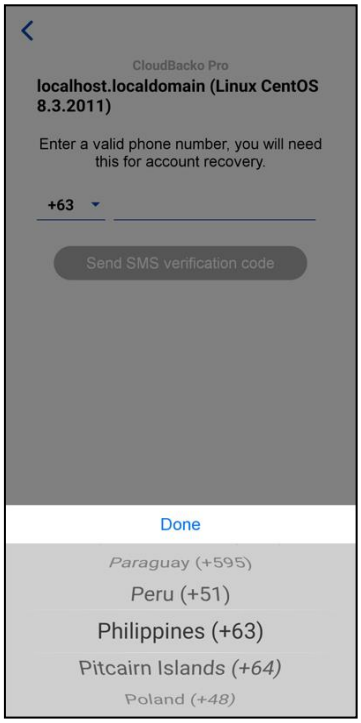
e. In the CloudBacko app, go to 2FA to enter the phone number for account recovery. Tap **Enter recovery phone number**.

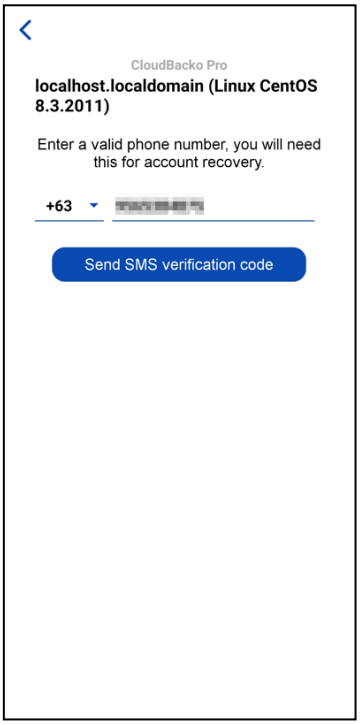
> **NOTE**
> Although push notification and TOTP will still work if the recovery phone number registration is not completed, it is still strongly recommended to complete **step e** as you will not be able to access the CloudBacko Pro if you lose your mobile device which also means loss of access to backup data.



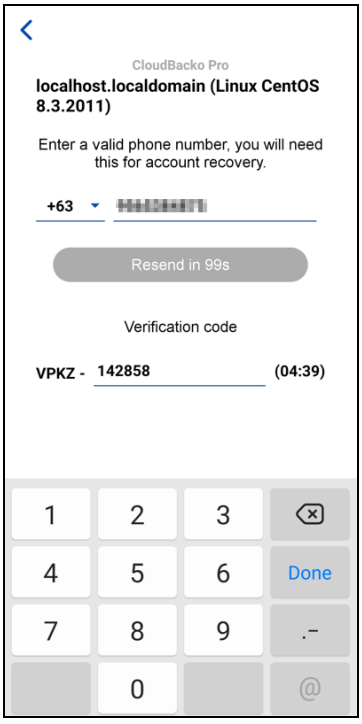


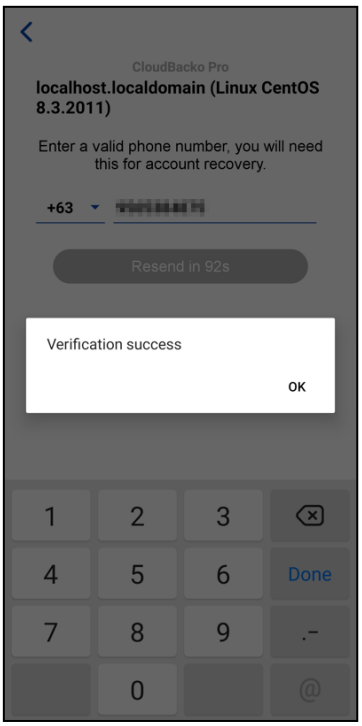
Select your country code and enter your phone number then click **Send SMS verification code**.





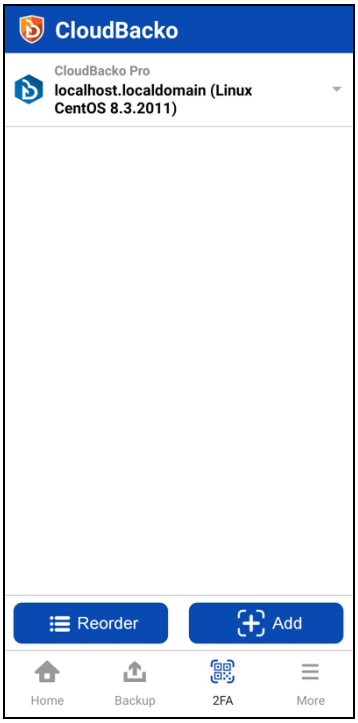
Enter the verification code sent to your mobile device.

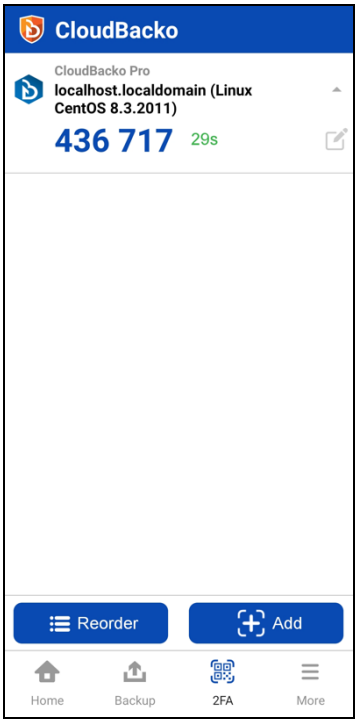




Sample verification code.

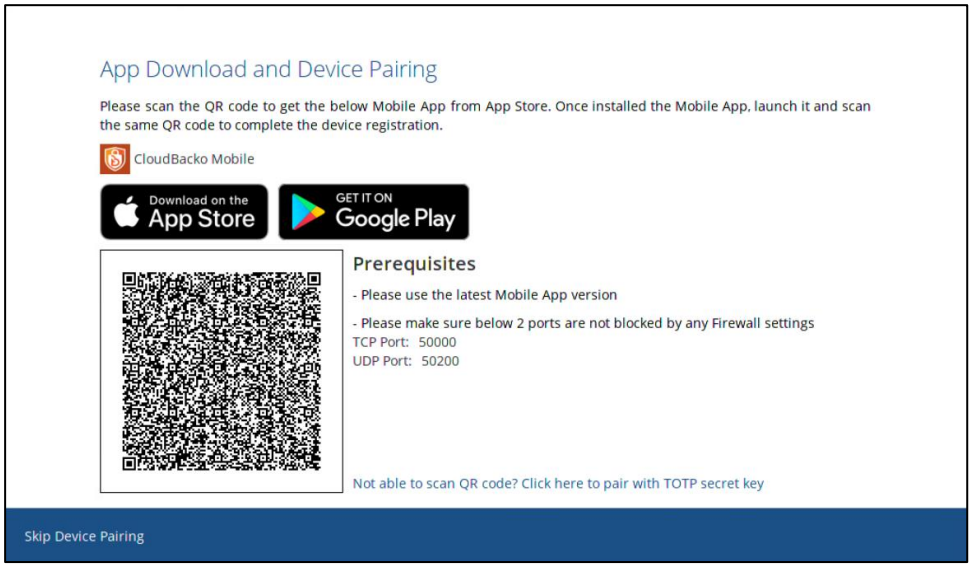
Successfully verified the phone number for account recovery.



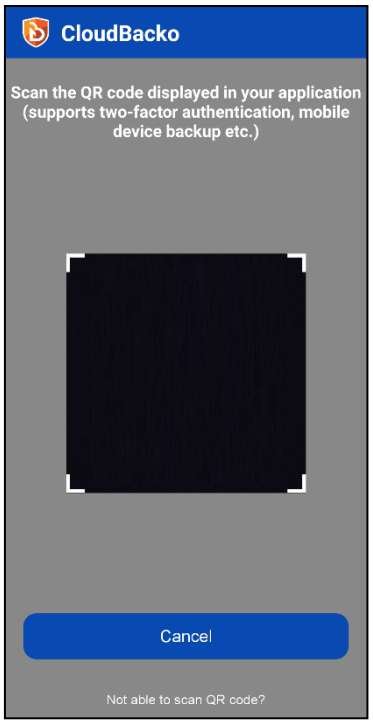


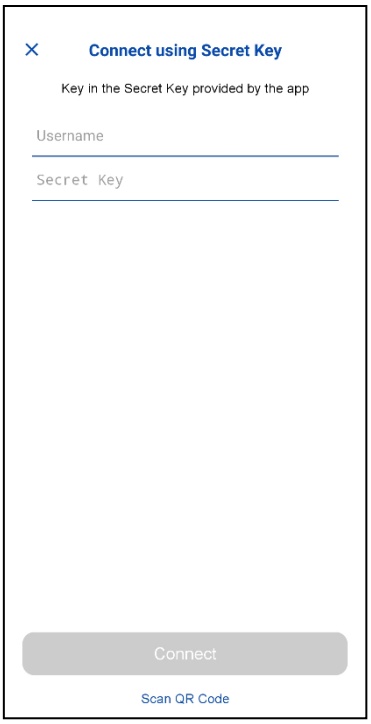
TOTP only

a. Click **Not able to scan QR code? Click here to pair with TOTP secret key** link to complete the device registration for two-factor authentication (TOTP only) feature.

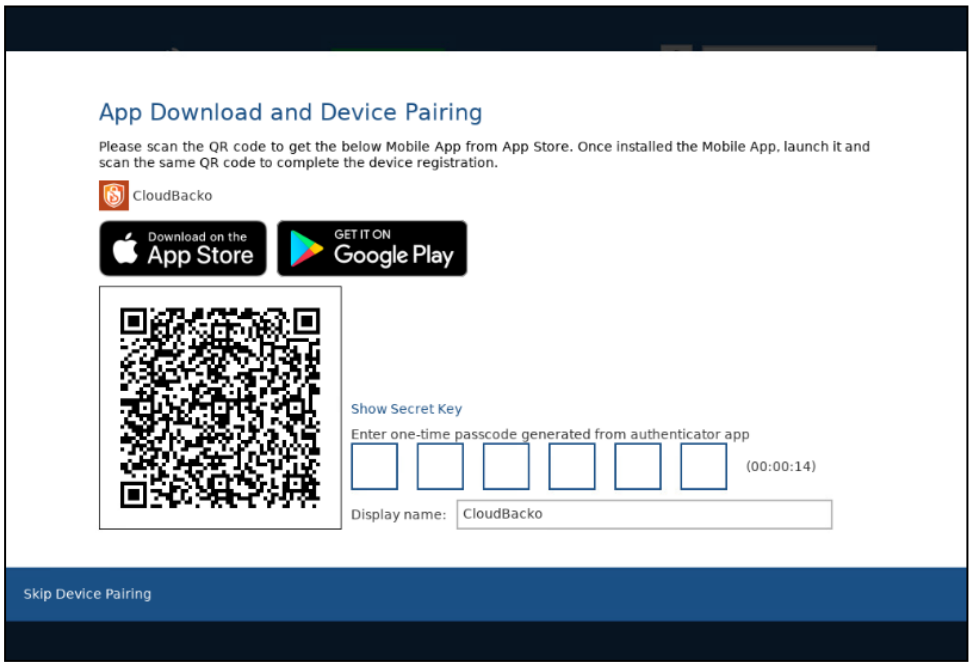


b. In the CloudBacko app, go to **2FA**. Tap the **Not able to scan QR code?** link.

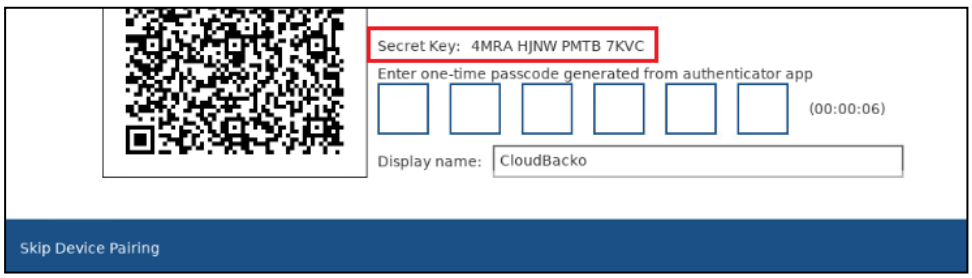




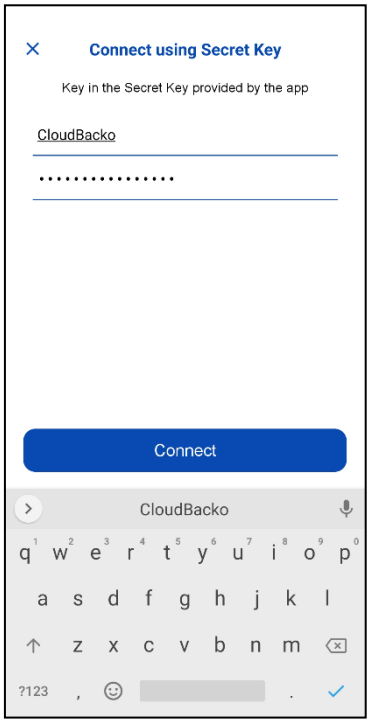
To see the secret key, click the **Show Secret Key** link to display the 16-digit secret key. And enter the display name.

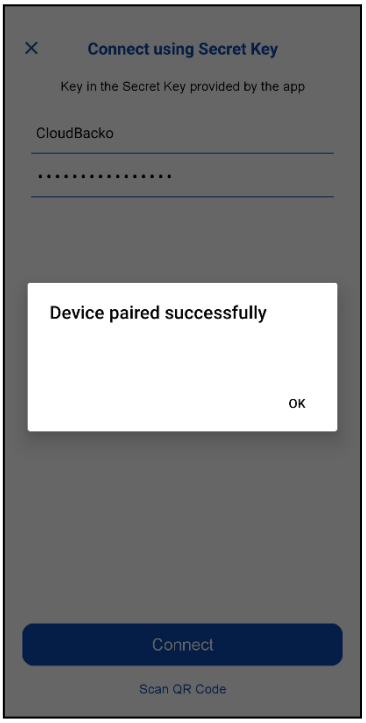


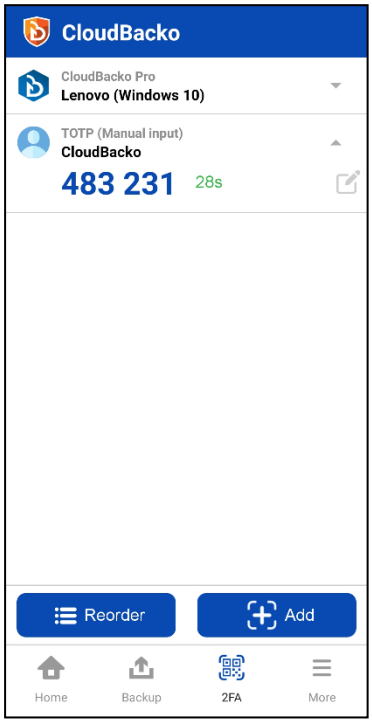
Once **Show Secret Key** is clicked, it will be displayed.



c. Enter the Username and Secret Key from CloudBacko Pro then tap **Connect** then **OK**.

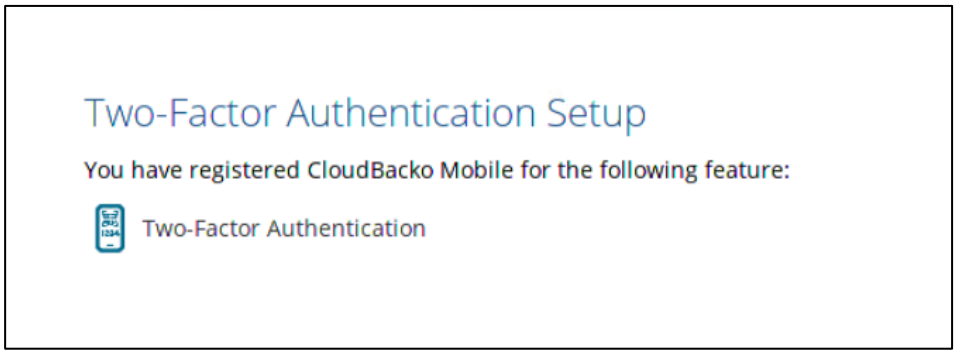




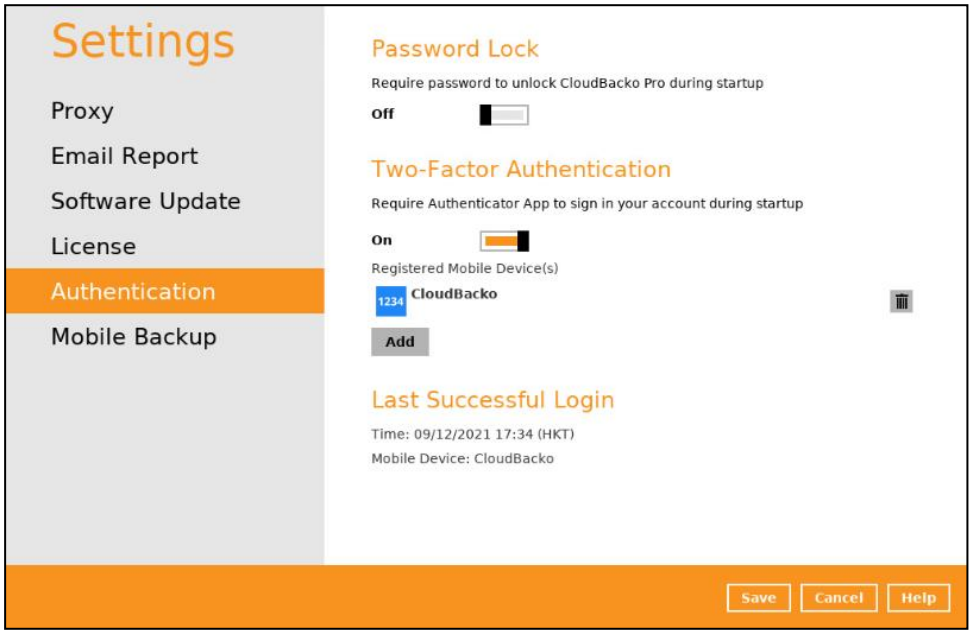


Enter the one-time passcode from the CloudBacko app.

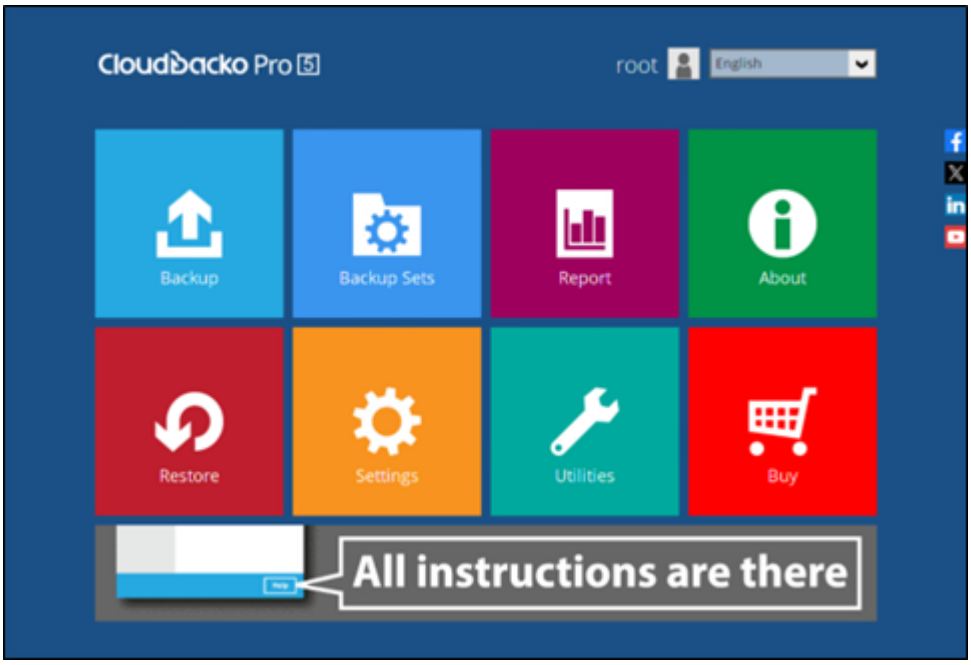
d. Once the registration is successful, the following screen will be displayed. You have now registered your device for two-factor authentication then click **OK**.



The device will now be available under **Settings** > **Authentication** > **Two-Factor Authentication**.



5. After successful login, the following screen will appear.



NOTE

- Please refer to the CloudBacko App v1 User Guide for Android and iOS – Appendix A: Troubleshooting Login if you are experiencing problems logging into CloudBacko Pro with Two-Factor Authentication with CloudBacko app.
- For instructions on how to register a device using third-party TOTP authenticator please refer to Appendix L.

6.2.2 Subsequent logins with 2FA

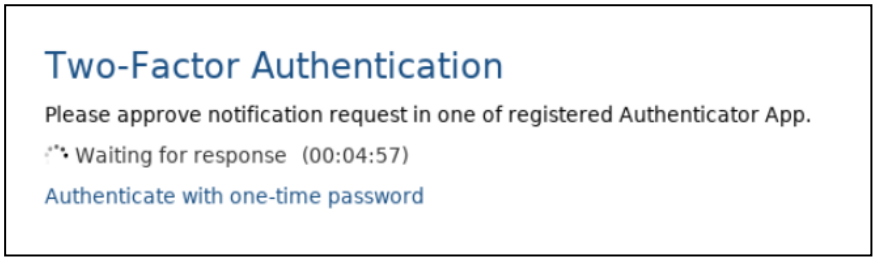
For subsequent logins to CloudBacko Pro with two-factor authentication, please follow the steps below:

1. A shortcut icon of CloudBacko Pro will be available on your desktop after installation. Double click the icon to launch the application.

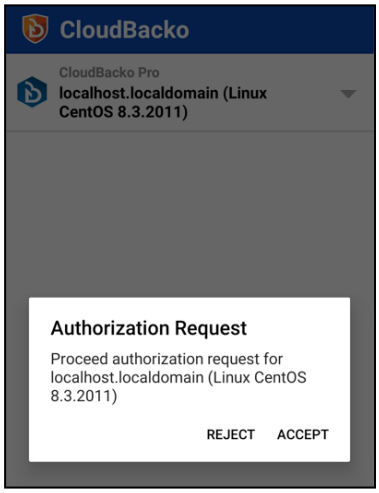
2. One of the two authentication methods will be displayed to continue with the login:
   - Push Notification and TOTP when using CloudBacko app or,
   - TOTP only

- If **CloudBacko app** was configured to use Push Notification and TOTP then there are two 2FA modes that can be used:
  - Push Notification (default)

    Push notification is default 2FA mode. Accept the login request on CloudBacko app to complete the login.

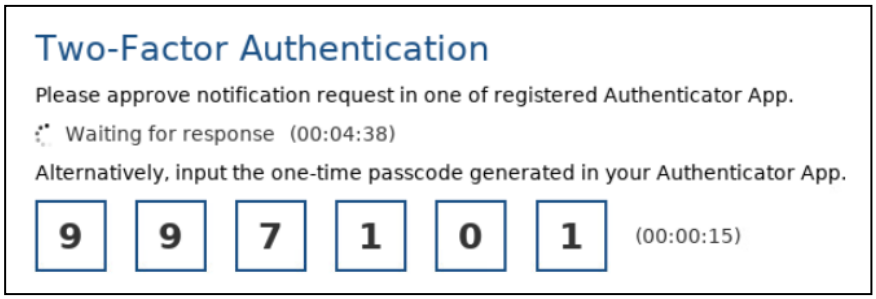


Example of the login request sent to CloudBacko app.

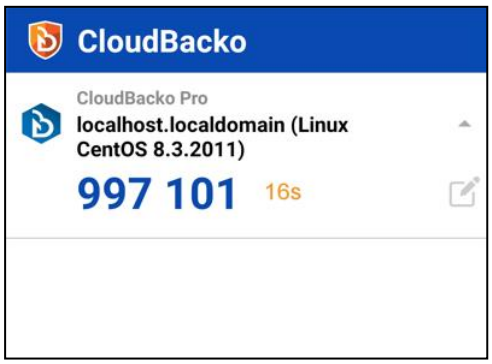


- TOTP

  However, if push notification is not working or you prefer to use one-time password, click the Authenticate with one-time password link, then input the one-time password generated from CloudBacko app to complete the login.



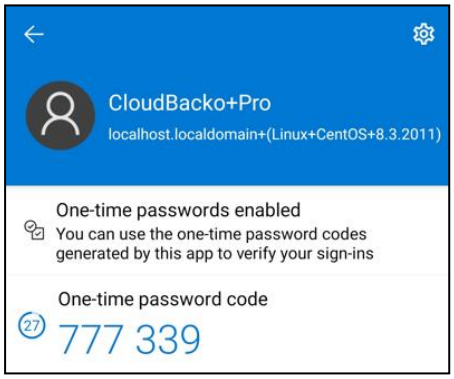
  Example of the one-time password generated from CloudBacko app to complete the login.



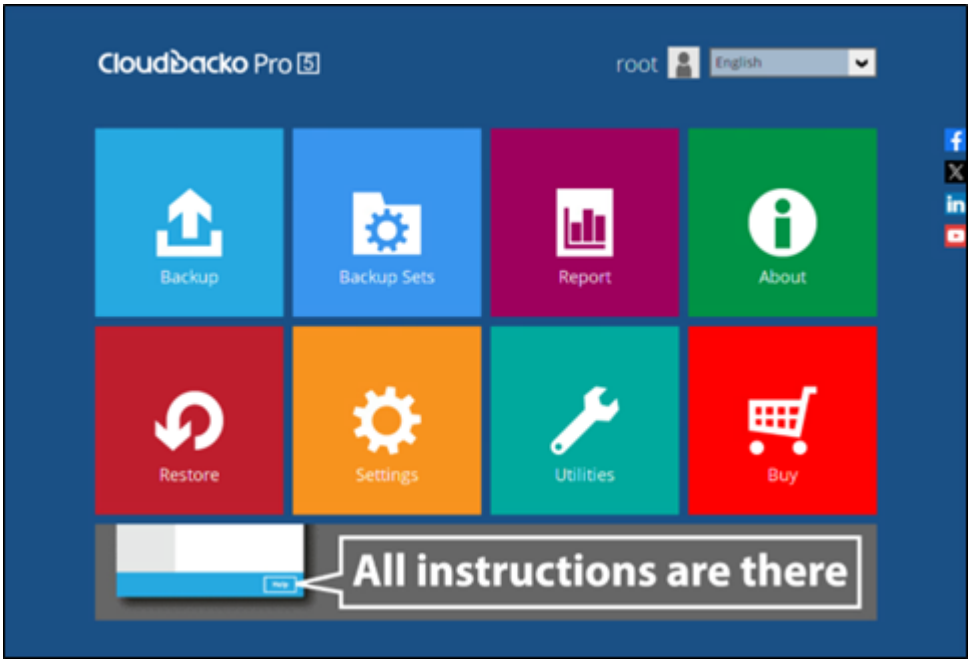
- **TOTP only**

  Enter the one-time password that is generated by the Authenticator App to proceed with login.

  Example of the one-time password that is generated in the third-party Authenticator App, Microsoft Authenticator.



3. After successful login, the following screen will appear.



NOTE

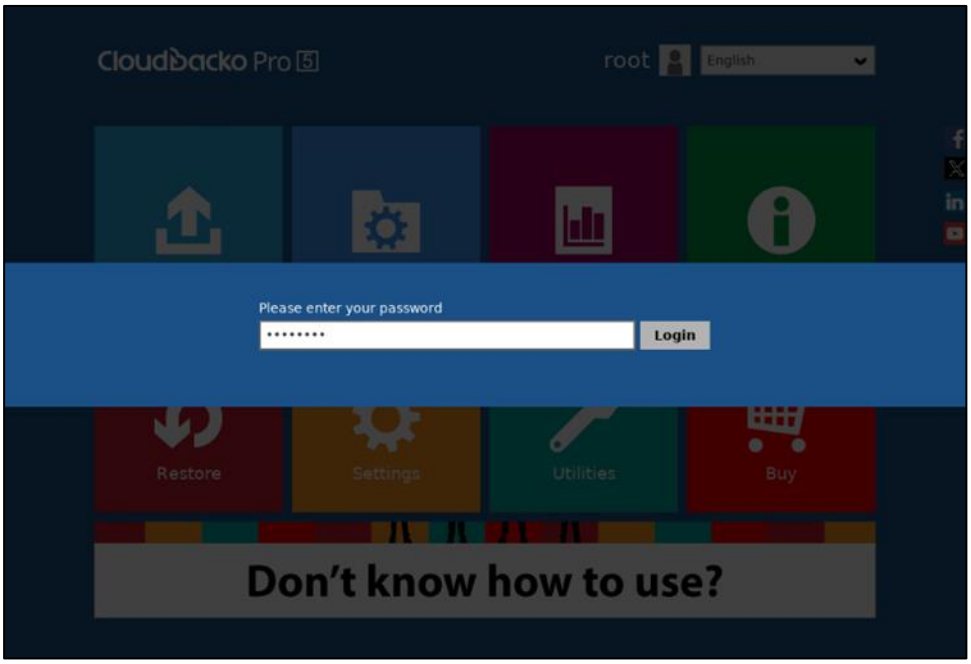
Please refer to the CloudBacko App v1 User Guide for Android and iOS – Appendix A: Troubleshooting Login if you are experiencing problems logging into CloudBacko Pro with Two-Factor Authentication with CloudBacko app.

6.2.3 Subsequent logins with 2FA and password lock

For subsequent logins to CloudBacko Pro with two-factor authentication and enabled password lock, please follow the steps below:

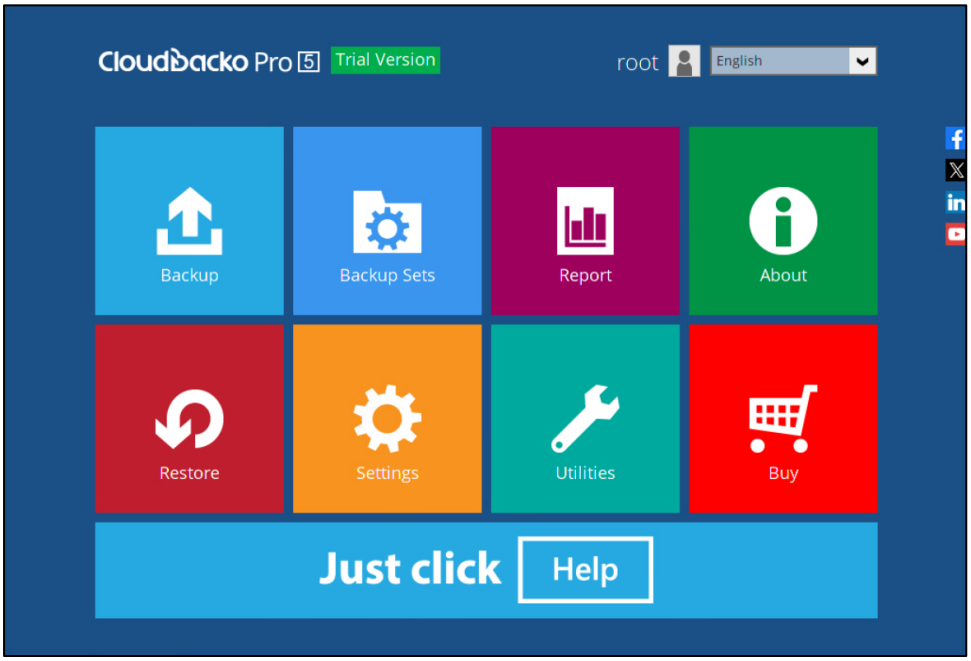
1. A shortcut icon of CloudBacko Pro will be available on your desktop after installation. Double click the icon to launch the application.

2. Enter password.



3. Follow the instructions in Chapter 6.2.2 to finish logging in with 2FA.

6.3 Trial Mode



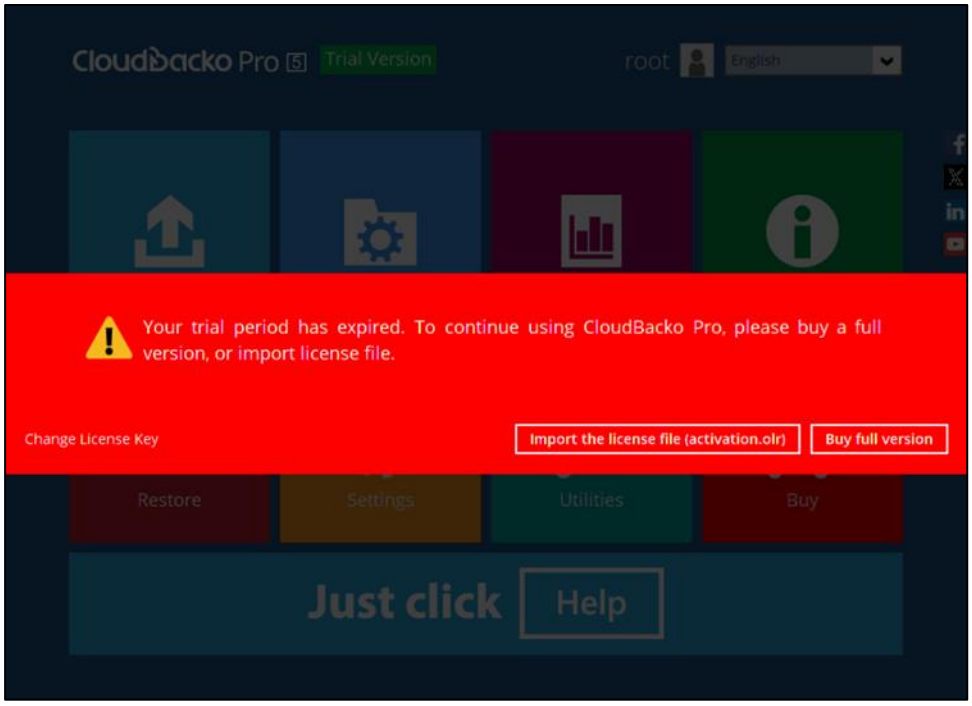
CloudBacko Pro will start in trial mode. Trial mode will expire after 30 days.

If you want to purchase a license key, please see these chapters:

1. Ch. 7.9 Buy
2. Ch. 7.9.1 Credit Card
3. Ch. 7.9.2 TT (Telegraphic Transfer)

An existing license key may be applied even if CloudBacko Pro is still in trial. Please see this chapter, Ch. 7.7.4 License.

- Expired Trial Mode

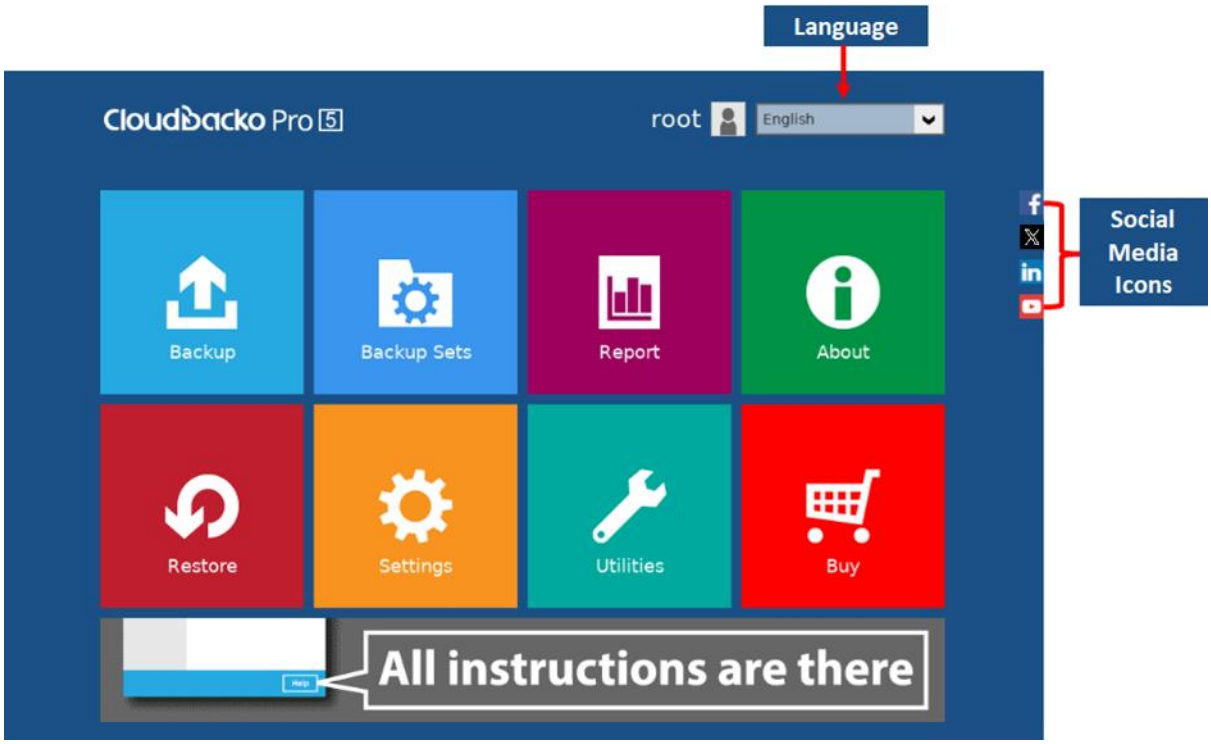


If you want to apply license key after Trial mode has expired, please check Appendix I: How to apply a license key to a CloudBacko Pro installation with an expired trial license?

- **CloudBacko License Key**

If you want to find your purchased CloudBacko Pro license key, please check Appendix J: Where to find the CloudBacko Pro purchase license key?

7 CloudBacko Pro Overview

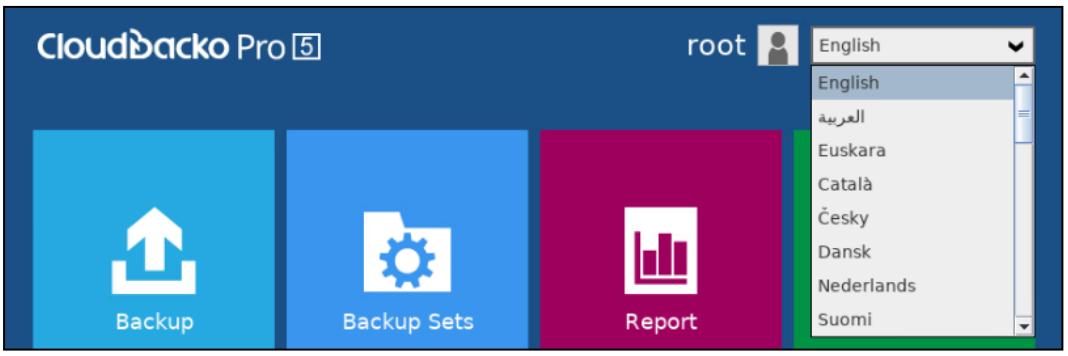


CloudBacko Pro main interface has 11 icons that can be accessed by the user, namely:

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

7.1 Language

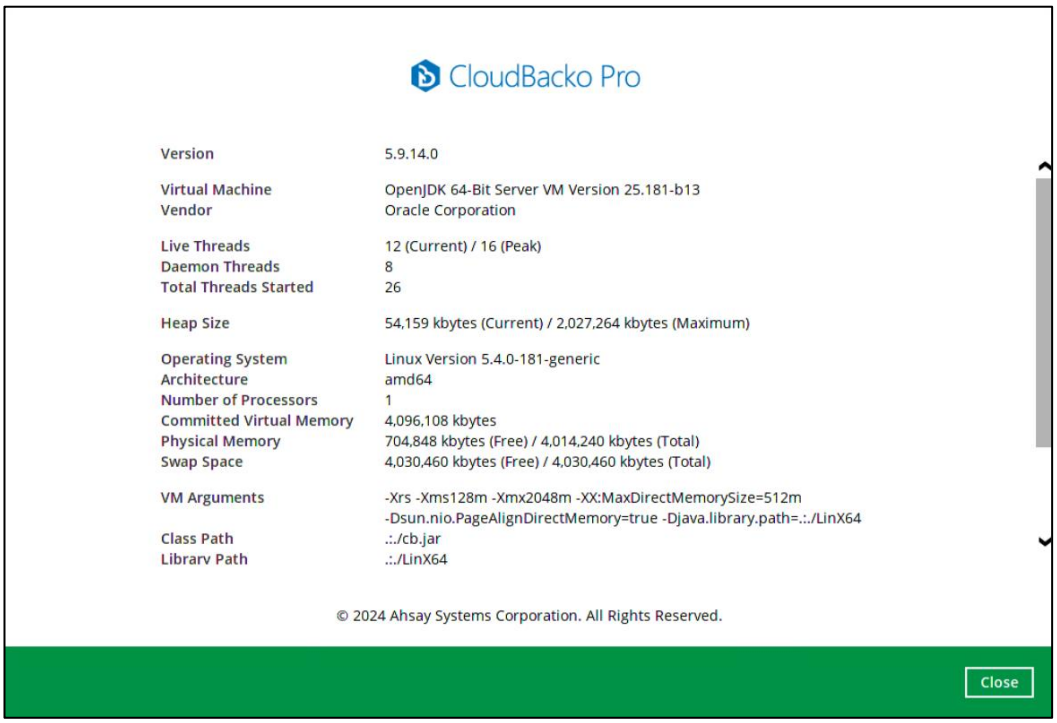
This option is used to change the language of the CloudBacko Pro interface. The list of the available languages depends on the backup service provider.



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

7.2 About

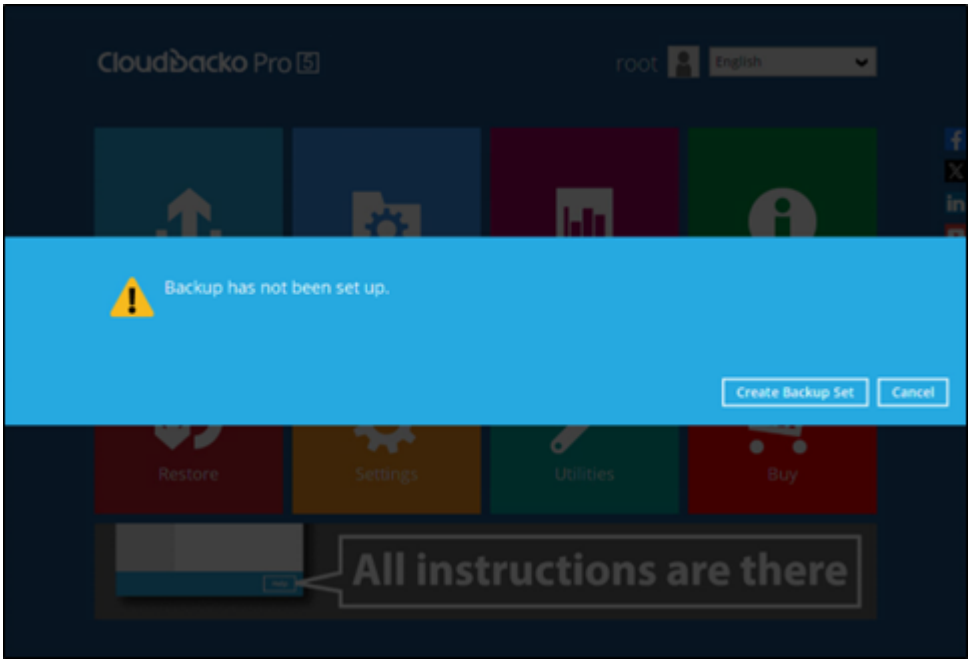
The **About** module displays the product version and system information of the machine where the CloudBacko Pro is installed.



7.3 Backup

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

When using CloudBacko Pro 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.

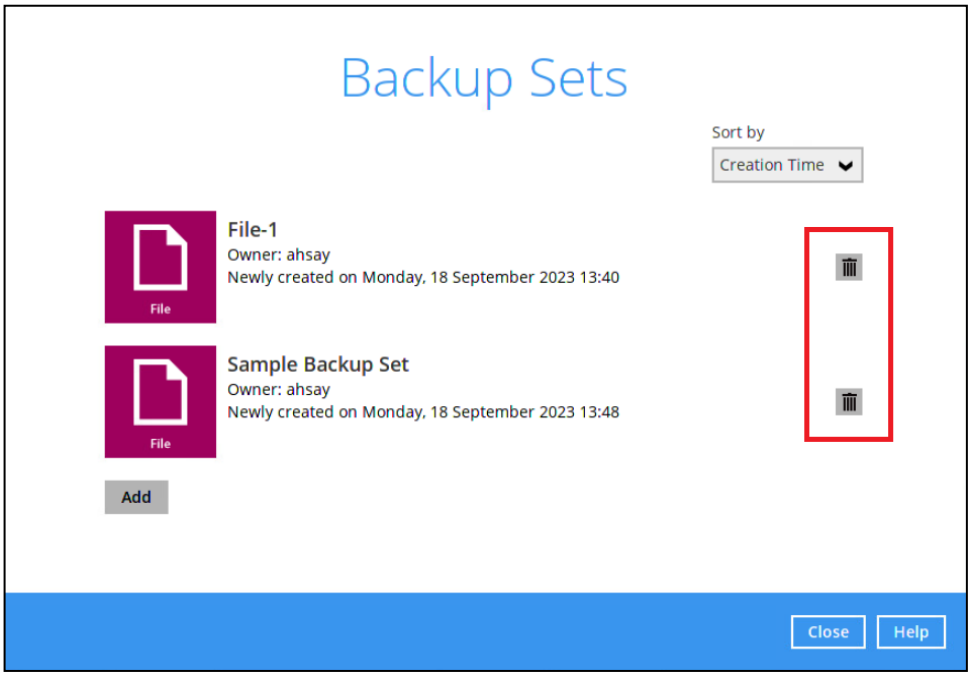
7.4 Backup Sets

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.

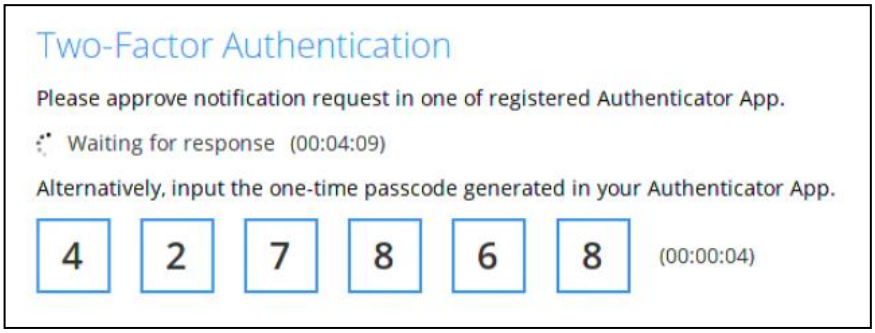
For instructions on how to create a backup set, refer to Chapter 8 Create a Backup Set.

To delete a backup set, follow the instructions below:

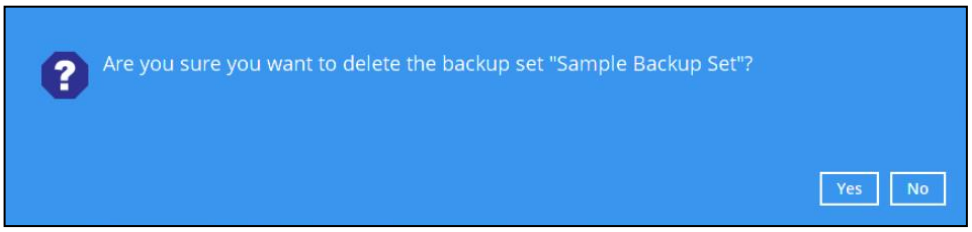
1. Click on the delete icon on the right side of the backup set that you want to delete.



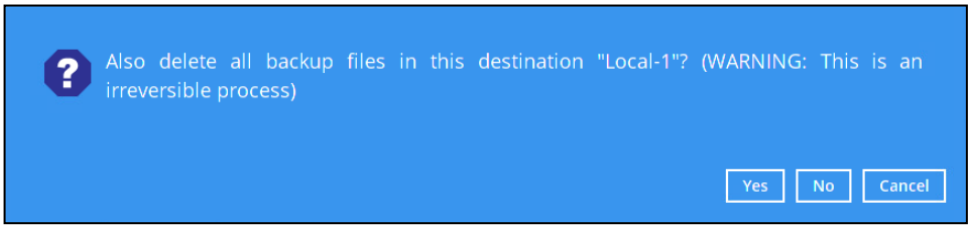
2. If the account is registered for 2FA, accept the push notification or enter the one-time password. Otherwise, skip to the next step.



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



4. 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.



5. 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:

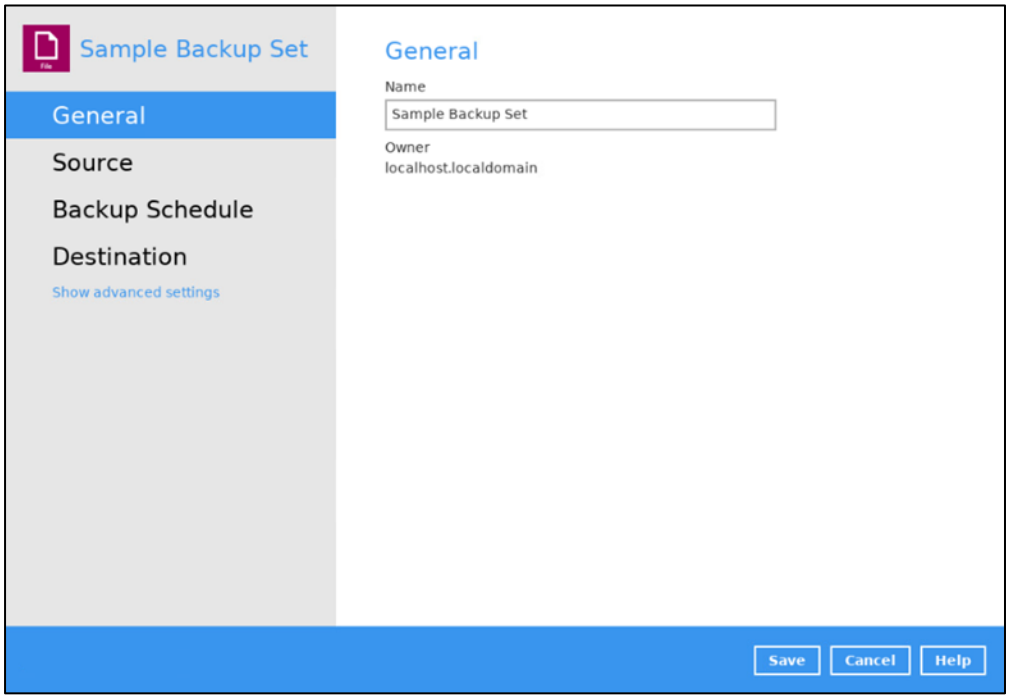
- General
- Source
- Backup Schedule
- Destination

Show advanced settings

- Deduplication
- Retention Policy
- Command Line Tool
- Bandwidth Control
- Others

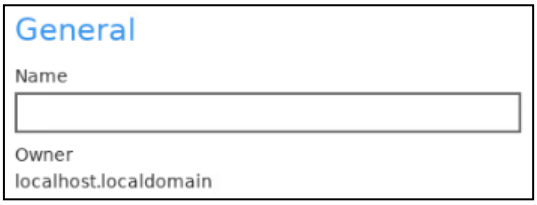
7.4.1.1 General

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.

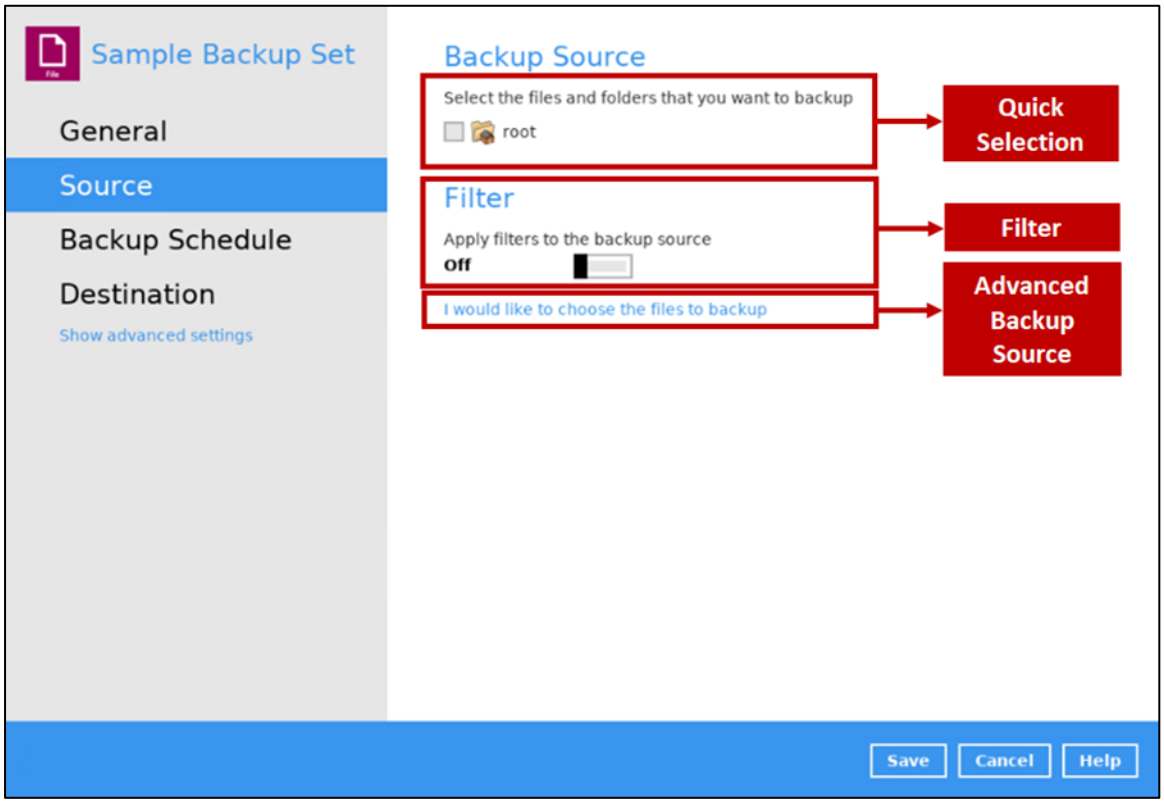


2. Click the **Save** button to save the updated backup set name.

NOTE
In assigning a backup set name, make sure that it does not have an identical name.

7.4.1.2 Source

This allows the user to select from the available options when selecting a backup source.



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

Option	Description
Quick Selection	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 Selection

This option allows the user to quickly select a backup source to be backed up.

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
root		If root is selected, all files and/or folders located in the following location ***/root*** will be backed up this includes: ***/root/Desktop*** ***/root/Documents*** ***/root/Downloads*** ***/root/Music*** ***/root/Pictures*** ***/root/Public*** ***/root/Templates*** ***/root/Videos*** This selection also includes some Linux 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. ***/root/.cache*** ***/root/.bash_history*** ***/root/.bashrc*** ***/root/.cbp***

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

1. Select a backup source.

2. Click the **Save** button to save the selected backup source.

Option 2: Filter

The Filter Backup Source is an alternative way to select a backup source which does not require Windows User Authentication login password even if the backup schedule is enabled unless the filter backup source is located on a network drive.

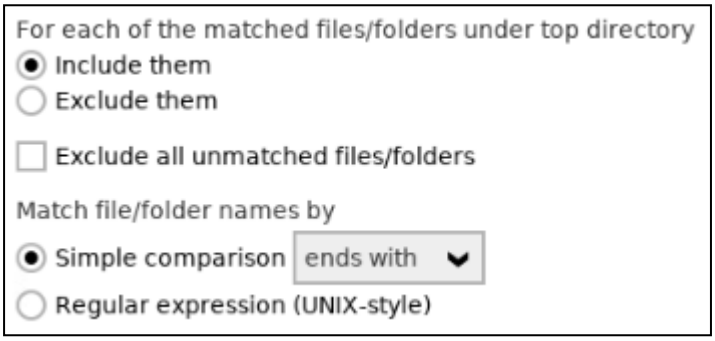
To select files and/or folders to back up using the Filter Backup Source, follow the steps below:

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

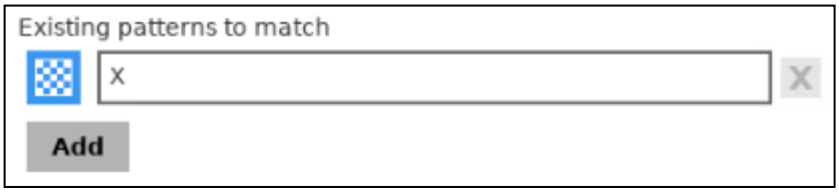
2. Click the **Add** button to create filter.

3. Assign a desired name to the backup filter.

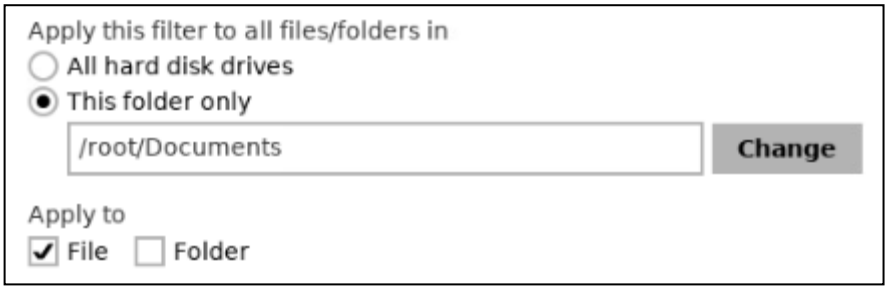
4. Select from the options below.



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

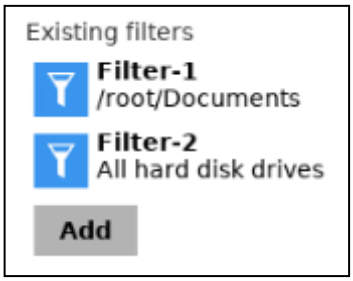


6. Select whether you would like to apply the filter to all files and/or folders in all hard disk drives or to a specific folder only. If 'This folder only' is selected, click the **Change** button to select the specific folder that you would like to apply the filter to.



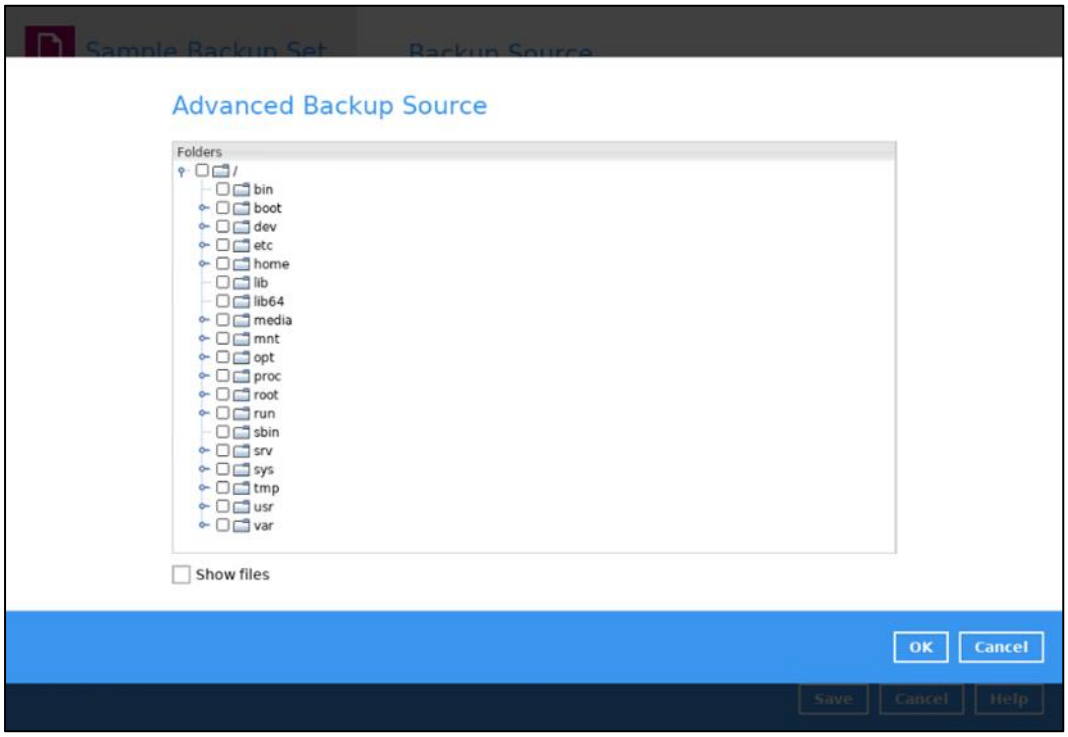
7. Click the **OK** button to save the created filter, then click the **Save** button to save the settings. Once you run a backup, all files and/or folders that match the applied filter will be backed up.

8. Multiple backup filters can be created.



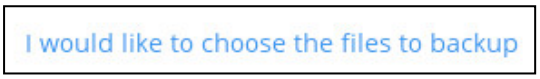
Option 3: Advanced Backup Source

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

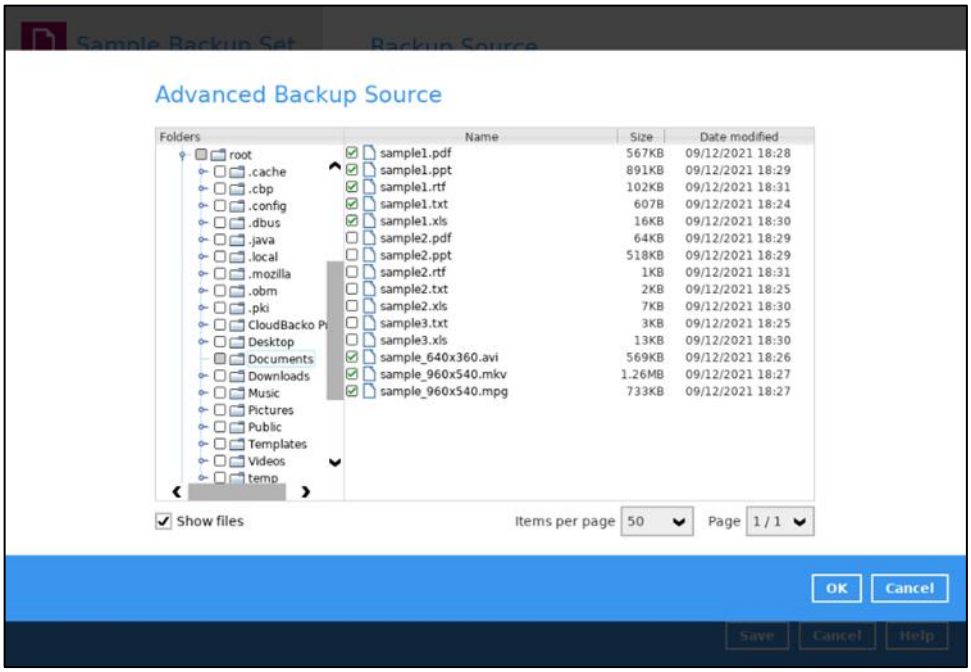


To select files and/or folders using the Advanced Backup Source, follow the steps below:

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



2. In the Advanced Backup Source window, 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 save the settings.

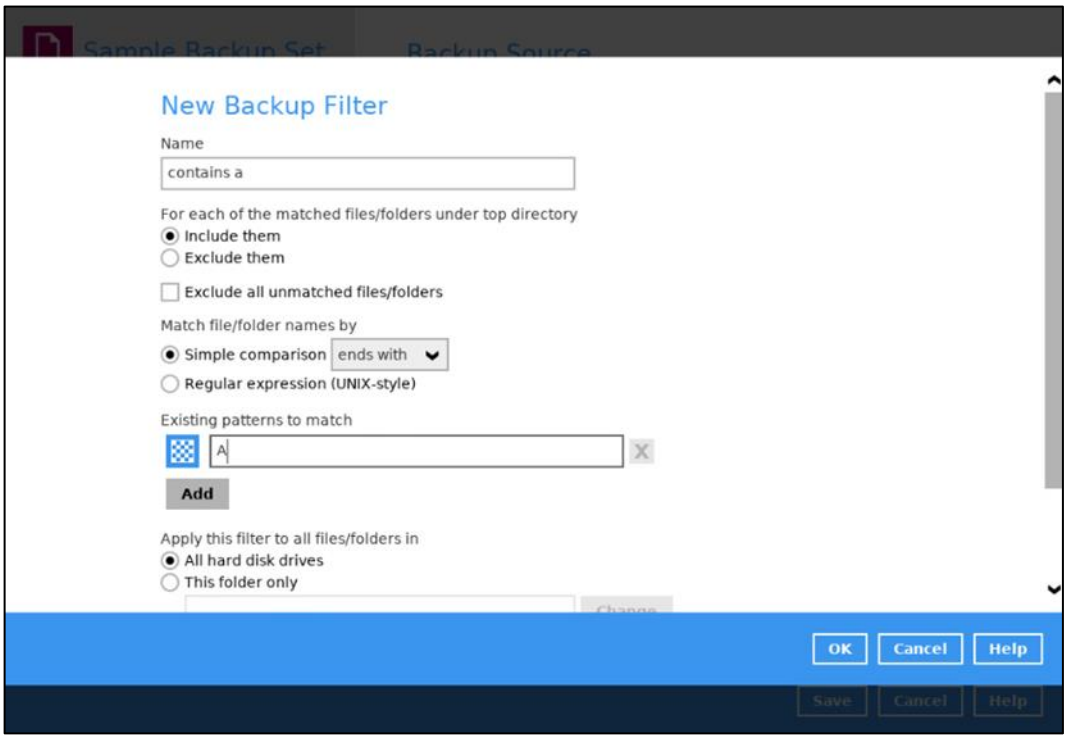
In selecting files and/or folders to back up, the three (3) options are combinable and can be used simultaneously. Please refer to the example scenarios below for details:

Scenario 1 (Quick Selection + Filter)

You can use the quick selection 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 which will be applied to the backup source.



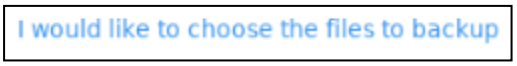
3. Click the **OK** button to save the created filter, then click the **Save** button to save the settings.

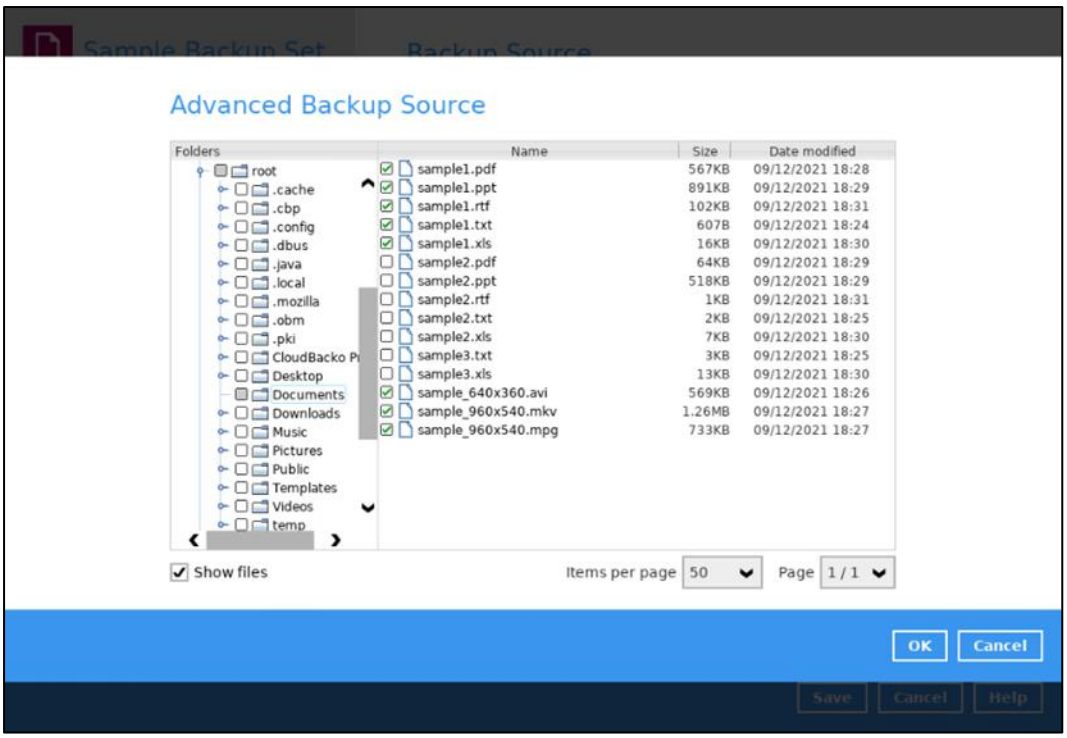
Scenario 2 (Quick Selection + Advanced Backup Source)

You can use the quick selection 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' and select the files and/or folders that you would like to back up



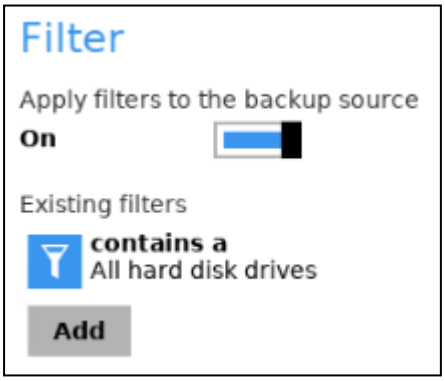


3. Click the **OK** button to save the selection, then click the **Save** button to save the settings.

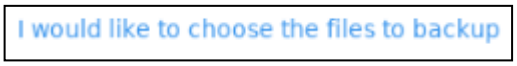
Scenario 3 (Filter + Advanced Backup Source)

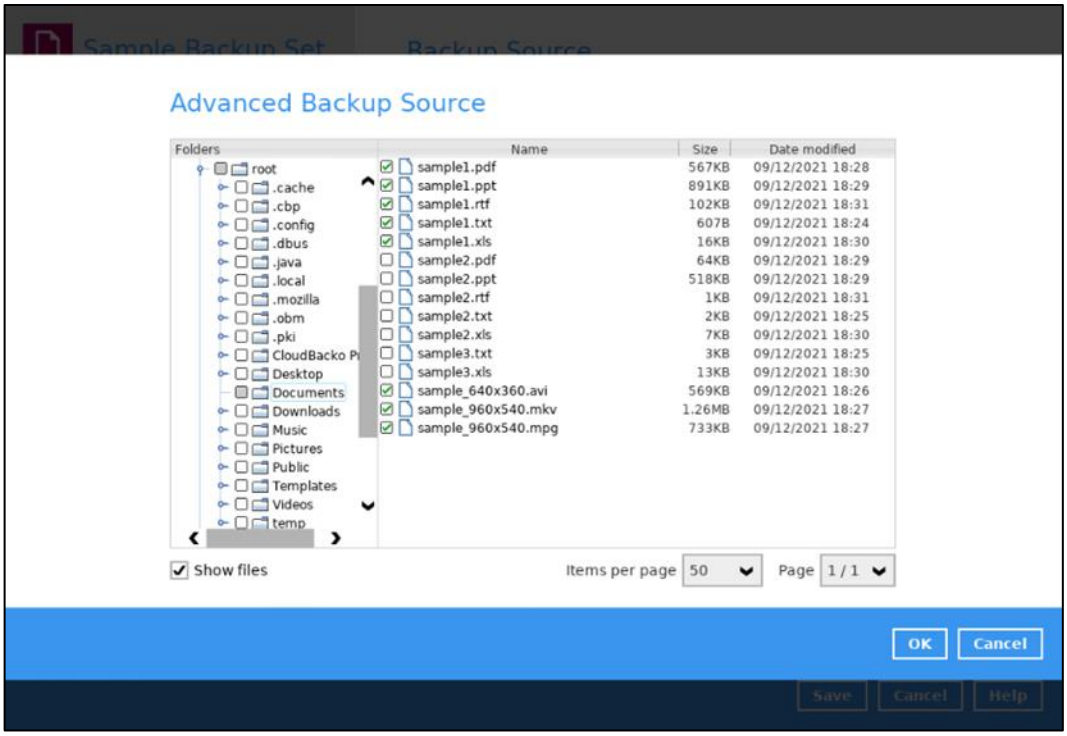
You can use the filter backup source and choose files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

1. Create a filter.



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

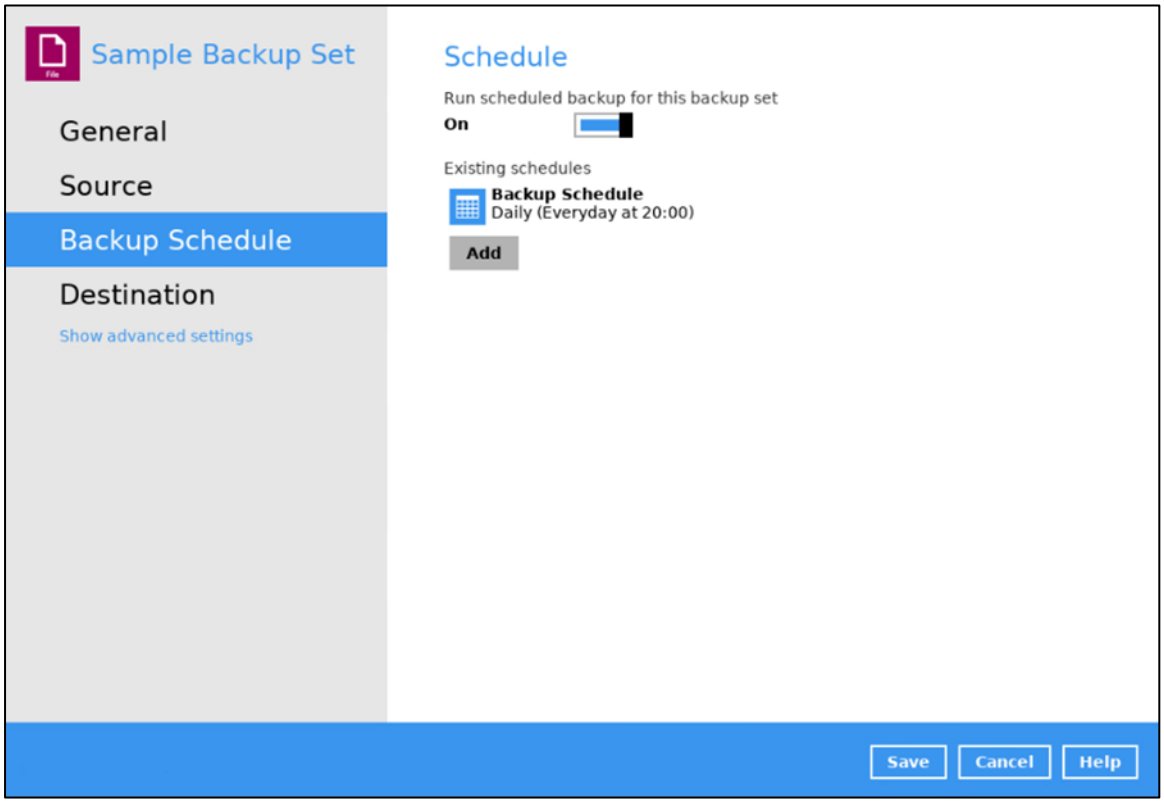




3. Click the **OK** button to save the selection, then click the **Save** button to save settings.

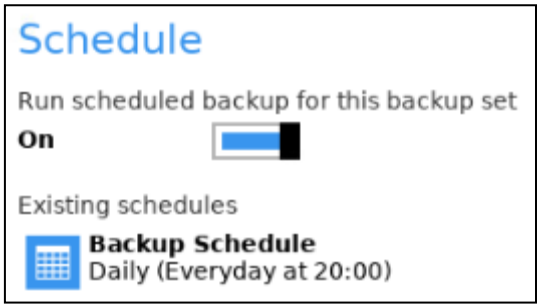
7.4.1.3 Backup Schedule

This feature allows the user to assign a backup schedule for the backup job to run automatically.

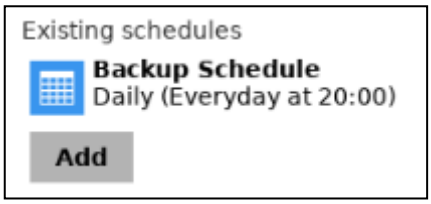


To configure a backup schedule, follow the steps below:

1. Swipe the lever to the right to turn on the backup schedule setting. The backup schedule is configured as “Daily at 20:00” by default.

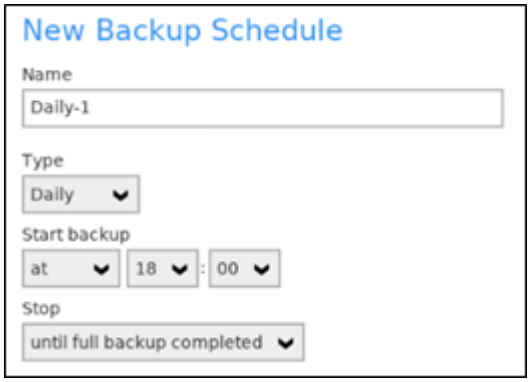


2. Select an existing backup schedule to modify or click the **Add** button to create a new one.

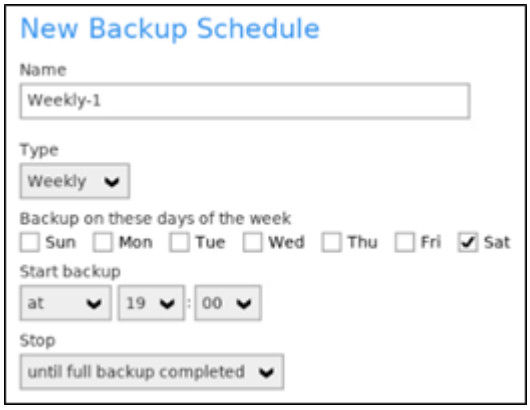


3. In the New Backup Schedule window, configure the following backup schedule settings.
   - **Name** – the name of the backup schedule.
   - **Type** – the type of the backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.

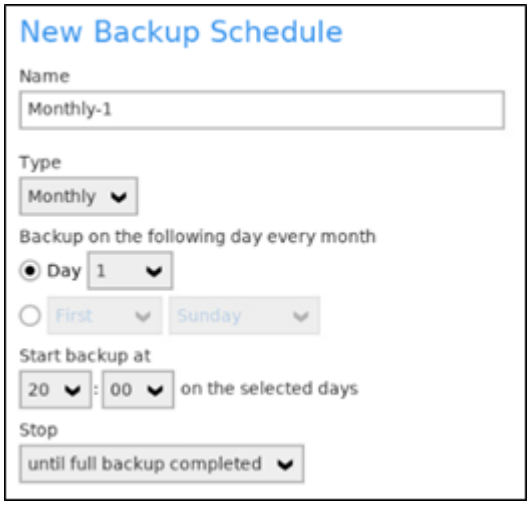
- **Daily** – the time of the day or interval in minutes/hours when the backup job will run.



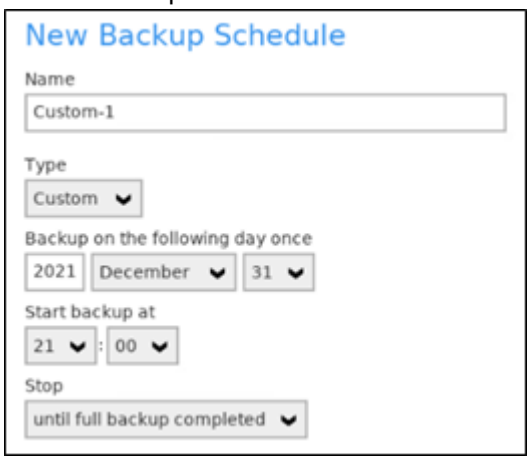
- **Weekly** – the day of the week and the time of the day or interval in minutes/hours when the backup job will run.



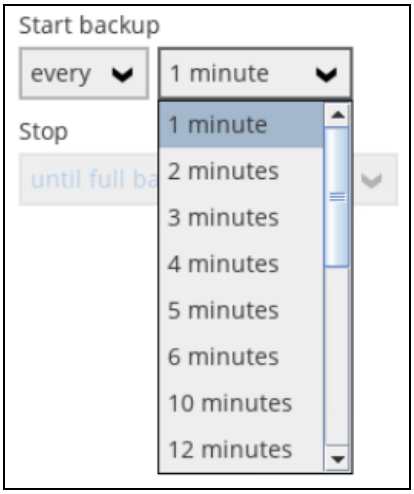
- **Monthly** – the day of the month and the time of the day when the backup job will run.

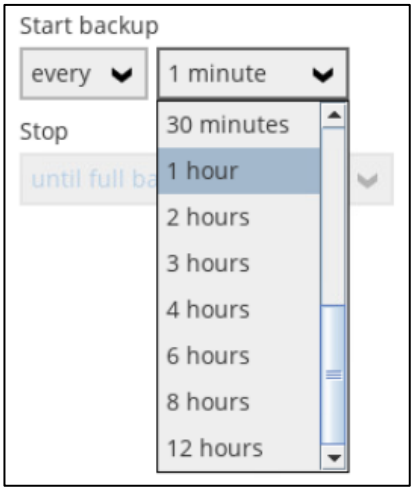


- **Custom** – a specific date and the time when the backup job will run.



- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job at a specific time.
  - **every** – this option will start a backup job in intervals of minutes or hours.
    - minute interval, 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, or 30 minutes
    - hourly interval, 1, 2, 3, 4, 6, 8, 10, or 12 hours





Here is an example of backup set that has a daily and weekly backup schedule.

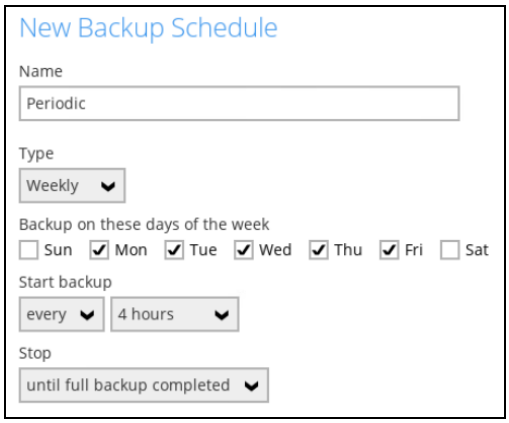


Figure 1.1

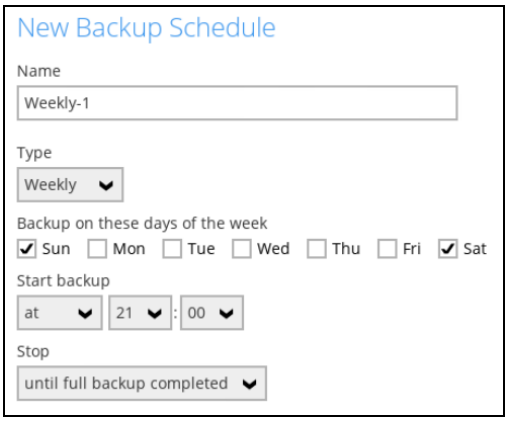


Figure 1.2

Figure 1.1 – Periodic schedule every 4 hours Monday - Friday during business hours

Figure 1.2 – Normal schedule run at 21:00 or 9:00 PM daily on Saturday & Sunday during weekend non-business hours

- **Stop** – the stop time of the backup job. This only applies to schedules with start backup "at" and is not supported for periodic backup schedule (start backup "every")
  - **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.
  - **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

    The number of hours must be enough to complete a backup of all files in the backup set. For small files in a backup, if the number of hours is not enough to back up all files, then the outstanding files will be backed up in the next backup job. However, if the backup set contains large files, this may result in partially backed up files.

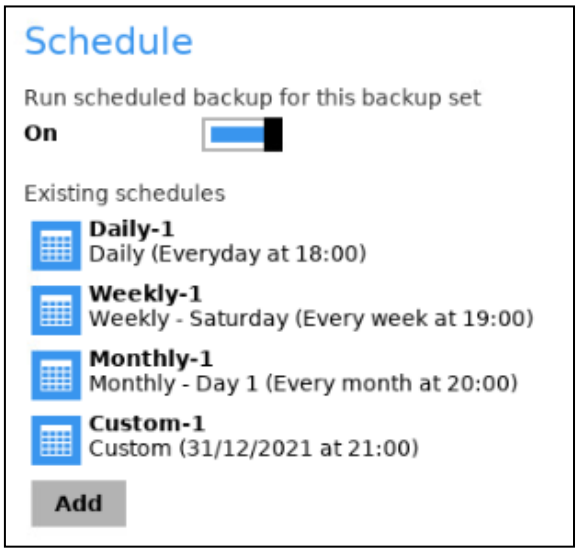
    For example, if a backup has 100GB file size which will take approximately 15 hours to complete on your environment, but you set the "stop" after 10 hours, the file will be partially backed up and cannot be restored. The next backup will upload the files from scratch again.

    The partially backed up data will have to be removed by running the data integrity check.

    As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.

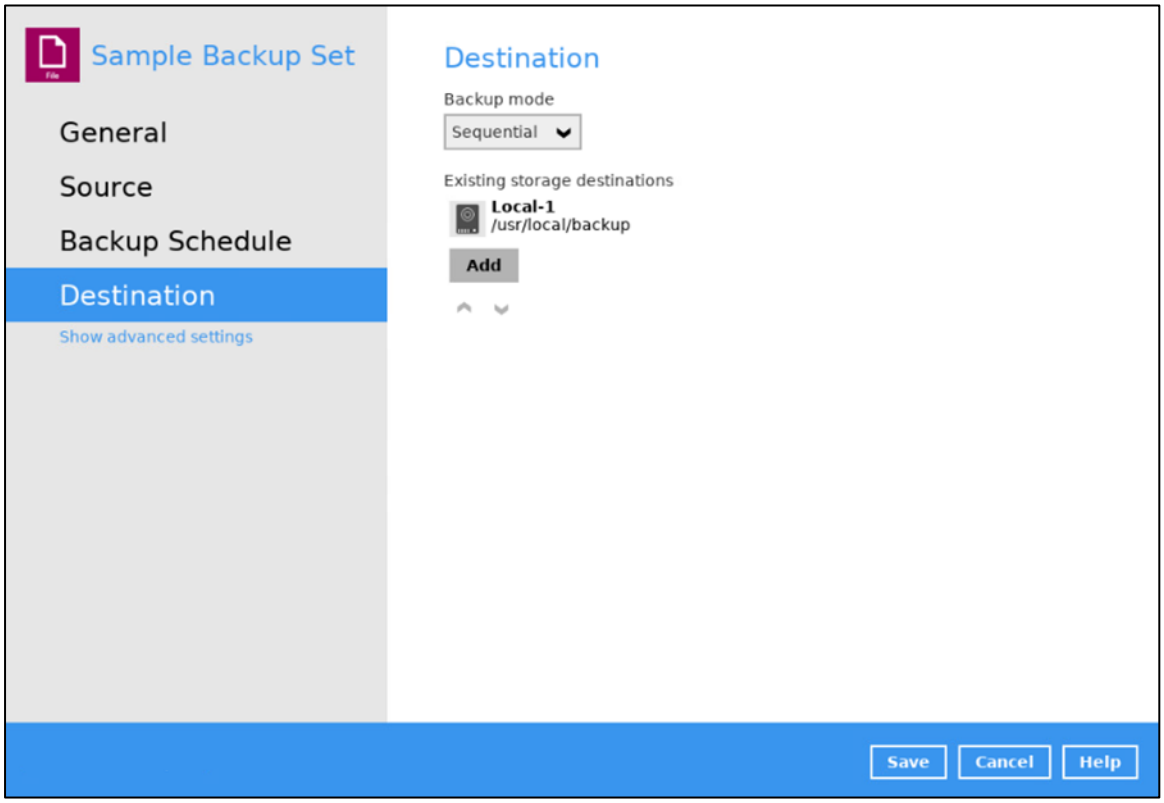
4. Click the **OK** button to save the configured backup schedule settings.
5. Click the **Save** button to save the settings.

Multiple backup schedules can be created.

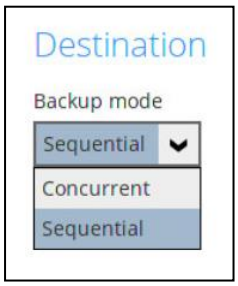


7.4.1.4 Destination

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



There are two (2) different types of backup mode in performing a backup:



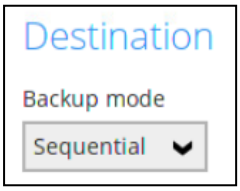
Backup mode	Description
Sequential	This is the configured backup mode by default. This backup mode will run a backup job to each backup destination one by one.
Concurrent	This backup mode will run a backup job to all backup destinations simultaneously.

Comparison between Sequential and Concurrent Backup mode

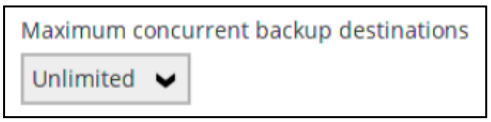
Backup mode	Pros	Cons
Sequential	Takes less resources in the local machine (e.g. memory, CPU, bandwidth, etc.) to complete a backup job.	Backup job is slower than in concurrent mode since the backup job will upload the backup data to the selected backup destinations one at a time.
Concurrent	Backup job is faster than in Sequential mode.	Requires more resources in the local machine (e.g. memory, CPU, bandwidth, etc.) to complete a backup job.
	Maximum number of concurrent backup destinations can be configured.	

To modify the Backup Mode, follow the steps below:

1. Go to Backup Sets, then choose a backup set.
2. Select the **Destination** tab in the backup set settings.
3. Click the drop-down button to select a backup mode.



4. If “Concurrent” is selected, click the drop-down button to select the no. of maximum concurrent backup destinations.



5. Click the **Save** button to save the selected backup mode.

Starting with version 5.7, a new type of destination is introduced, in the form of immutable storage destination. This prevents backup data that is saved in immutable destination from being deleted or overwritten.

Only the following destinations supports immutable storage:

- Amazon S3
- AWS S3 Compatible Cloud Storage
- Backblaze
- Google Cloud Storage
- Microsoft Azure
- Wasabi

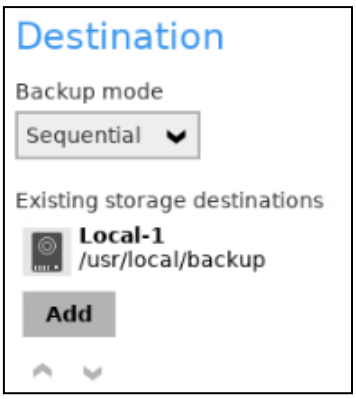
An “Immutable” checkbox is provided to be able to create an immutable storage destination.

These are the requirements to be able to setup an immutable storage destination:

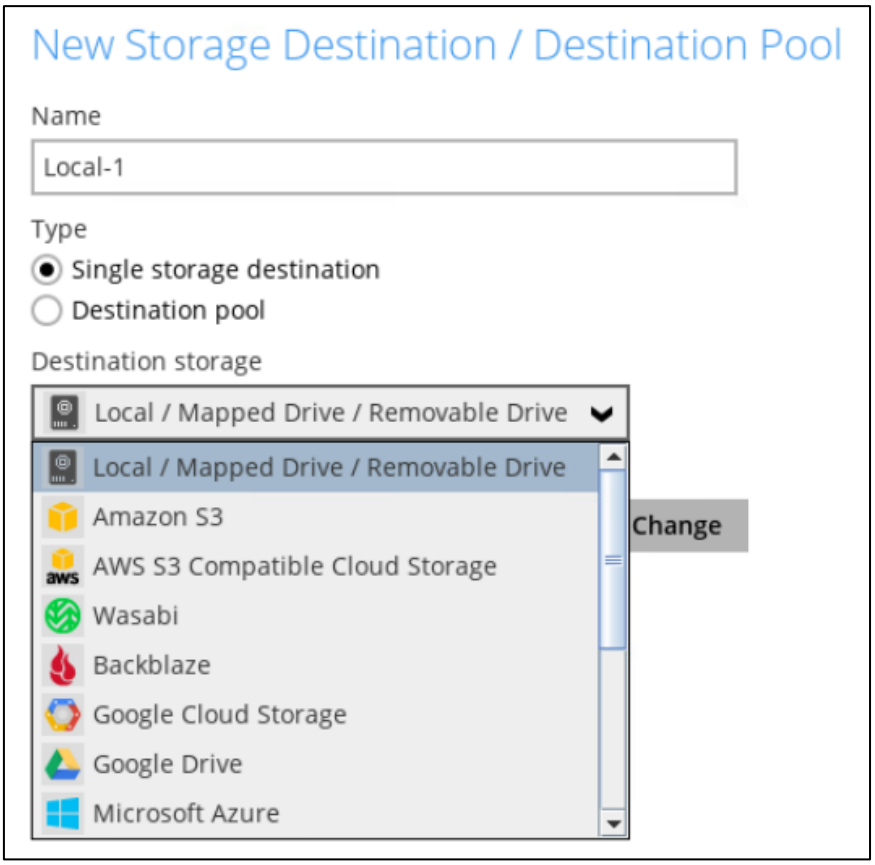
- The user account must have a device registered for 2FA.
- The user account of the storage destination must not be setup with delete permission.

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

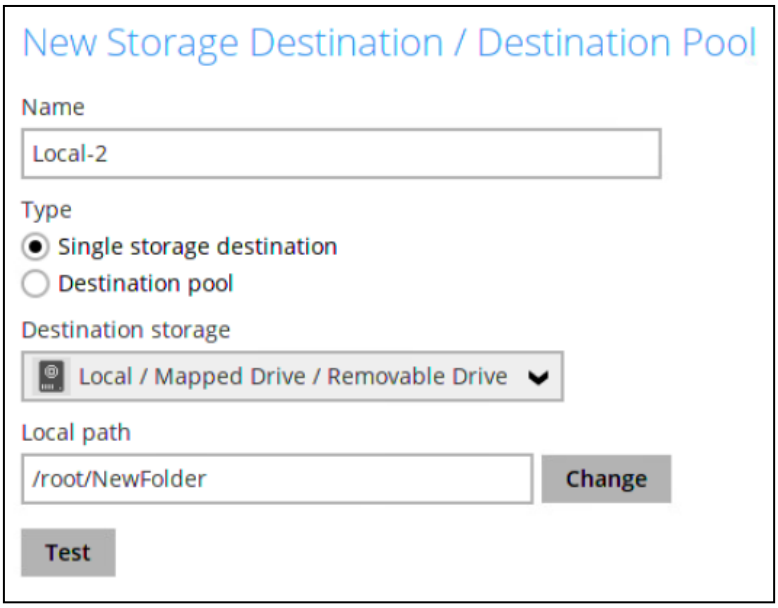
1. Click the **Add** button.



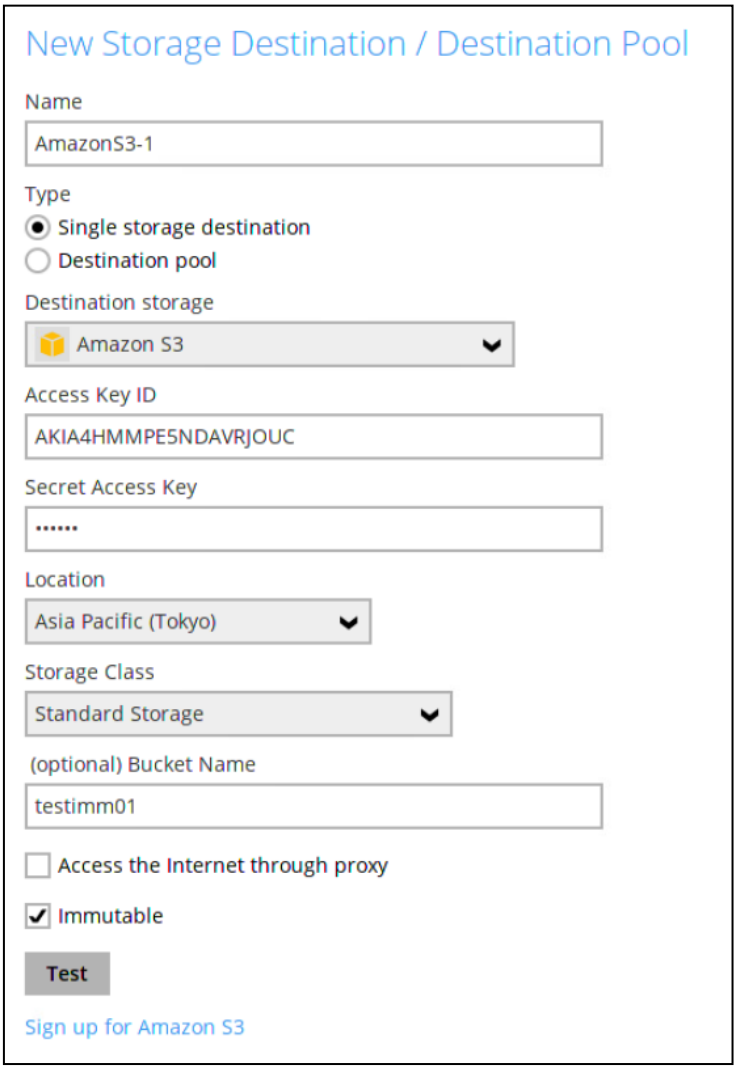
2. Click the drop-down button to select a backup destination.



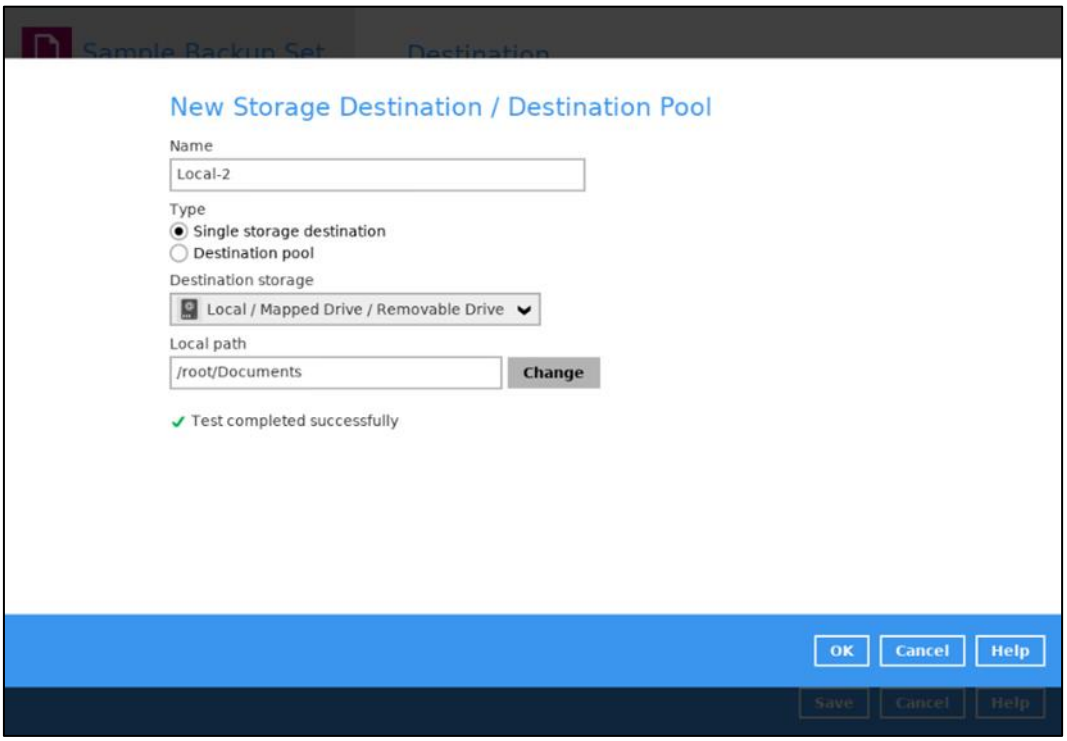
3. If the **Local / Mapped Drive / Removable Drive** is selected, click the **Change** button to select a new storage destination, then click the **Test** button to validate access to it.



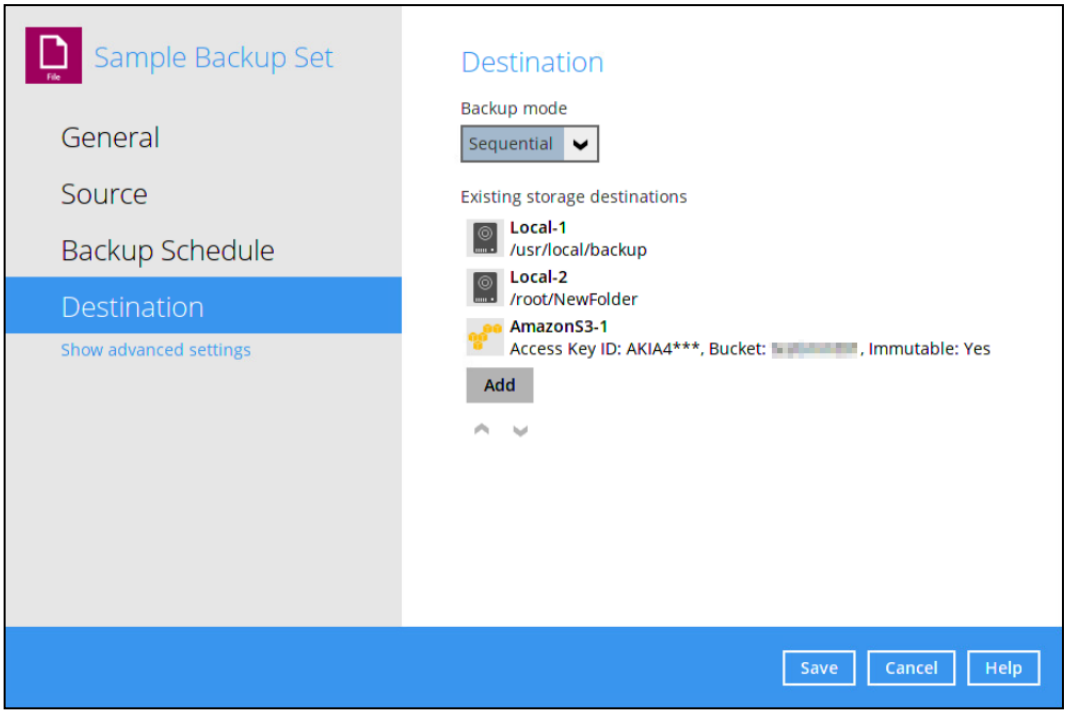
If you want to create an immutable storage destination, select one of the supported destinations then provide the needed information. Check 'Immutable' then click the **Test** button to validate access to it.



4. Click the **OK** button to save the added storage destination.



5. Click the **Save** button to store the updated backup mode and the added storage destination.



NOTE

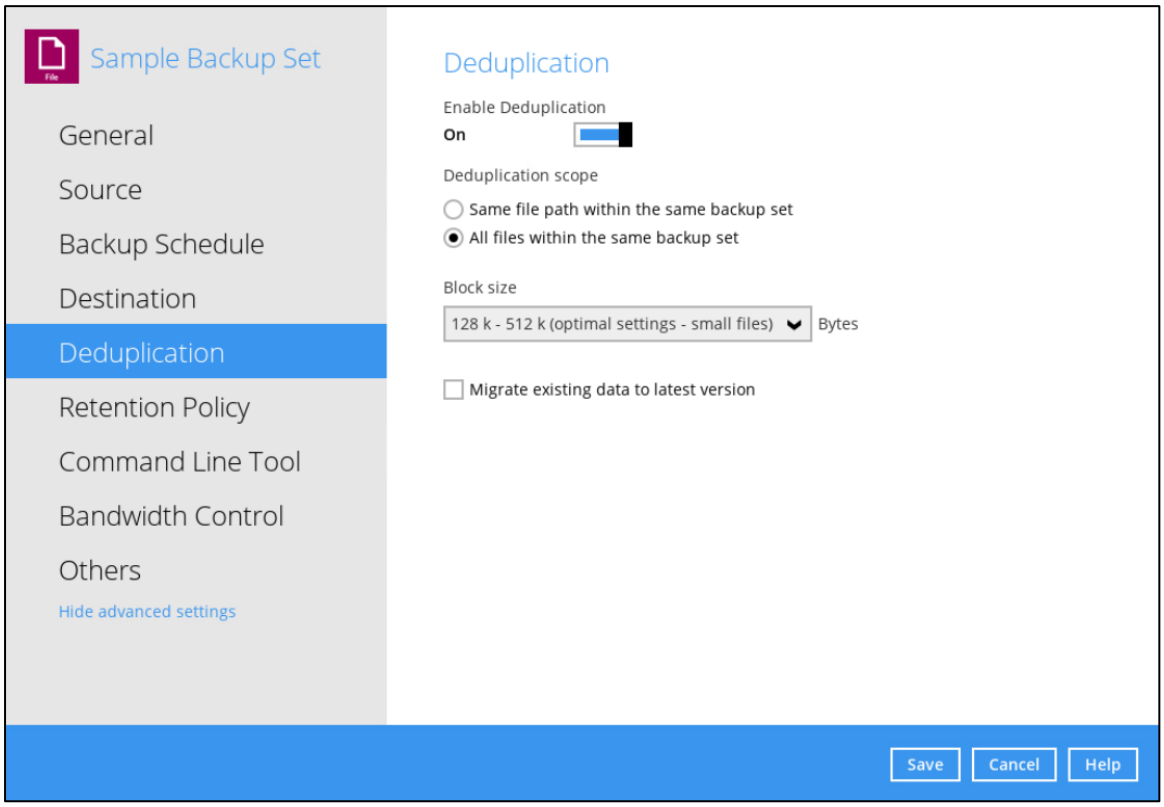
The immutable status of a destination is included in the details, it indicates whether Yes or No if the particular destination is setup as an immutable storage destination or not.

7.4.1.5 Deduplication

Starting with CloudBacko Pro v5.0.0.0 or above, the In-File Delta feature (i.e., Incremental, Differential and Full) will be replaced with Deduplication. This feature is **On (enabled)** by default.

When this feature is **On (enabled)** for the backup set, a checksum verification of each backup file which was split into several blocks of varying size will be performed to compare its content and identify which block is duplicated, thus will perform deduplication of data.

When this feature is **Off (disabled)** for the backup set, a checksum verification of each backup file will not be performed, thus the duplicated data will NOT be removed or deduplicated during a backup job.



There are two (2) types of Deduplication scope:

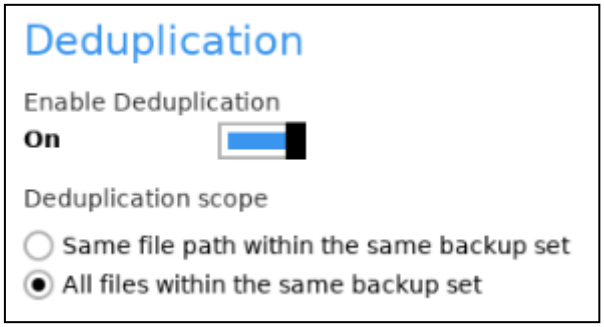
Deduplication	Description
Same file path within the same backup set	This type of Deduplication will deduplicate data under the same path during a backup job.
All files within the same backup set	This type of Deduplication will deduplicate data under the same backup set during a backup job. This option is only applicable for Meter Licenseand will be charged per storage size used.

Migrate Data

When this option is enabled, the existing data will be migrated to the latest version during a backup job. This option is disabled by default.

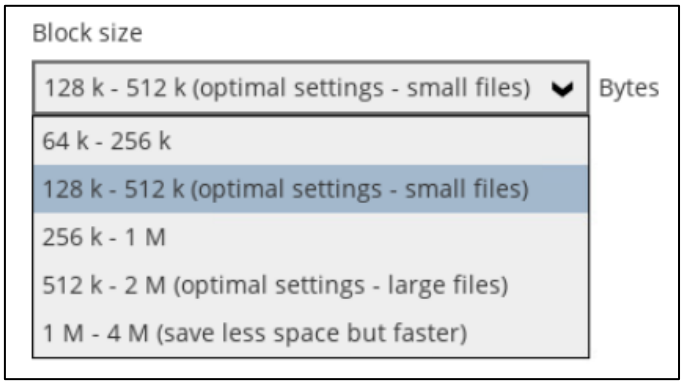
To configure the deduplication settings, follow the instructions below:

1. Select the Deduplication scope.



2. Click the drop-down button to select the block size that will be used for the deduplication data block.

   The optimal setting is good for frequently changed source data, as this is the smallest block deduplication will use to compare and determine if the data is new and should be uploaded or discarded as duplicate. The larger the deduplication block size, the less efficient it would be but faster as there are less blocks of data to create. Frequent changes to this setting is not advisable since all data may need to be reuploaded because the previous block size and new block size are now different.



3. Tick the checkbox if you want the existing data to be migrated to the latest version during a backup job.

4. Click the **Save** button to store the modified Deduplication settings.

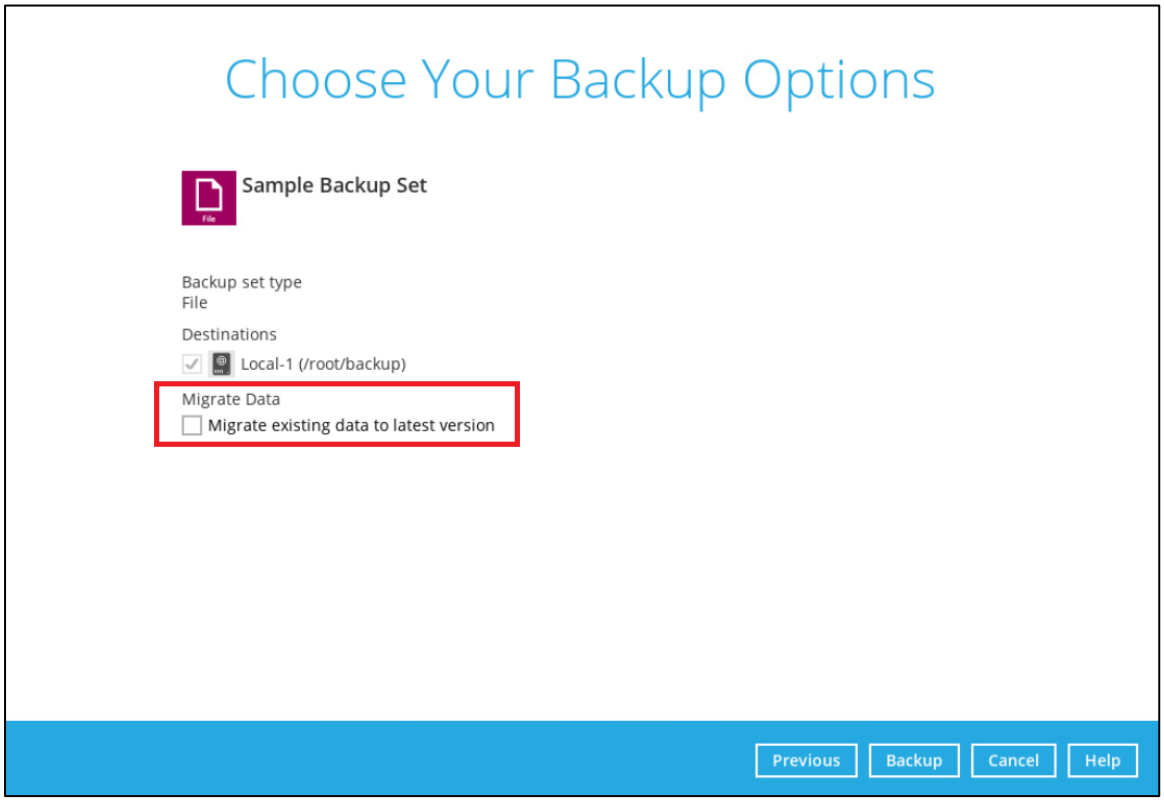
NOTE

In case the Deduplication setting is **Off (disabled)** for the backup set, the Migrate Data option will not be displayed.

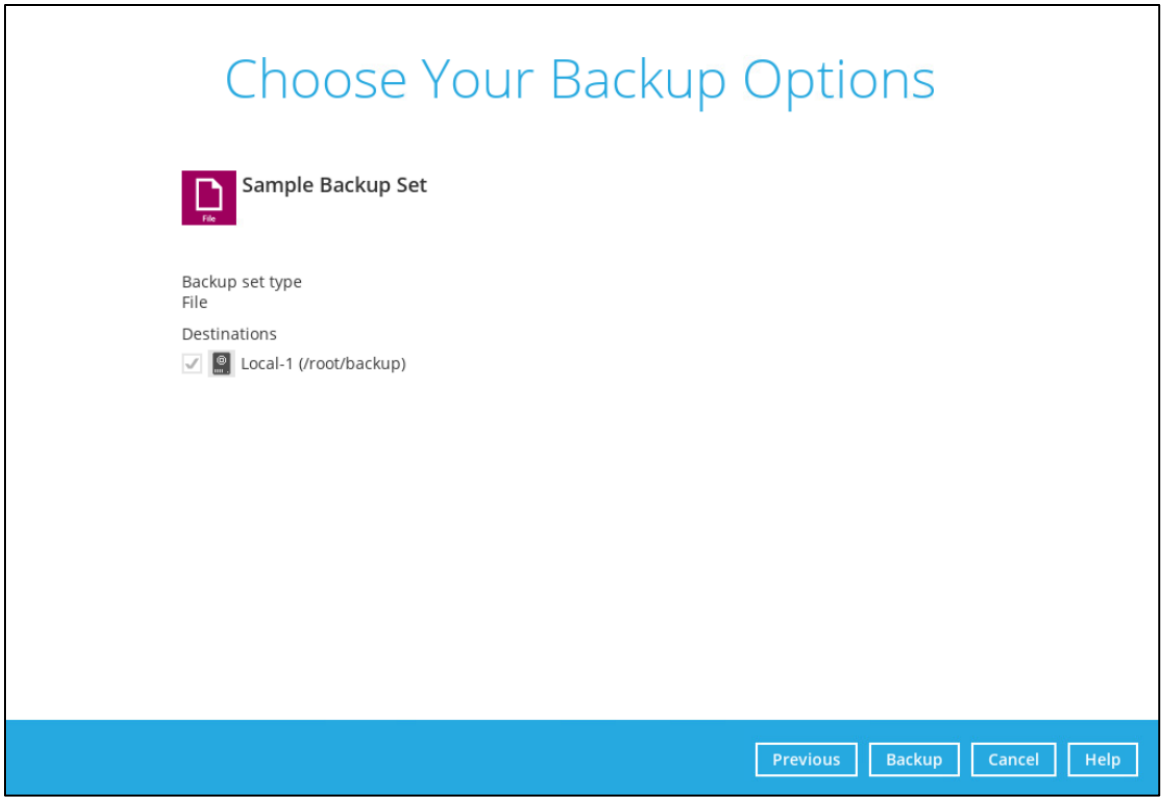
Run Backup Job

When the Deduplication feature is enabled for the backup set, a **Migrate Data** option will be available which can be configured before starting a backup job.

Below is an example of a backup set with Deduplication setting **enabled**.



Below is an example of a backup set with Deduplication setting **disabled**.



7.4.1.6 Retention Policy

When CloudBacko Pro 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.

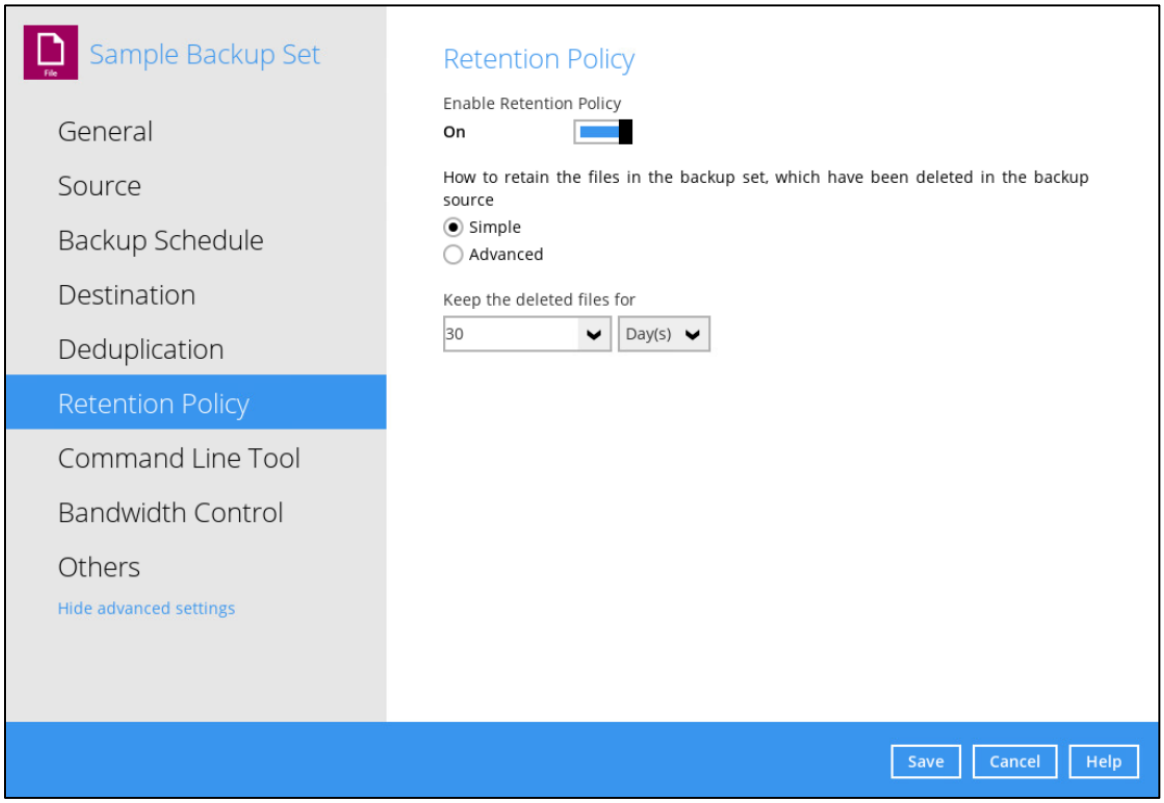
Data Area is the place where backed up files and/or folders are stored.

While the **Retention Area** is the 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.

There are two (2) different types of Retention Policy:

Type	Description
Simple	A simple retention policy is a basic policy where the retained files (in the Retention Area) are removed automatically after the user specifies the number of days or backup jobs.
Advanced	An advanced retention policy defines a more advanced and flexible policy where the retained files (in the Retention Area) are removed automatically after a combination of user defined policy.

Comparison between Simple and Advanced Retention Policy

Control	Simple	Advanced
Backup Jobs	Can keep the deleted files for specified number of backup job(s)	Not applicable
Days	Can keep the deleted files for specified number of day(s)	Can keep the deleted files for specified number of day(s)
Type	Not applicable	➢ Daily ➢ Weekly ➢ Monthly ➢ Quarterly ➢ Yearly ➢ Custom
User-defined name	Not applicable	Applicable

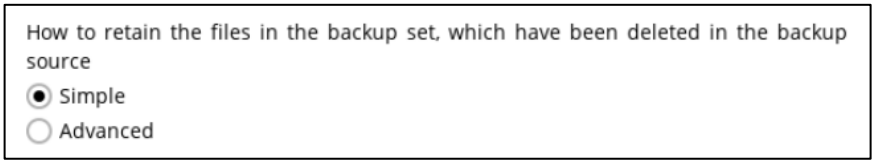
WARNING

When files and/or folders in the retention area exceed the Retention Policy setting, they are permanently removed from the backup set and cannot be restored

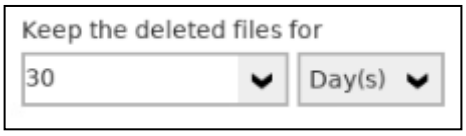
To configure a **Simple Retention Policy**, follow the steps below:

1. Slide the switch to the right to turn on **Enable Retention Policy**.

2. Select “Simple” from how to retain the files.



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.

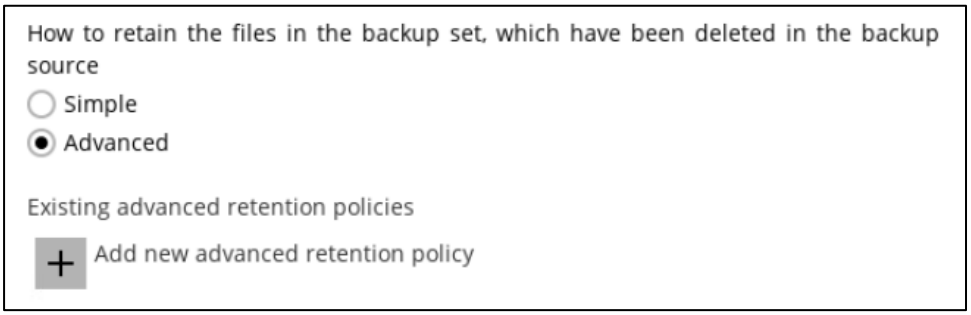


4. Click the **Save** button to store the configured retention policy.

To configure an **Advanced Retention Policy**, follow the steps below:

1. Slide the switch to the right to turn on **Enable Retention Policy**.

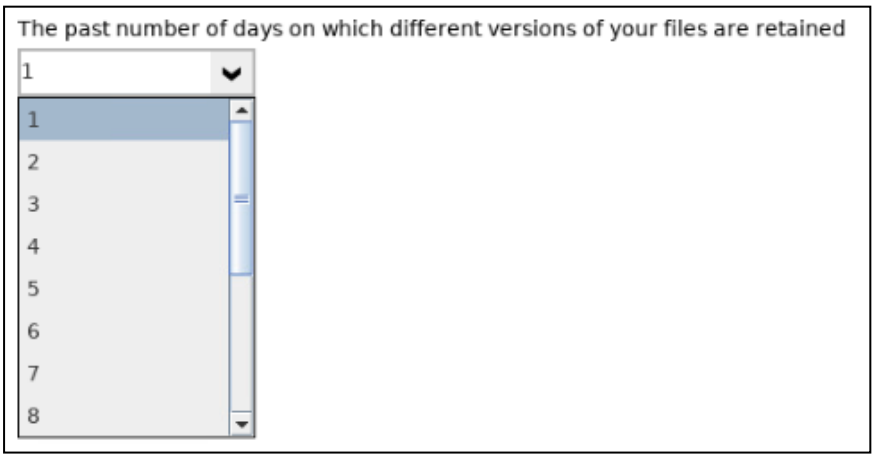
2. Select “Advanced” from how to retain the files, then click “**+**” to add a retention policy.



3. Enter a name for the Retention Policy.

4. Select a type.

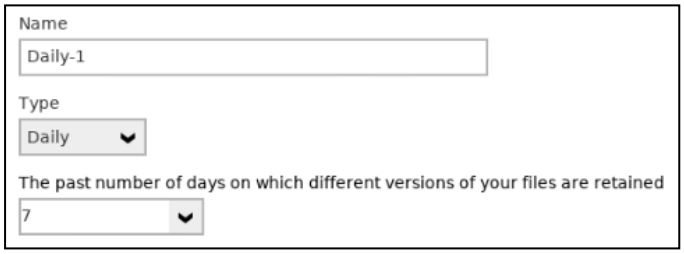
5. Select the number of days the deleted files will be kept in retention.



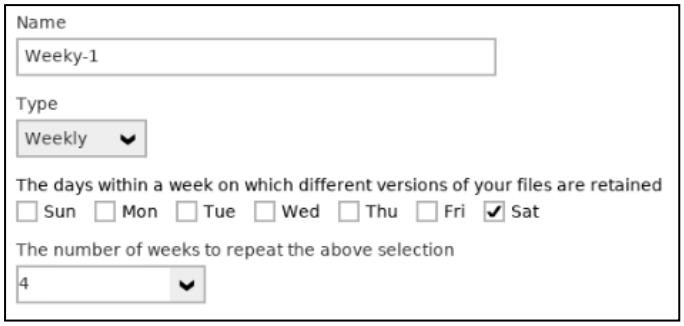
6. Click **OK** to save the advanced Retention Policy, then click **Save** to store the settings.

For further details about how to configure an advanced Retention Policy for each type (i.e., Daily, Weekly, Monthly, Quarterly, Yearly), refer to the examples below:

- **Example no. 1**: To keep the retention files for the last seven (7) days:

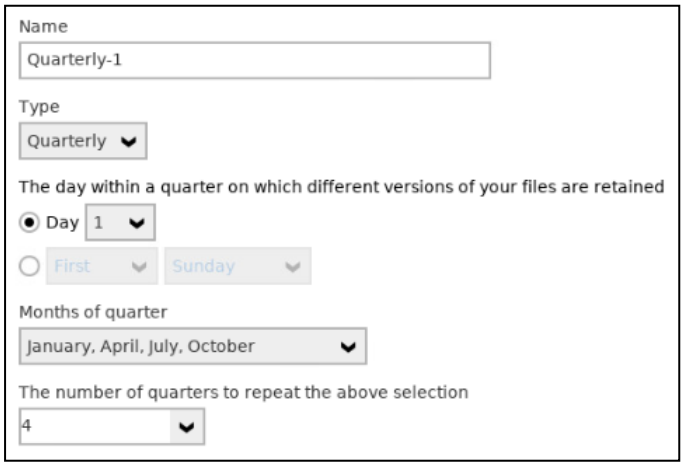


- **Example no. 2**: To keep the retention files for the last four (4) Saturdays:

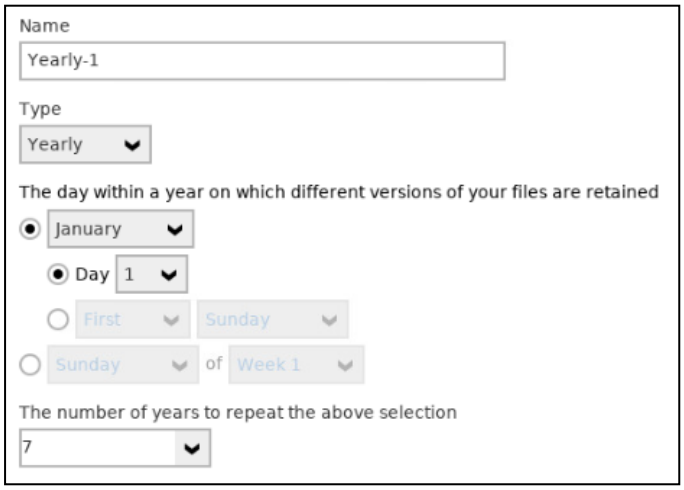


- **Example no. 3**: To keep the retention files for the 1st day of each month for the last three (3) months:

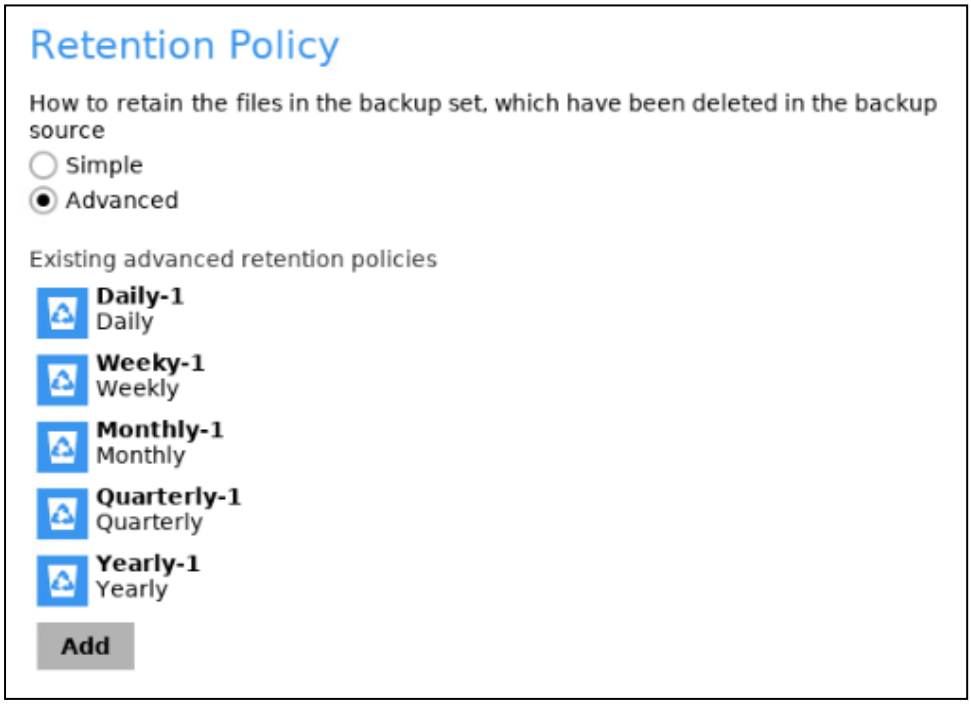
- **Example no. 4**: To keep the retention files for the 1st day of each quarter for the last four (4) quarters:



- **Example no. 5**: To keep the retention files for the 1st day of each year for the last seven (7) years:



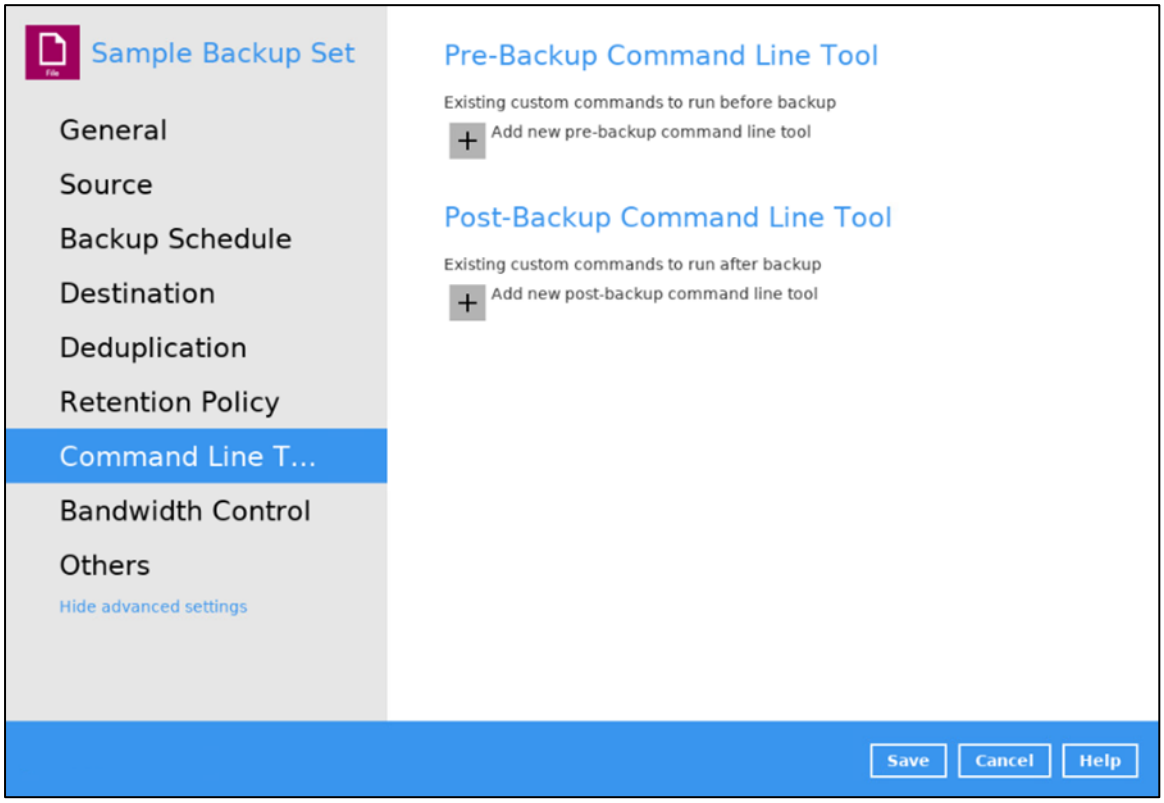
Multiple Advanced Retention Policy can be created.



7.4.1.7 Command Line Tool

This feature allows the user to configure a pre-backup or post backup command which can be; an operating system level command, a script or batch file, or third-party utilities to run before and/or after a backup job.

e.g. Connecting to a network drive and disconnecting a network drive, stopping a third-party database (not officially supported by CloudBacko Pro) to perform a cold backup, and restarting a third-party database after a backup.



Requirements and Best Practices

- **Error and Exception Handling**

  Each pre-backup command or batch file should have an error and exception handling. If a pre-backup command contains an error, although an unhandled error may not hinder the backup job process, and the backup job is successful, it will result to a status indicating completed backup with warning(s).

  For more details about backup report status, please refer to Backup Reports in Chapter 7.5 CloudBacko Pro Overview.

- **Command or Batch File Compatibility**

  Make sure that each command (pre-backup and post-backup) are tested thoroughly before including them to the backup job.

- **Scheduled Backup**

  If the scheduled backup job is set to stop after x no. of hours, make sure that the duration of the running backup job will not be affected. You may need to adjust the number of hours in the backup schedule configuration. Please refer to Backup Schedule for more details.

- **Pre-backup Command Limitation**

  A reboot or shutdown must not be used in the pre-backup command. Otherwise, the machine will shut down immediately that will result to a status indicating “Backup not yet finished”.

- **Post-backup Command Recommendation**

  It is recommended to include a timeout for a post-backup command to shut down the machine. This is to ensure that the CloudBacko Pro has enough time to complete the backup process.

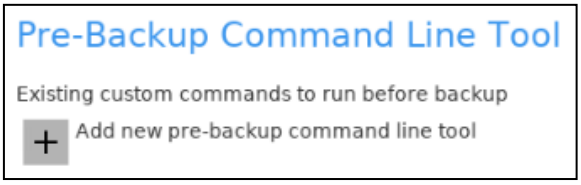
There are three (3) fields in the command line tool:

Field	Description
Name	The user-defined name of the pre-backup or post-backup command.
Working Directory	The location in the local machine which the pre-backup or post-backup command will run at, or the location of the command or created batch file.
Command	The **pre-backup** or **post-backup** command which can be defined as a native command or batch file.

Pre-backup Command Line Tool

A pre-backup command is used to execute an action or process before the start of a backup job. To create a pre-backup command, follow the steps below:

1. Click the add **+** button to add a new pre-backup command line too.



2. Complete the following details:

   - **Name**

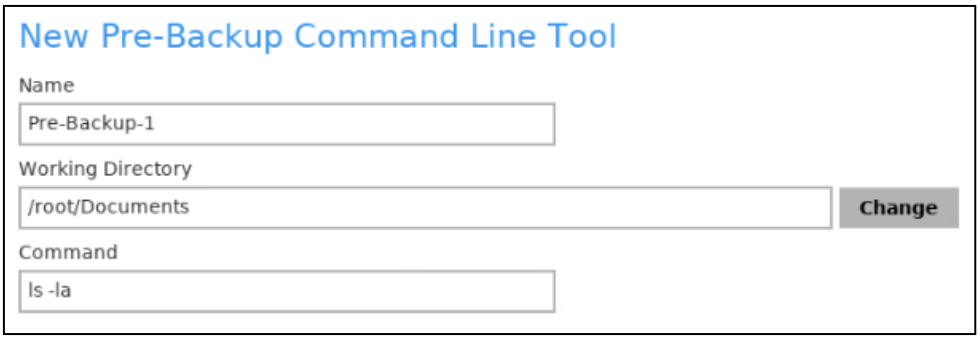
     Assign a desired name to the pre-backup command.

   - **Working Directory**

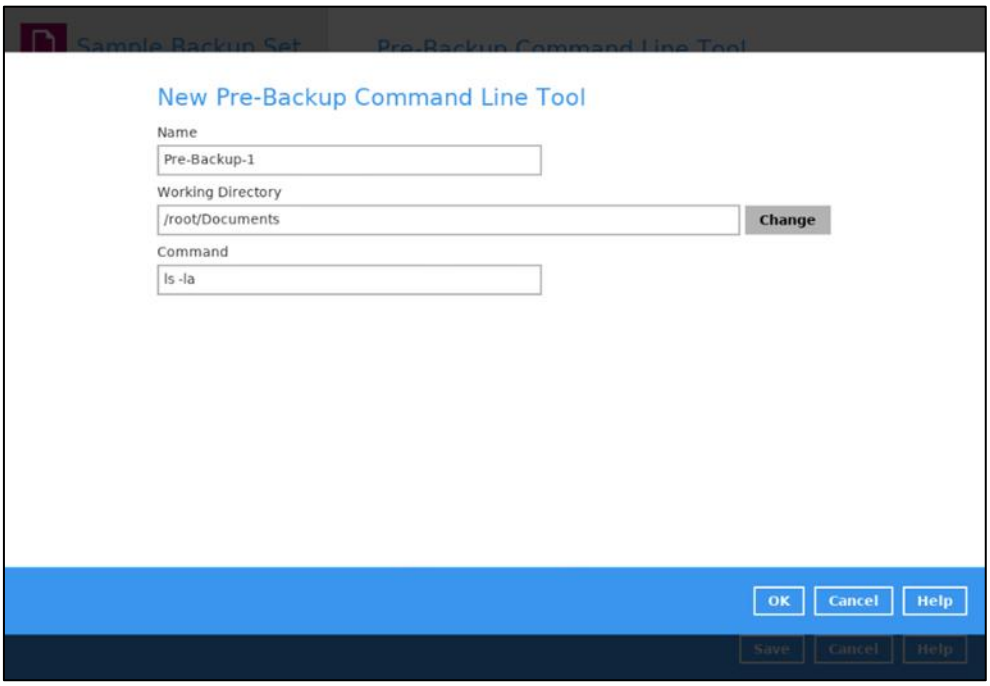
     Click the **Change** button to locate the working directory of the command.

   - **Command**

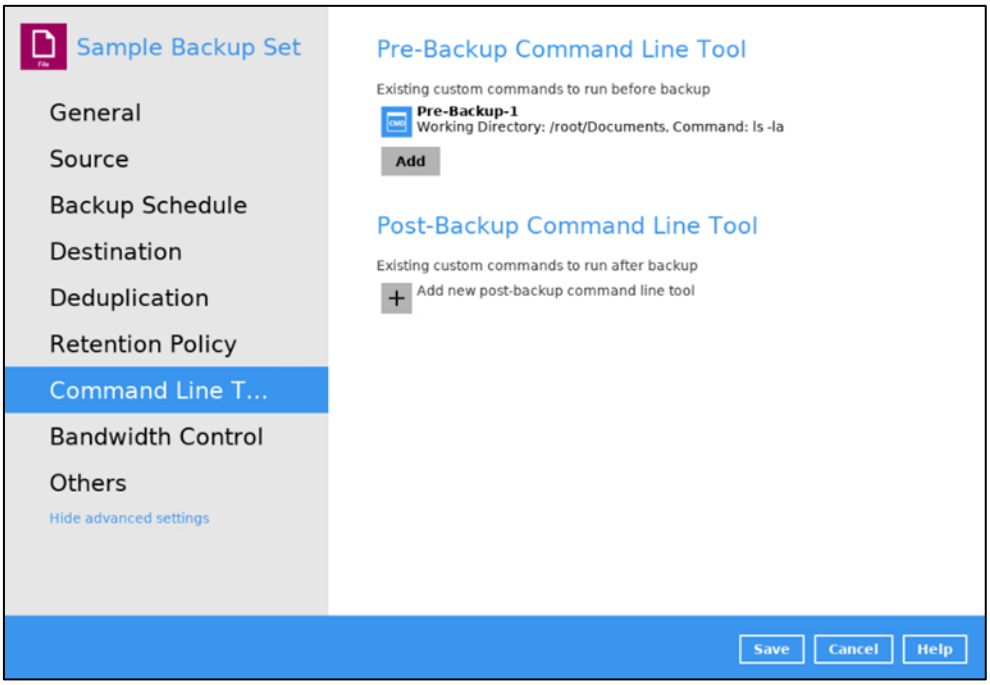
     Input a command to be run before a backup job. In this example, the pre-backup command will display the list of the directories.



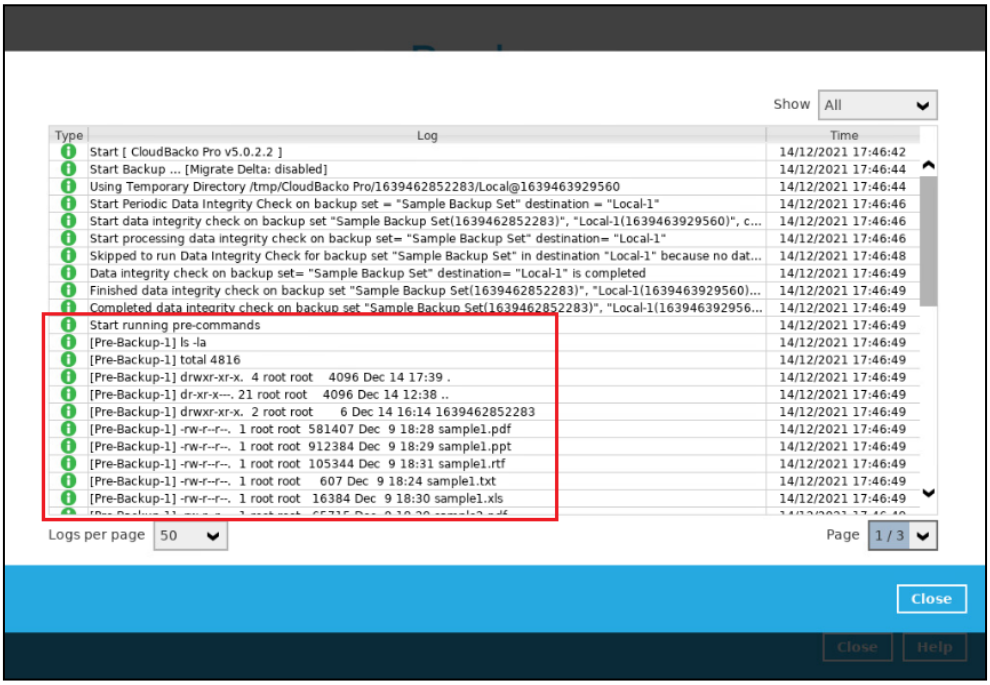
3. Click the **OK** button to save the created pre-backup command.



4. Click the **Save** button to save the settings.



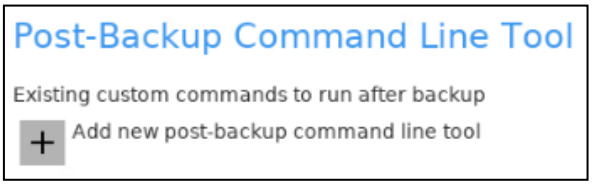
5. Once the backup job is complete, click the button to display the backup report log where you can check if the pre-backup command is successful.



Post-backup Command

A post-backup command is used to execute an action or process after a backup job. To create a post-backup command, follow the steps below:

1. Click the add **+** button to add a new post-backup command line too.



2. Complete the following details:

   - **Name**

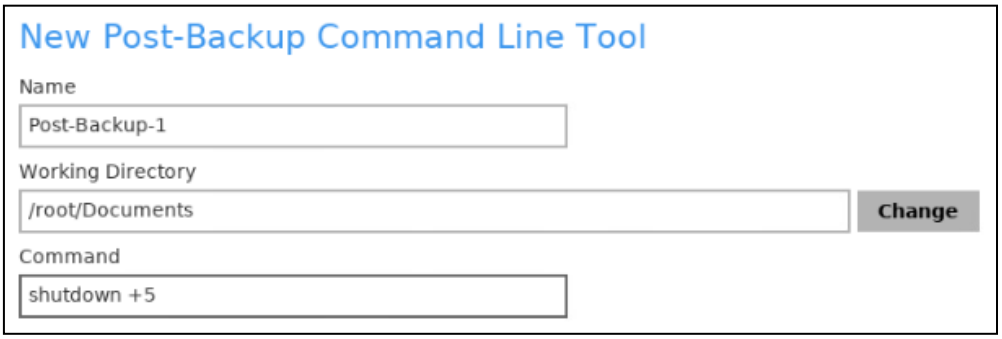
     Assign a desired name to the post-backup command.

   - **Working Directory**

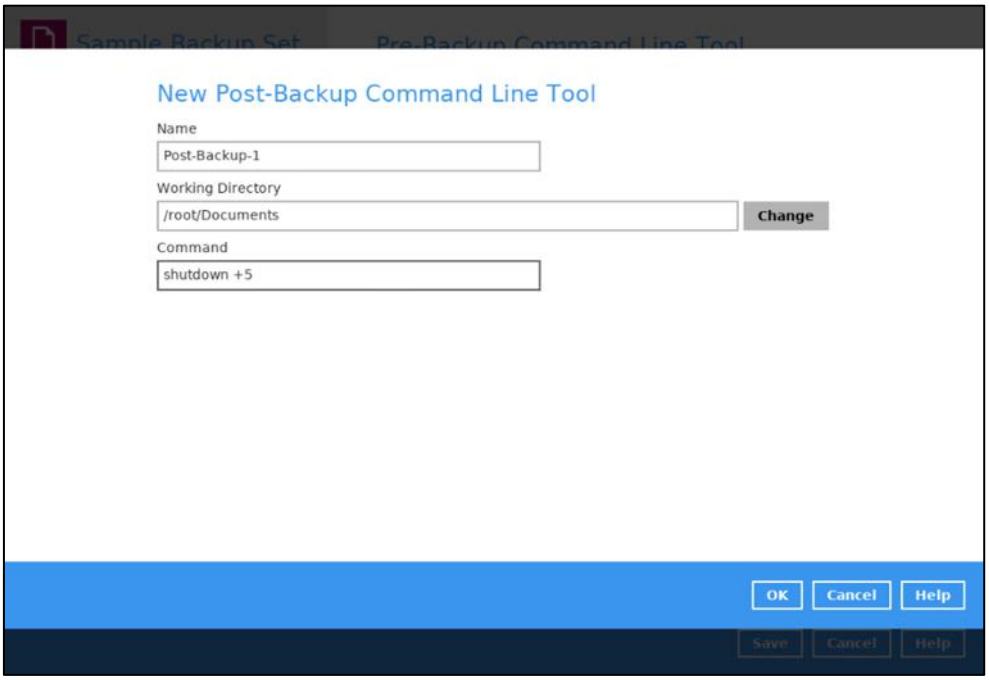
     Click the **Change** button to locate the working directory of the command.

   - **Command**

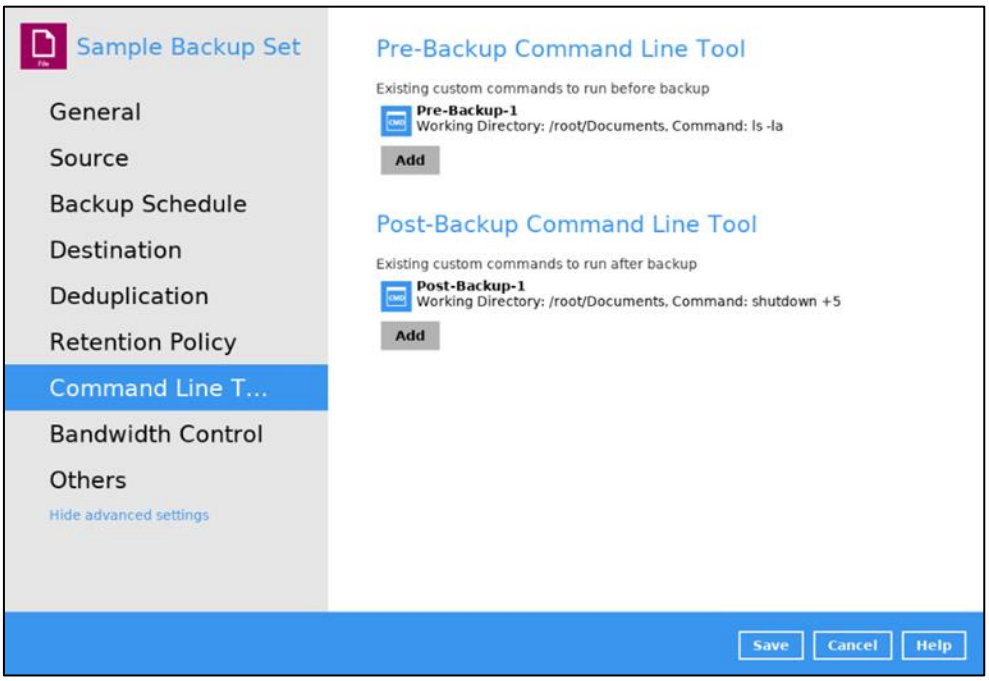
     Input a command to be run after a backup job. In this example, the post-backup command will display the list of the directories.



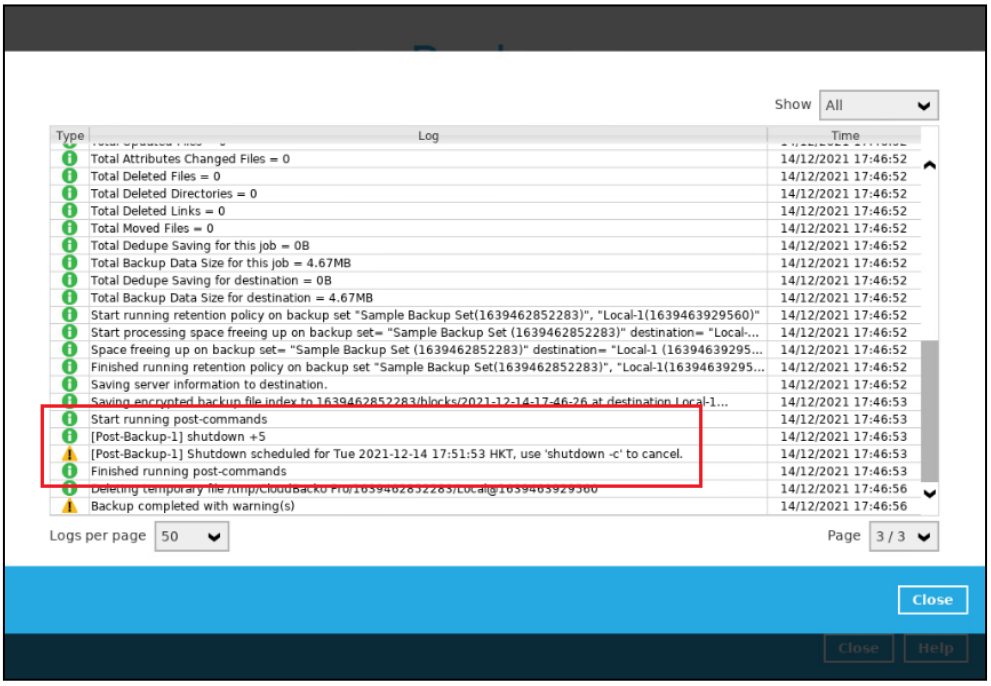
3. Click the **OK** button to save the created post-backup command.



4. Click the **Save** button to save the settings.

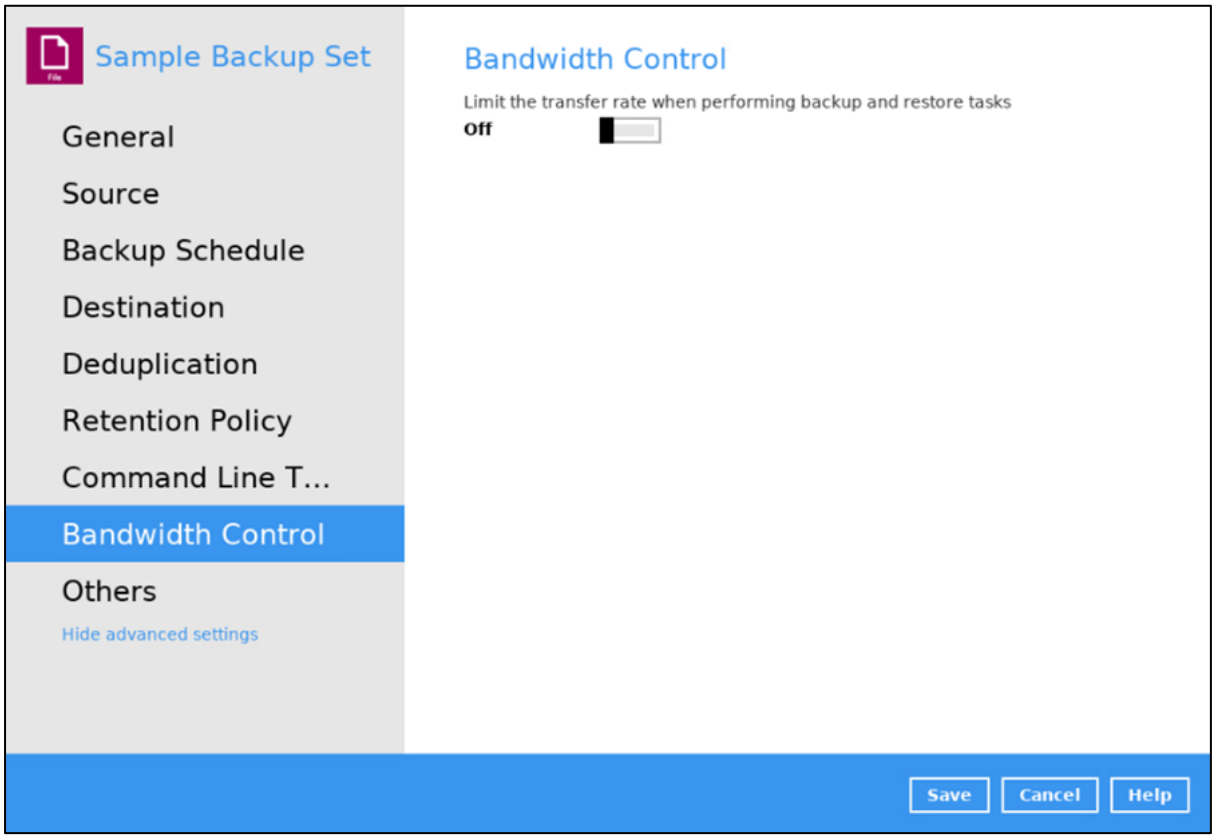


5. Once the backup job is complete, click the  button to display the backup report log where you can check if the post-backup command is successful.



7.4.1.8 Bandwidth Control

This feature allows the user to limit the amount of bandwidth used by backup traffic between specified times. This bandwidth control is configured as disabled by default.



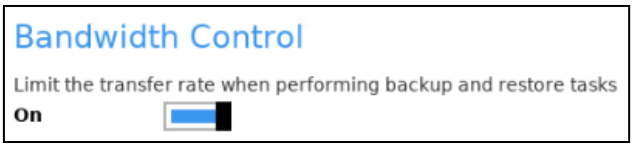
There are two (2) types of bandwidth control:

Bandwidth Control Type	Description
Independent	Each backup and restore has its assigned bandwidth.
Share	All backup and restore operations are sharing the same assigned bandwidth.

NOTE
Share mode does not support performing backup job on multiple destinations concurrently.

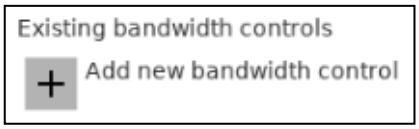
To enable the bandwidth control setting, follow the steps below:

1. Slide the lever to the right to turn on the bandwidth control.



2. Select a bandwidth control mode.

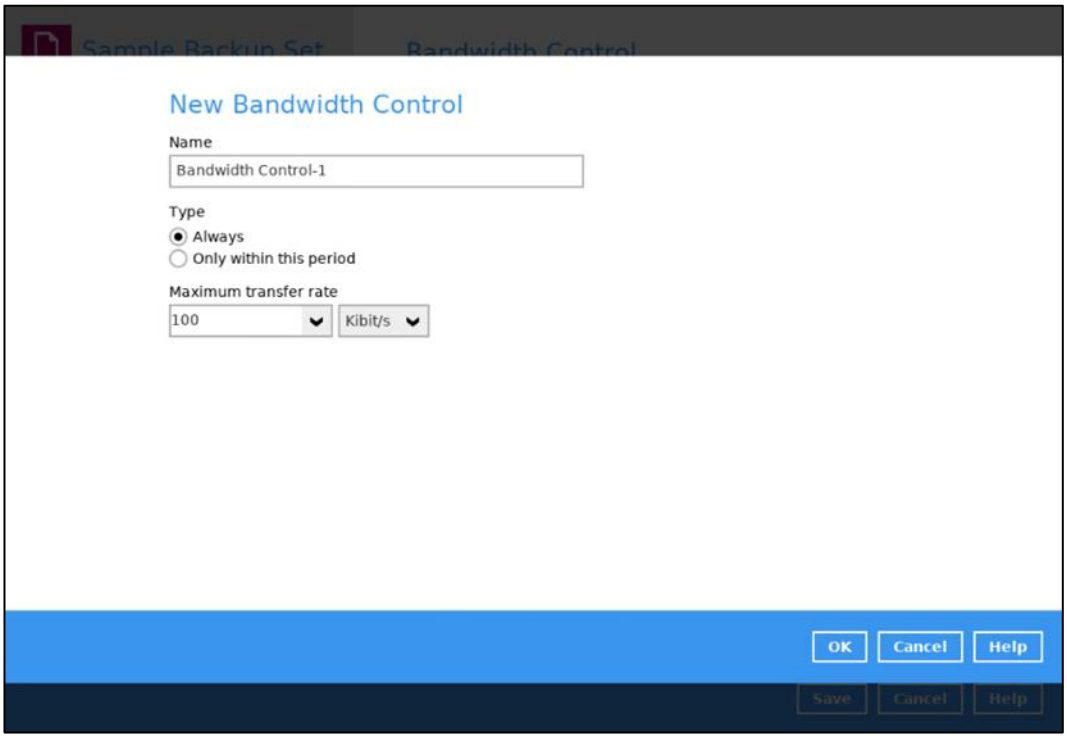
3. Click the **Add** button to create a modified bandwidth control.



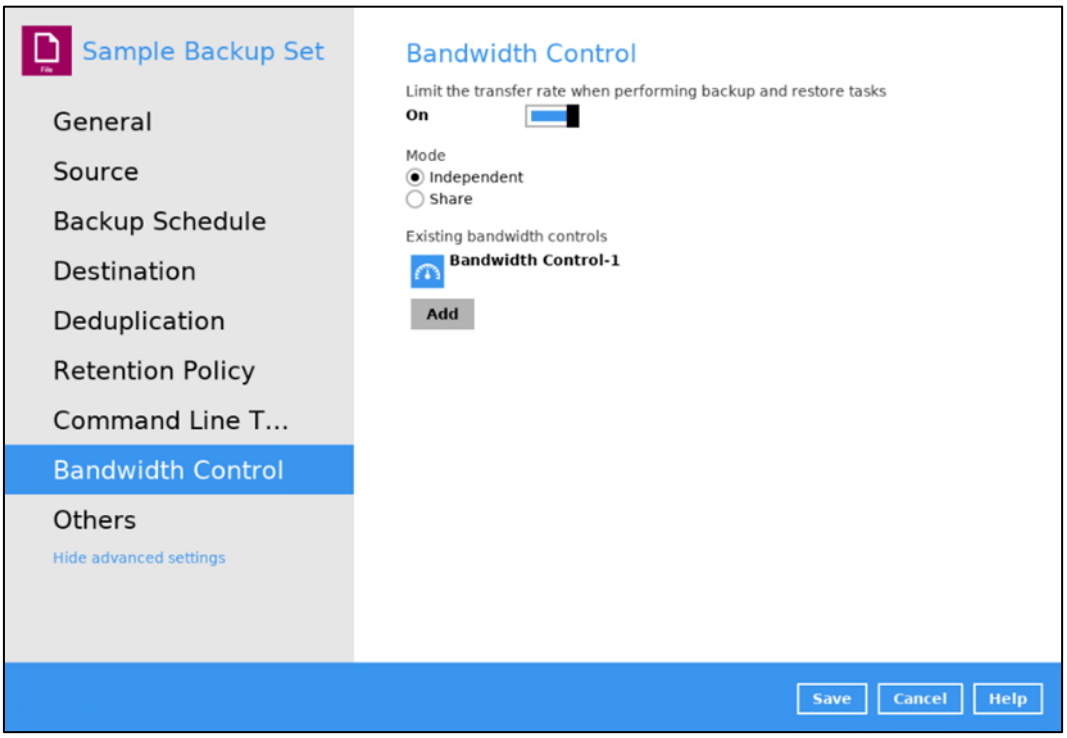
4. Complete the following fields then click the **OK** button to save the new bandwidth control.

- **Name**
- **Type**
- **Maximum transfer rate**

Field	Description
Name	The name of the bandwidth control set.
Type	The type of enforced bandwidth control period.
Maximum transfer rate	The maximum bandwidth used.



5. Click the **Save** button to store the settings.



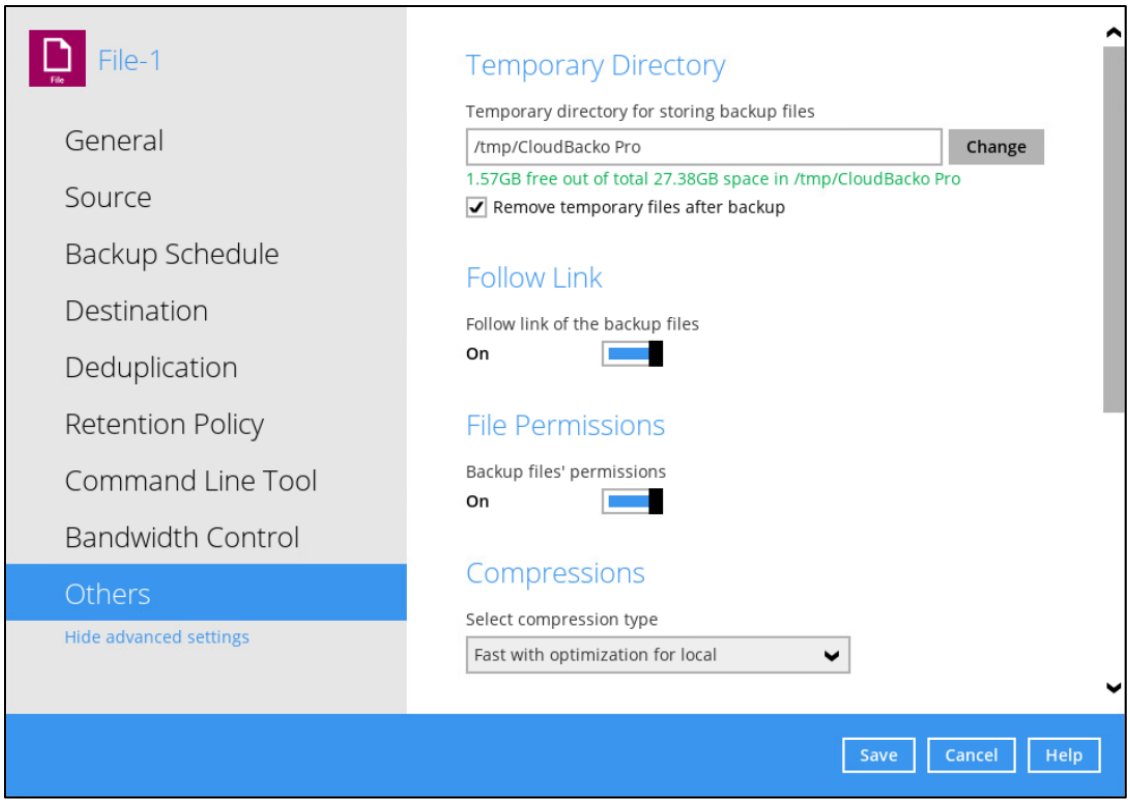
7.4.1.9 Others

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

- Temporary Directory
- Follow Link
- File Permissions
- Compressions
- Encryption
- Recycle Bin
- Restore Drill

Temporary Directory

The CloudBacko Pro 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.

NOTE

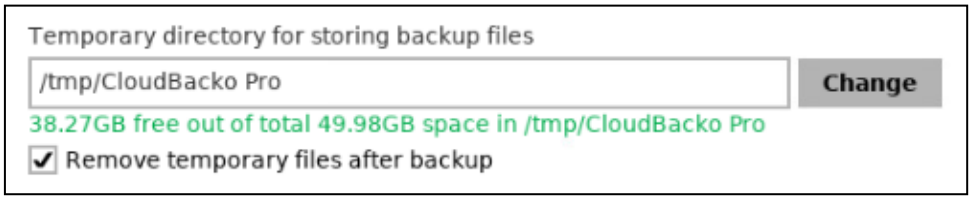
For best practice, the temporary directory should be located on a local drive for optimal backup and restore performance.
And should not be located on:

- System drive, as the System drive is used by Windows 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:

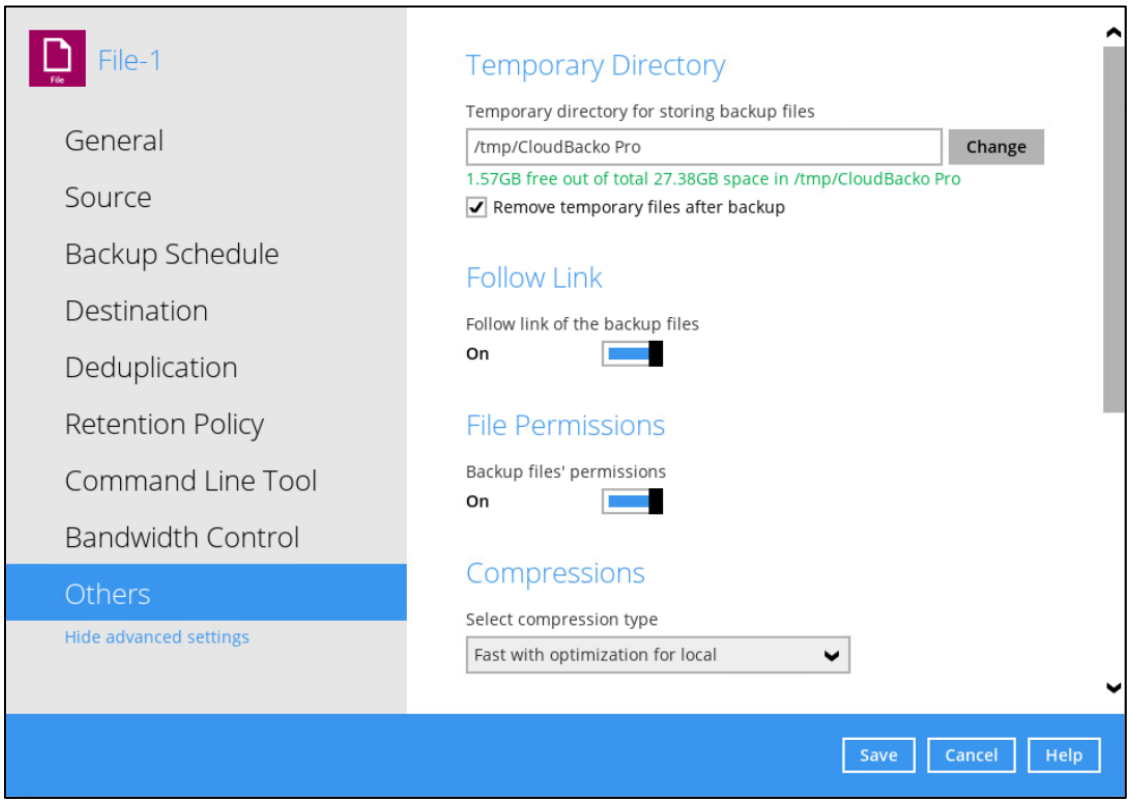
1. Click the **Change** button to select a directory path for storing temporary data.



2. Click the **Save** button to store settings.

Follow Link

This feature allows the user to enable or disable the follow link which defines the NTFS junction or symbolic link during a backup job. This feature is configured as enabled by default.

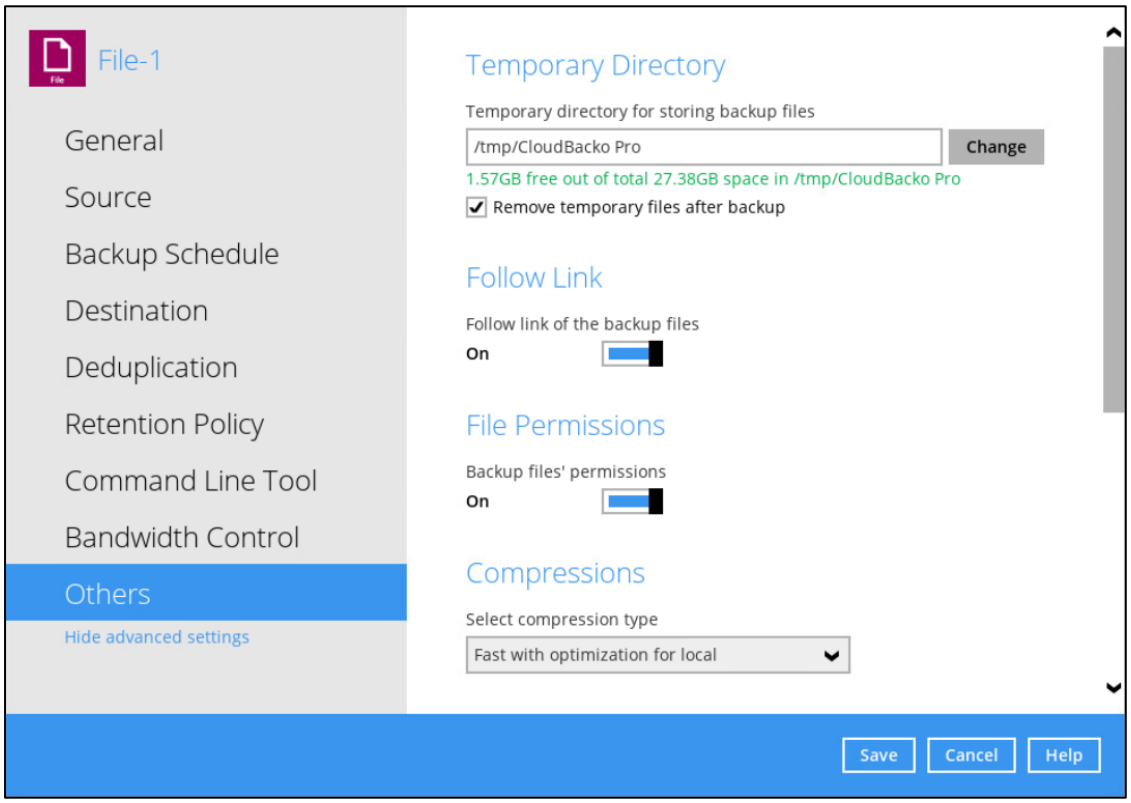


NOTE

The Follow Link feature is only applicable for File Backup Sets.

File Permissions

This allows the user to enable or disable the backup file permission which backups the operating system file permission of the data selected as backup source. This option is enabled by default.



1. Slide the lever to the right to turn on the File Permissions option. Otherwise, slide to the left to turn it off.

2. Click the **Save** button to save the settings.

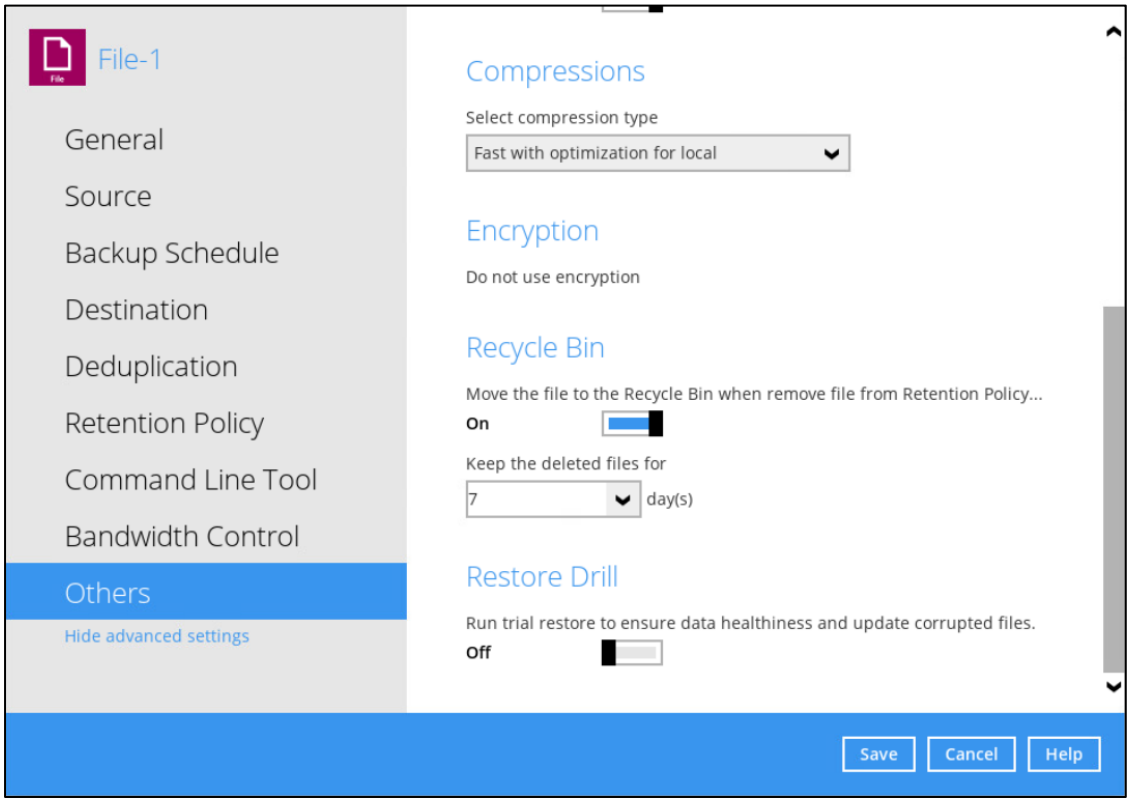
NOTE
Applicable for File Backup Sets only

Compressions

This feature is used to enable compression of data during a backup job. When the compression is enabled, the CloudBacko Pro will compress all the files before it is backed up to the backup destination(s). Newly create backup sets are configured to use **Fast with optimization for local**.

These are the four (4) compression types:

- **No Compression** - No compression of file will be made
- **Normal** - Compressed file size is the smallest but with high CPU usage
- **Fast** - Compressed file size is larger than Normal Compression but with lower CPU usage
- **Fast with optimization for local** - Compressed file size is larger than Fast Compression but with the lowest CPU usage

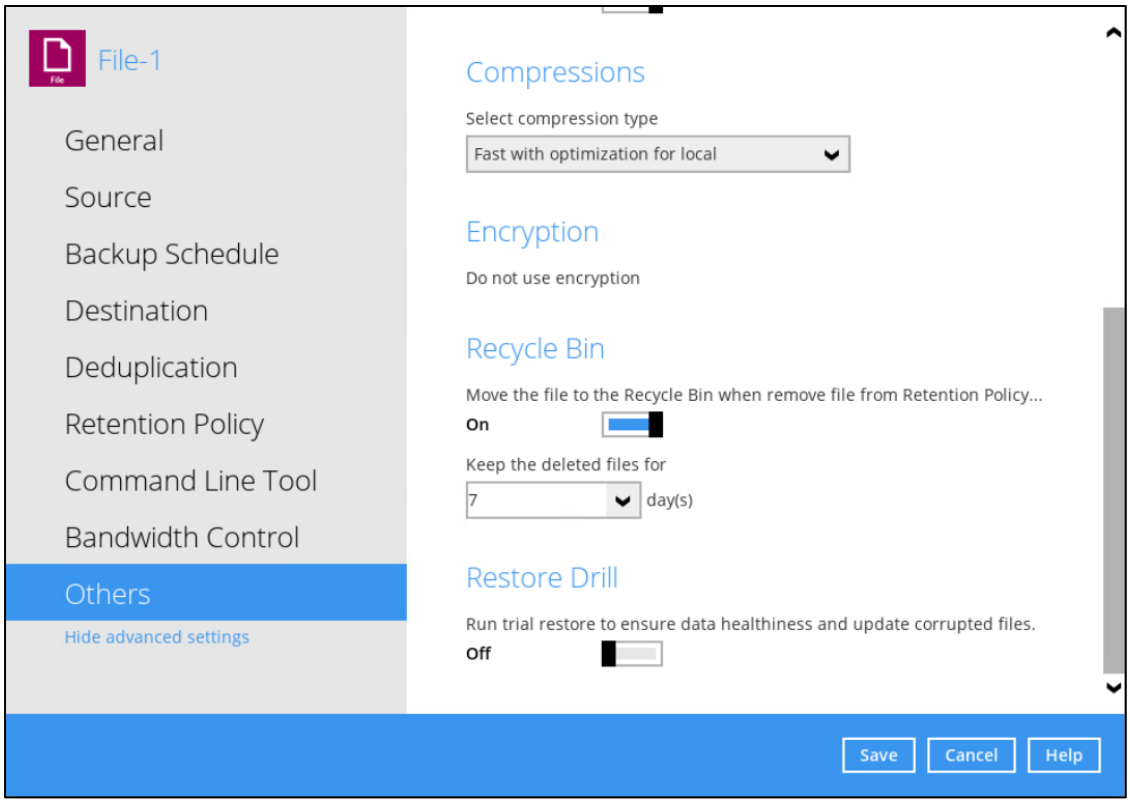


NOTE

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.

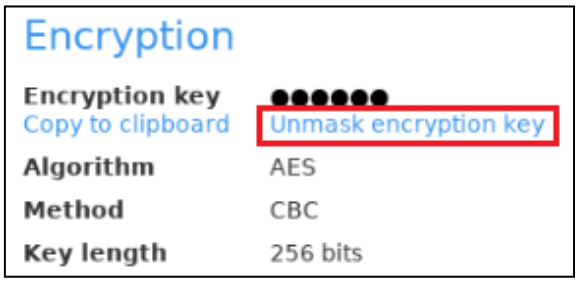
Encryption

This feature allows the user to view the encryption settings.



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

1. Click **Unmask encryption key** to display the encryption key of the backup set.



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

Recycle Bin

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

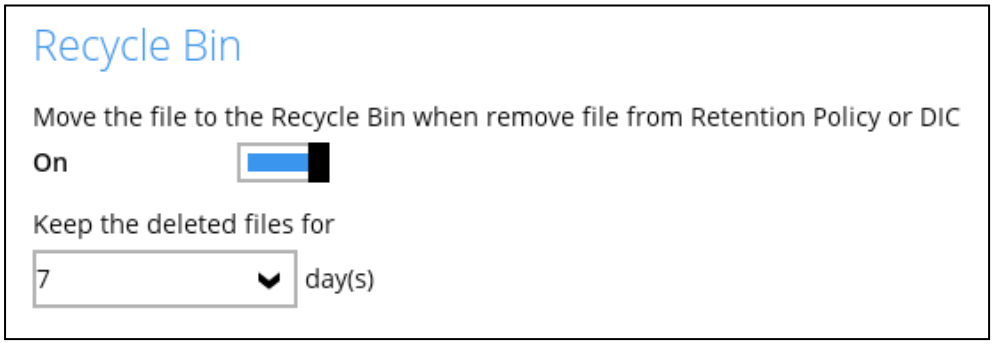
This is how the Recycle Bin will treat deleted data:

- Data in the Recycle Bin will consume Quota.
- It does not move the data in another location within the storage, instead the index tracks xxxxxx.bak files and its 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

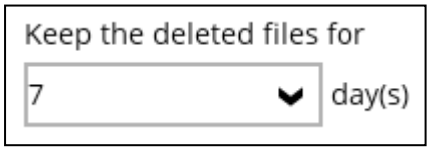
When reverting index, new data will be lost.

This is enabled by default set with 7 days.



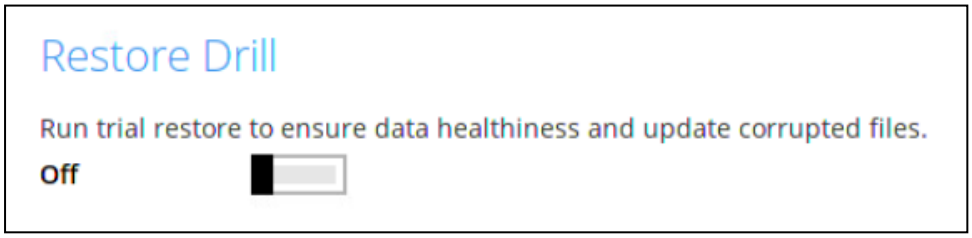
To set the number of days, follow the steps below:

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

This feature is used to run a trial restore to detect corrupted data. It helps to ensure that backup data is always restorable since it will alert users regarding the corrupted data, which requires running the backup job either manually or via schedule to fix.



To configure the restore drill, follow the instructions below:

1. Go to Backup Sets, then select a backup set.
2. Click the **Others** tab in the backup set settings.
3. Enable the Restore Drill by sliding the lever to the right.
4. Select the interval in months when the restore drill will run.

5. Click **Save** to apply the settings.

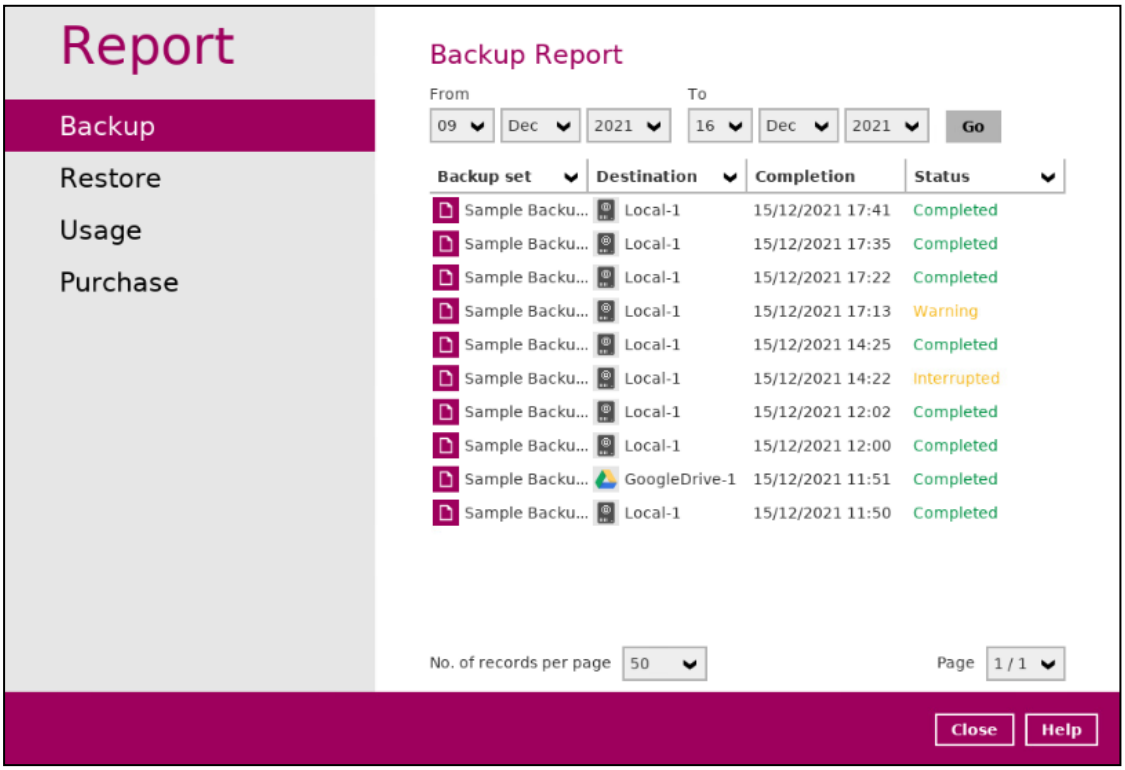
In order to receive an email report after a restore drill job was run, ensure that you have set up your email in Settings > Email Report. For more information on how to do this please refer to Ch. 7.7.2 Email Report. The report received will depend on this setting.

7.5 Report

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

There are four (4) options available for this feature, namely:

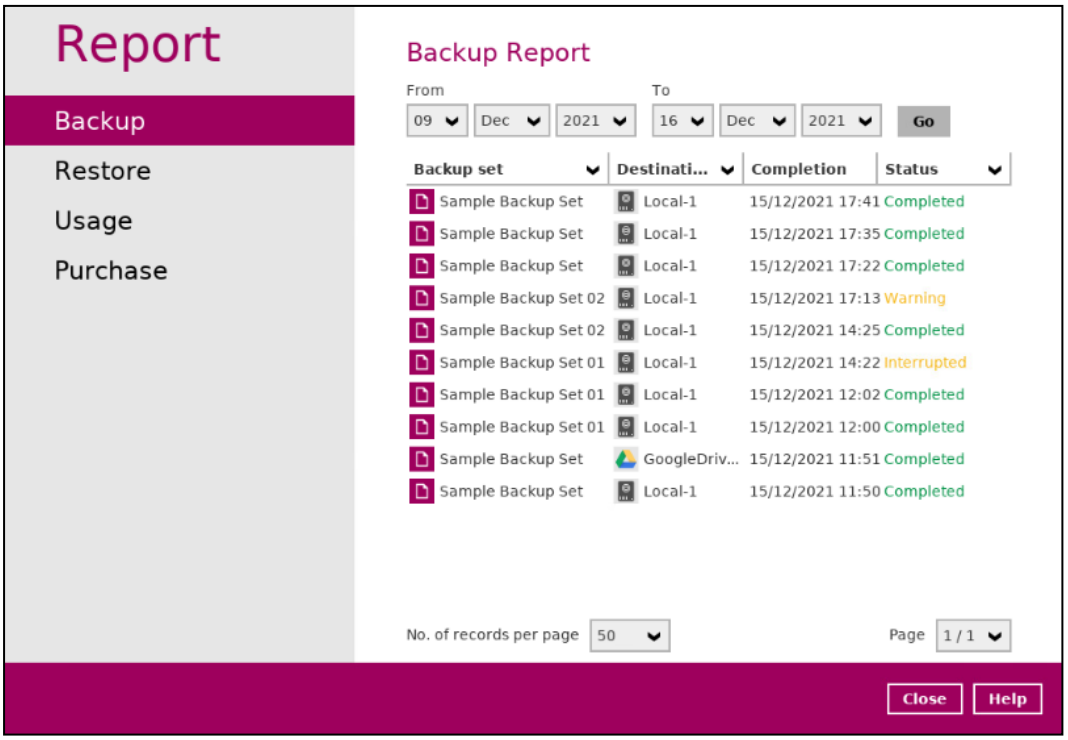
- Backup
- Restore
- Usage
- Purchase



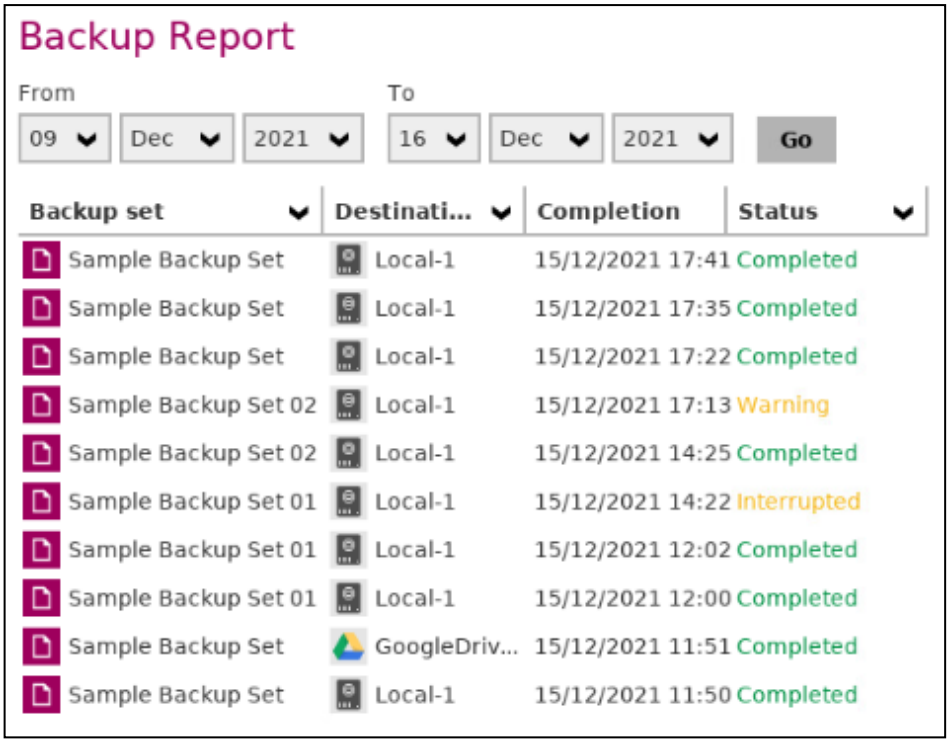
7.5.1 Backup

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

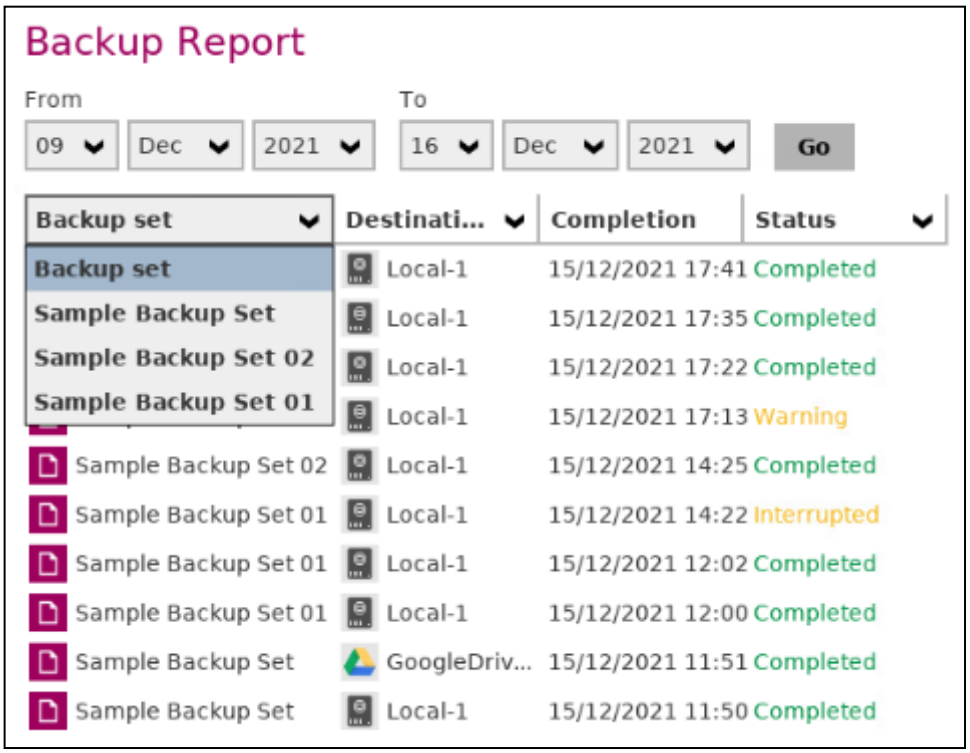
- Date range
- Backup set
- Destination
- Status



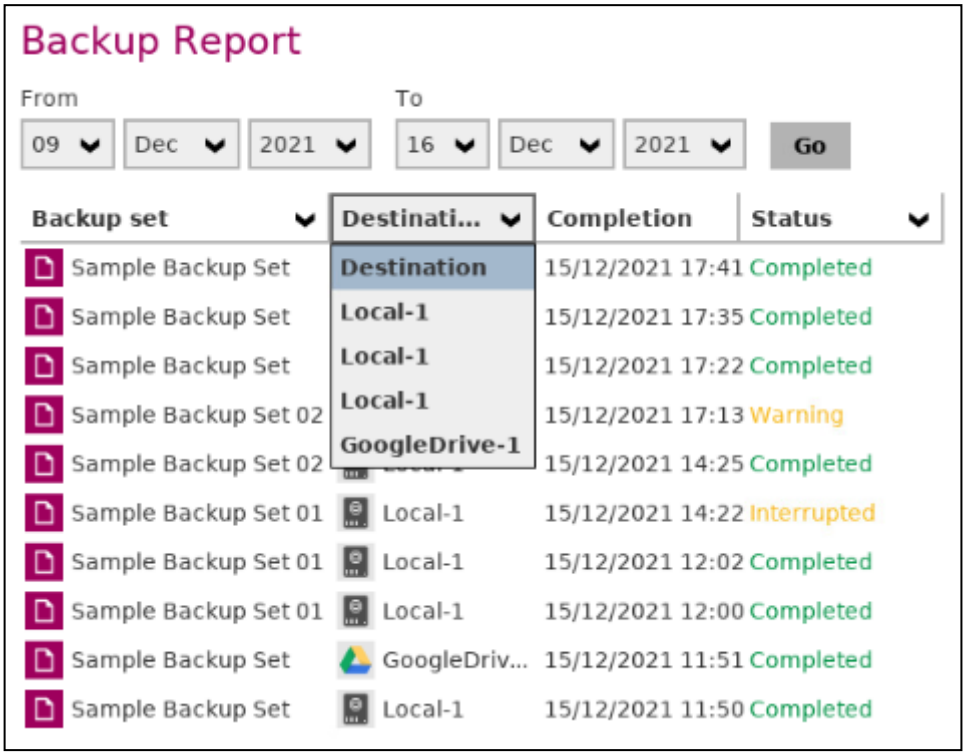
By setting the **Date range**, you will see the list of all backup report(s) within that period.



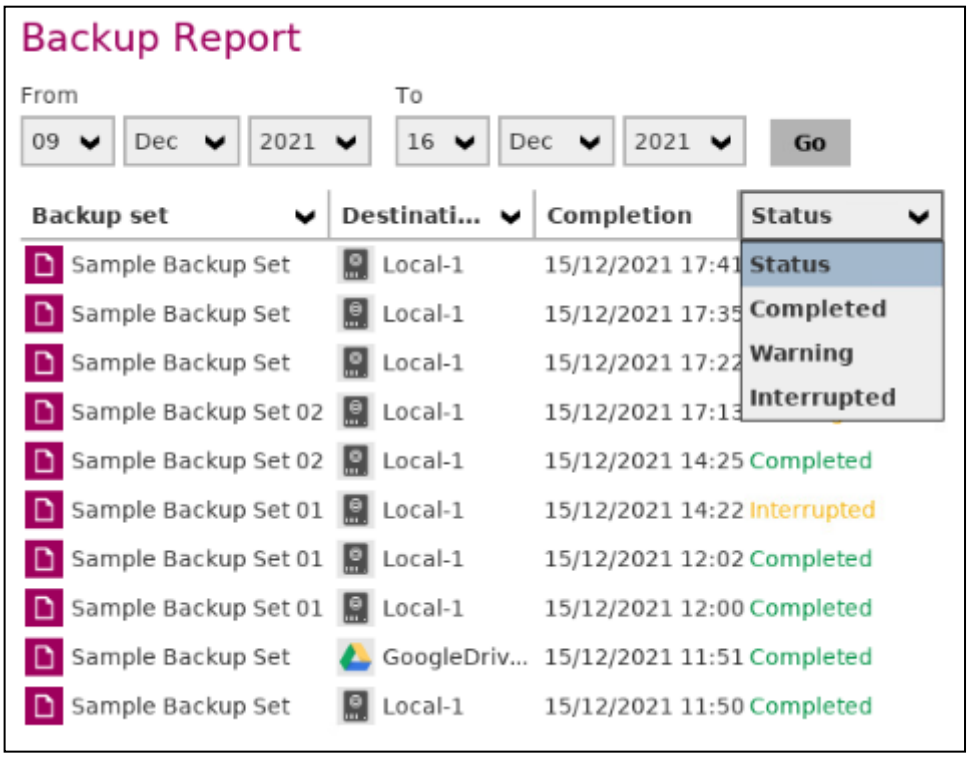
You can view the backup report(s) of a specific backup set by using the **Backup set** filter.



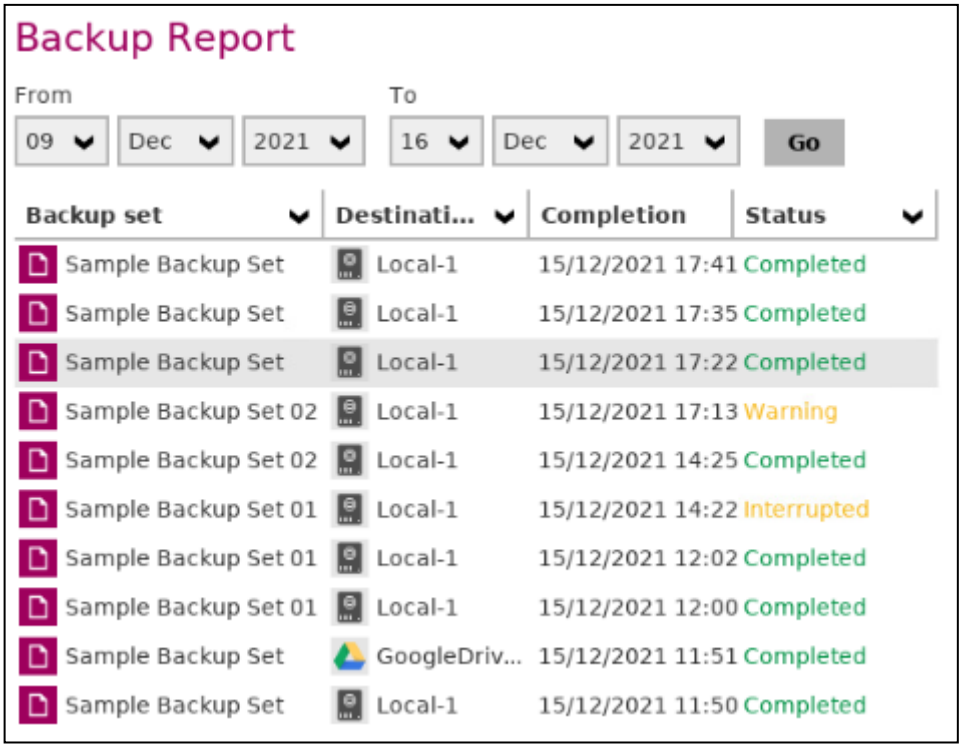
If you want to see the backup report(s) in your selected storage location, use the **Destination** filter.



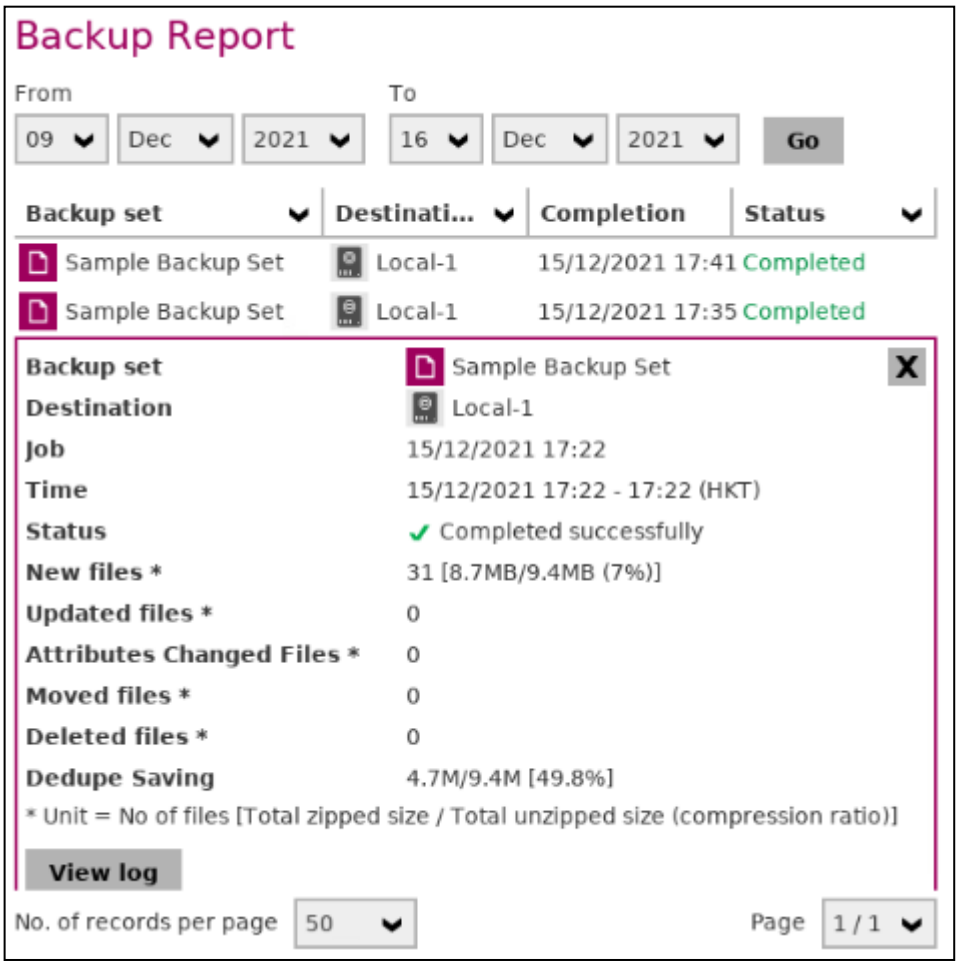
By applying this filter, all backup reports with the same **Status** will be shown.



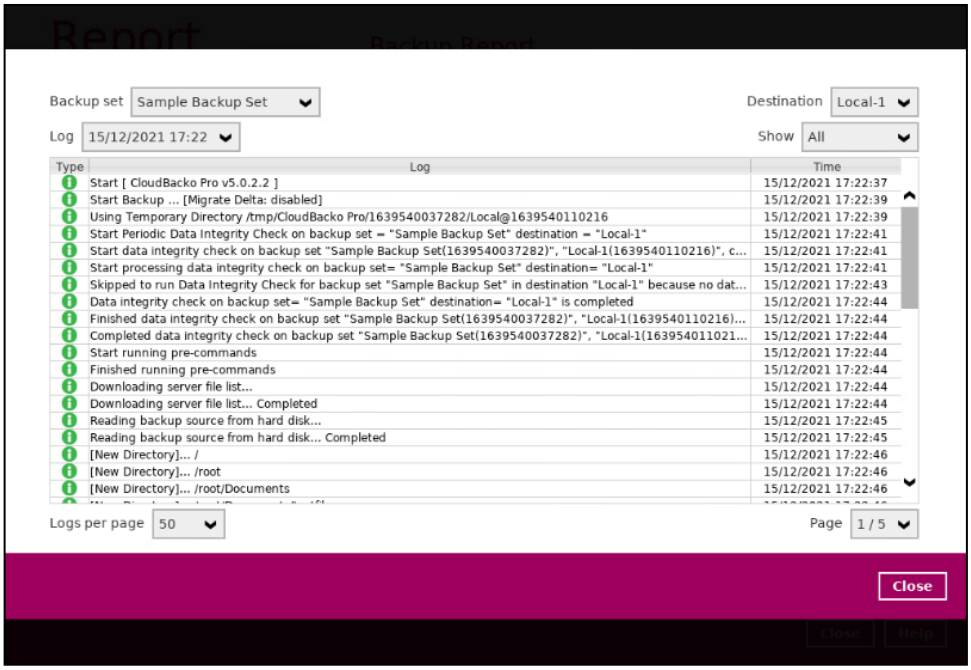
In order to see a backup report in detail, select a backup set.



Click **View log** to see the event log during a backup.

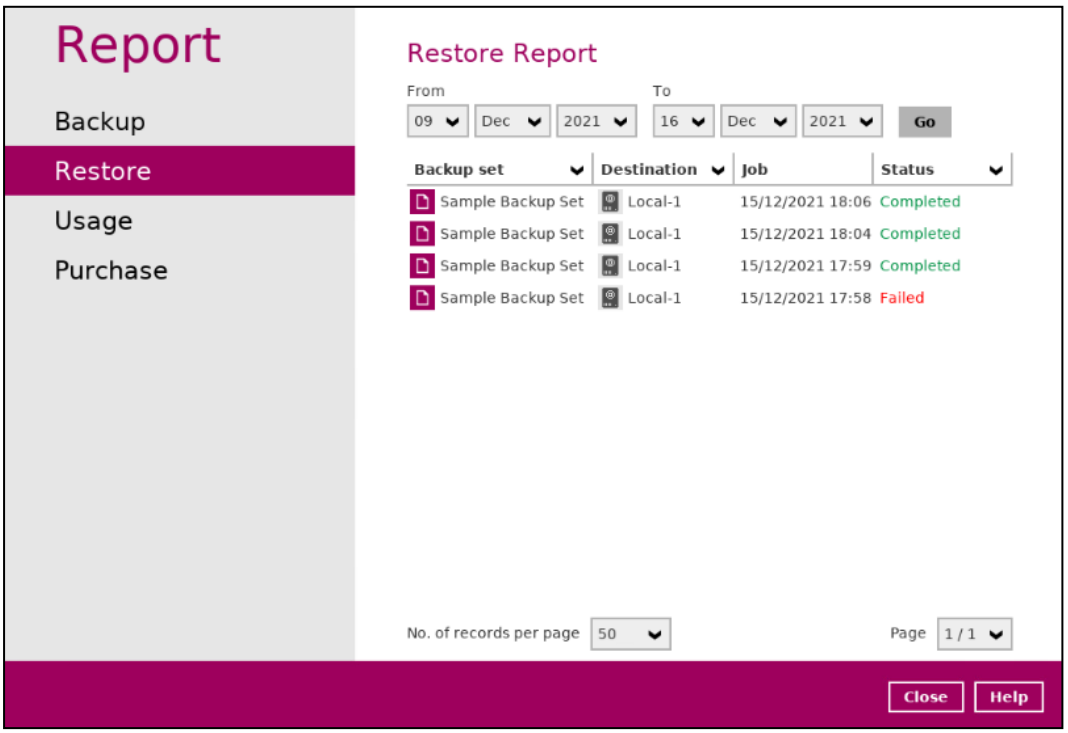


Backup set, **time**, **destination,** and **status** can be filtered here. You can also choose to view the number of logs per page.



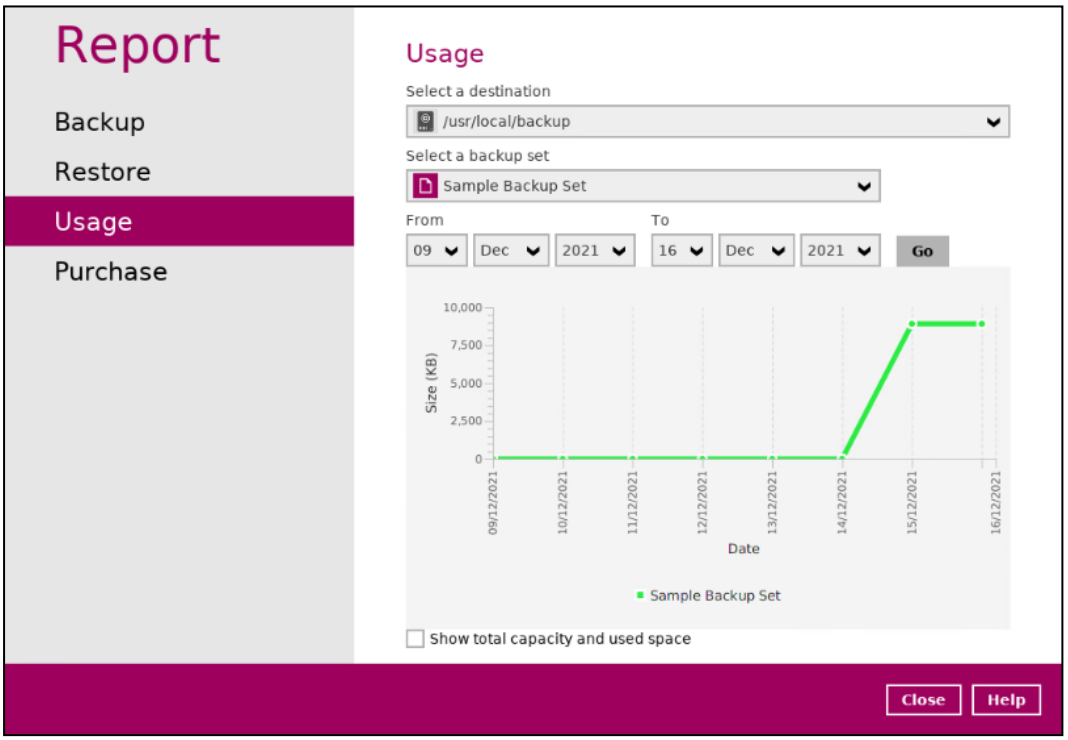
7.5.2 Restore

This feature is used for viewing restore report(s). You can also apply filter on **Date range**, **Backup set**, **Destination,** and **Status** here.



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.



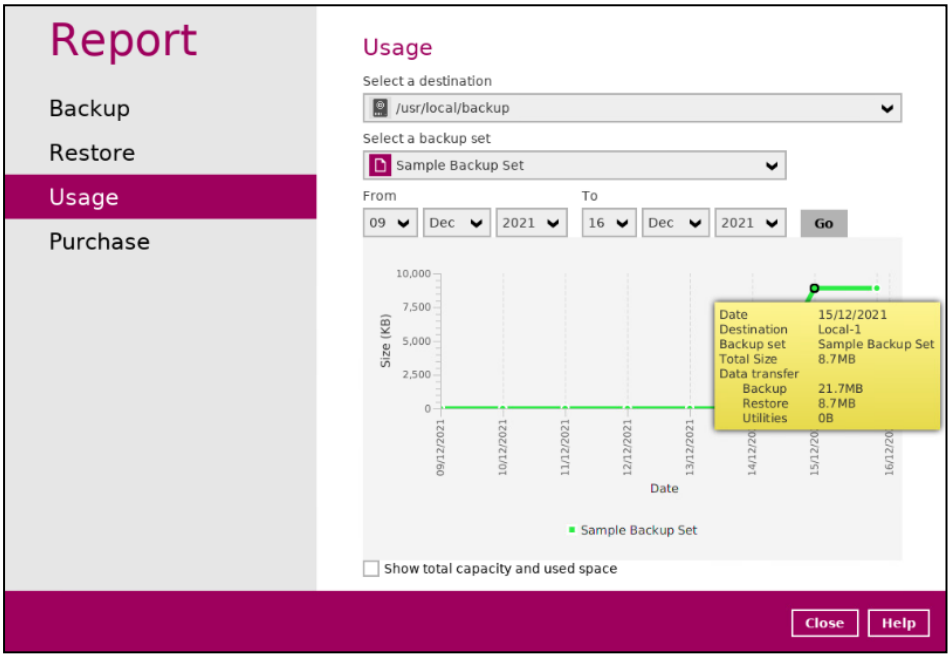
- **Storage Statistics**

  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:

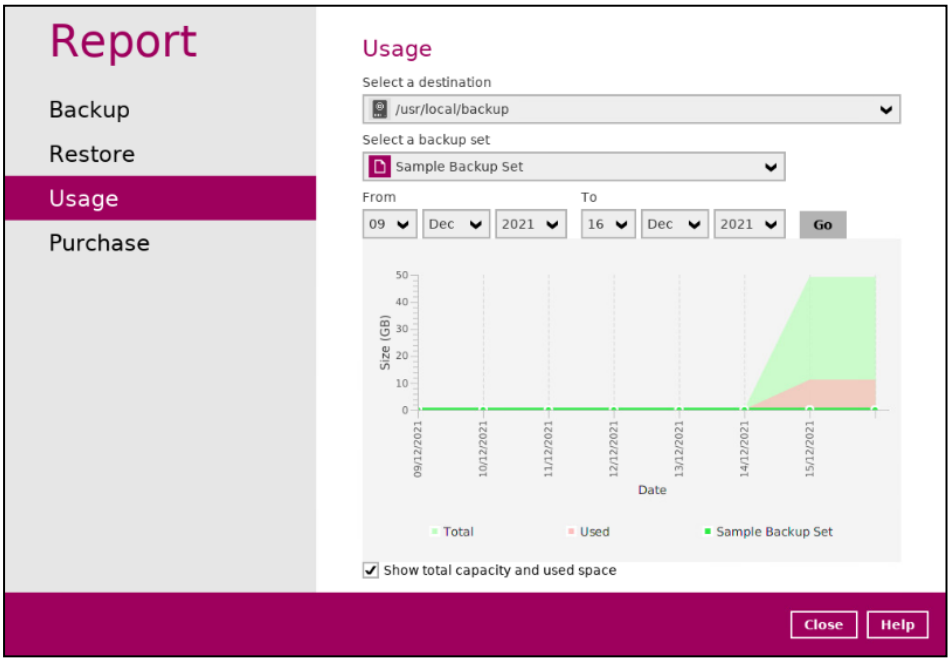
  1. Backup job
  2. Periodic Data Integrity Check (PDIC)
  3. Data Integrity Check (DIC)
  4. Space Freeing Up
  5. Delete Backup Data

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.

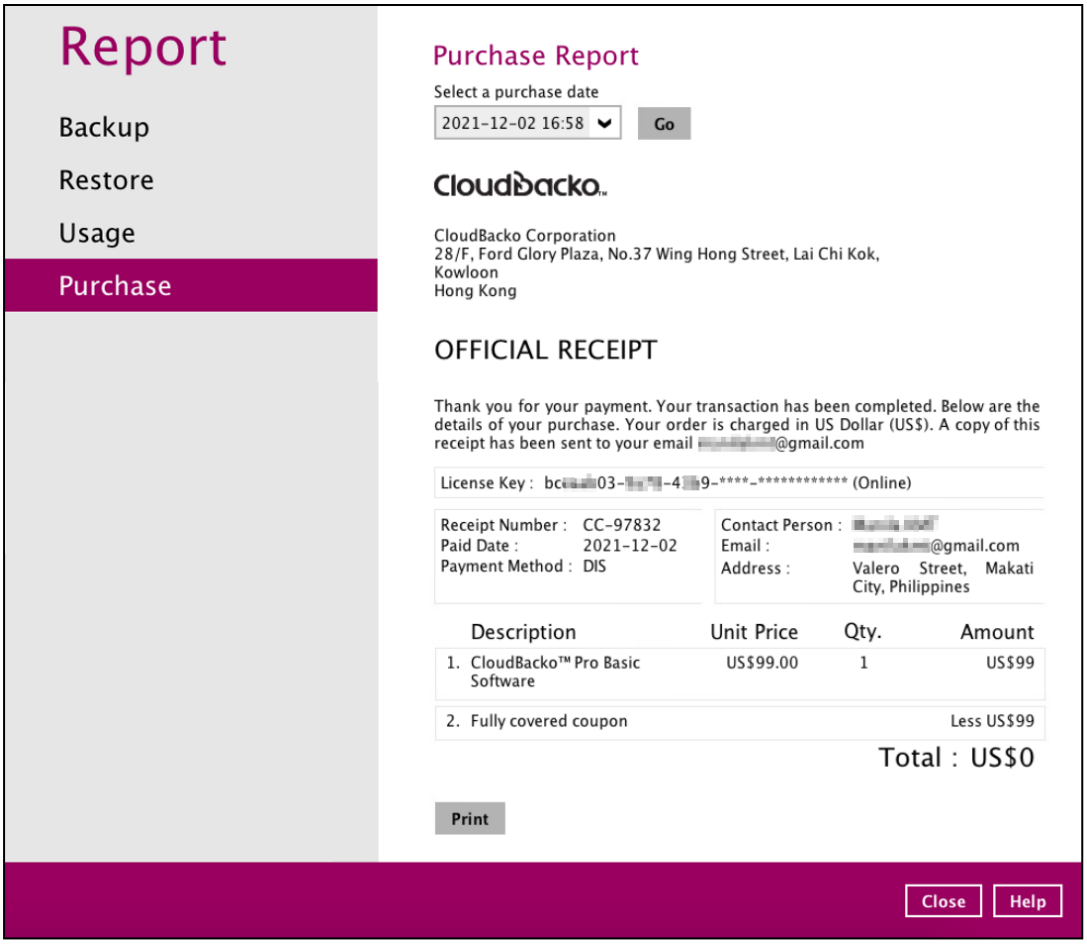
To check the total capacity and used space, tick the checkbox.



7.5.4 Purchase

This feature is used for viewing purchase report(s) for license key and/or modules purchased based on the license key which is currently applied on CloudBacko Pro.

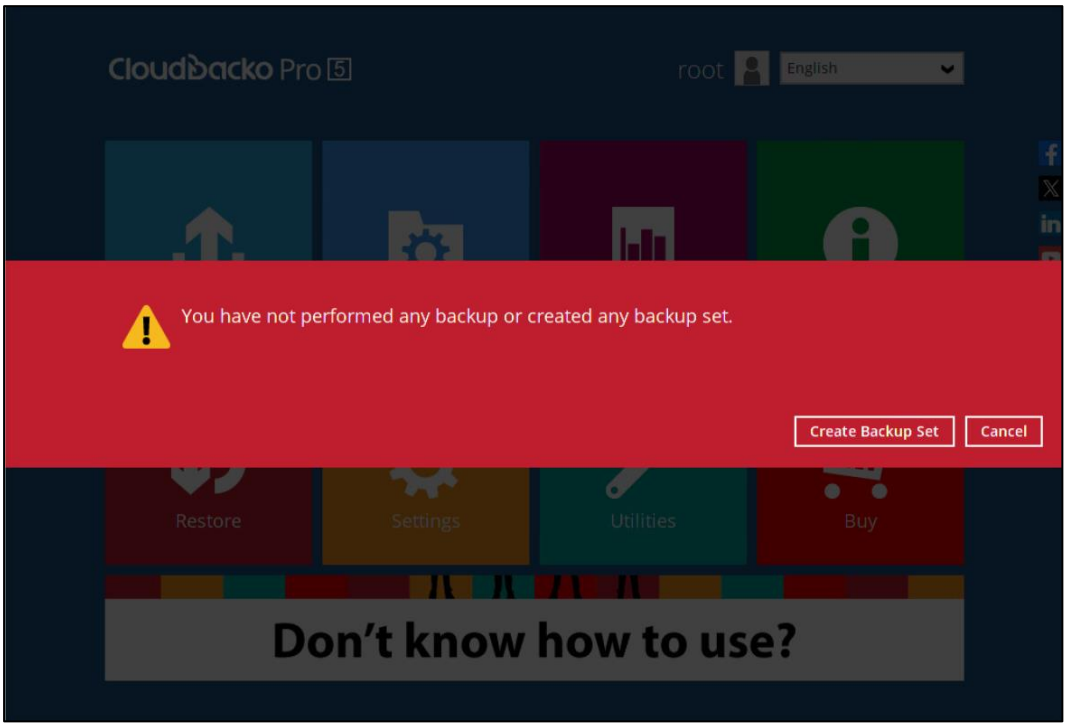
You can select a purchase date and search for a specific report.



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 Pro 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.

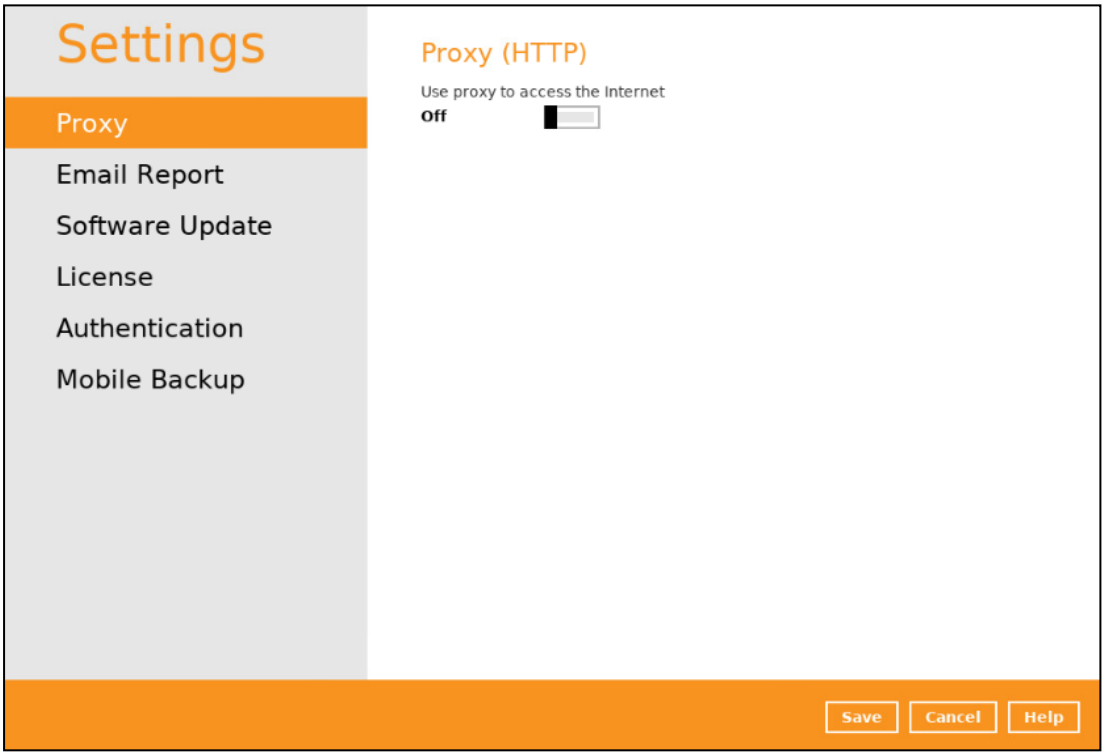


For instructions on how to do a restore, refer to Chapter 11 Restore Data.

7.7 Settings

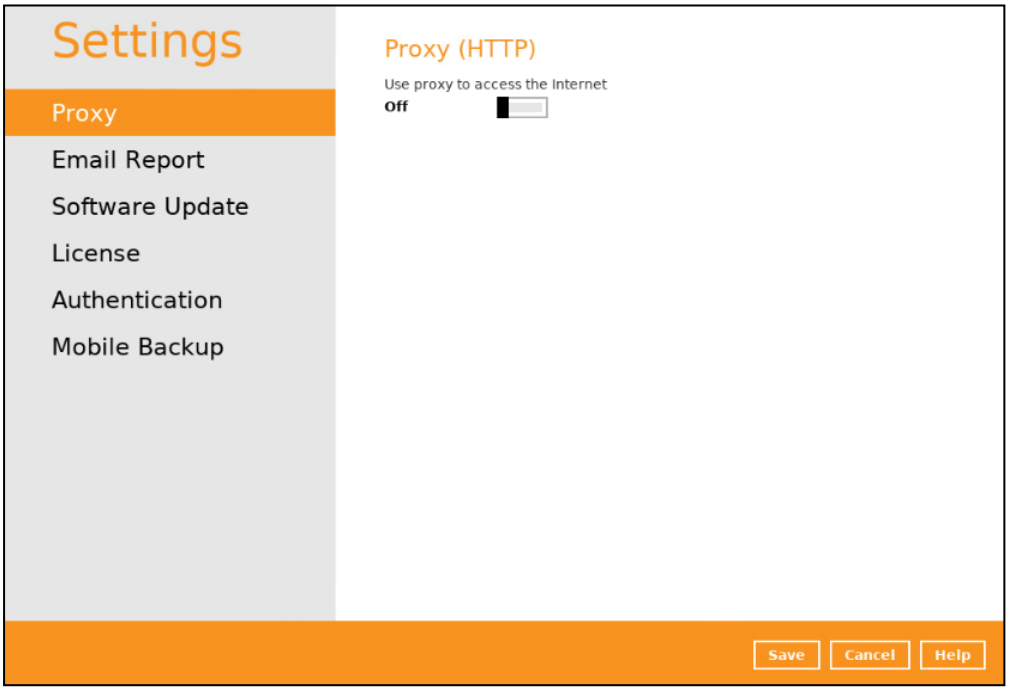
Settings consist of six (6) sub modules:

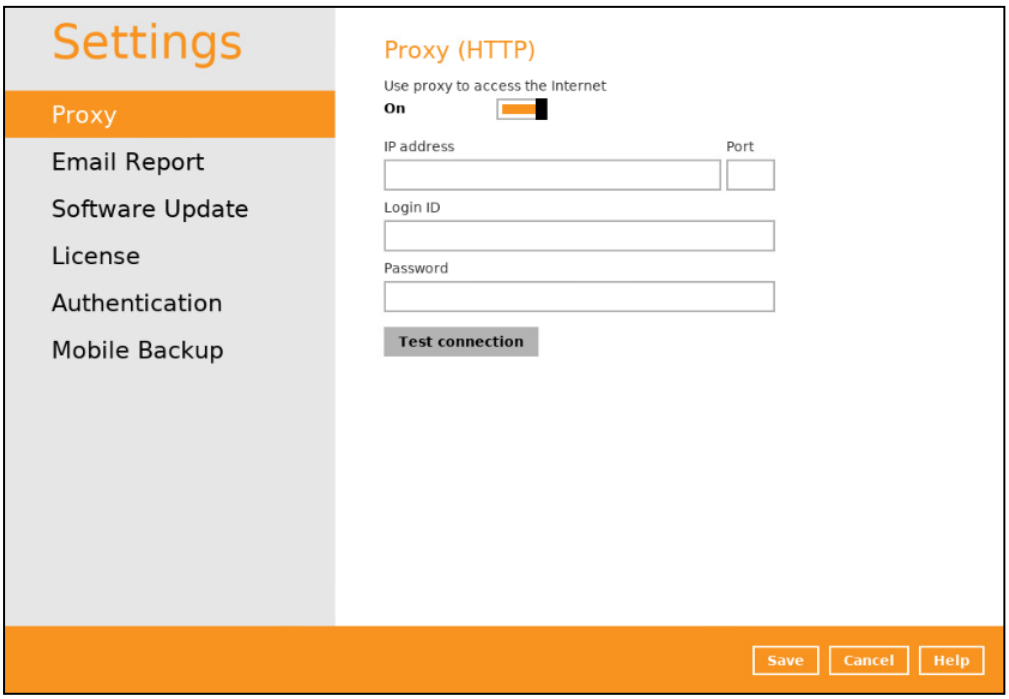
- Proxy
- Email Report
- Software Update
- License
- Authentication
- Mobile Backup



7.7.1 Proxy

To enable the Proxy Settings, follow the instructions below.

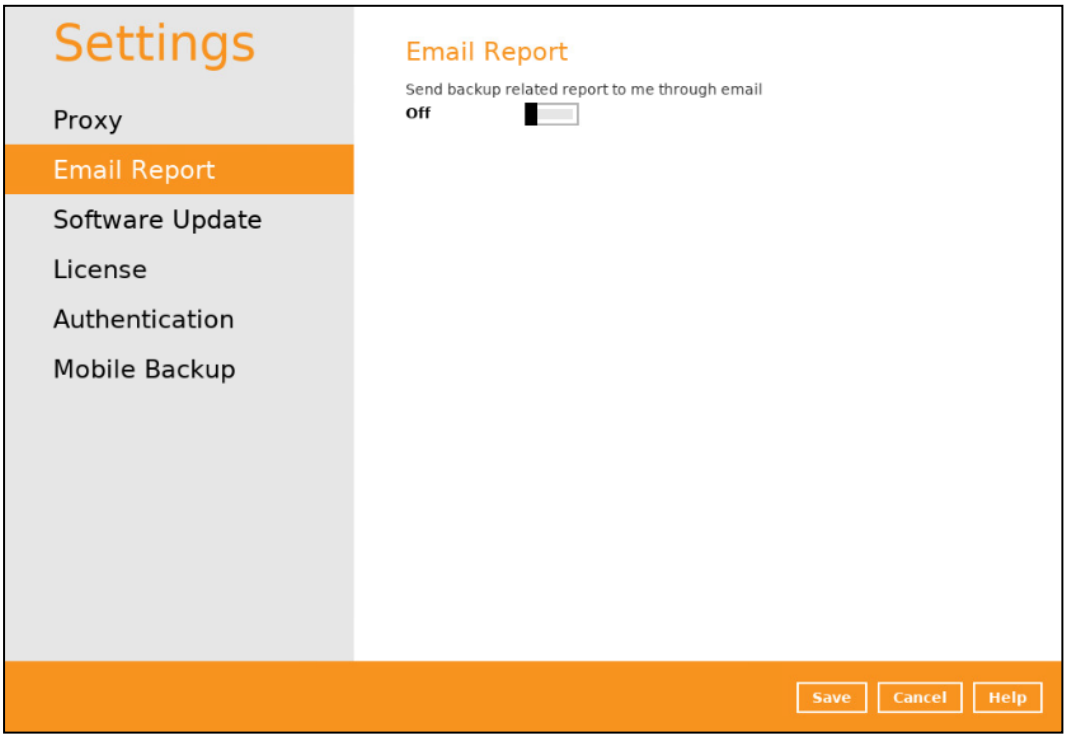




1. Complete the following fields:
   - IP address
   - Port
   - Login ID
   - Password
2. Click **Test Connection** to validate the connection.
3. Click **Save** to store the settings.

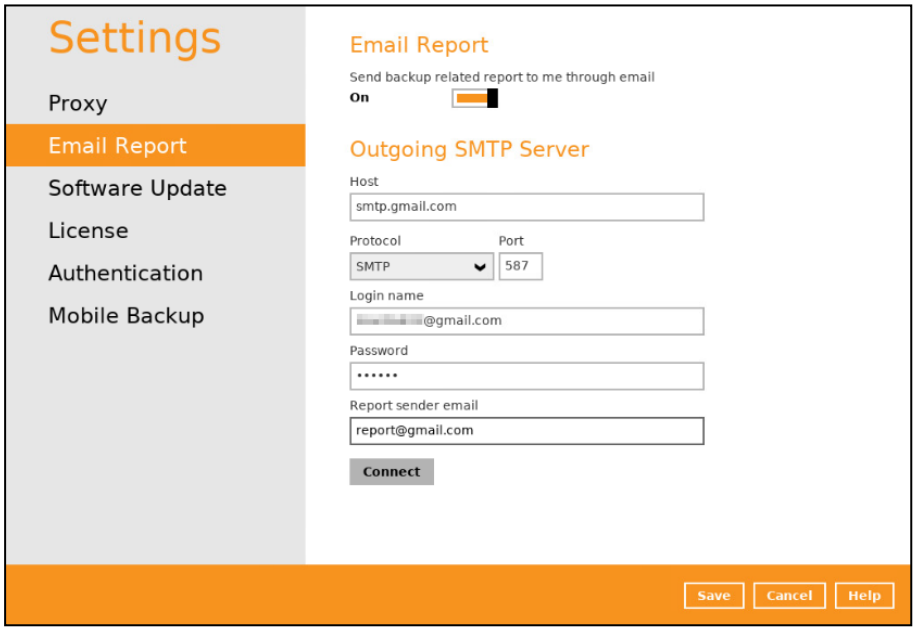
7.7.2 Email Report

The email report will send notifications for backup errors or warnings, missed backup reports, storage alert and restore drill report.

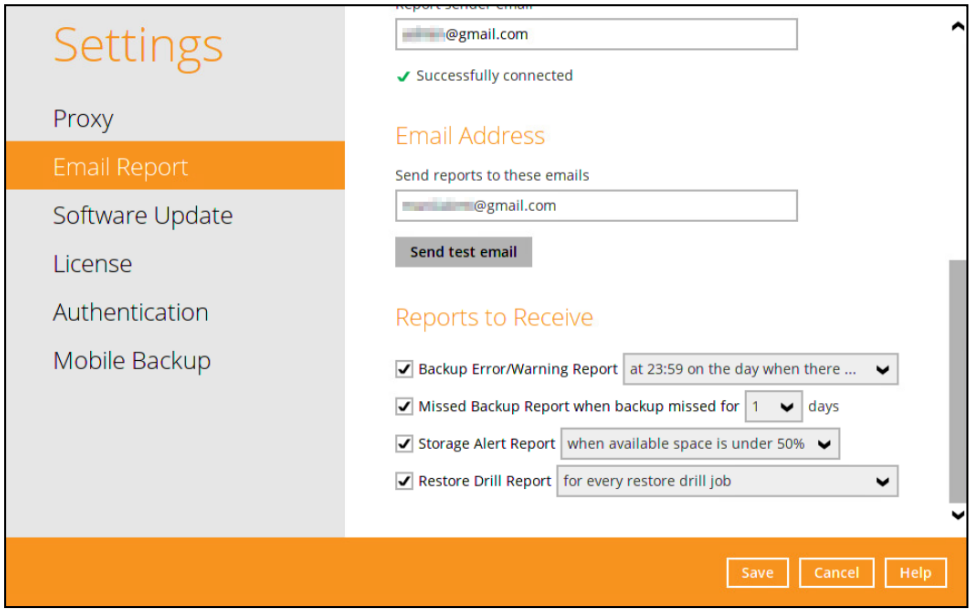


To enable the Email Report feature, follow the instructions below:

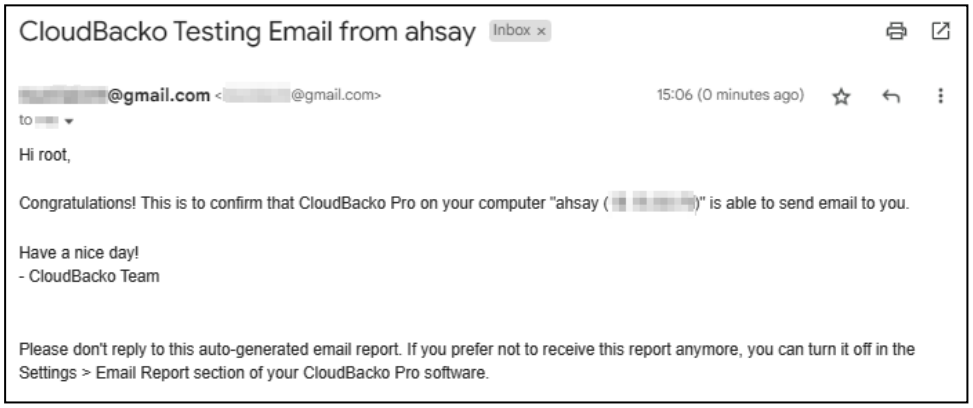
1. Complete the following fields then click **Connect** to validate the connection.
   - Host
   - Protocol
   - Port
   - Login name
   - Password
   - Report sender email



If succesfully connected, the email address where the report will be sent should be displayed as well as the list of reports to be received. Enter a valid email then click **Send test email**.



Below is the sample screenshot of the test email.

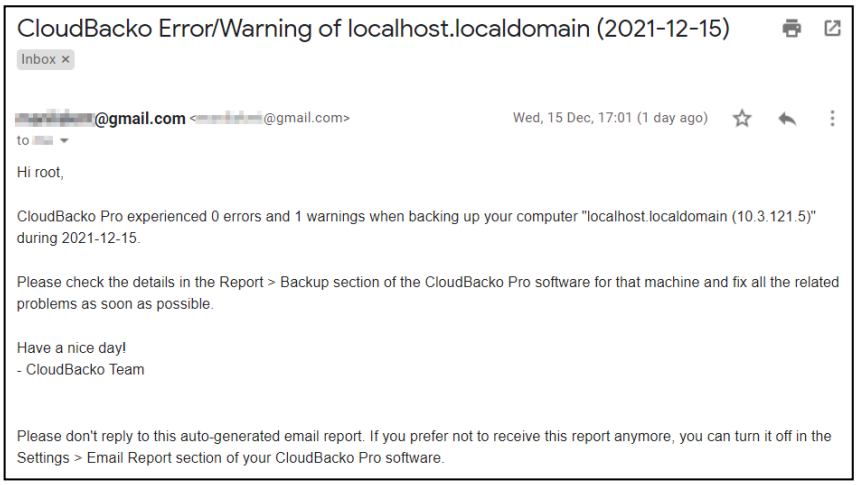


2. Select the reports you want to receive by ticking the checkboxes then click the **Save** button to store the settings.

- Backup Error/Warning Report
  - at 23.59 on the day when there are error or warning
  - at 23:59 everyday, when there are no error or warning
- Missed Backup Report when backup missed for a specific number of days
  - Number of days: from 1 to 30
- Storage Alert Report
  - when available space is under 50%
  - when available space is under 40%
  - when available space is under 30%
  - when available space is under 20%
  - when available space is under 10%
- Restore Drill Report
  - for every restore drill job
  - for every restore drill job with corrupted data found

These are sample reports:

- Backup Error/Warning Report



CloudBacko Error/Warning of localhost.localdomain (2021-12-15)

Inbox ×

[redacted]@gmail.com <[redacted]@gmail.com> Wed, 15 Dec, 17:01 (1 day ago)

to [redacted]

Hi root,

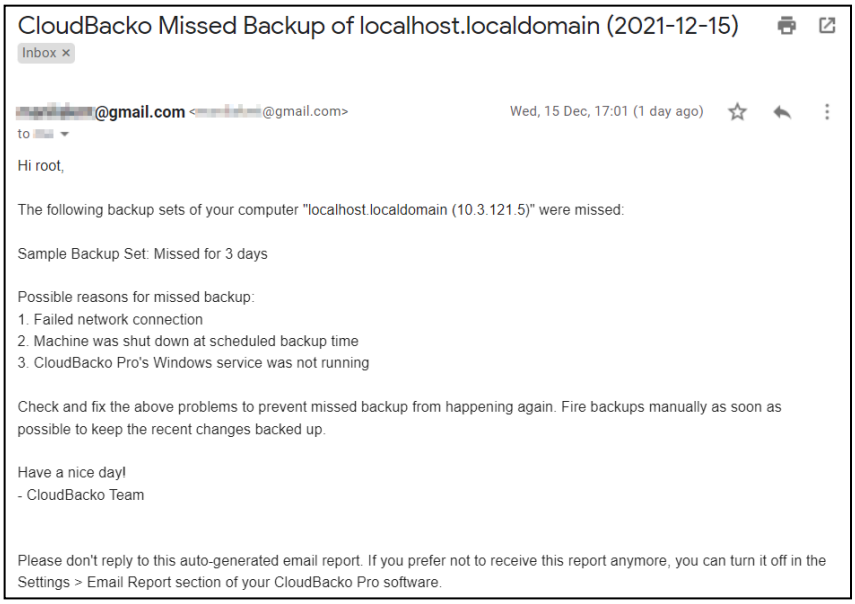
CloudBacko Pro experienced 0 errors and 1 warnings when backing up your computer "localhost.localdomain (10.3.121.5)" during 2021-12-15.

Please check the details in the Report > Backup section of the CloudBacko Pro software for that machine and fix all the related problems as soon as possible.

Have a nice day!
- CloudBacko Team

Please don't reply to this auto-generated email report. If you prefer not to receive this report anymore, you can turn it off in the Settings > Email Report section of your CloudBacko Pro software.

- Missed Backup Report when backup missed for a specific number of days



CloudBacko Missed Backup of localhost.localdomain (2021-12-15)

Inbox ×

[redacted]@gmail.com <[redacted]@gmail.com> Wed, 15 Dec, 17:01 (1 day ago)

to [redacted]

Hi root,

The following backup sets of your computer "localhost.localdomain (10.3.121.5)" were missed:

Sample Backup Set: Missed for 3 days

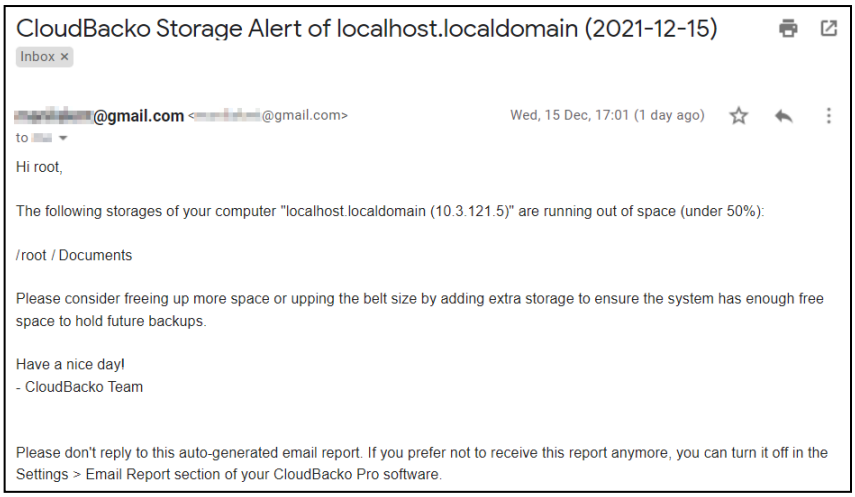
Possible reasons for missed backup:
1. Failed network connection
2. Machine was shut down at scheduled backup time
3. CloudBacko Pro's Windows service was not running

Check and fix the above problems to prevent missed backup from happening again. Fire backups manually as soon as possible to keep the recent changes backed up.

Have a nice day!
- CloudBacko Team

Please don't reply to this auto-generated email report. If you prefer not to receive this report anymore, you can turn it off in the Settings > Email Report section of your CloudBacko Pro software.

- Storage Alert Report



CloudBacko Storage Alert of localhost.localdomain (2021-12-15)

Inbox ×

[redacted]@gmail.com <[redacted]@gmail.com> Wed, 15 Dec, 17:01 (1 day ago)

to [redacted]

Hi root,

The following storages of your computer "localhost.localdomain (10.3.121.5)" are running out of space (under 50%):

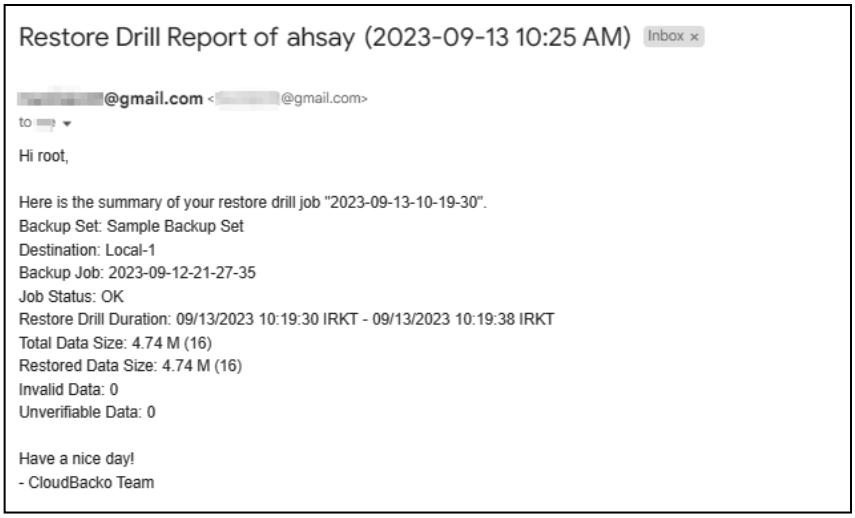
/root / Documents

Please consider freeing up more space or upping the belt size by adding extra storage to ensure the system has enough free space to hold future backups.

Have a nice day!
- CloudBacko Team

Please don't reply to this auto-generated email report. If you prefer not to receive this report anymore, you can turn it off in the Settings > Email Report section of your CloudBacko Pro software.

- Restore Drill Report



Restore Drill Report of ahsay (2023-09-13 10:25 AM) Inbox ×

[redacted]@gmail.com <[redacted]@gmail.com>
to [redacted]

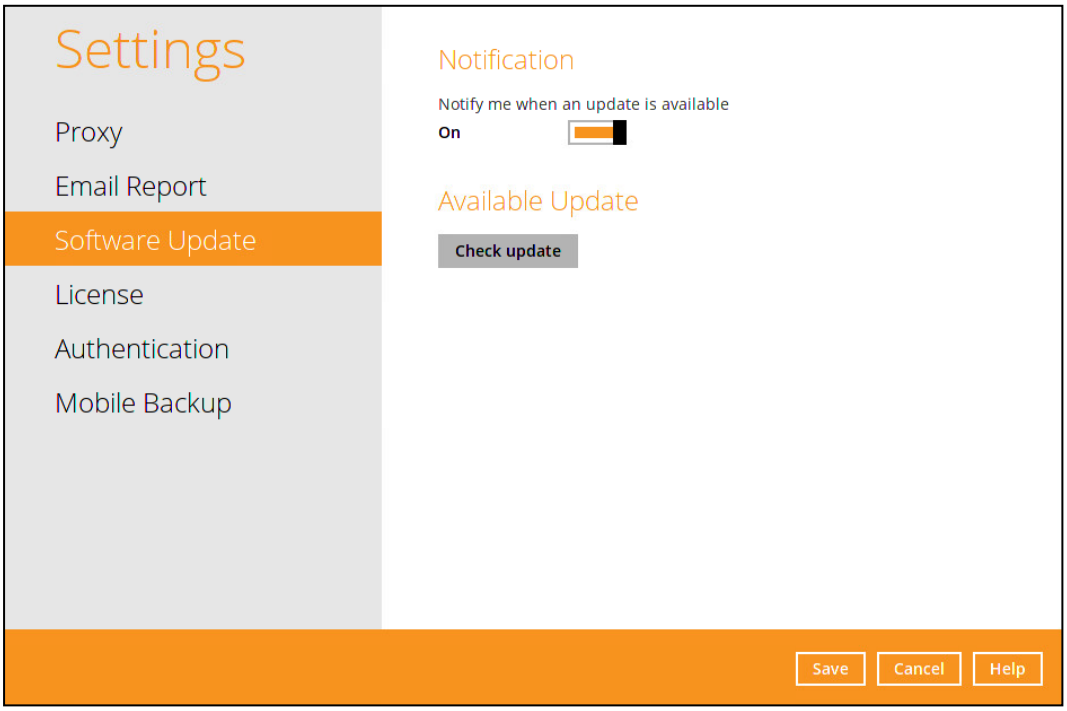
Hi root,

Here is the summary of your restore drill job "2023-09-13-10-19-30".
Backup Set: Sample Backup Set
Destination: Local-1
Backup Job: 2023-09-12-21-27-35
Job Status: OK
Restore Drill Duration: 09/13/2023 10:19:30 IRKT - 09/13/2023 10:19:38 IRKT
Total Data Size: 4.74 M (16)
Restored Data Size: 4.74 M (16)
Invalid Data: 0
Unverifiable Data: 0

Have a nice day!
- CloudBacko Team

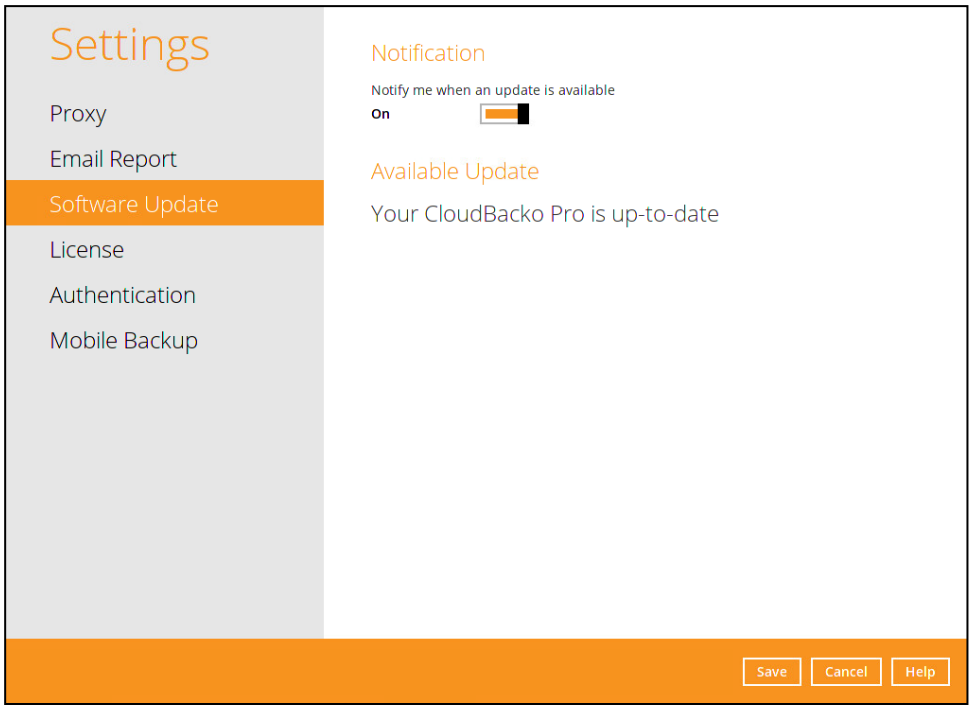
7.7.3 Software Update

The Software Update module allows the user to enable the notifications when an update is available and check if there is an available update. By default, the notification is enabled.

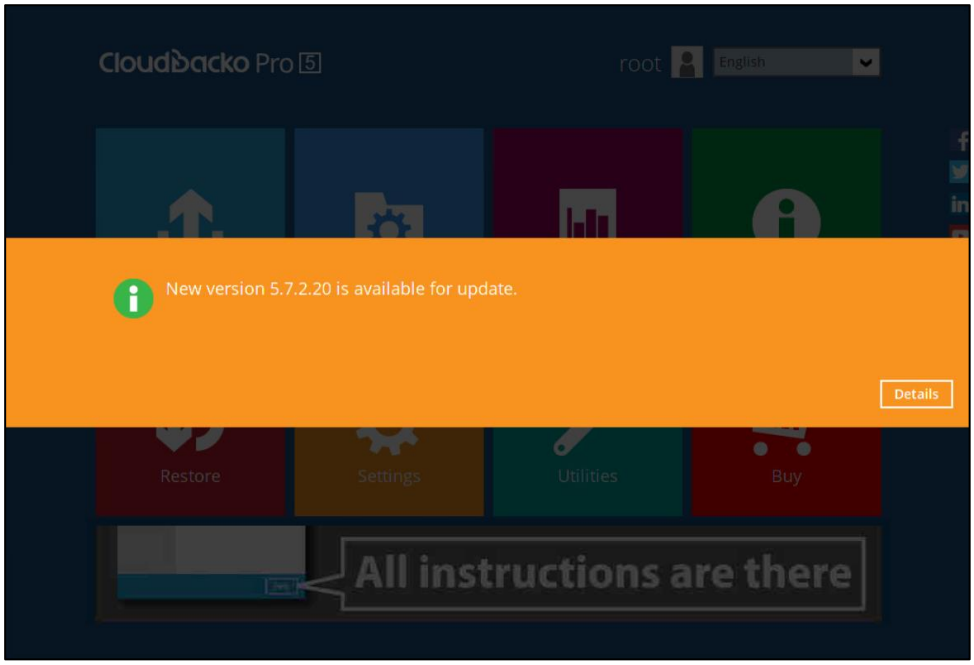


To check for the available Update, follow the instructions below:

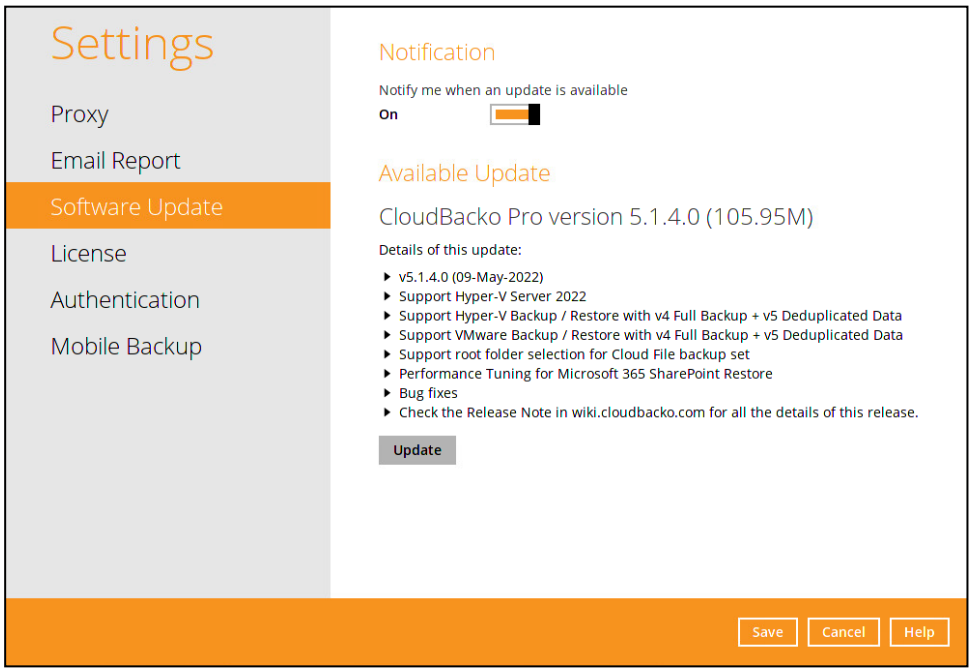
1. Click the **Check update** button.
2. If there is no available update, it will display this message, **"Your CloudBacko Pro is up-to-date"**.



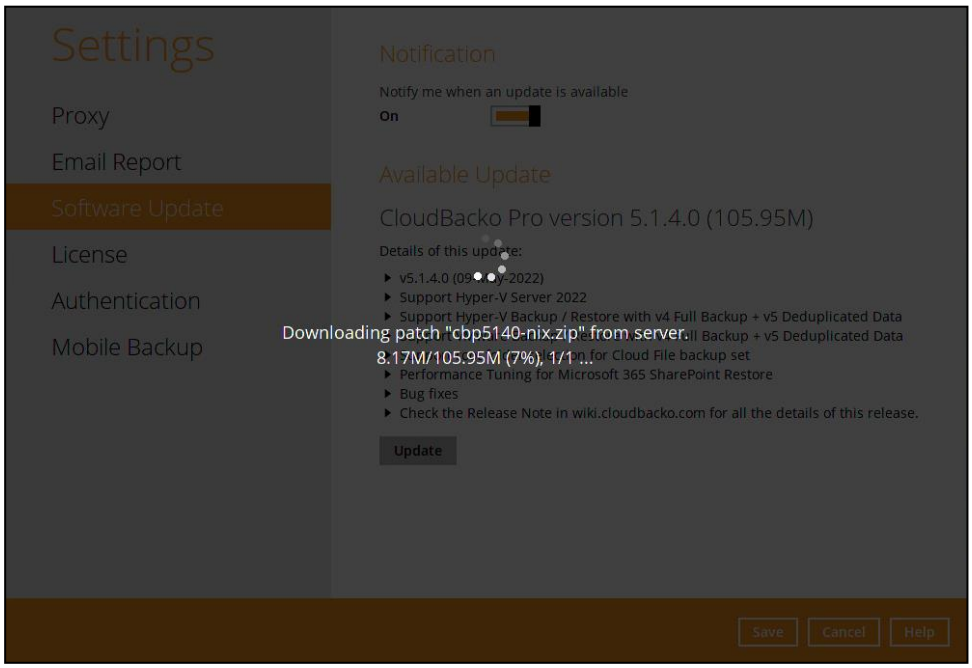
3. However, if there is an available update, upon launching the CloudBacko Pro, an alert message will prompt that there is an available version for update. Click **Details** to proceed.



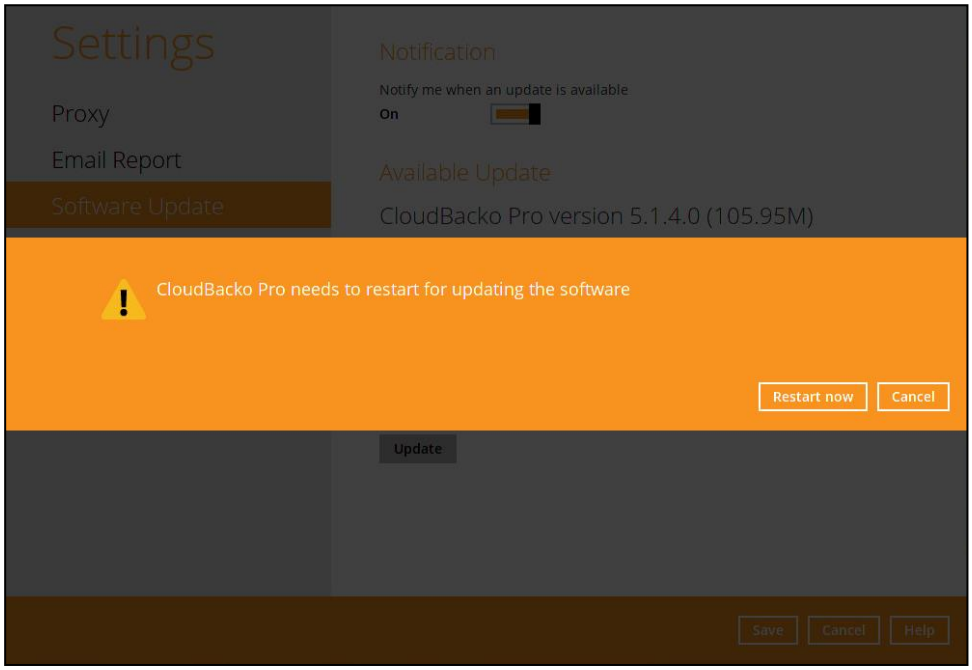
4. Upon clicking the Details button, it redirects the users to the Software Update module under Settings. It shows the details of the update. Click **Update** to proceed



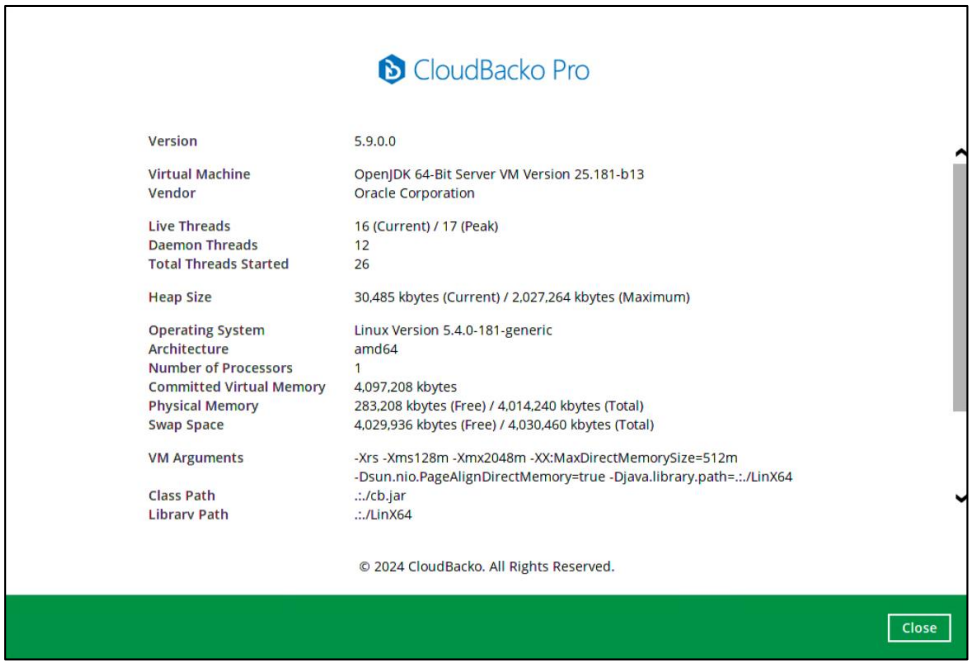
5. It will show the download progress of the latest patch.



6. Once download is completed, it will prompt an alert message that the CloudBacko Pro needs to restart to update the software. Click **Restart now** to proceed. Otherwise click **Cancel** to abort restarting.

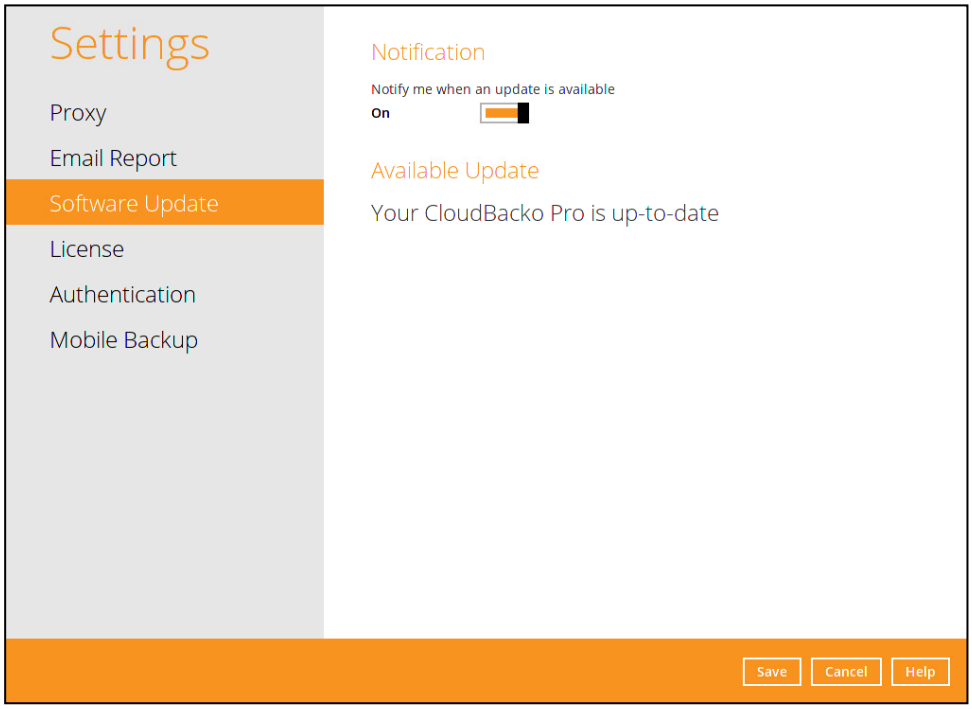


7. The CloudBacko Pro should launch automatically. To check if the update is successful, Go to the **About** module



OR

Go to **Settings > Software Update**, click **Check update.**



7.7.4 License

The License module shows the current license key applied along with the licenses and module usage. Also, it allows the customer to apply full license key to a trial version of CloudBacko Pro.

- License Key

  Displays the current license key. It could be a trial or full license key.

- Change License Key

  This feature allows the customer to apply a full license key.

- Mode

  Displays the mode of the license key either Online or Offline license. Online license key requires a fixed internet connection.

- Version

  Displays the version of the installed CloudBacko whether it is trial or full version. For trial license, it will indicate the number of days before the trial expires.

- Buy full version (Displays in trial version only)

  This feature allows the customer to buy the full version of the CloudBacko Pro.

- Modules (Displays in trial version only)

  This are the following modules enabled for CloudBacko Pro.

  - CloudBacko Pro software
  - Cloud File Backup Module
  - IBM Lotus Domino Backup Module
  - IBM Notes Backup Module
  - Microsoft Exchange Server Backup Module
  - Microsoft SQL Server Backup Module
  - Tibero Database Server
  - Microsoft Hyper-V Backup Module
  - Microsoft Windows System Backup Module
  - MySQL / MariaDB Backup Module
  - Microsoft 365 Backup Module
  - Oracle Database Server Backup Module
  - VMware Backup Module

- Installations (Displays in full version only)

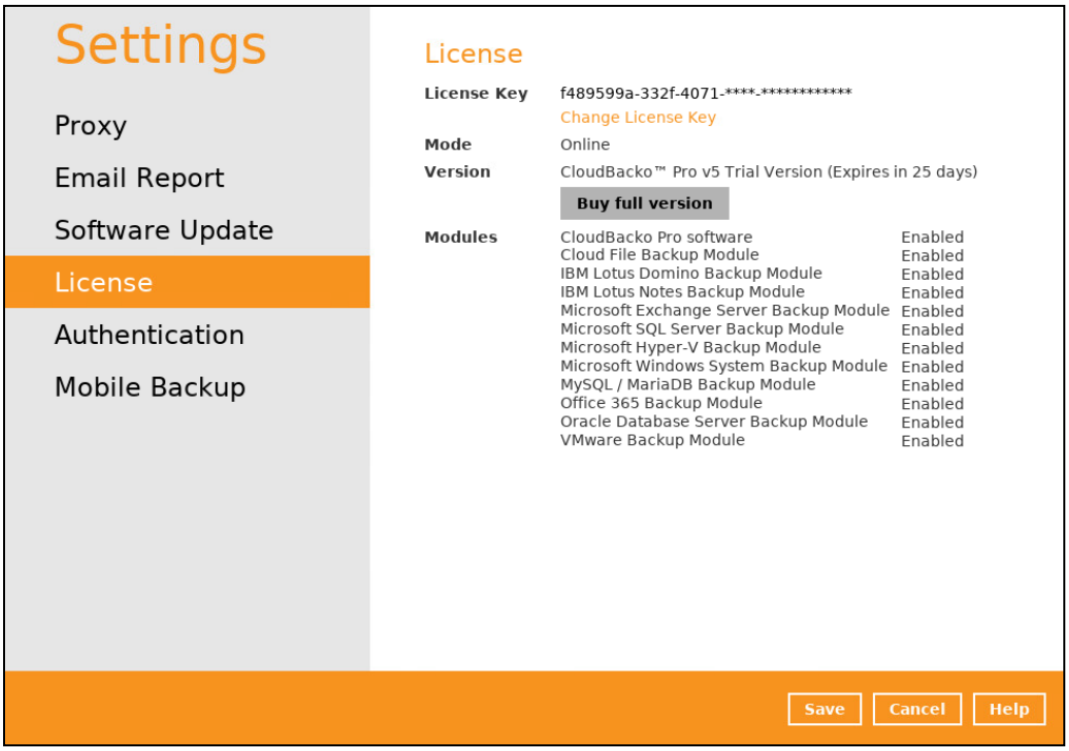
  - Item – these are the software and modules allowed for CloudBacko Pro.

    - CloudBacko Pro software
    - Cloud File Backup Module
    - IBM Lotus Domino Backup Module
    - IBM Notes Backup Module
    - Microsoft Exchange Server Backup Module
    - Microsoft SQL Server Backup Module
    - Tibero Database Server
    - Microsoft Hyper-V Backup Module
    - Microsoft Windows System Backup Module
    - MySQL / MariaDB Backup Module
    - Microsoft 365 Backup Module
    - Oracle Database Server Backup Module
    - VMware Backup Module
    - Linux Bare Metal Backup Module
    - PostgreSQL Backup Module

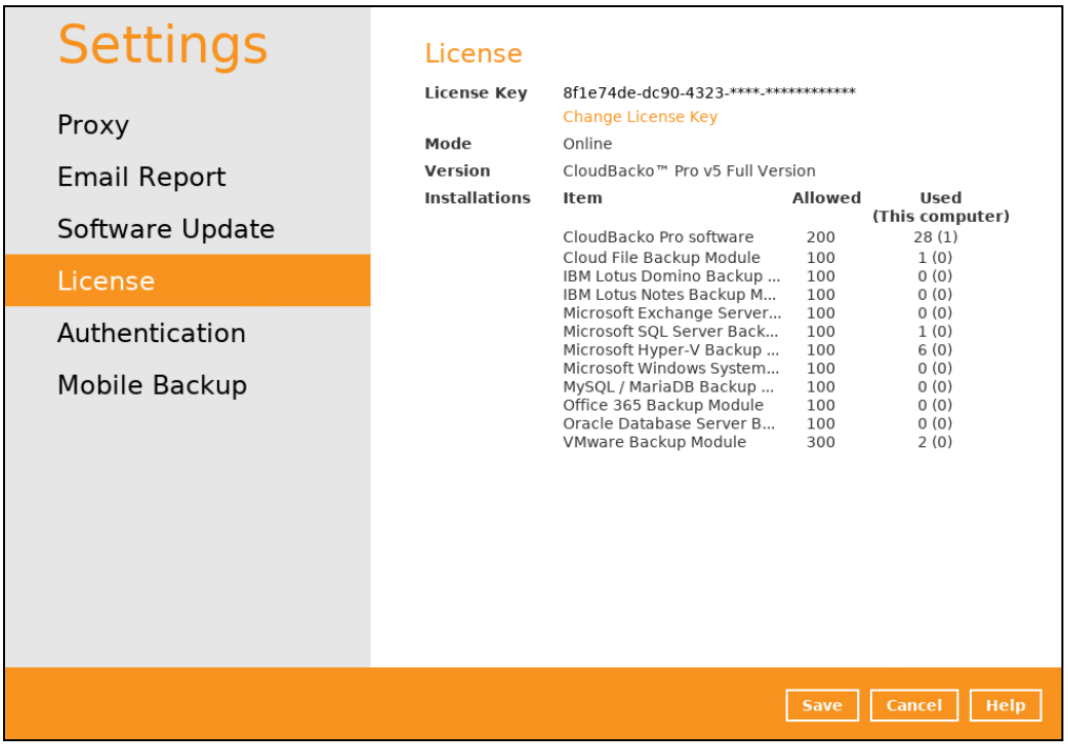
  - Allowed – displays the allowed number for each module for CloudBacko Pro.

- Used (This computer) – displays the total number of used software or add on modules on all computers. The number in brackets refers to the used software or add on modules on the current computer.

This is a sample screenshot for a trial version of CloudBacko Pro.

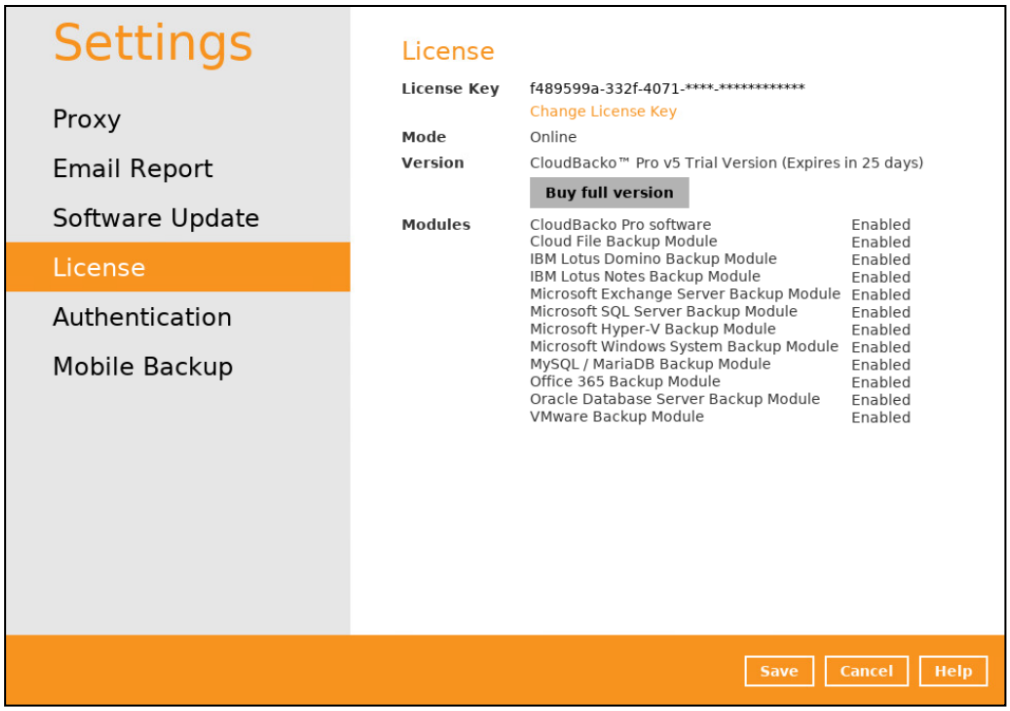


This is a sample screenshot for a full version of CloudBacko Pro.

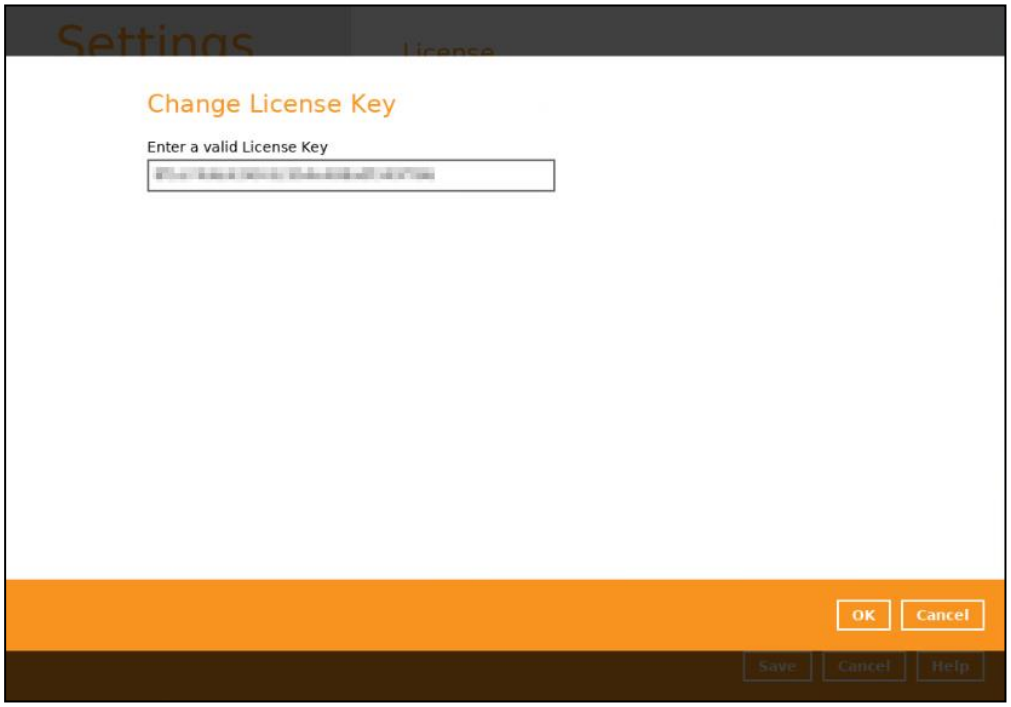


To apply a license key, follow the instructions below:

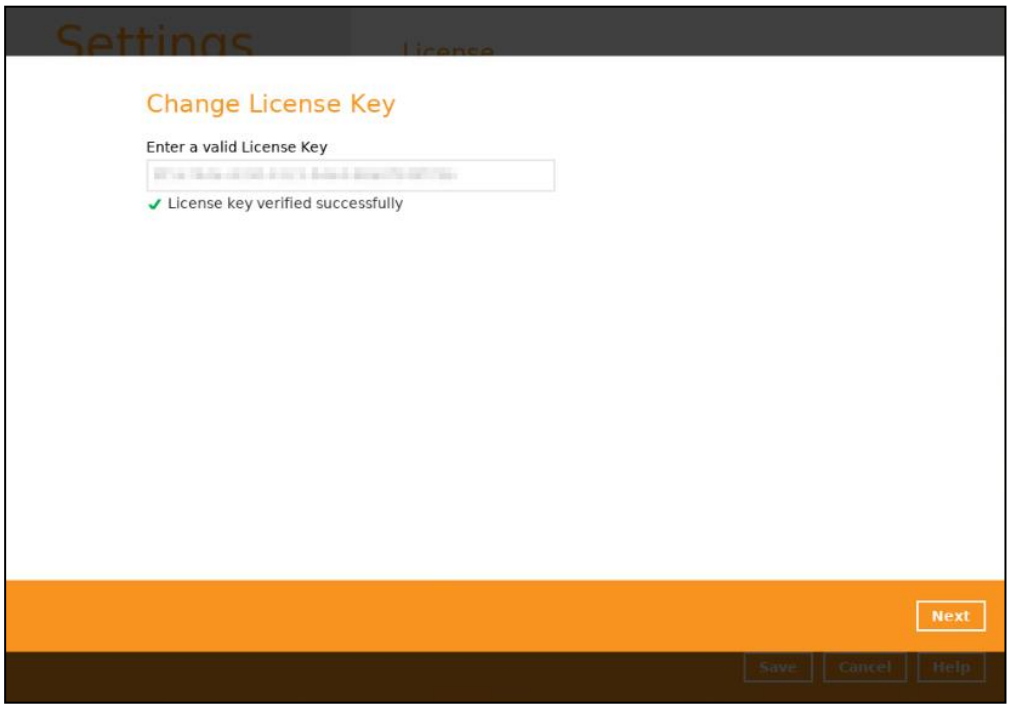
1. Click **Change License Key.**



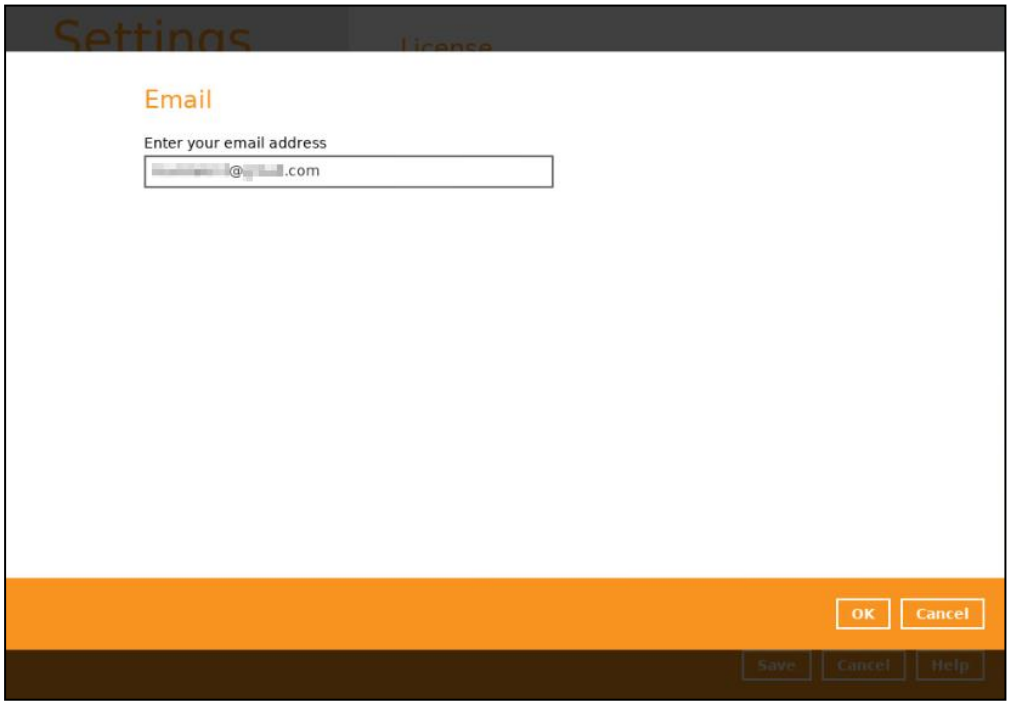
2. Enter a valid license key then click **OK**.



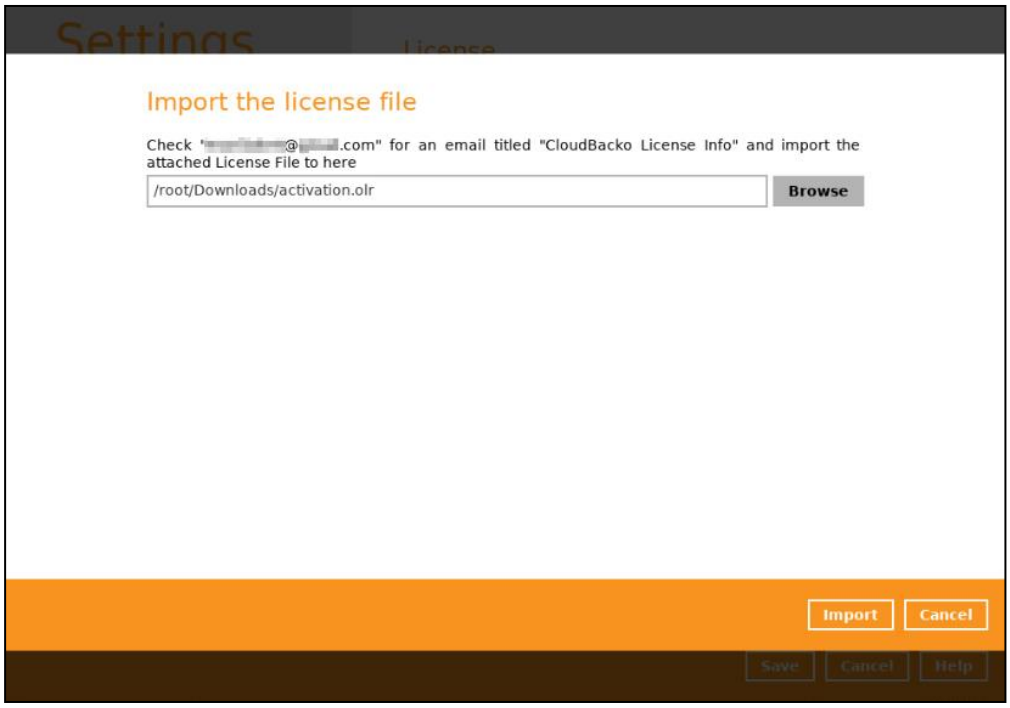
3. Once license key is verified click **Next**.



4. Enter a valid email address.

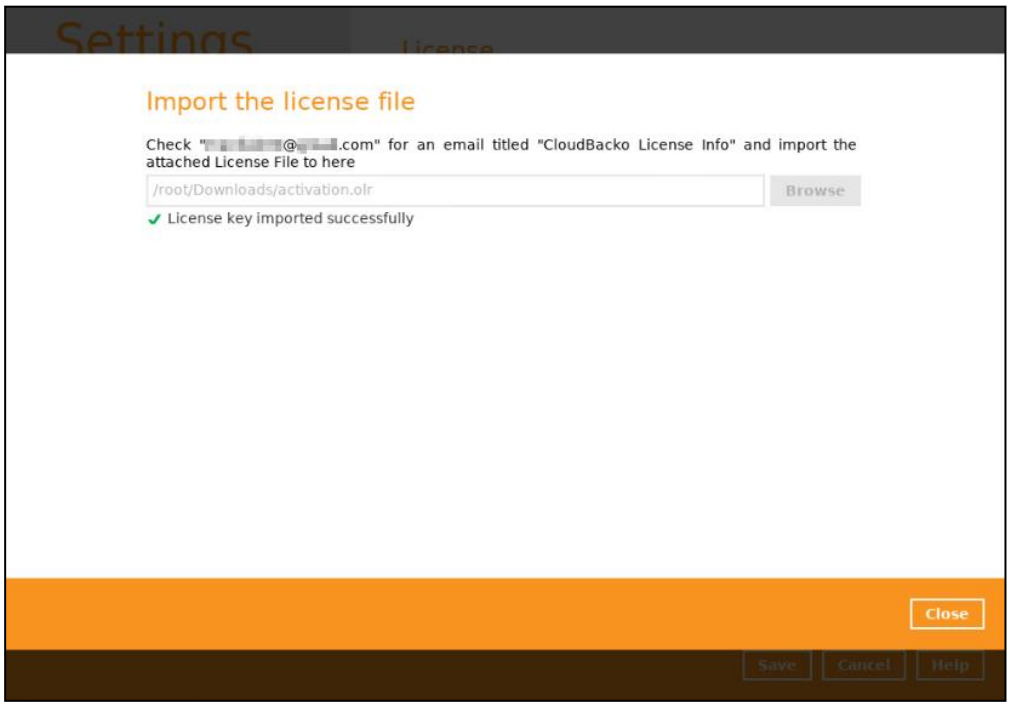


5. Click **Browse** to search for the **activation.olr** sent thru email. Click **Import** to process the activation.

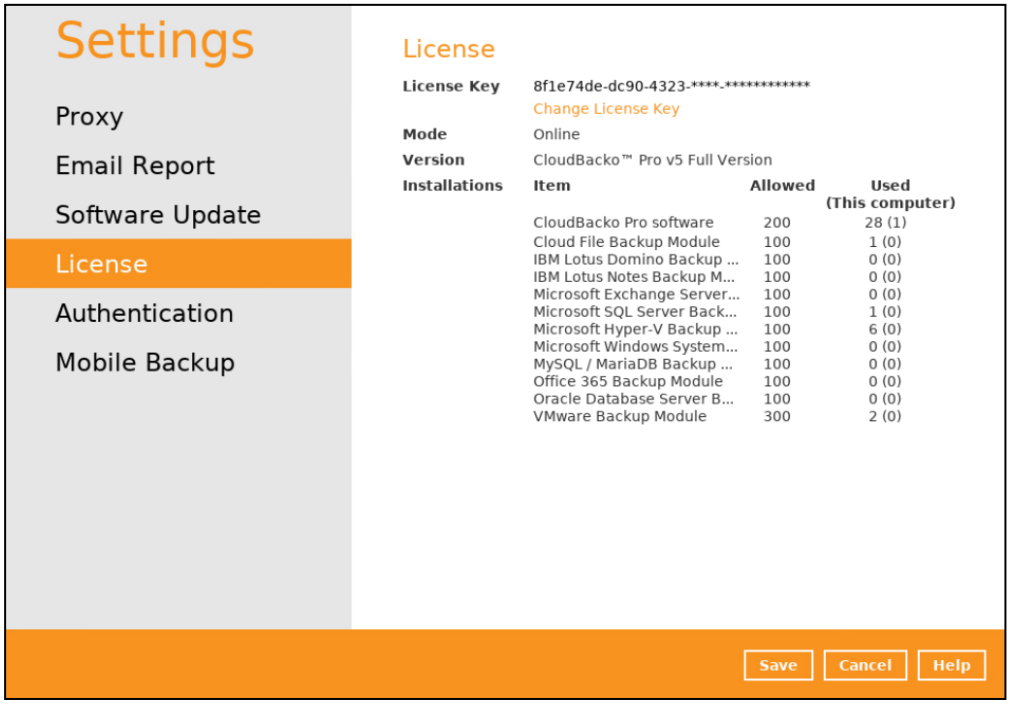


An example of the email with activation.olr attached.

6. Click **Close** to return to the main screen.



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



7.7.5 Authentication

You can use the Authentication function to:

- Enable or disable the "Password Lock". Change the password of the "Password Lock".
- Enable or disable the "Two-Factor Authentication".
- Add one or more device(s) registered for Two-Factor Authentication (2FA).

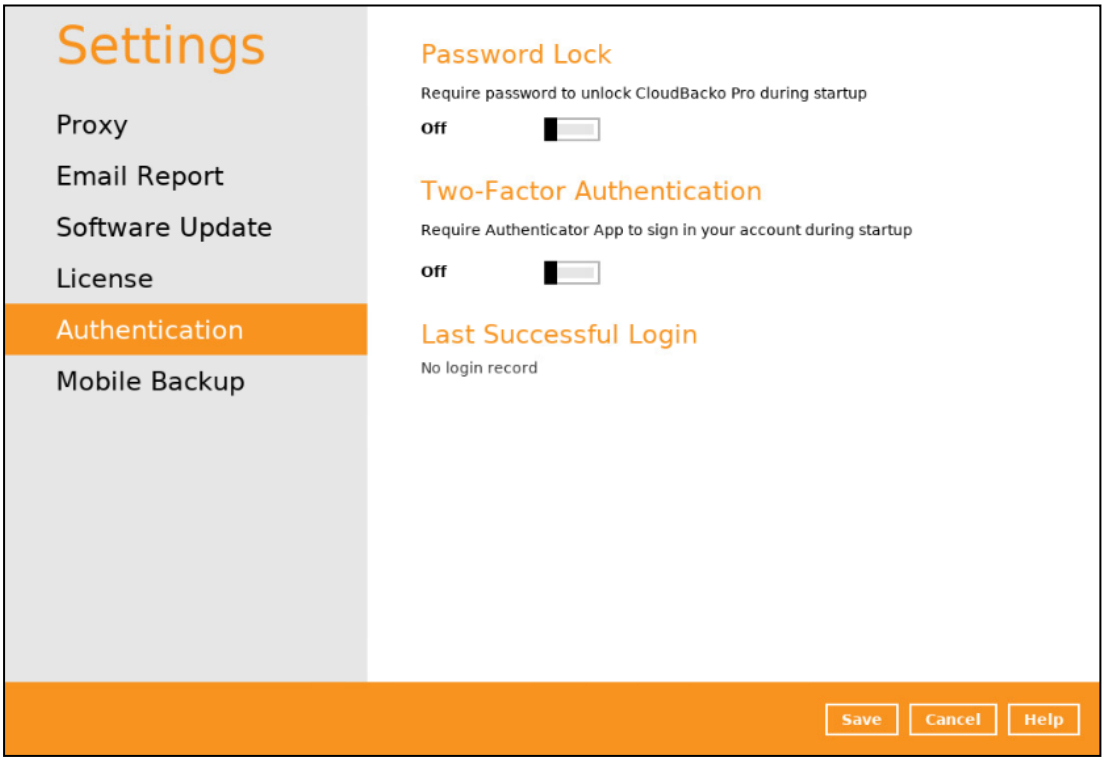
> **NOTE**
> Please refer to the CloudBacko App v1 User Guide for Android and iOS for the detailed step-by-step procedure.

- Re-pair with authenticator.

  This is used once migration is completed to re-pair withauthenticator to enable the sign-in using push notification feature and disable the one in the original device.

- Remove one or more device(s) registered for Two-Factor Authentication (2FA).
- View details of the "Last Successful Login" for Password Lock and Two-Factor Authentication (2FA).

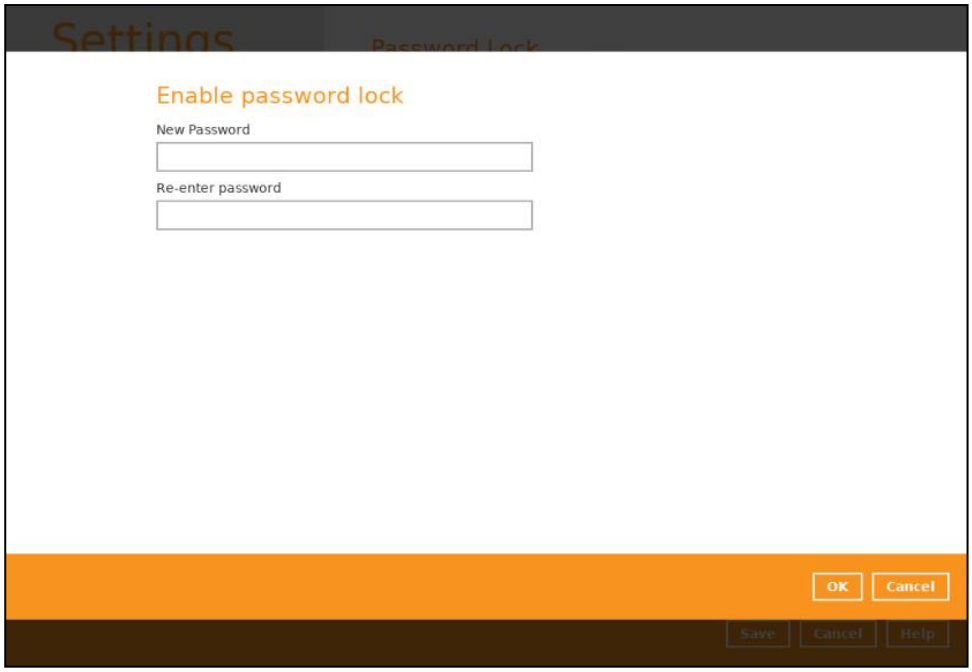
> **NOTE**
> - If both the "Password Lock" and Two-Factor Authentication are enabled, users will be prompted to enter the "Password Lock" first before the Two-Factor Authentication (2FA).
> - For Two-Factor Authentication (2FA), you can register your mobile device on both CloudBacko app and a third-party TOTP Authenticator (e.g. Google Authenticator, Microsoft Authenticator, and LastPass Authenticator).



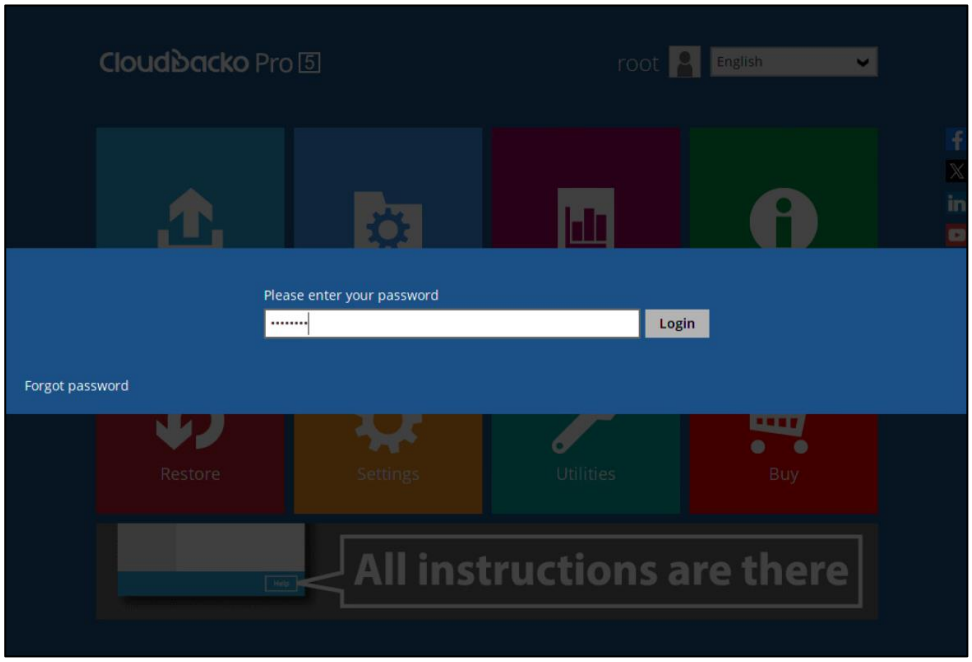
Password Lock

To enable the Password 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.

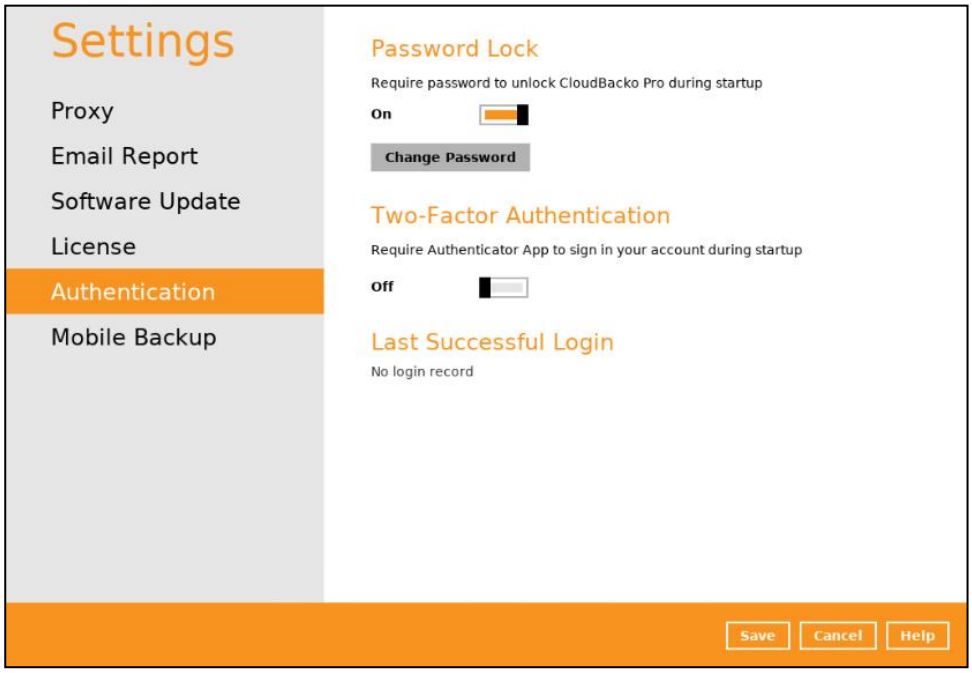


3. Click **OK** then click **Save** button to store the settings.
4. Upon launching the CloudBacko Pro, it is required to enter the password to login.

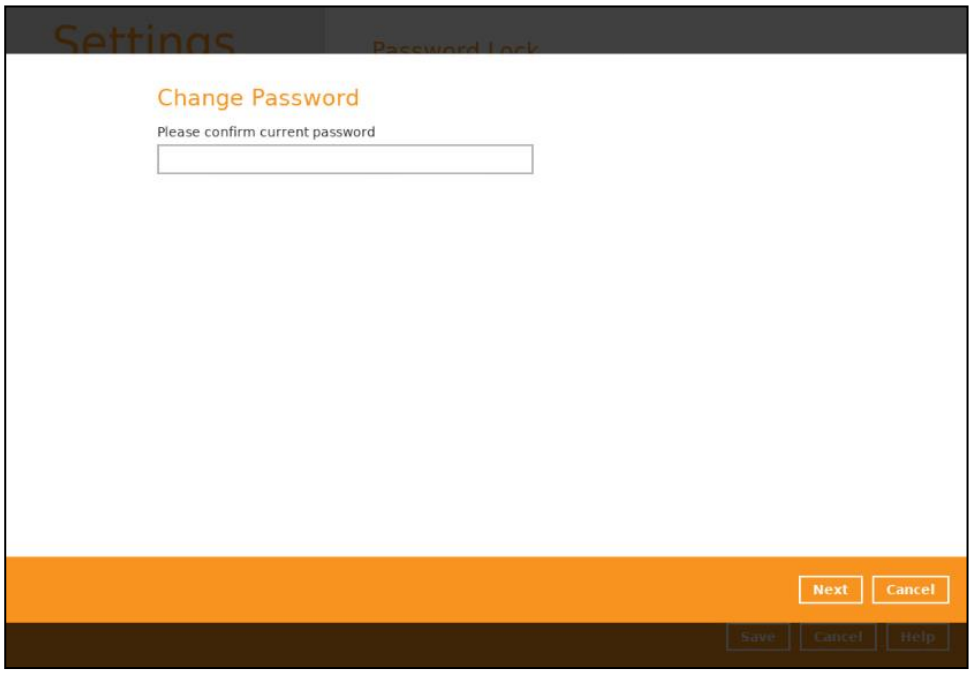


To change the password, follow the instructions below:

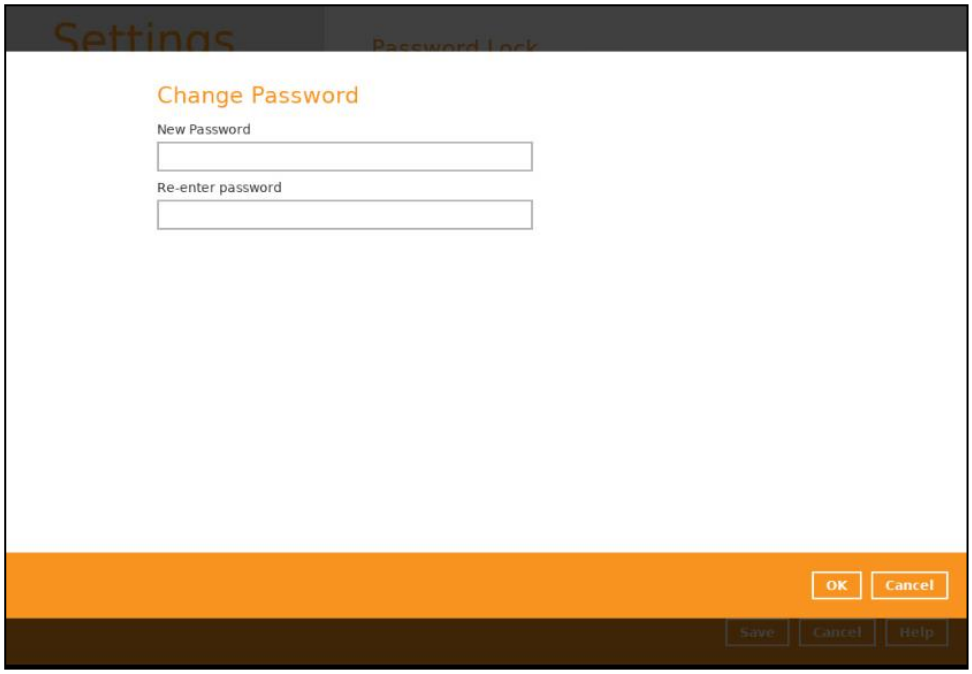
1. Click the **Change Password.**



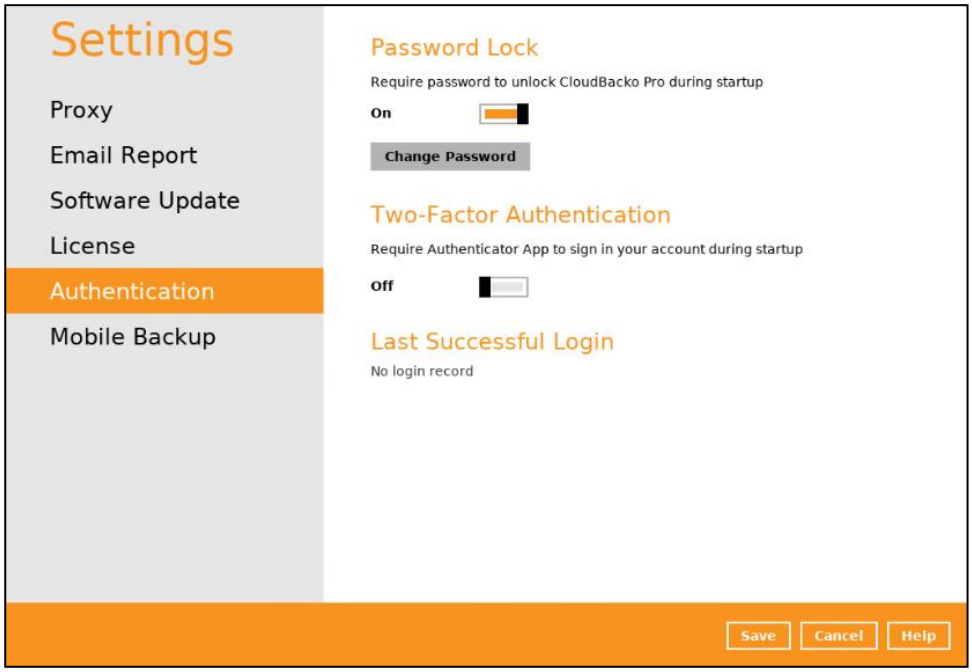
2. Enter the current password then click **Next**.



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

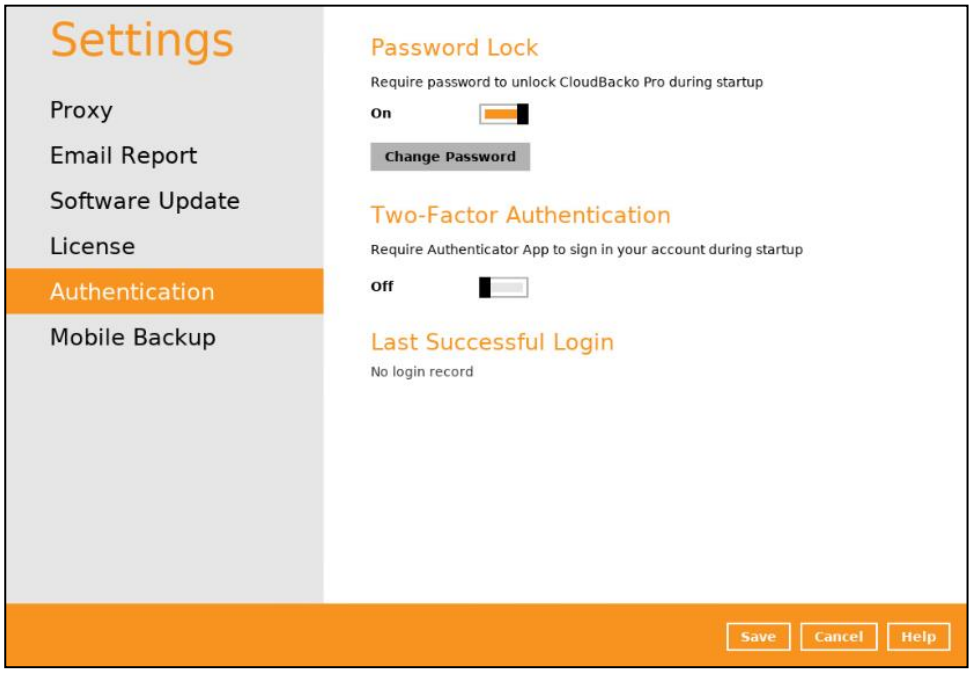


4. Click **Save** to store the settings.

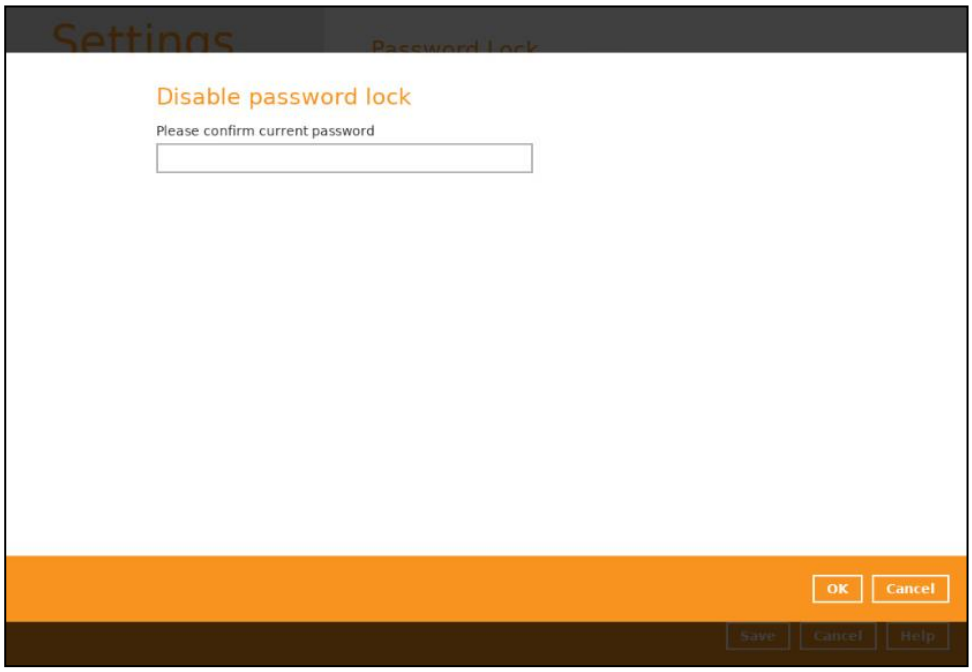


To disable the Password Lock feature, follow the instructions below:

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



2. Enter the current password for authentication purposes and click **OK**.



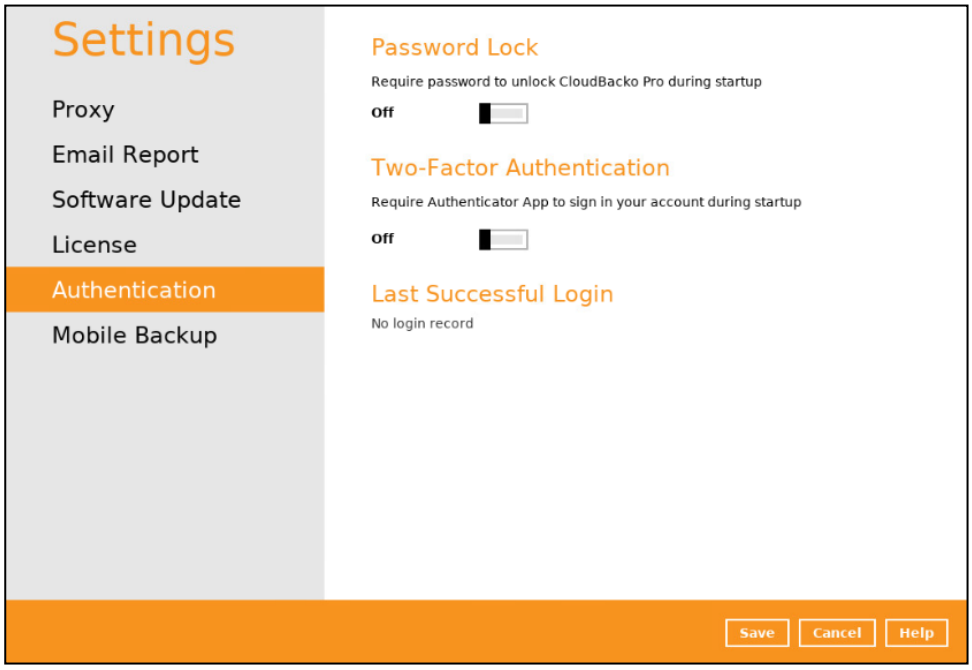
3. Click the **Save** button to store the settings.

Two-Factor Authentication

To enable the two-factor authentication feature and add a mobile device, follow the instructions below:

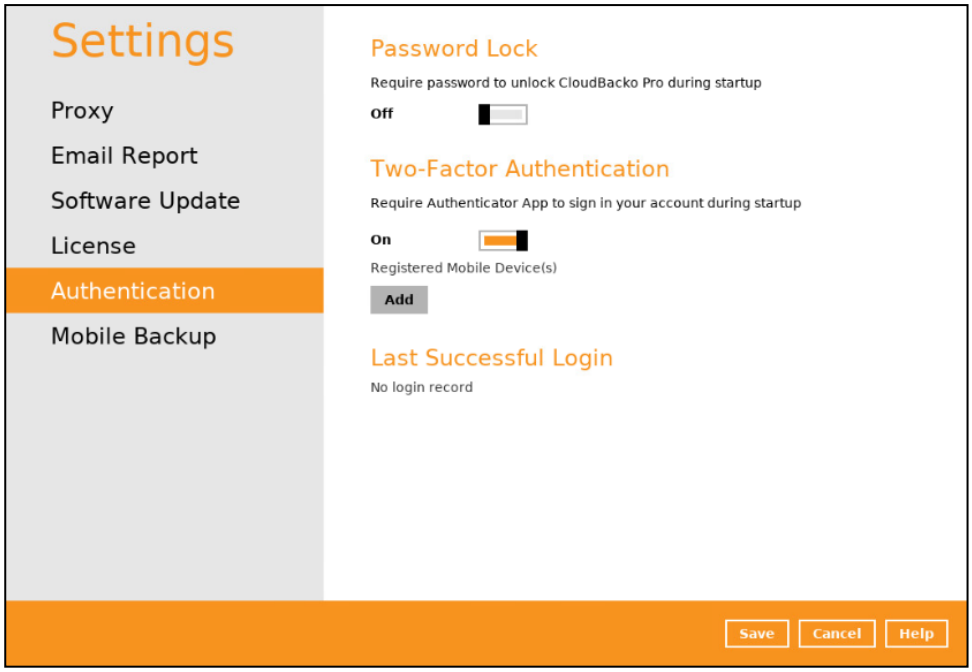
NOTE
The CloudBacko app or a third-party **TOTP Authenticator** is needed for 2FA.

1. Go to **Settings** > **Authentication > Two-Factor Authentication**.



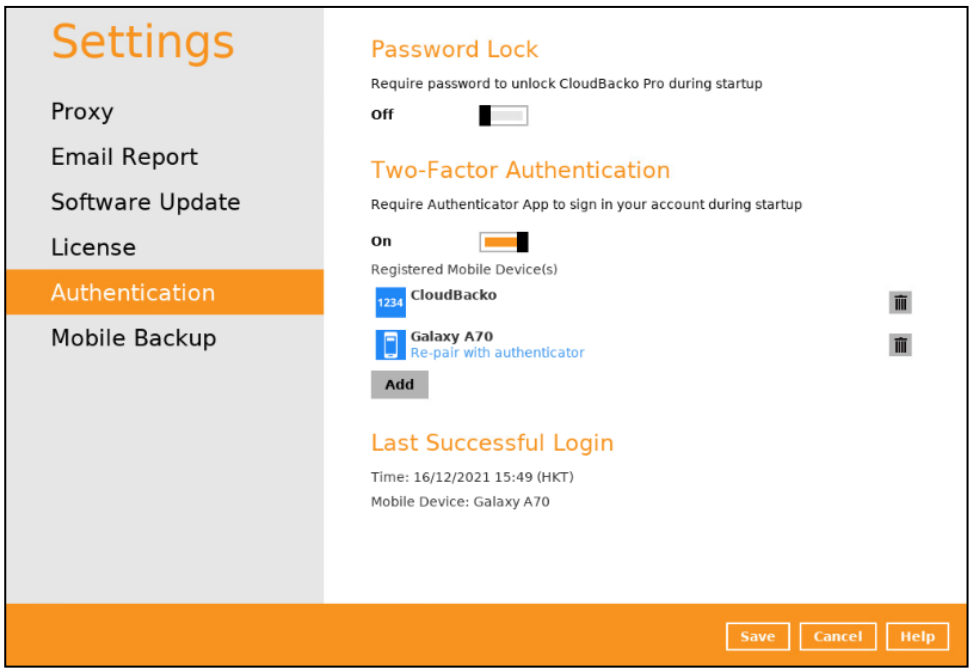
2. Swipe lever to the right to turn it on. Click **Add**.

   For the detailed step-by-step procedure on how to add a mobile device, please refer to CloudBacko App v1 User Guide for Android and iOS.

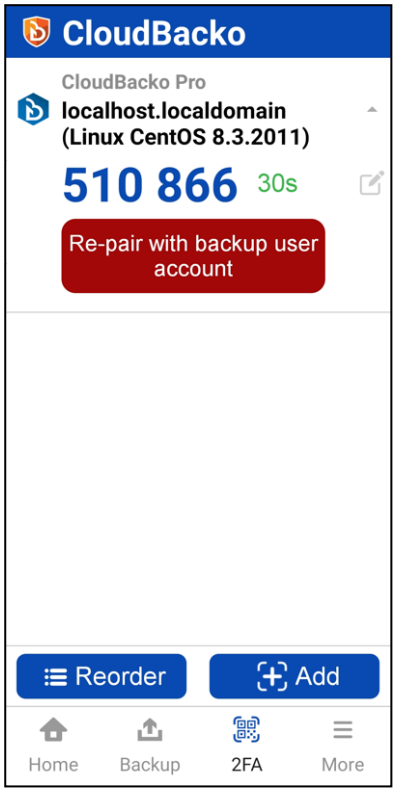


To re-pair the authenticator, follow the instructions below:

1. Go to **Settings** > **Authentication > Two-Factor Authentication**. Click **Re-pair with authenticator**.

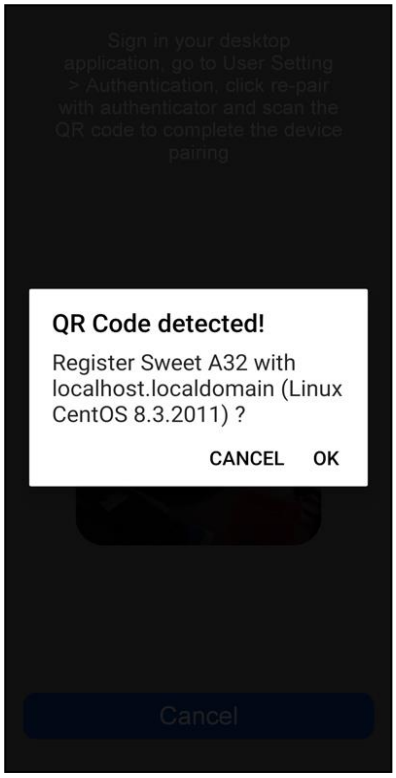


2. In the CloudBacko app, go to 2FA then tap **Re-pair with backup user account**.



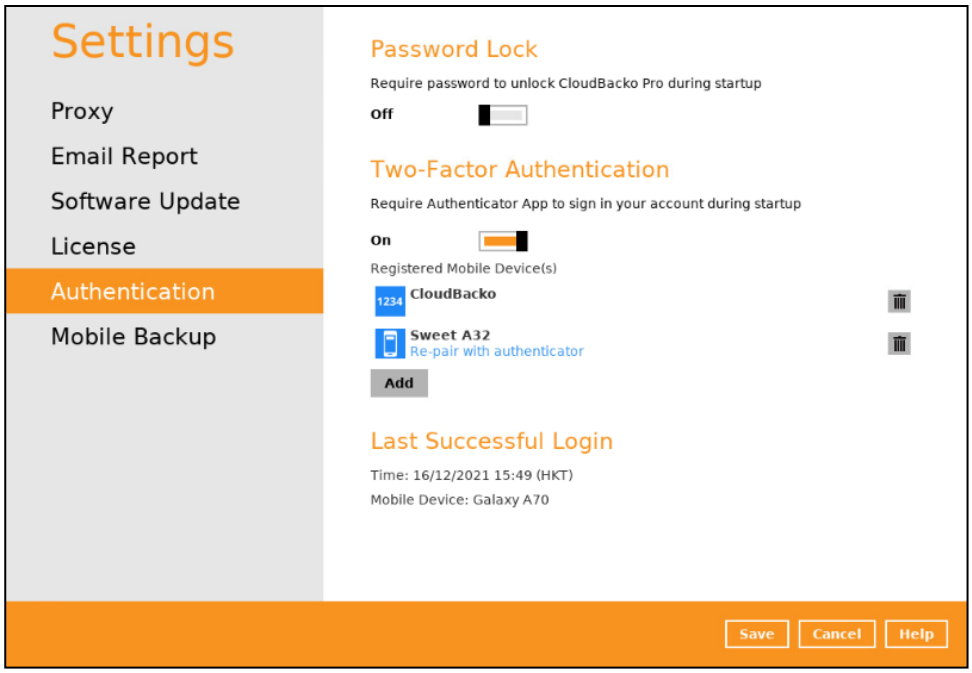
3. Scan the QR Code to re-pair with authenticator.

4. QR Code is detected, tap **OK** to proceed.



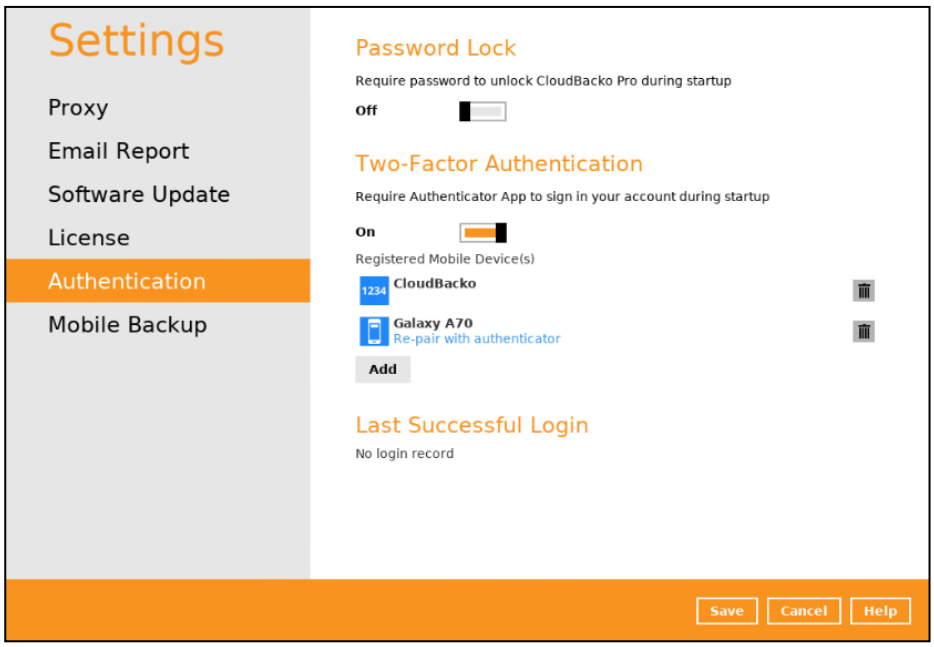
5. The migrated 2FA account has been successfully re-paired.

6. The original device will be changed by the replacement device.

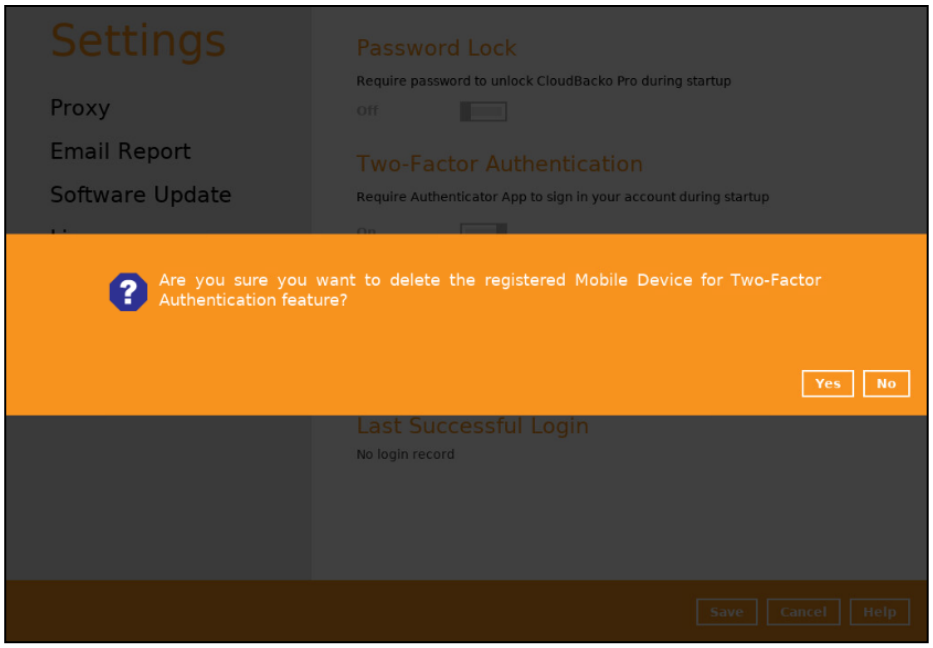


To remove a mobile device, follow the instructions below:

1. Click the  button on the right side of the registered mobile device.



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



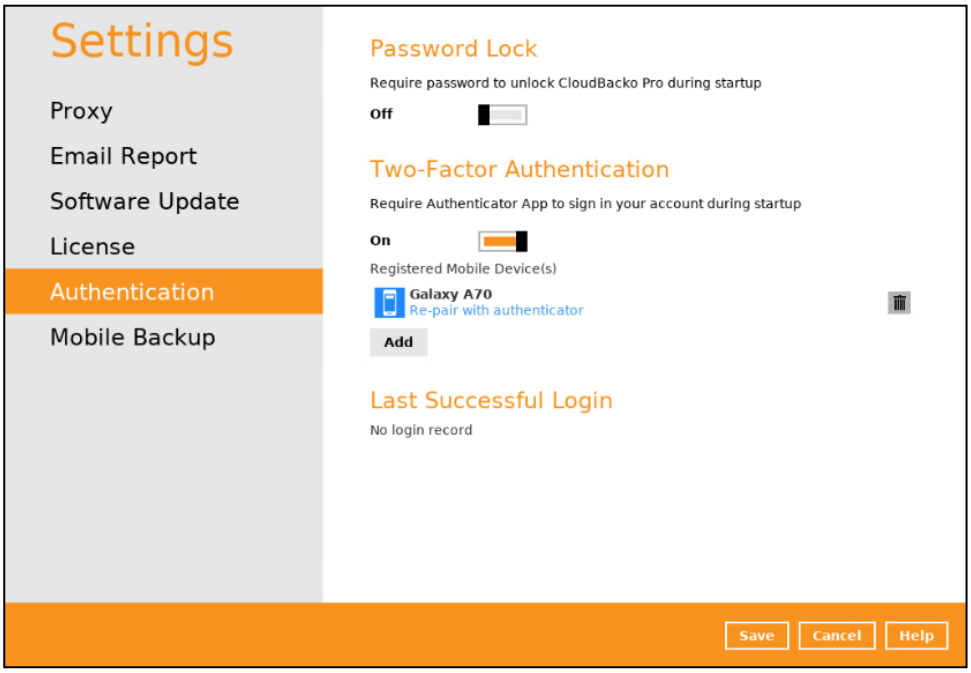
3. Mobile device is successfully removed.

To disable the two-factor authentication feature, follow the instructions below:

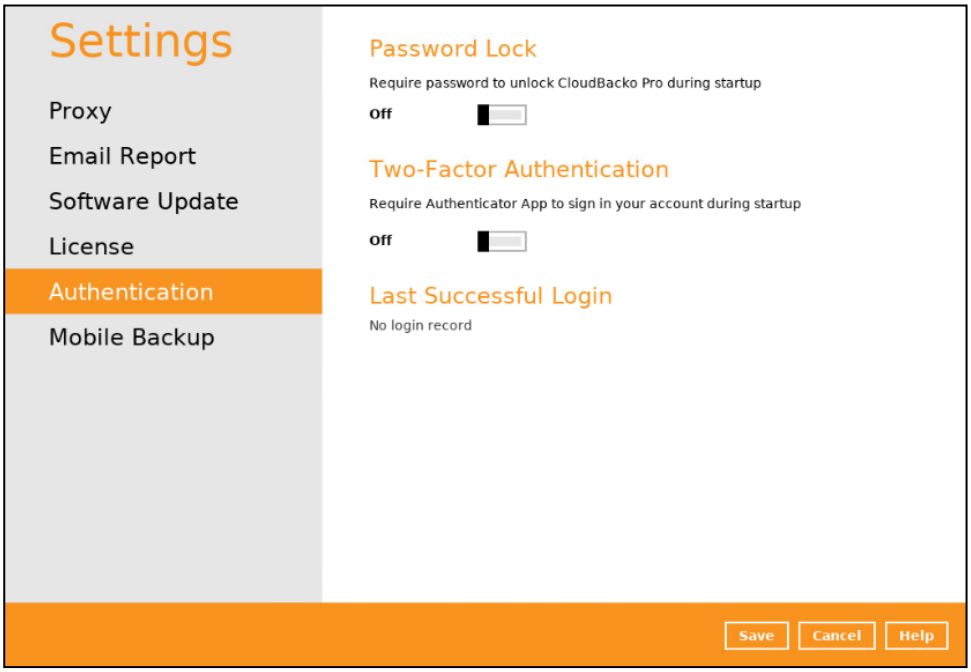
NOTE

Sliding the switch to right hand side will only turn off the two-factor authentication but it will not automatically delete the registered mobile device(s) for Two-Factor Authentication. If you need to delete the registered mobile device(s), this must be done manually first before disabling Two-Factor Authentication

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

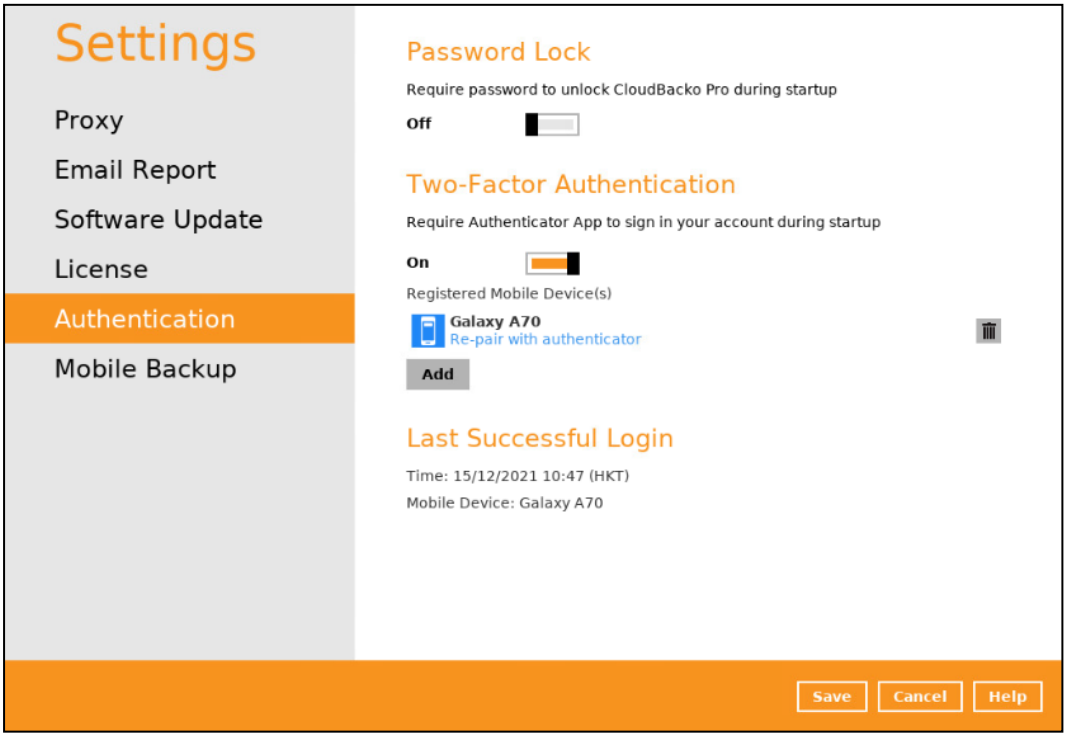


2. Click **Save** to save the settings.

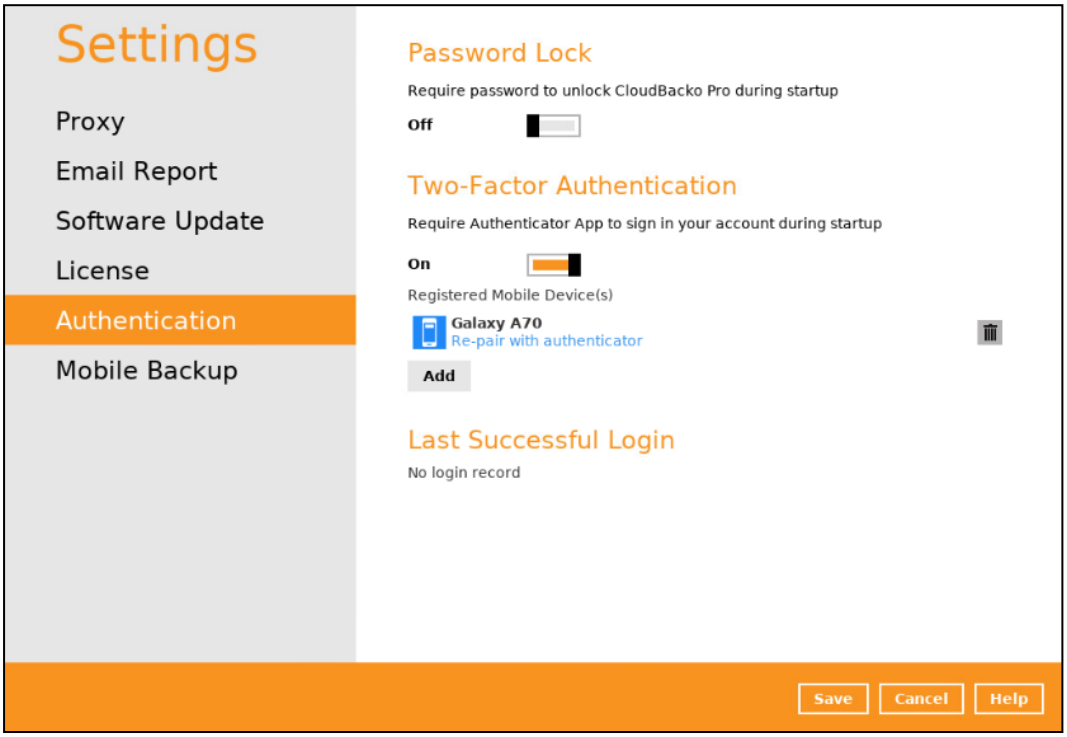


Last Successful Login

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.



7.7.6 Mobile Backup

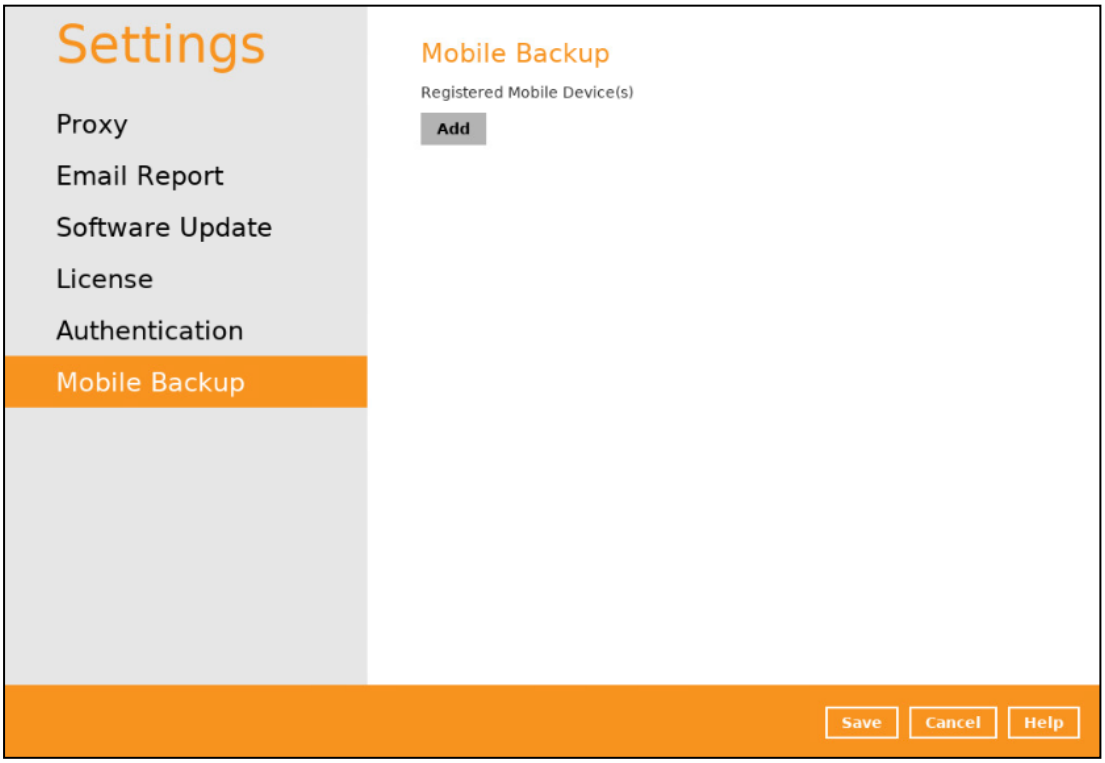
You can use the Mobile Backup function to:

- 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 device must be registered first for mobile backup on CloudBacko Pro.

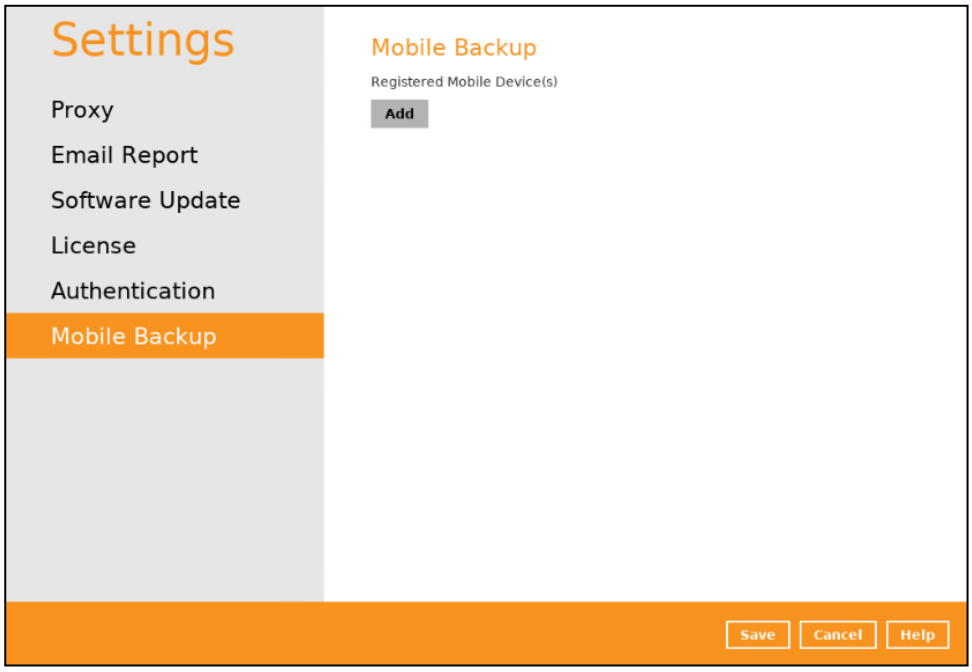
- Restore to a different mobile device on the same operating system.
- Restore to a different mobile device on another operating system, i.e., Android to iOS or iOS to Android.



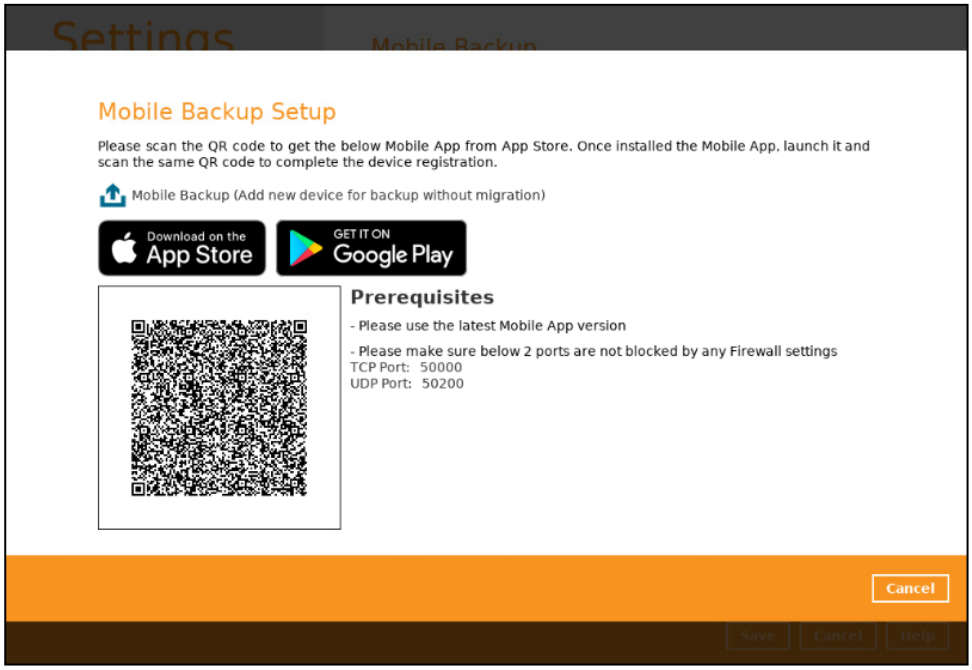
Add one or more device(s) registered for Mobile Backup

To add a mobile device, follow the instructions below:

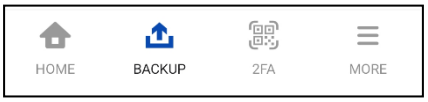
1. Go to **Settings** > **Mobile Backup** and click **Add**.

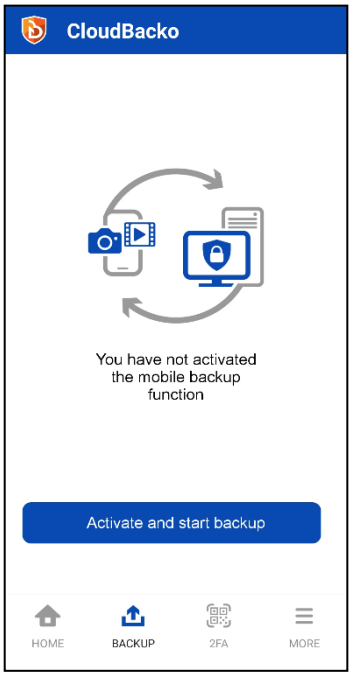


2. Download the CloudBacko app from Google Play Store for an Android device and from App Store for an iOS device, then scan the QR code.



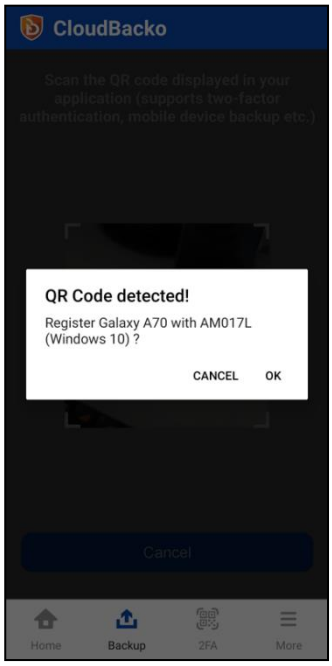
3. In the CloudBacko app, go to **BACKUP.** Tap the **Activate and start backup** link to scan the QR Code on the CloudBacko Pro.



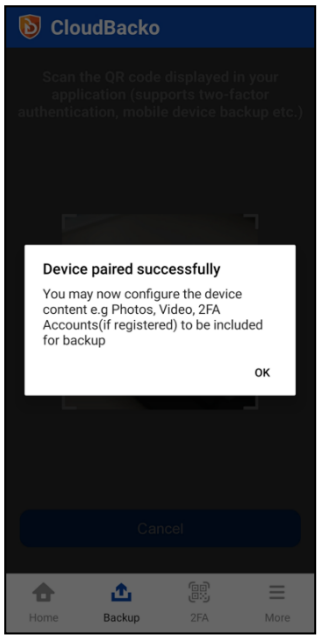


4. Scan the QR Code which can be found in CloudBacko Pro. Otherwise, tap **Cancel** to return to previous screen.

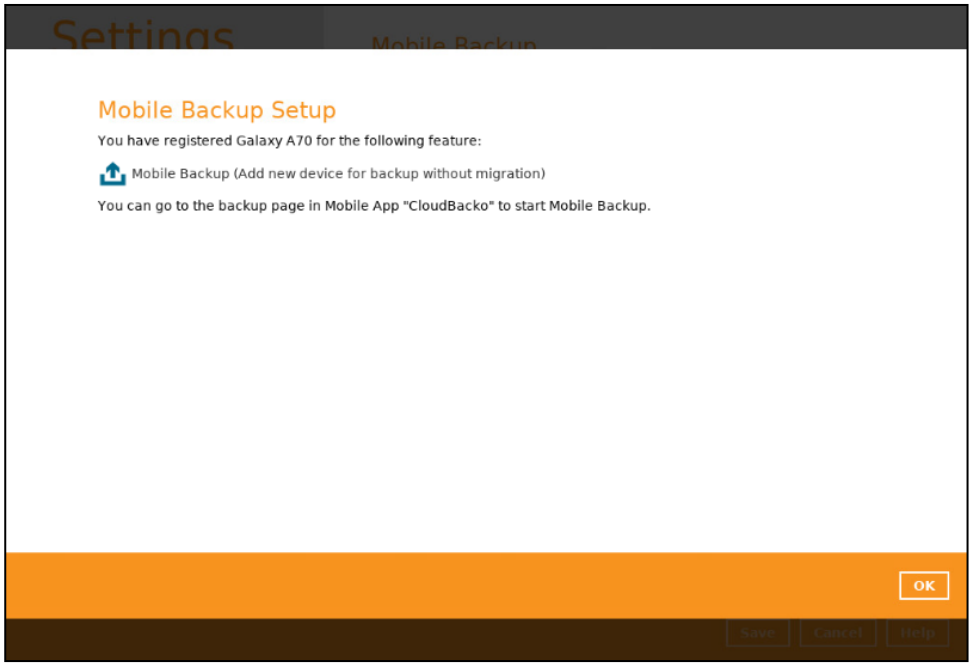
5. QR Code is detected, tap **OK** to proceed. Otherwise, tap **Cancel**.



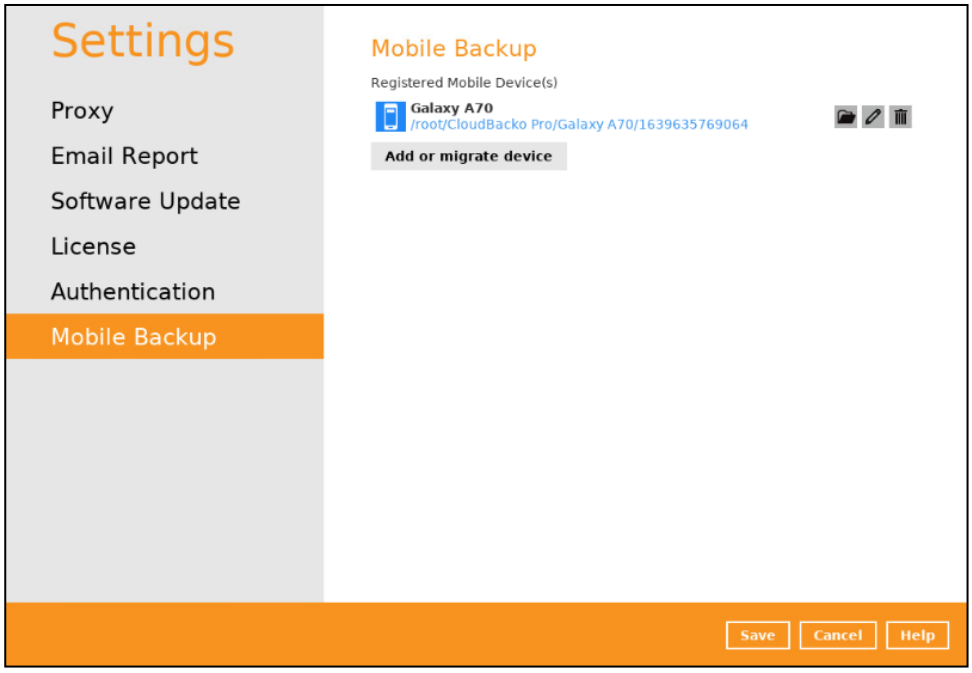
6. Mobile backup registration is successful. Tap **OK** to proceed.



7. The Mobile backup registration is successful in CloudBacko Pro. In this example, the registered mobile device is “Galaxy A70”. Click **OK** to return to previous screen.



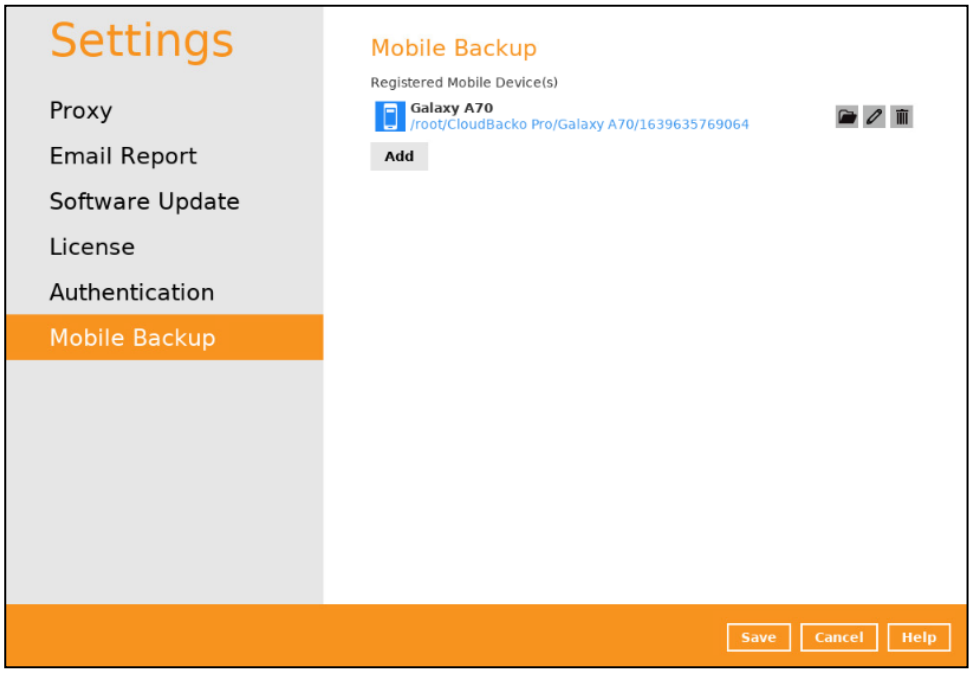
The registered mobile device will now be displayed in the Mobile Backup page.



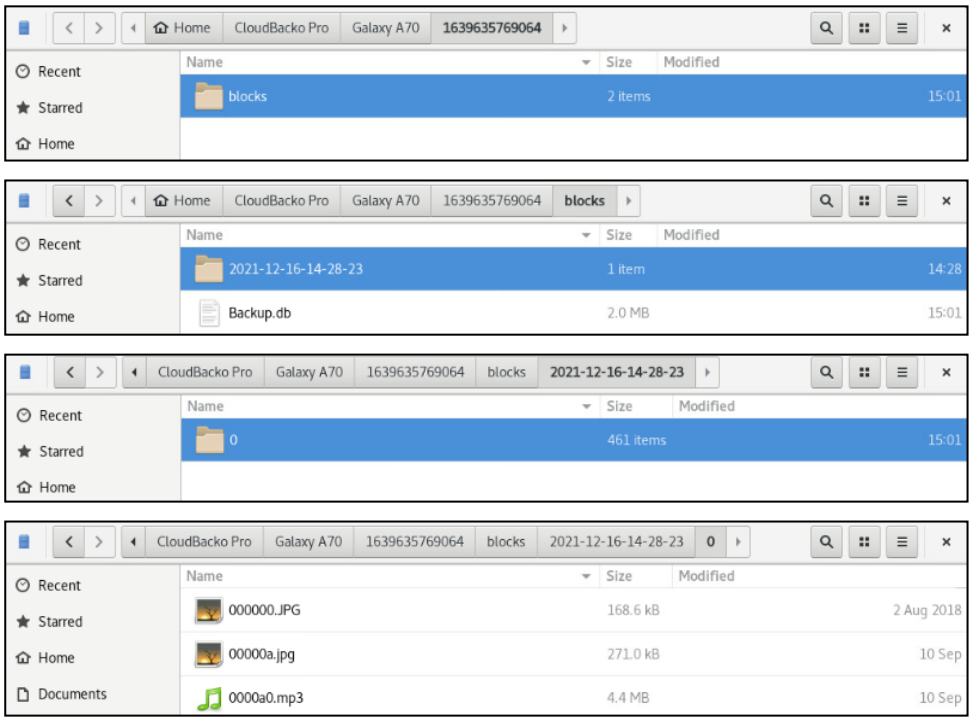
View backed up photos and videos saved in the mobile backup destination

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.



3. Once done, click the **X** button to exit.

Change mobile backup destination location 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.**

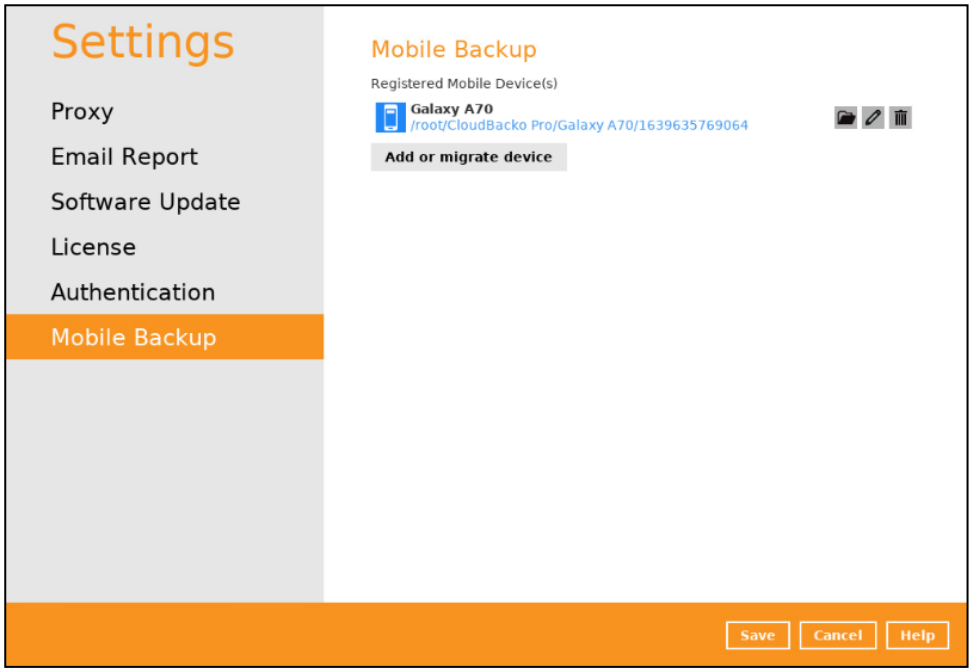
  If Free up space is disabled on the CloudBacko Mobile app, there are two (2) options available, copy the previously backed-up photos, videos, documents and 2FA accounts to the new location or continue to back up in the new location.

  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:

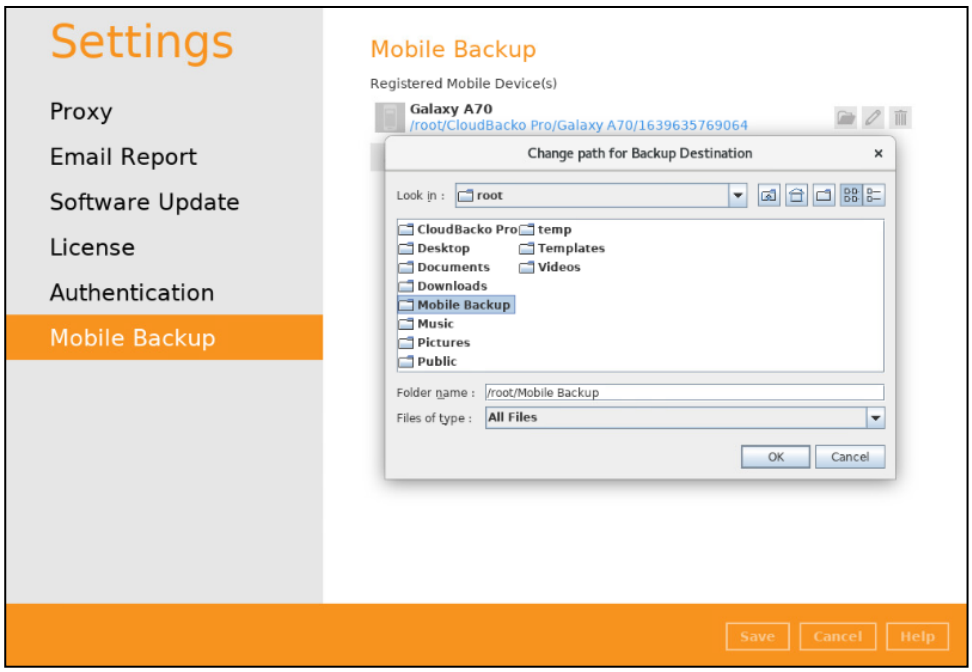
1. From the old location, secure a copy of the previously backed-up photos, videos, documents and 2FA accounts. Skip this step if Free up space is disabled and proceed to Step 2.
2. Launch **CloudBacko Pro**.

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



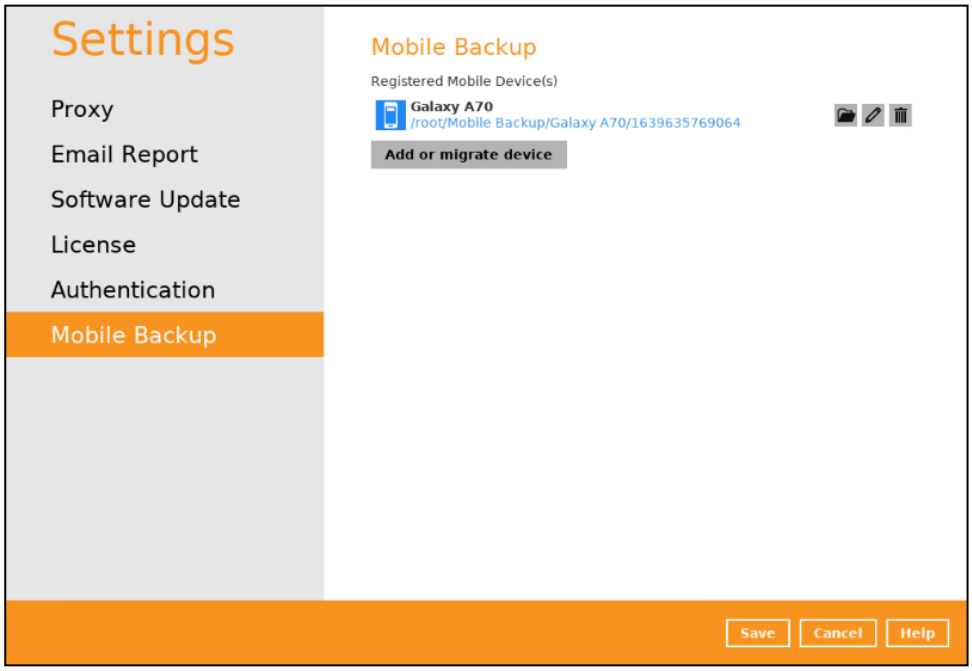
4. **Change path for Backup Destination** screen will be displayed. Select a new mobile backup destination then click **OK**.

   In this example, the new mobile backup destination will be **/root/Mobile Backup**.



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

   Mobile backup destination is successfully changed to **/root/Mobile Backup**.



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 to the new mobile backup destination.

Change mobile backup destination location to new machine

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, videos, documents and 2FA accounts 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.

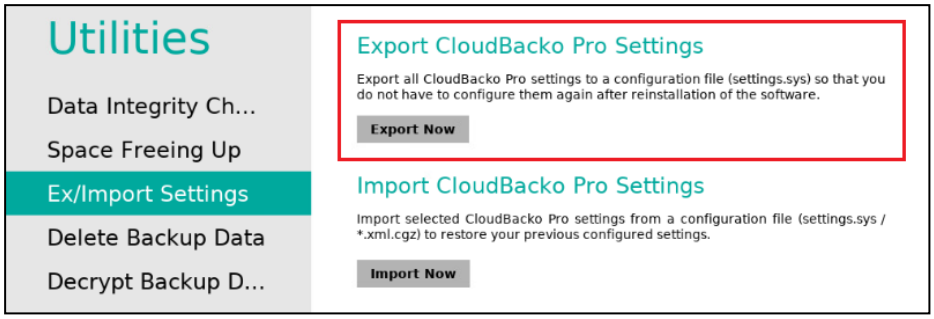
Even if Free up space is disabled, it is recommended to copy the previously backed-up photos, videos, documents and 2FA accounts to the new machine otherwise the photos, videos, documents and 2FA accounts on the mobile device will be backed-up again from scratch.

NOTE

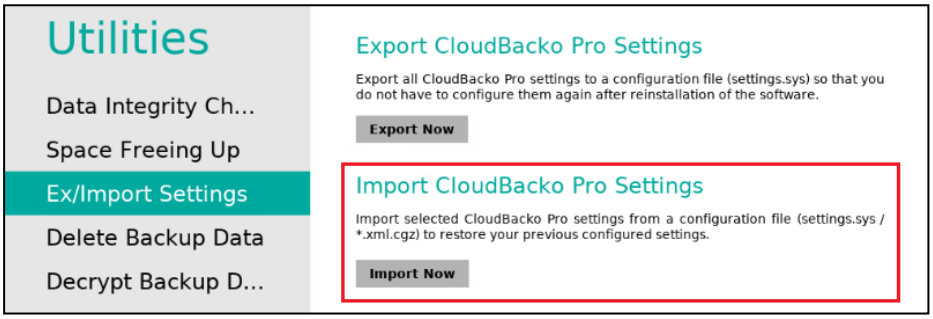
If the machine is lost/stolen, changing the mobile destination is not supported as it is required to re-register your mobile devices on CloudBacko Pro and perform backup of photos, videos, documents and 2FA accounts again.

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.

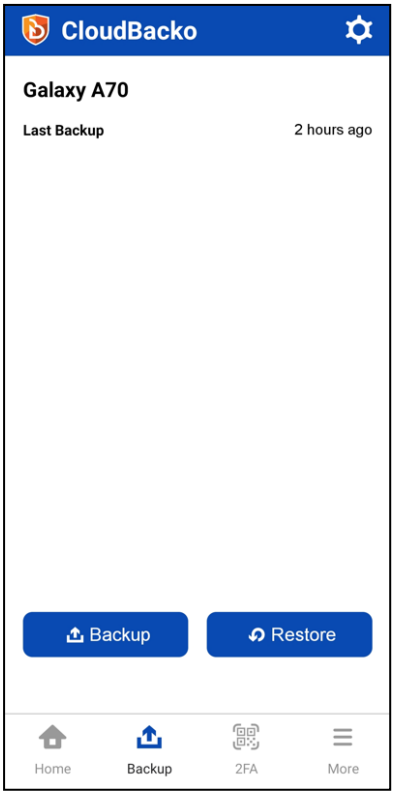


2. On the new machine, install **CloudBacko Pro**.
3. Apply the CloudBacko license to the new installation.
4. Copy the configuration file (settings.sys) from the old machine to the new machine. Import it by going to **Utilities** > **Ex/Import Setting** then click **Import Now**. Select the destination where the configuration file was saved.



5. If the mobile backup destination needs to be updated, please follow the steps on how to change mobile backup destination to a new location in the same local machine. Otherwise, skip this step and proceed to step 6.
6. Copy the previously backed-up photos, videos, documents and 2FA accounts from the old machine to the new mobile destination.

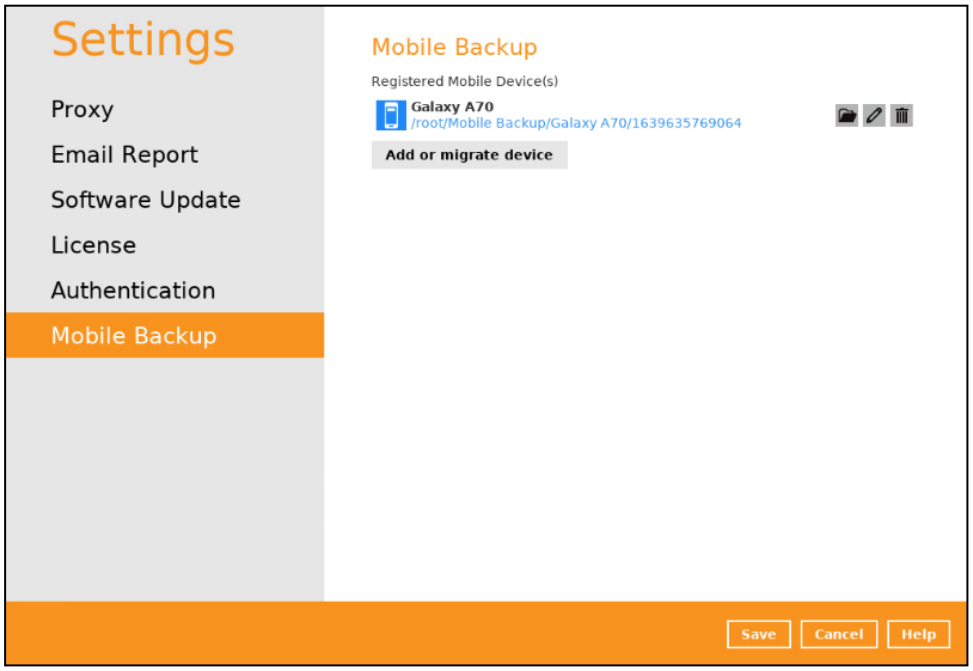
7. Restart the **CloudBacko Pro Services** on the newly installed CloudBacko Pro to restart the MBS.
8. Start backup of photos, videos, documents and 2FA accounts.



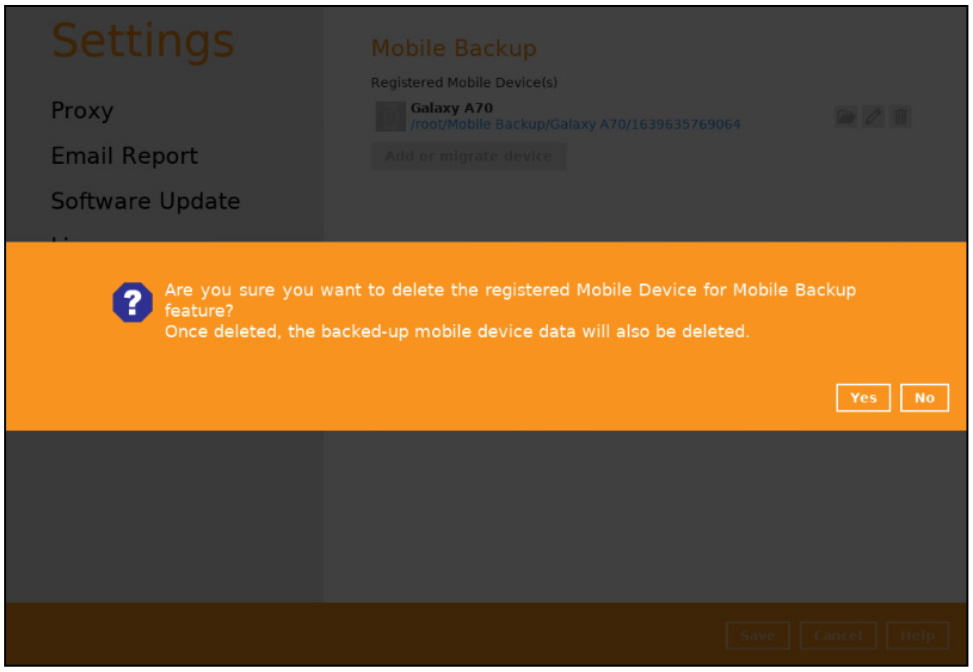
Remove one or more device(s) registered for Mobile Backup.

To remove a mobile device, follow the instructions below:

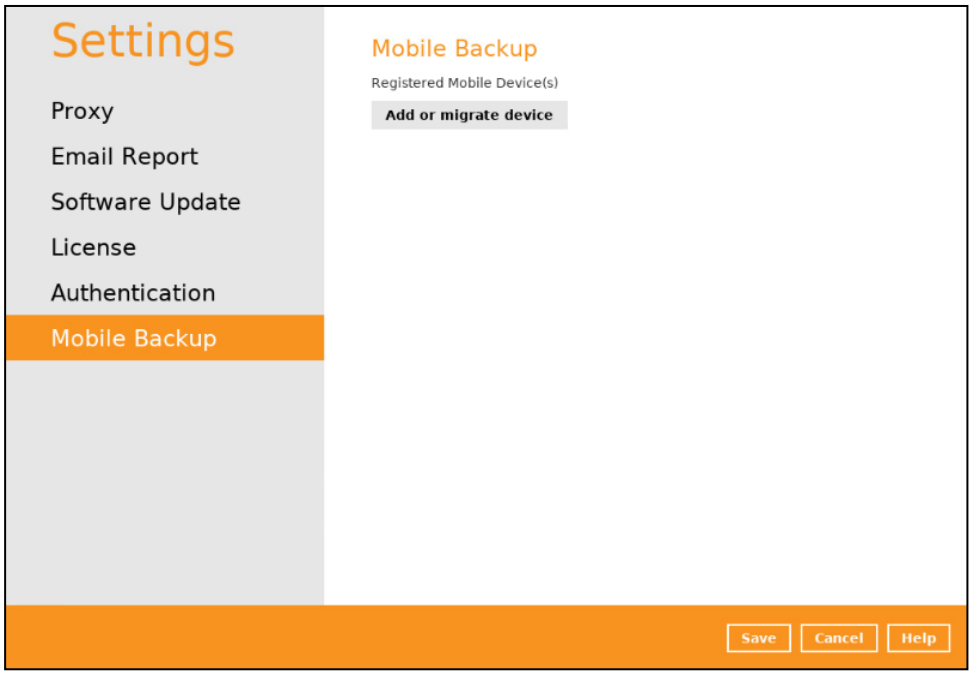
1. Click **Delete** icon on the right side of the registered mobile device.



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

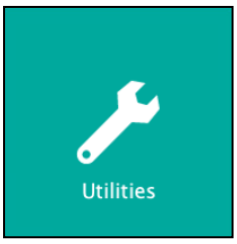


3. Mobile device is successfully removed along with any photos, videos, documents and 2FA accounts backed up in the mobile backup destination.



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.



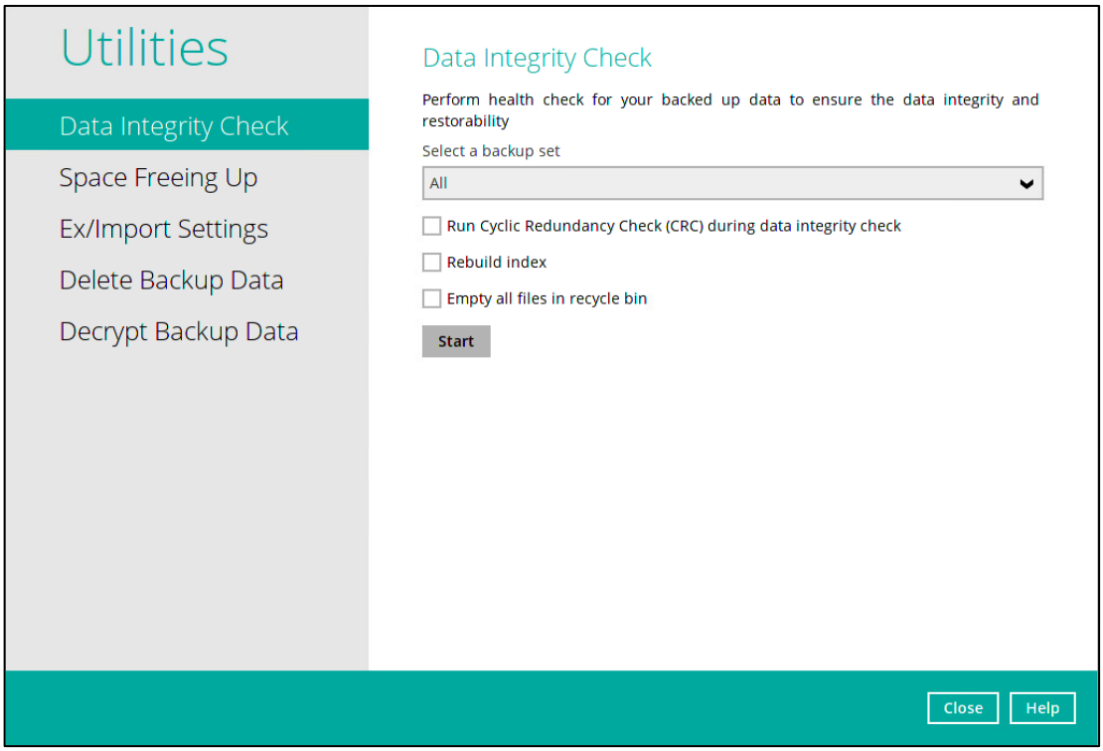
There are five (5) options available for this feature:

- Data Integrity Check
- Space Freeing Up
- Ex/Import 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.

These corrupted files will be removed from the backup destination(s). If these files still exist on the client machine on the next backup job, the CloudBacko Pro will upload the latest copy. However, if the corrupted files are in 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.

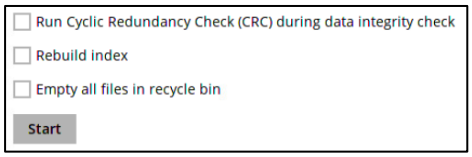
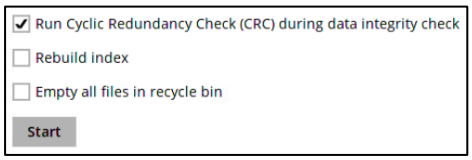
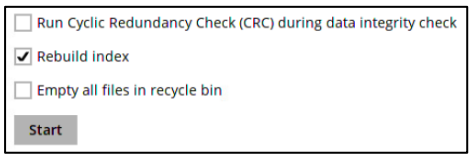
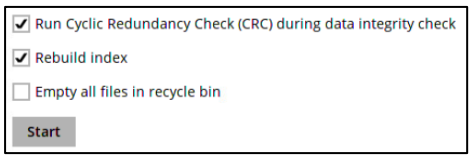
Rebuild Index

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**

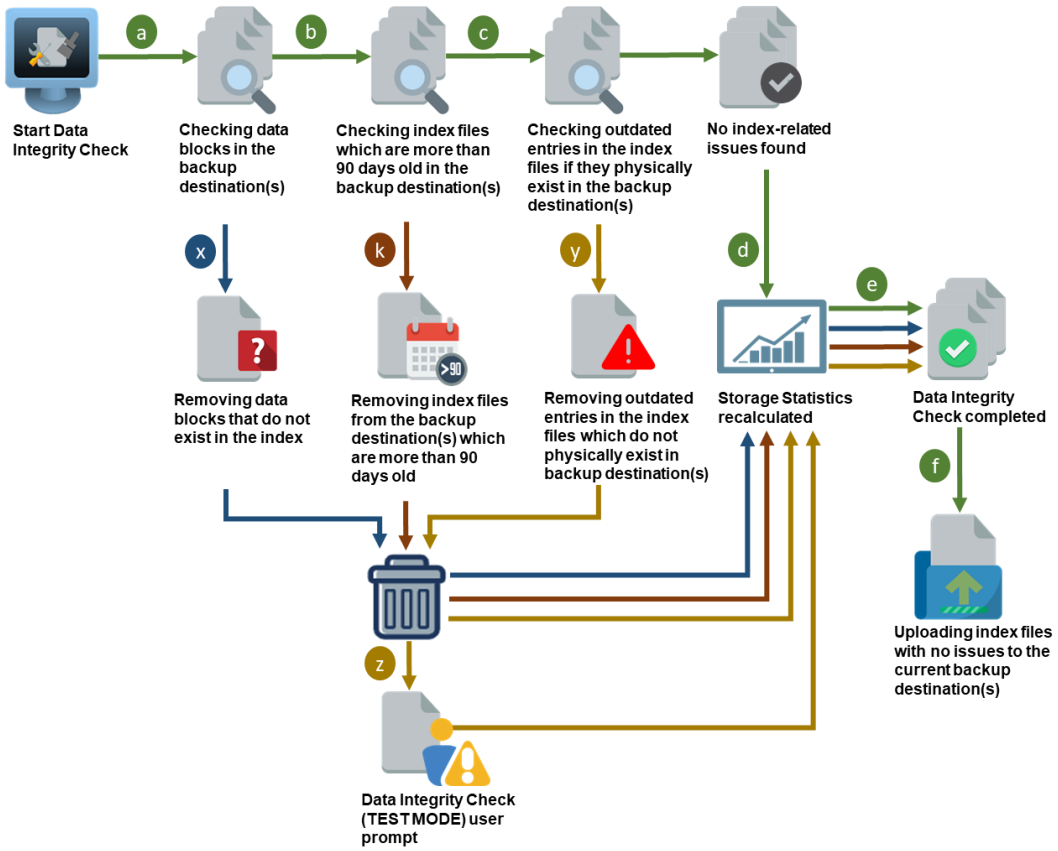
  Disabled Run Cyclic Redundancy Check (CRC) and Rebuild index (Default mode)
- **Option 2**

  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).

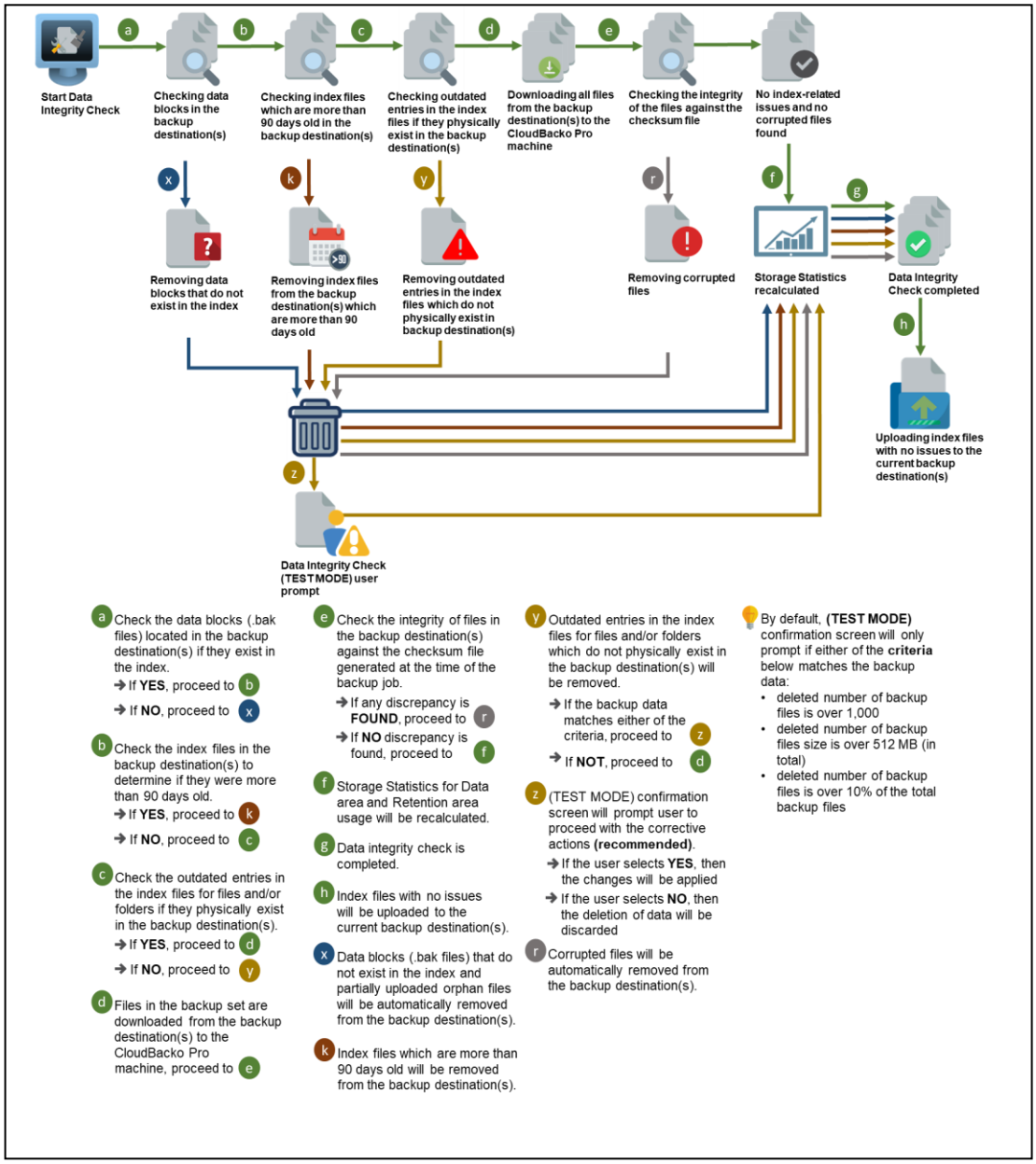
k Index files which are more than 90 days old will be removed from the backup destination(s).

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

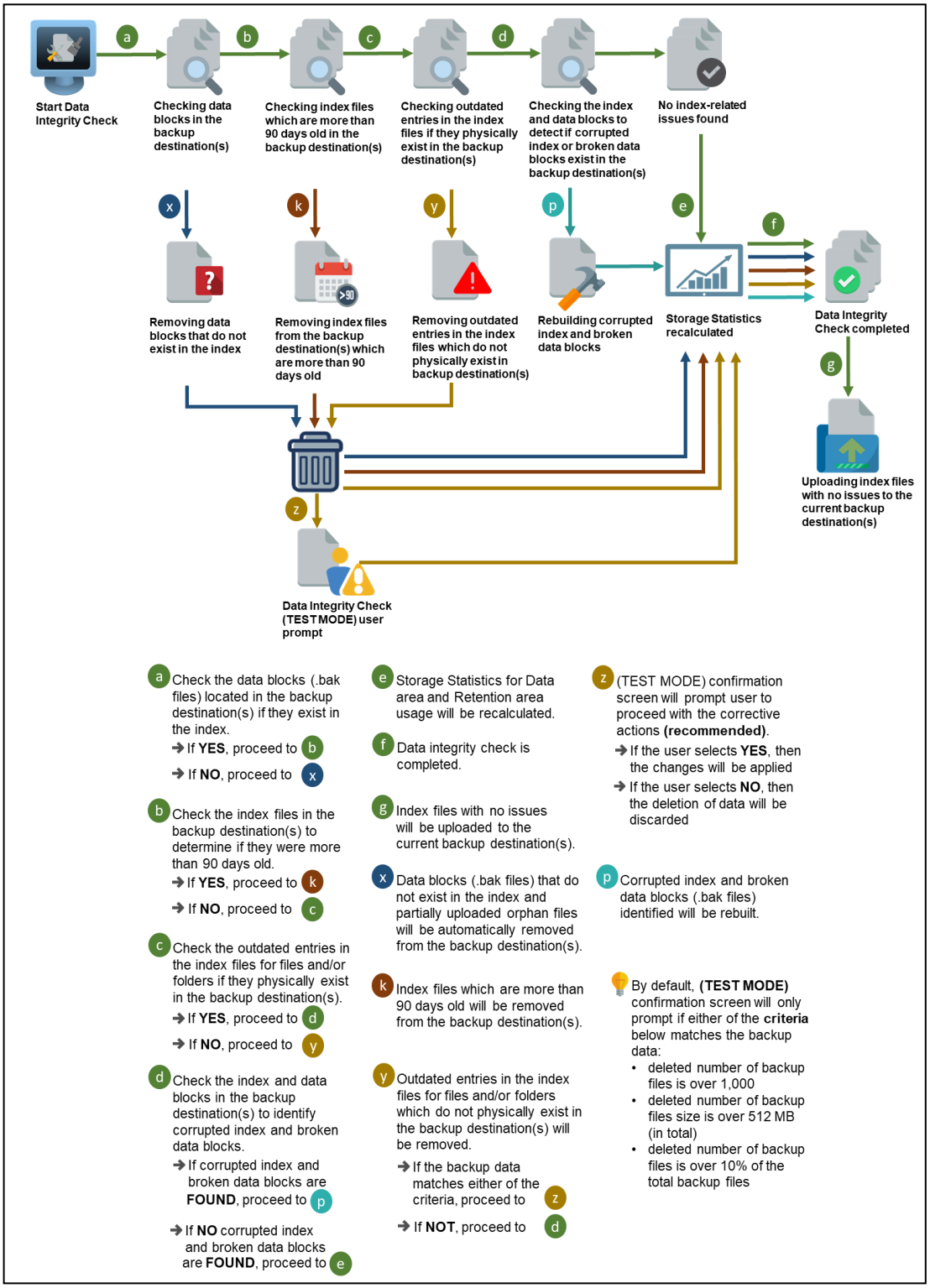
z (TEST MODE) confirmation screen will prompt user to proceed with the corrective actions **(recommended)**.
→ If the user selects **YES**, then the changes will be applied
→ If the user selects **NO**, then the deletion of data will be discarded

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).

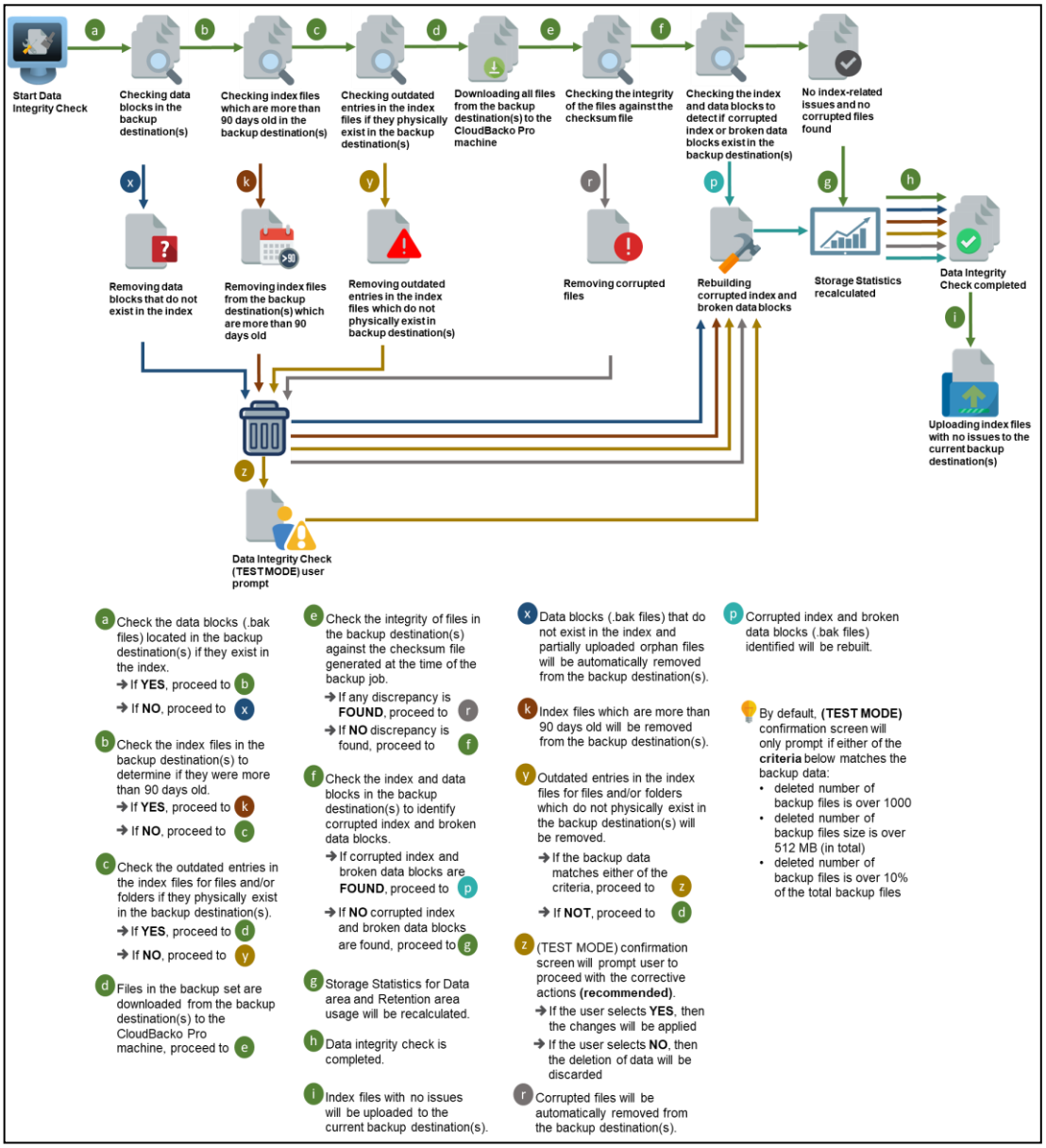
y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.
- ➔ If the backup data matches either of the criteria, proceed to z
- ➔ If **NOT**, proceed to d

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

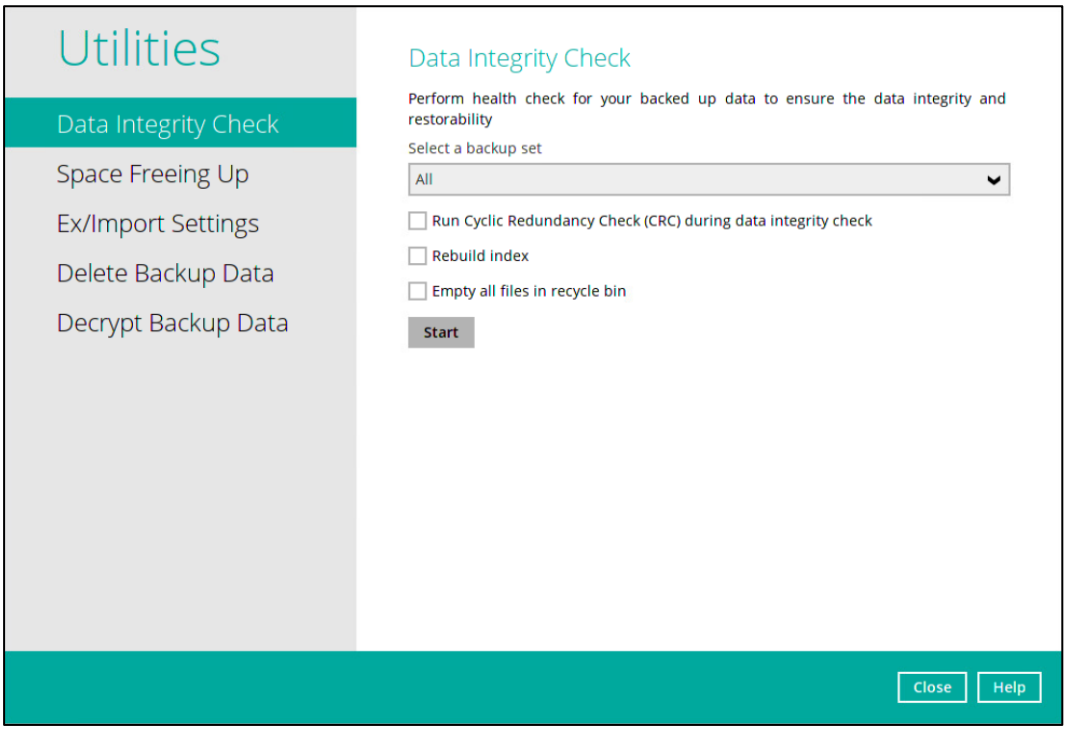
Option 4: Enabled Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Rebuild Index



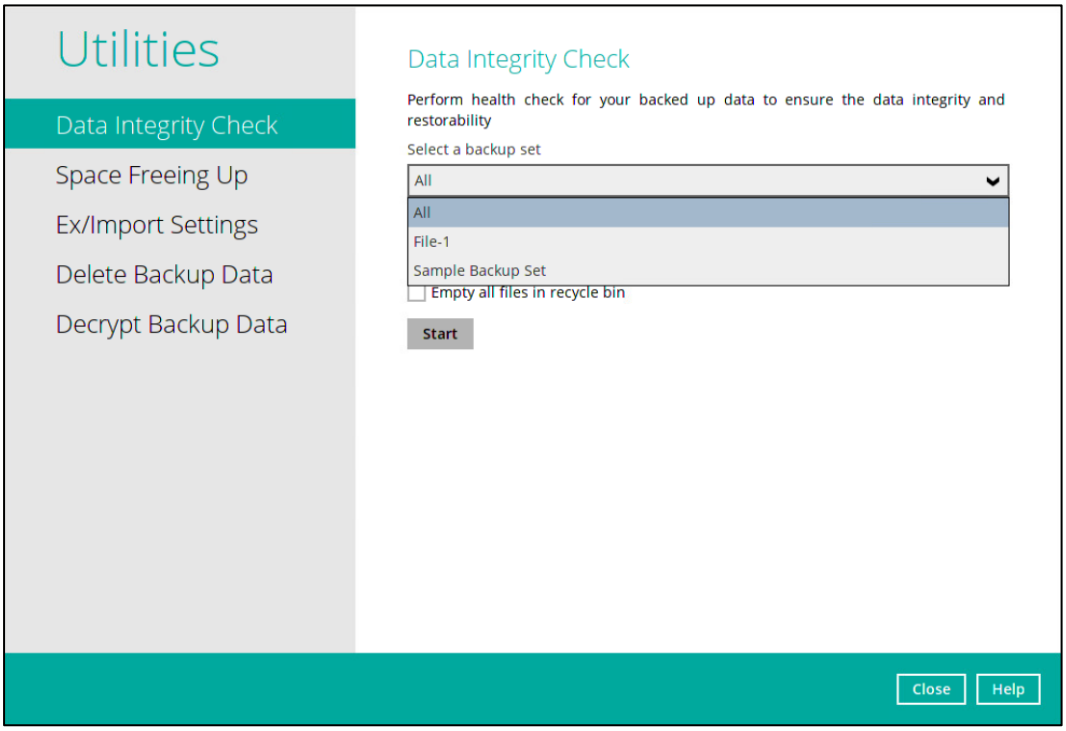
Perform a Data Integrity Check

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

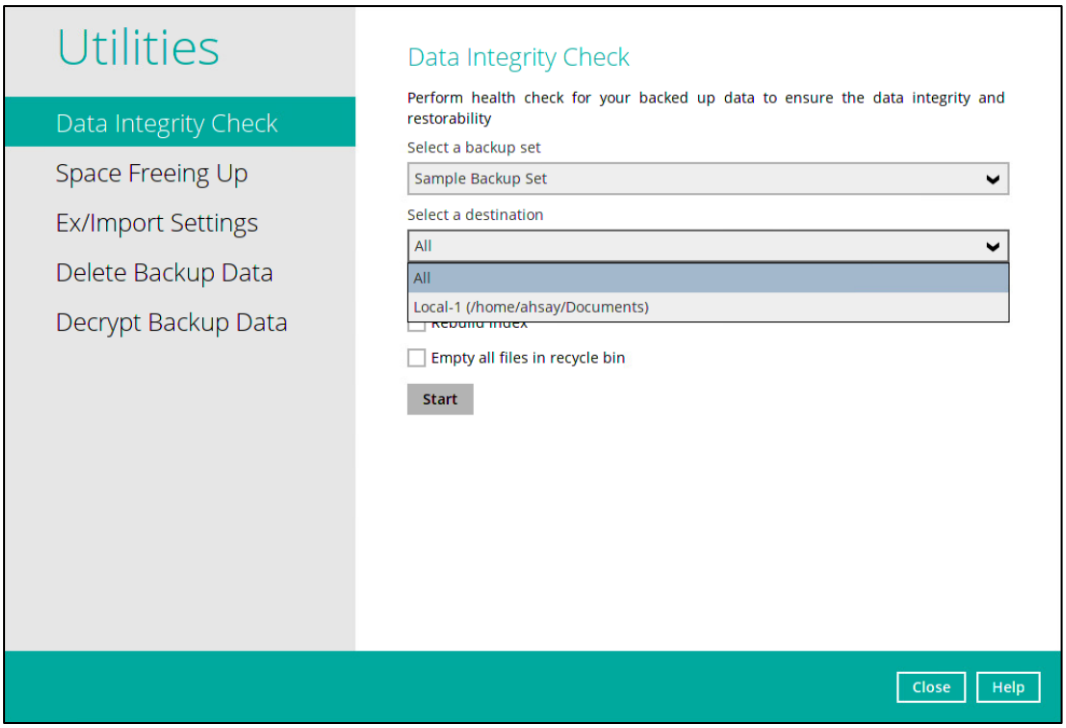
1. Go to the Data Integrity Check tab in the Utilities menu.



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

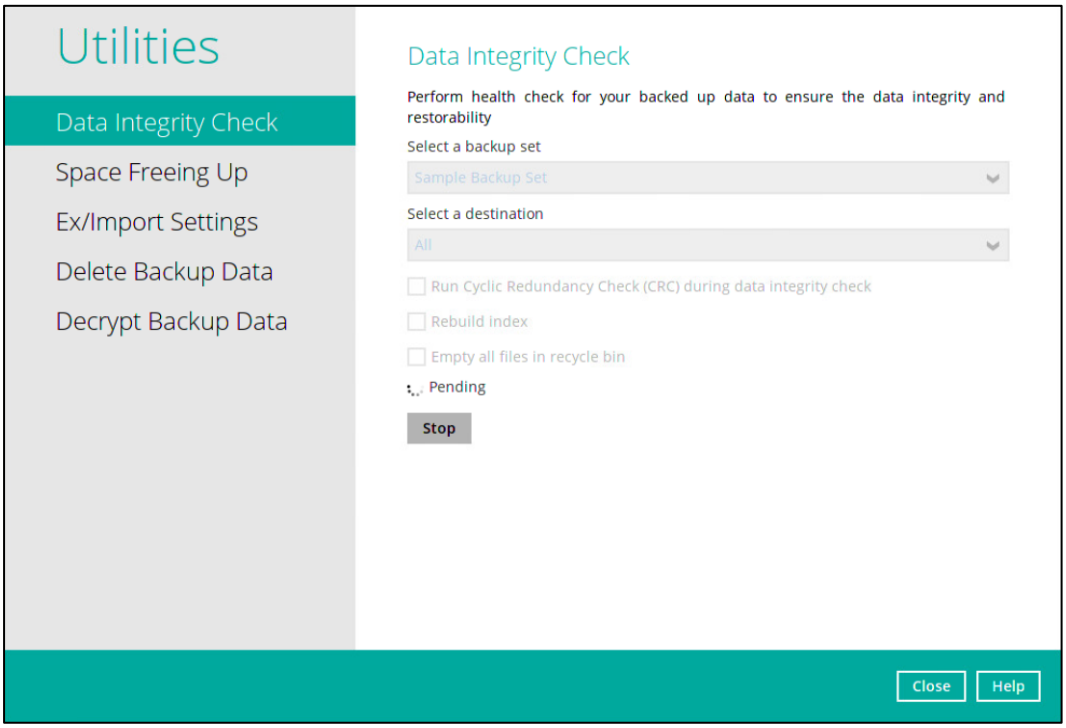


3. Click the drop-down button to select a backup destination.

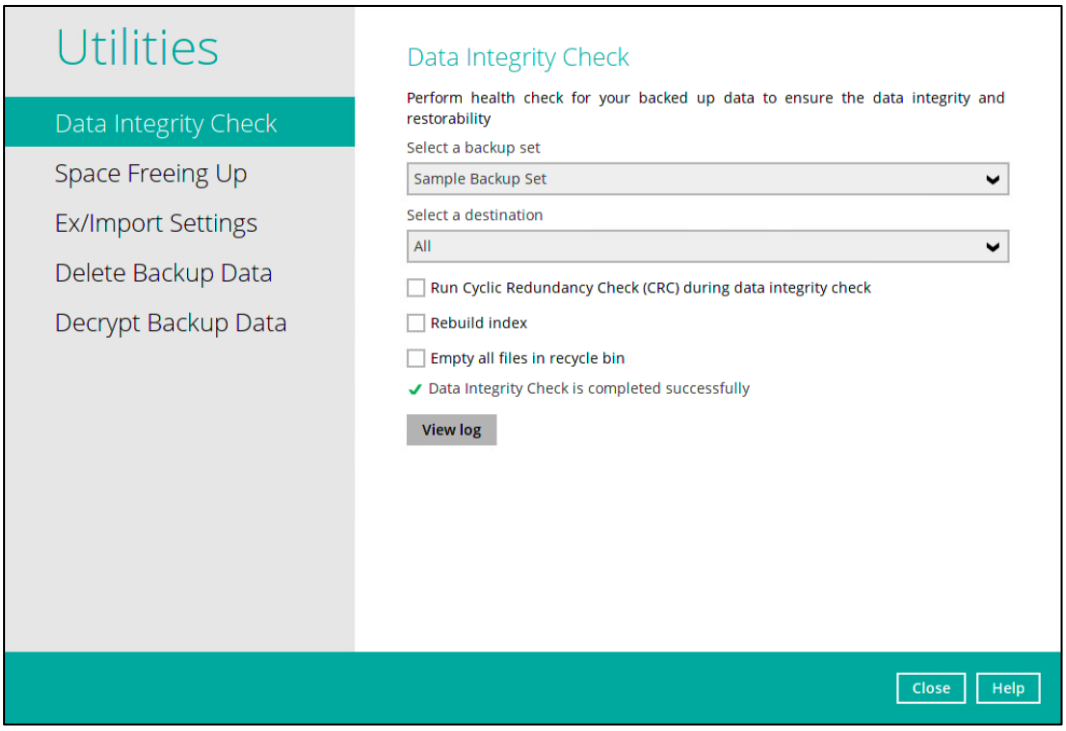


4. Click the **Start** button to begin the Data Integrity Check.

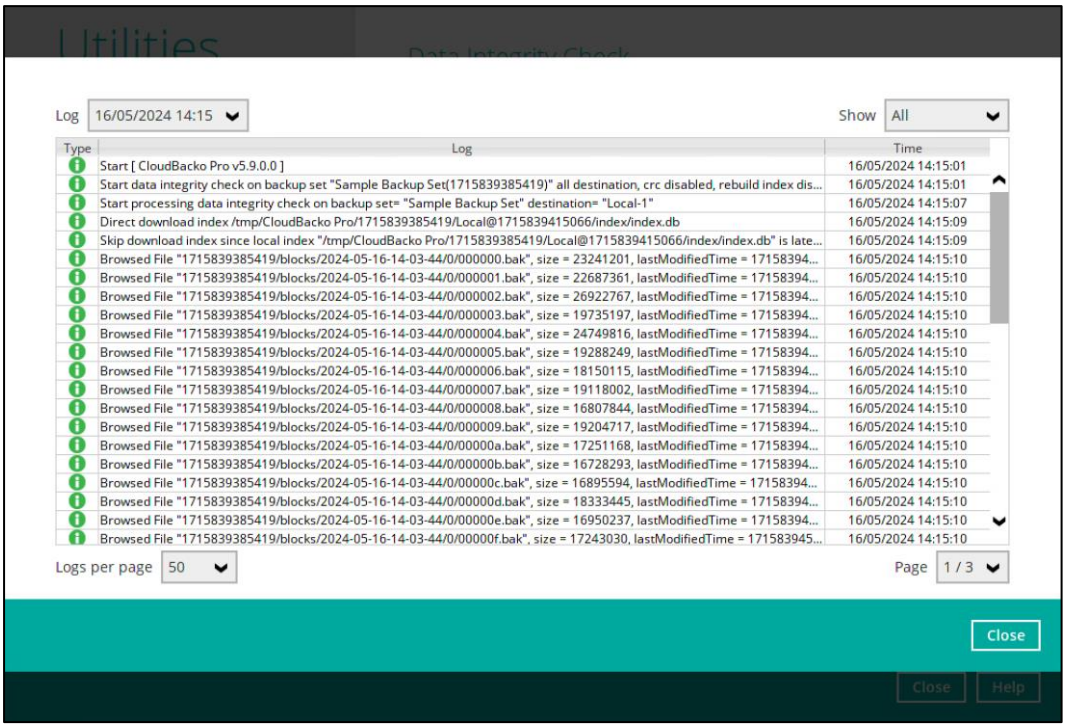
5. Data Integrity Check will start running on the selected backup set(s) and backup destination(s).



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

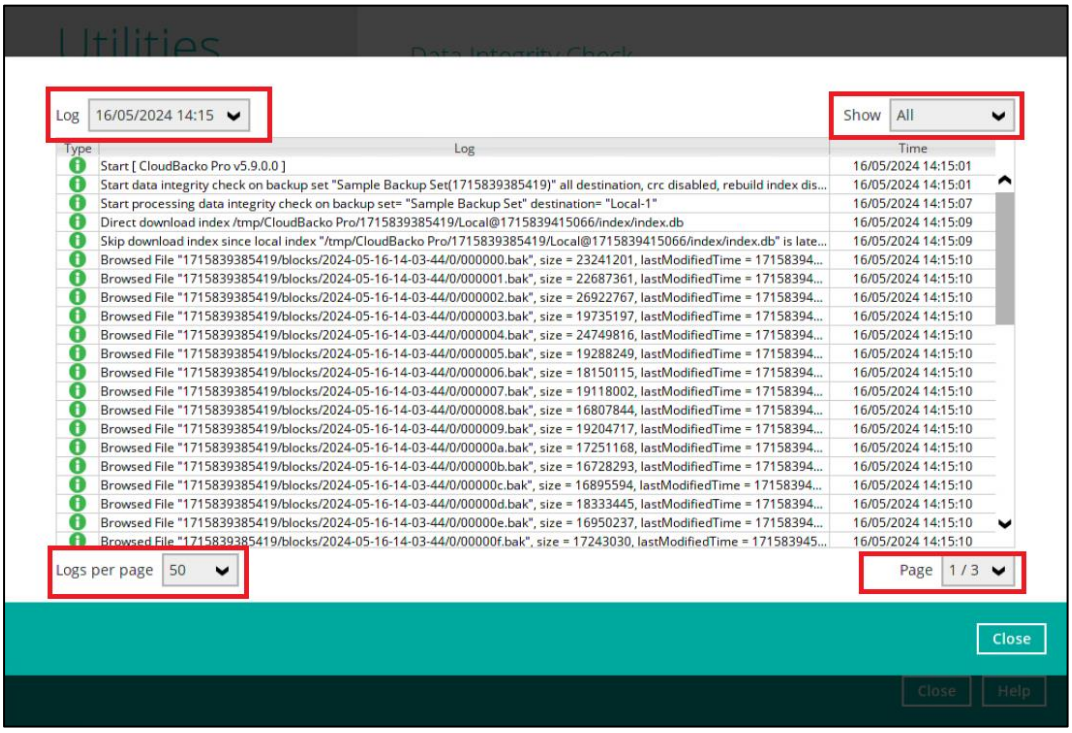


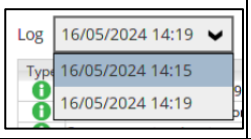
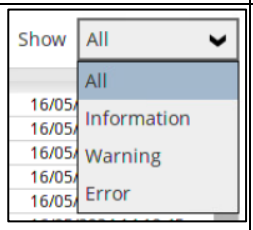
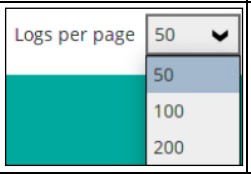
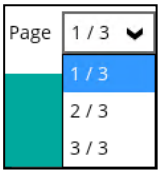
The detailed data integrity check log will be displayed.



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

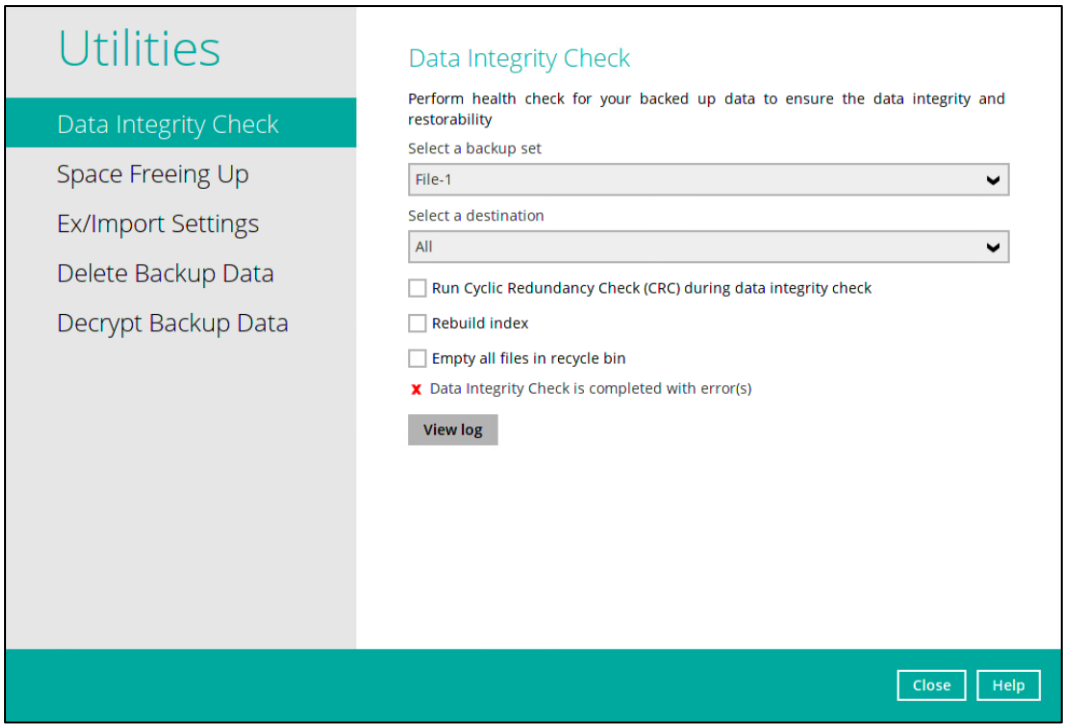
- Log filter
- Show filter
- Logs per page
- Page



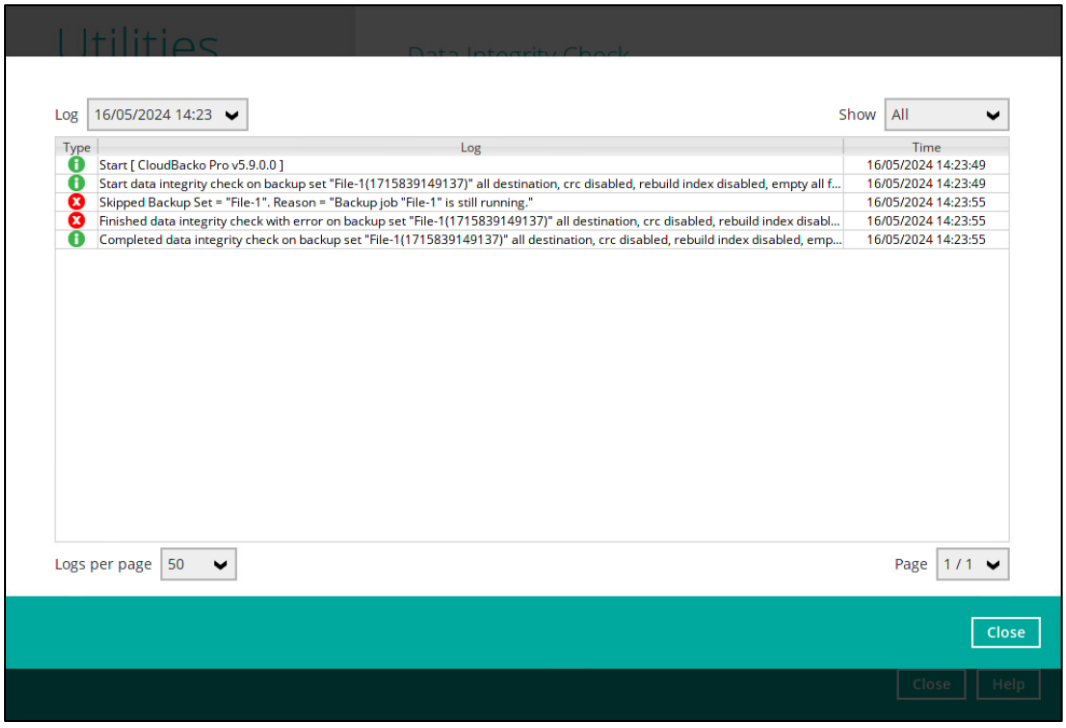
Control	Screenshot	Description
Log filter		This option can be used to display logs of the previous data integrity check jobs.
Show filter		This option can be used to sort the data integrity check log by its status (i.e. All, Information, Warning, and Error). With this filter, it will be easier to sort 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).

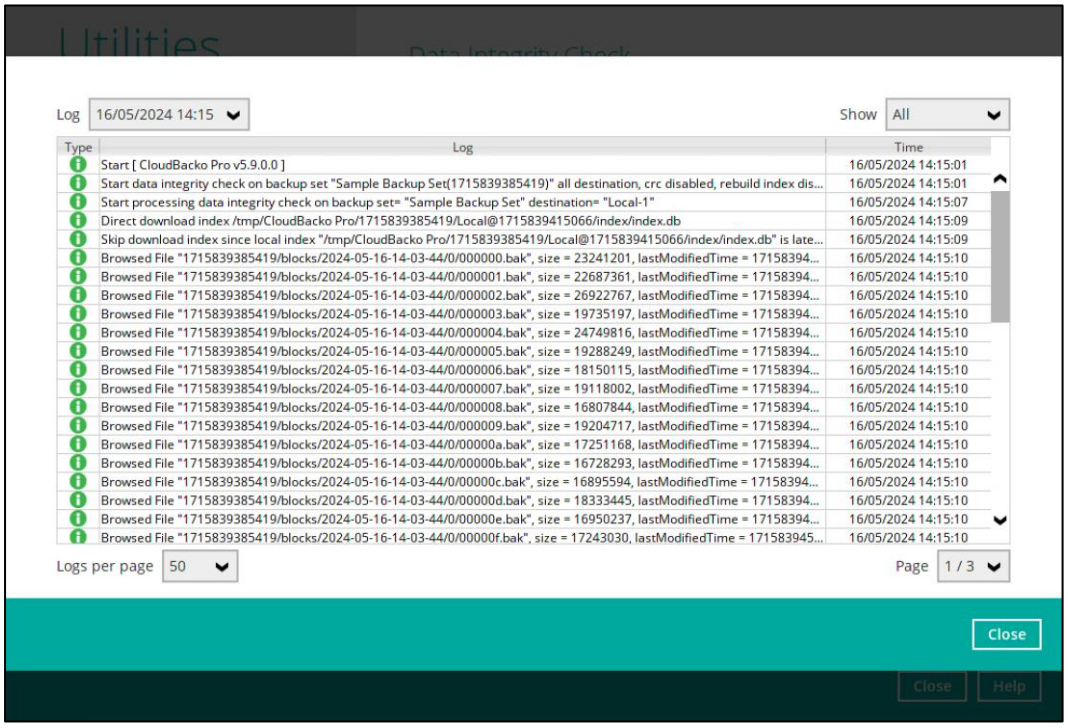


7.8.1.2 Data Integrity Check Result

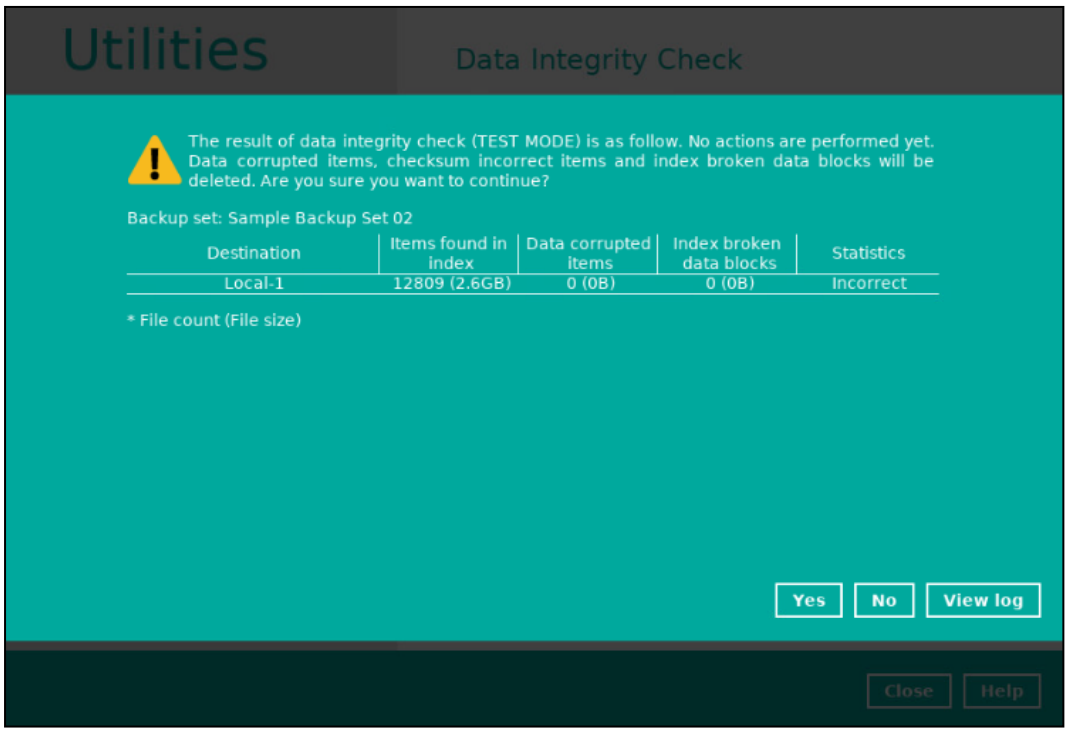
There are two possible outcomes after the completion of a data integrity check:

- 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 any index-related error(s) or data corrupted item(s) is 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** 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.

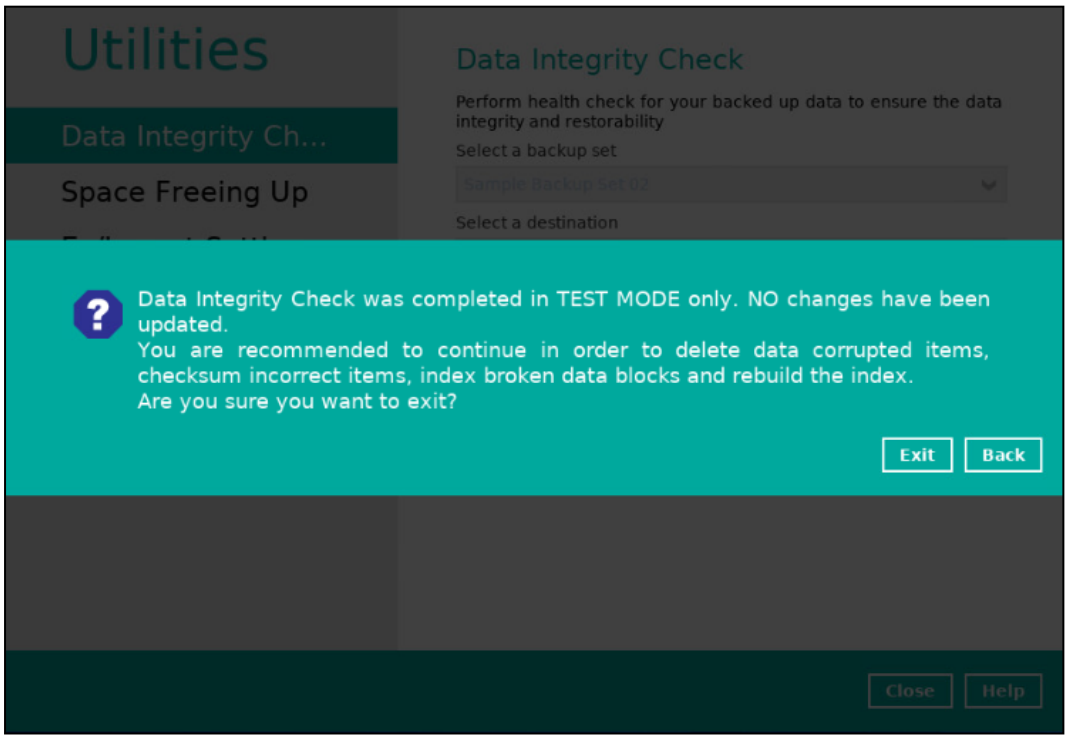
There are three options on the (TEST MODE) confirmation prompt:

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.

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



If the **Exit** button is clicked, the data integrity check result will be discarded.

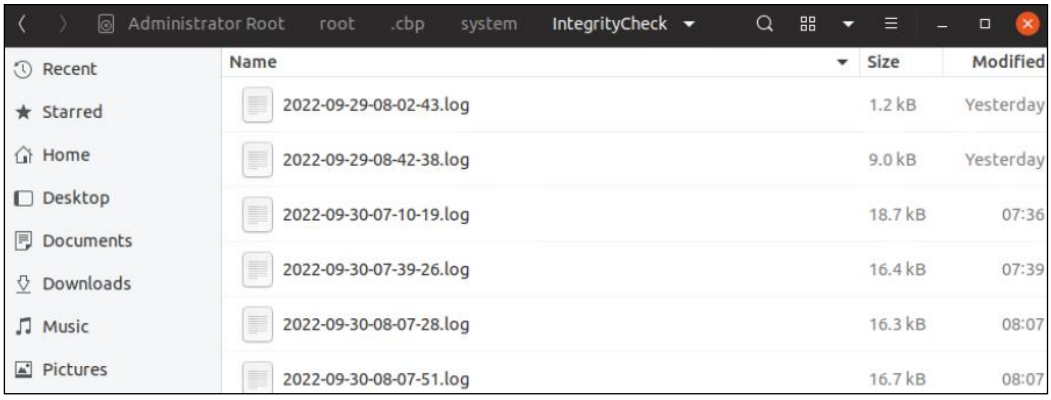
If the **Back** button is clicked, it will go back to the (TEST MODE) confirmation screen.

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 Pro, they can be viewed on the file system of the CloudBacko Pro machine. For CloudBacko Pro on Linux, the DIC logs are located in:

%UserProfile/.cbp/system/IntegrityCheck

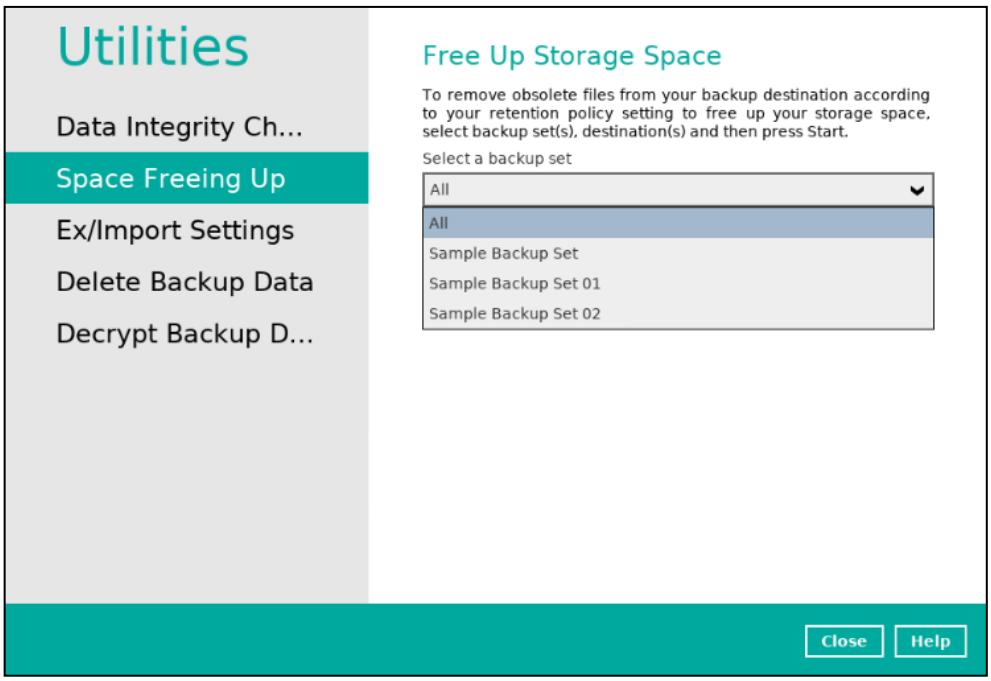


7.8.2 Space Freeing Up

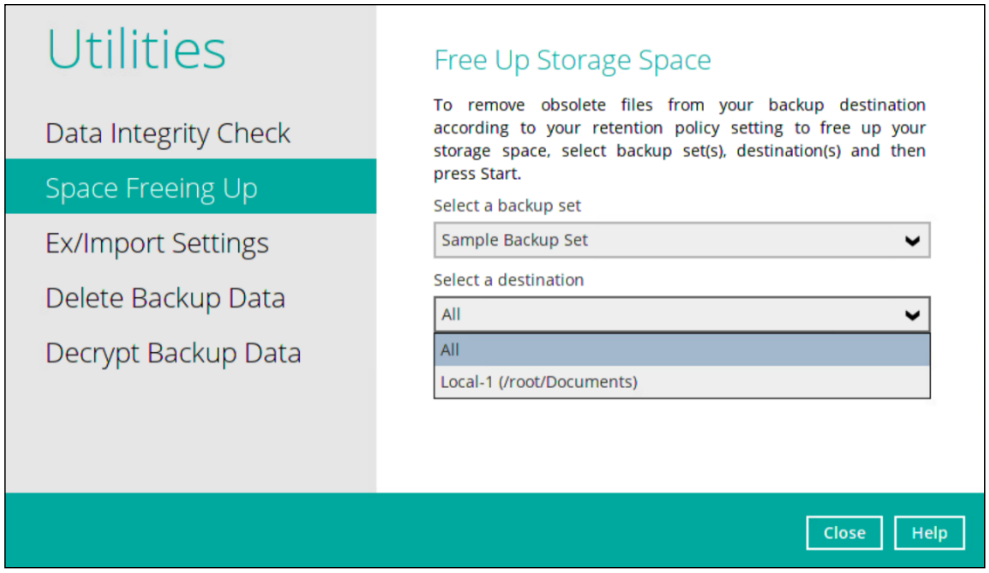
This feature is used to remove obsolete file(s) from your selected backup set and destination (manually start retention policy). After the Space Freeing Up job is completed, the storage statistics of the backup set(s) are updated.

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

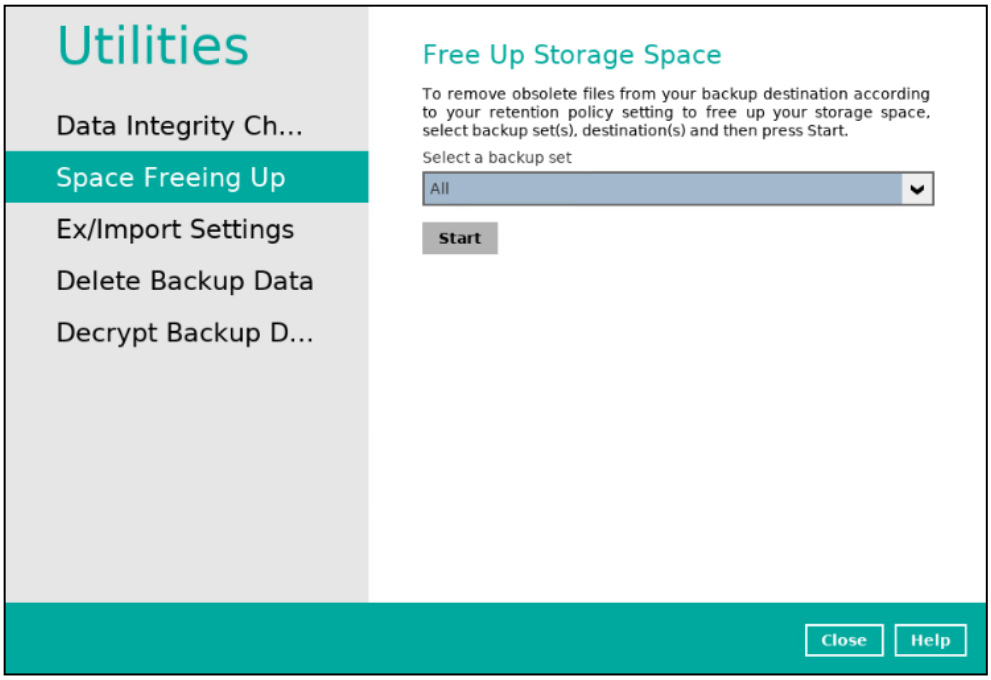
1. Select a backup set from the drop-down list.



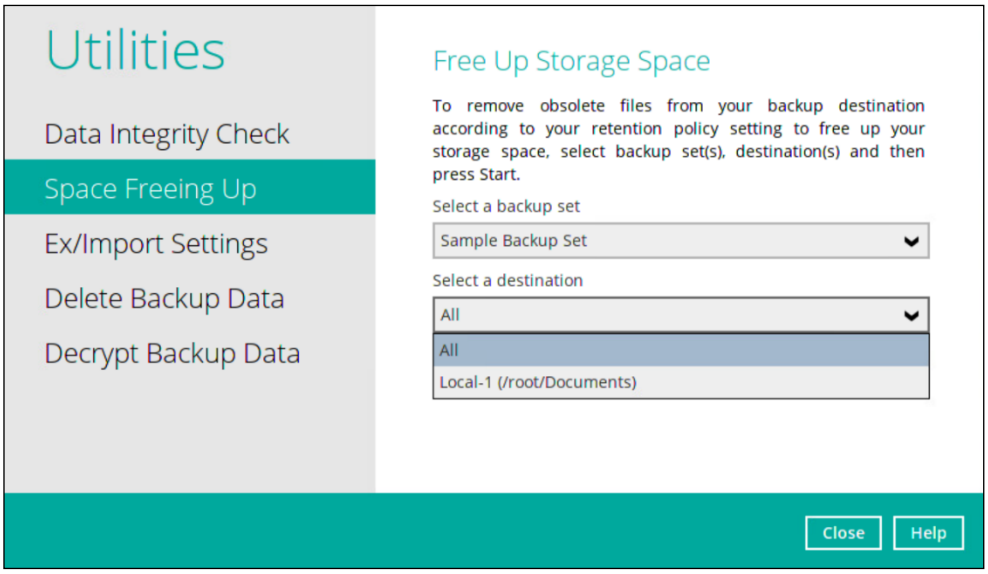
If you select a specific backup set, you will also have to choose a specific or **ALL** destination.

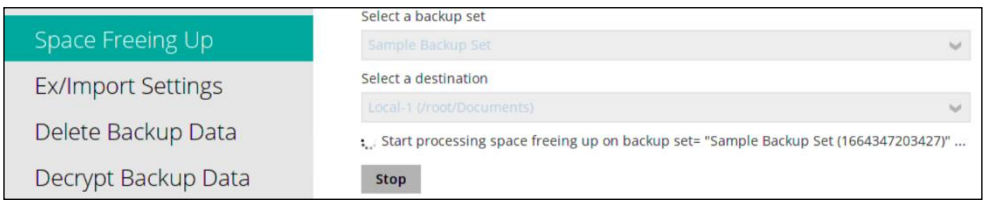


If you select **ALL** backup sets, you will not have to choose a destination.

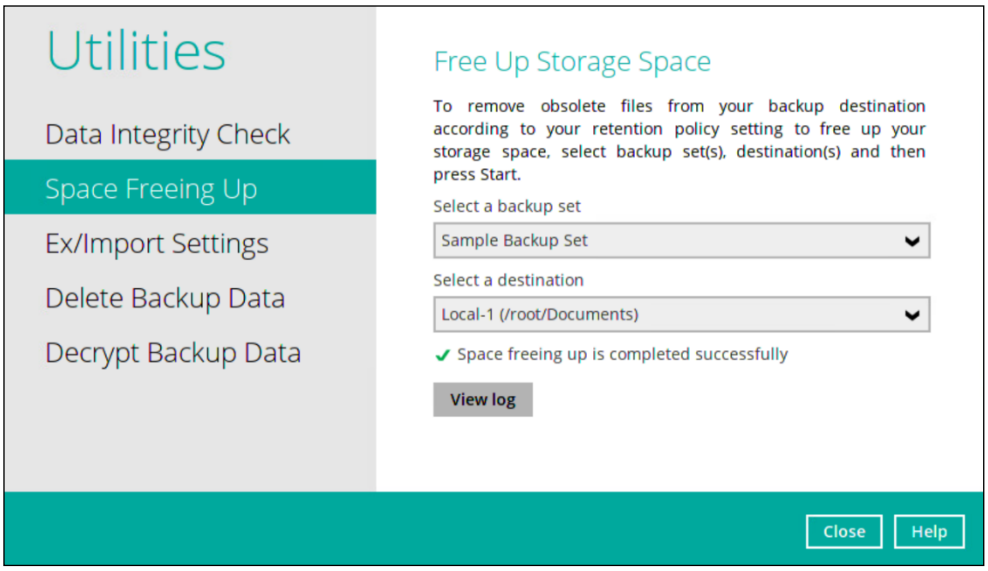


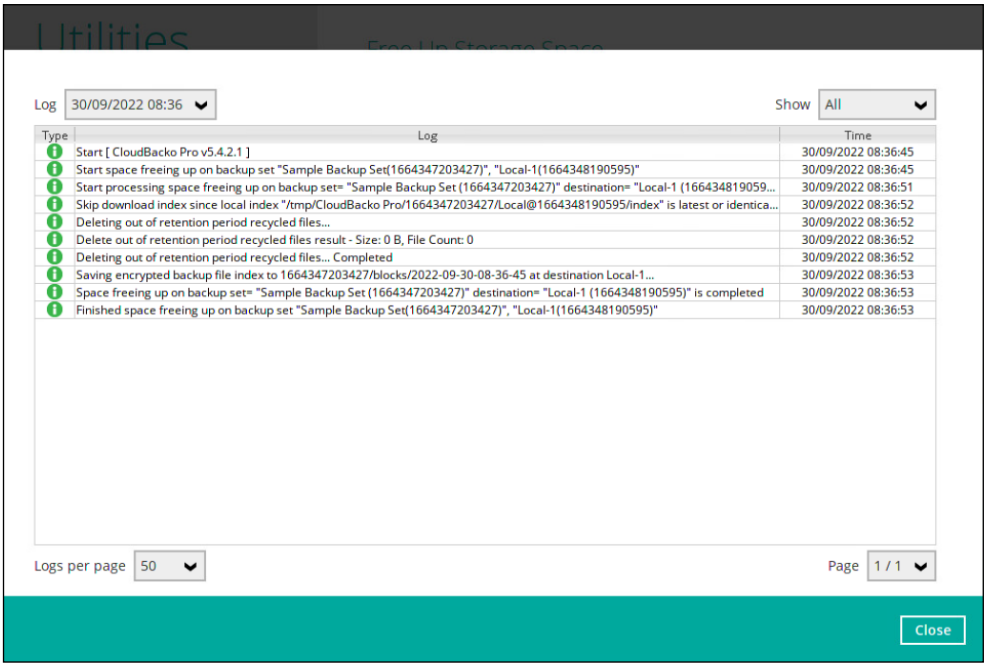
2. Once a backup set and destination have been selected, click **Start** to perform space free up.





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





7.8.3 Ex/Import Settings

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

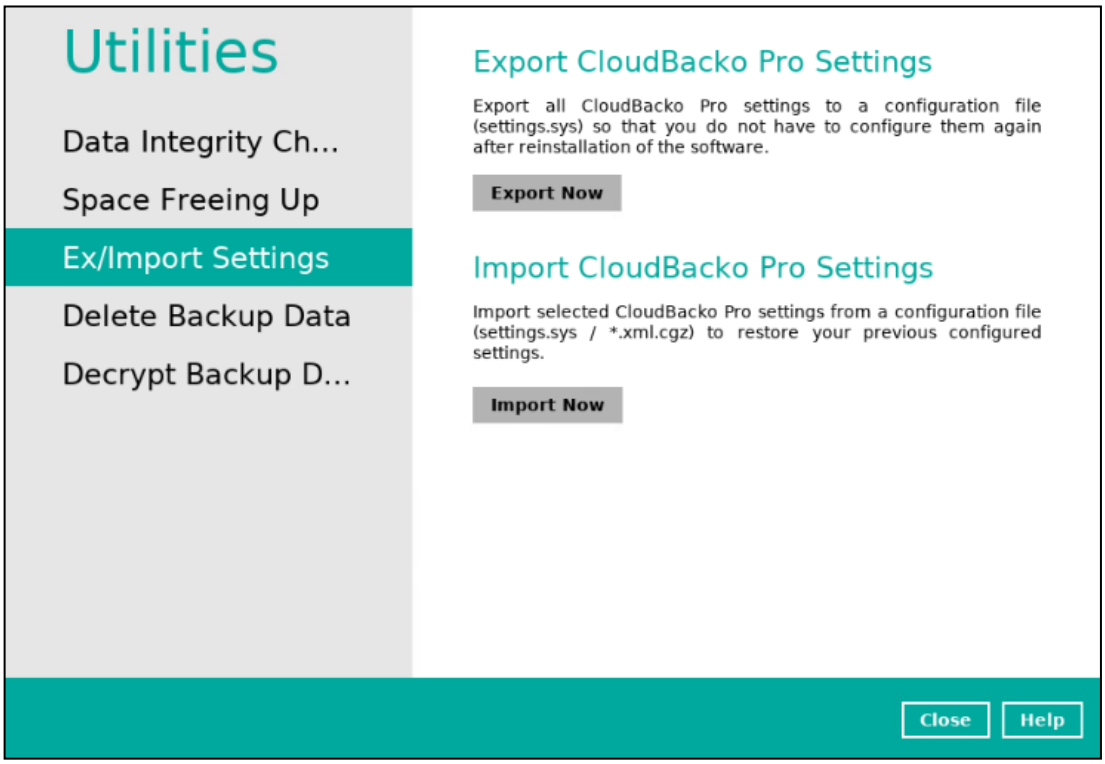
- Proxy Settings
- Email Report Settings
- Software Update Settings
- Windows Event log Settings (Windows Platform Only)
- Backup Set Settings

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

WARNING!

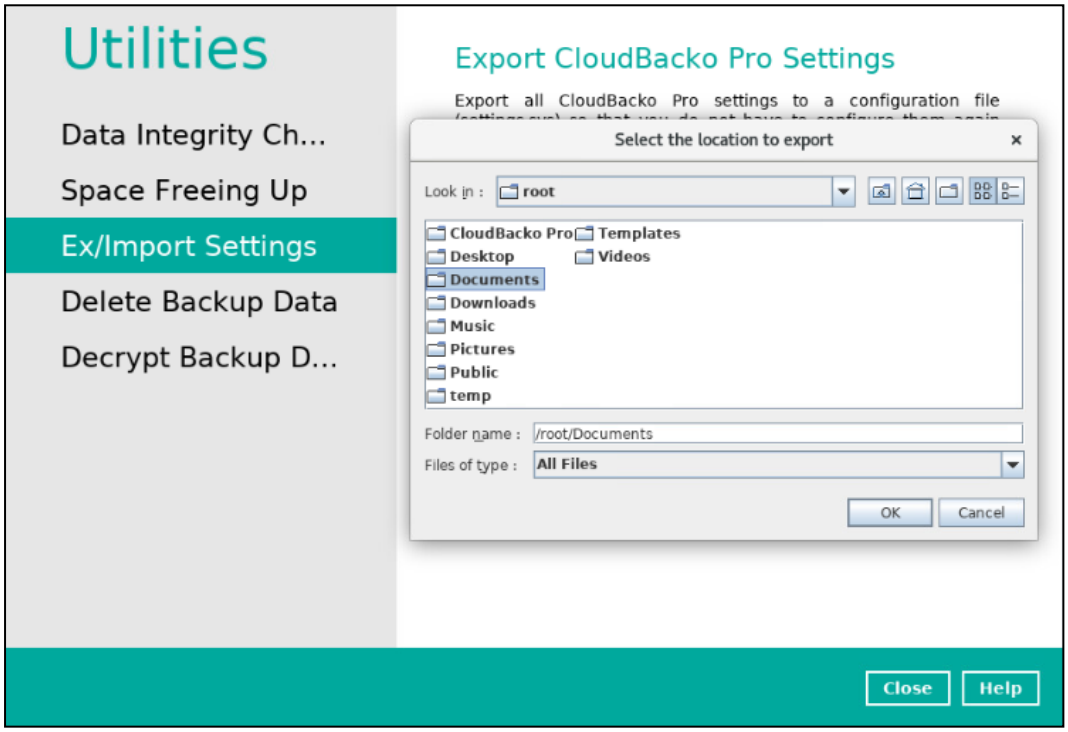
A separate copy of the settings.sys file should be saved in another location for safe keeping.

Otherwise, If the machine where the CloudBacko Pro 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 Pro.

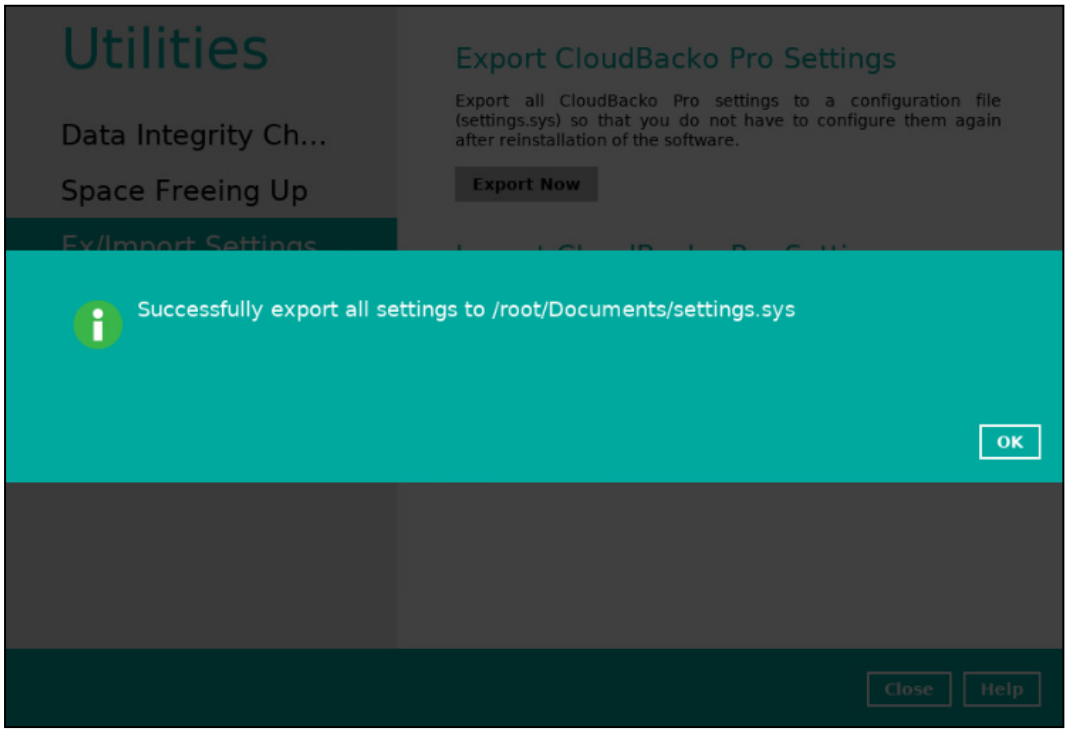


Export CloudBacko Pro Settings

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

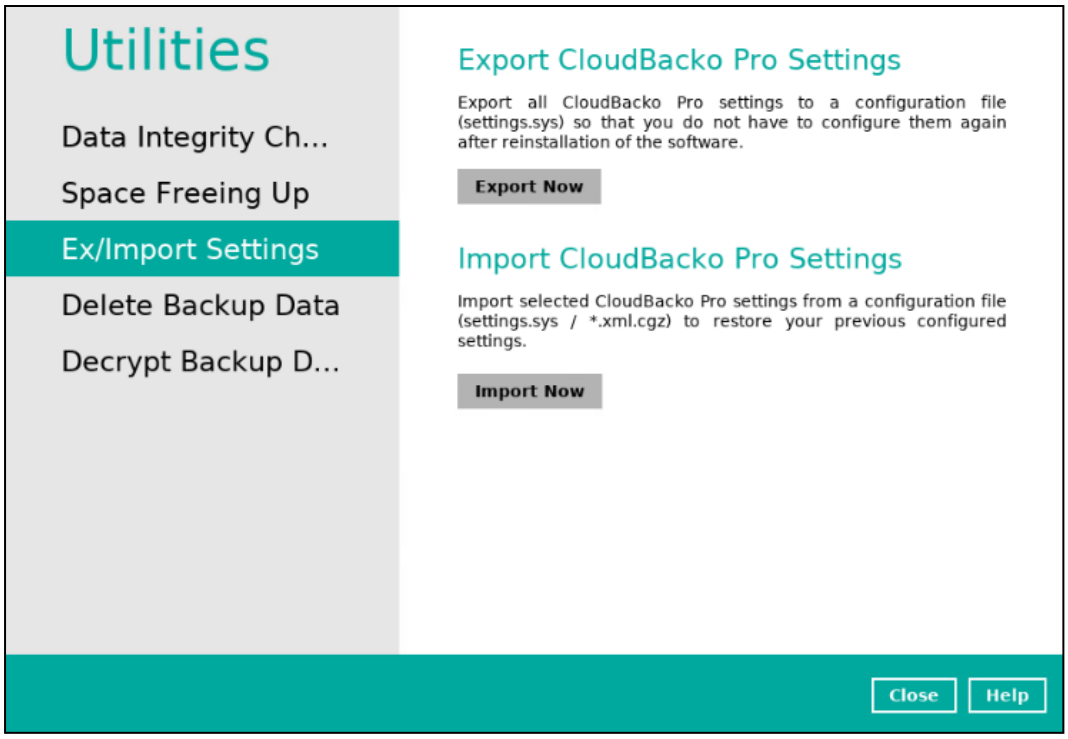


If the system.sys file is successfully exported to the preferred path, it will display a message containing the status and path of the CloudBacko Pro configuration file.

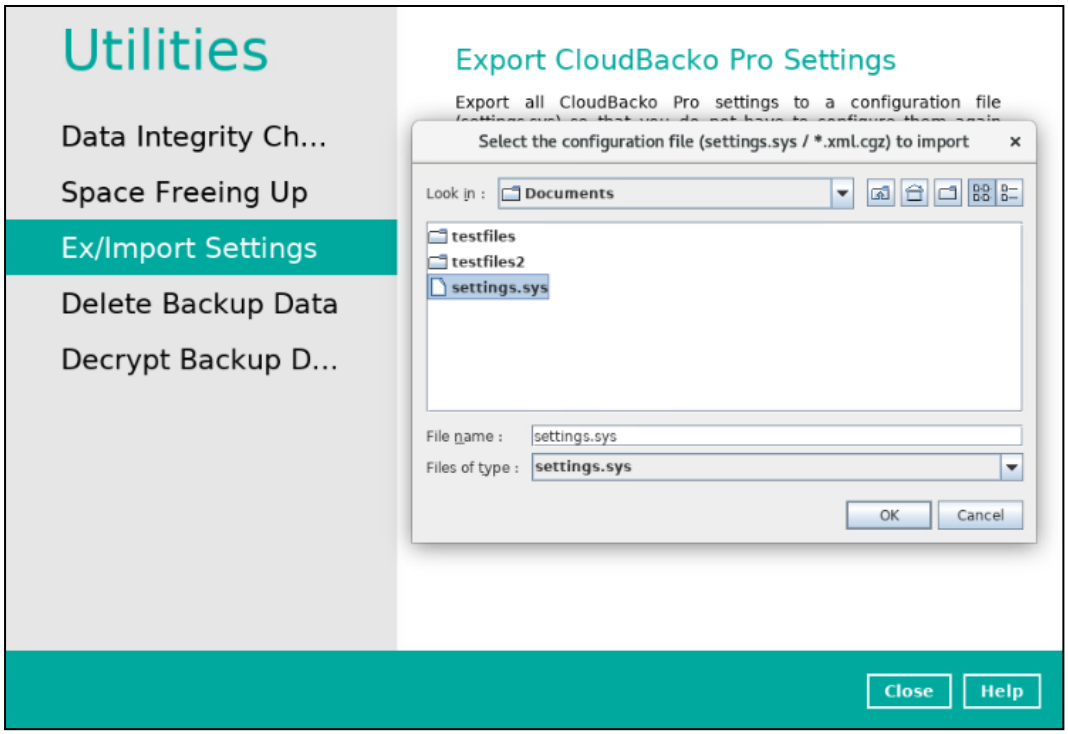


Import CloudBacko Pro Settings

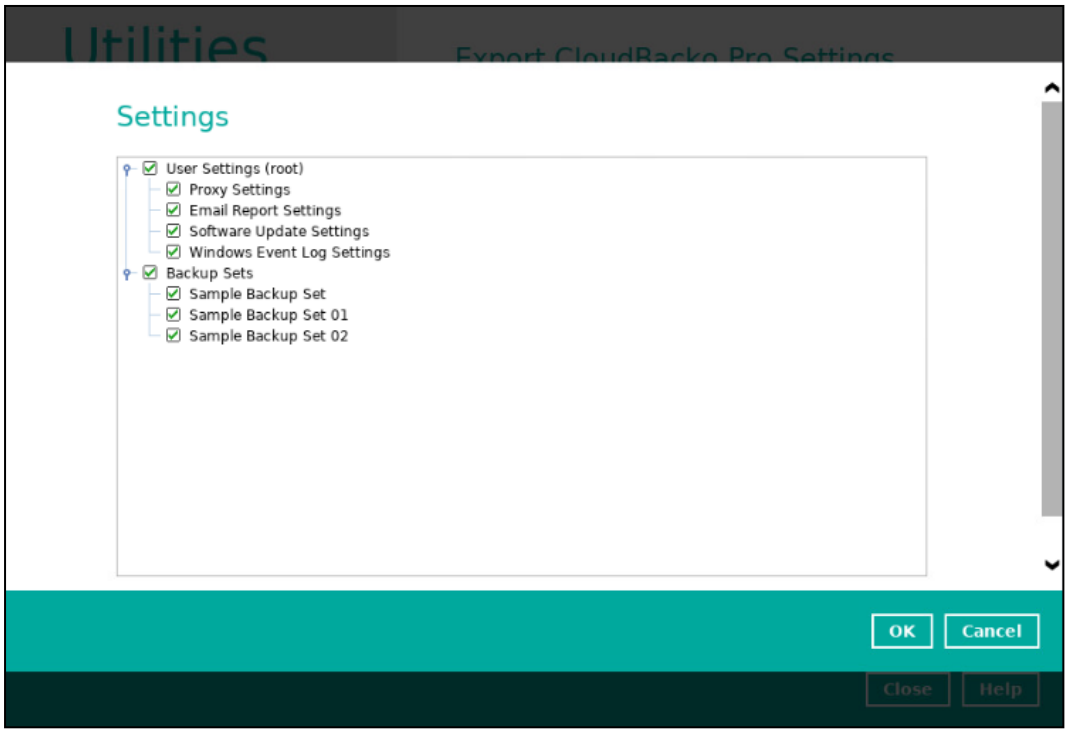
To import, click the **Import Now** button.



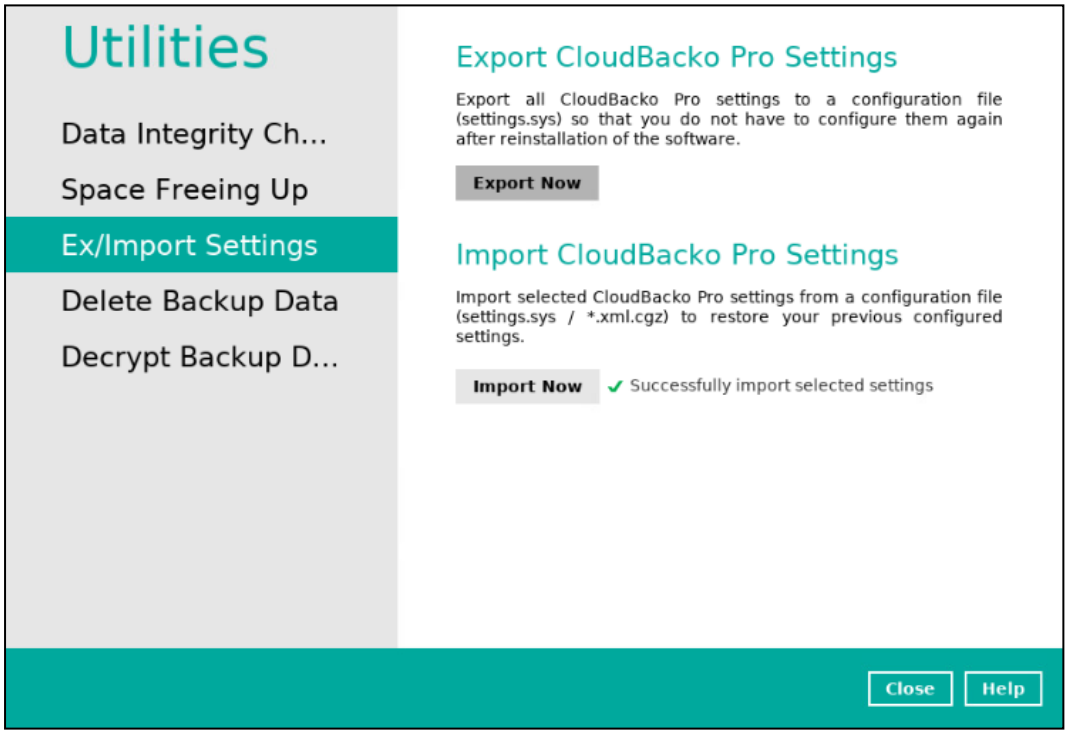
Select a path where the CloudBacko Pro configuration file (system.sys / .xml, .cgz) is stored then click **OK**.



It will show the following Settings: User Settings and Backup Sets. By default, all settings are included, however, there is an option to uncheck the checkboxes and choose the preferred settings.



If the system.sys / .xml, .cgz file is successfully imported, it will display a check sign besides the **Import Now** button with a successful status of imported settings.

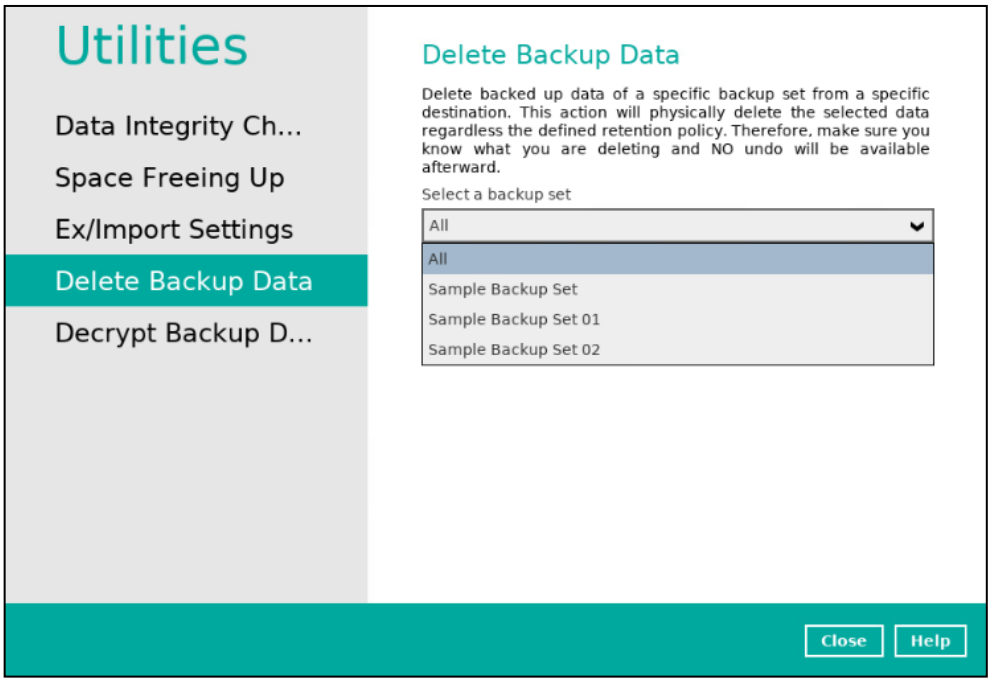


7.8.4 Delete Backup Data

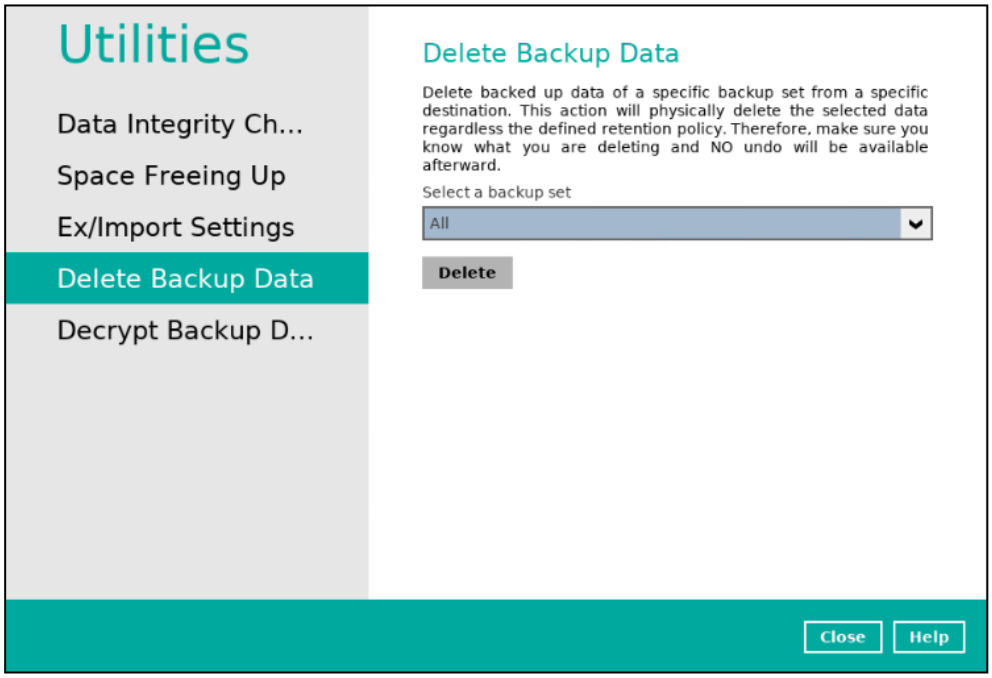
This feature is used to permanently delete backed up data from a backup set(s), destination(s), backup job, or delete all backed-up data. After the data is deleted, the storage statistics of the backup set(s) are updated.

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

1. Select a backup set to delete from.



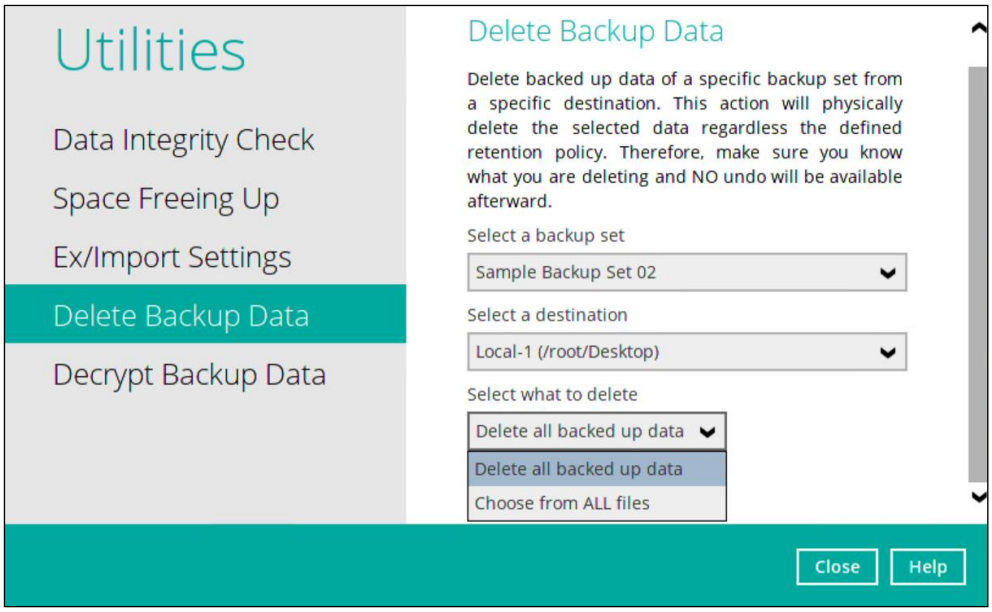
If you select a specific backup set, you will also have to choose a specific or **ALL** destination.



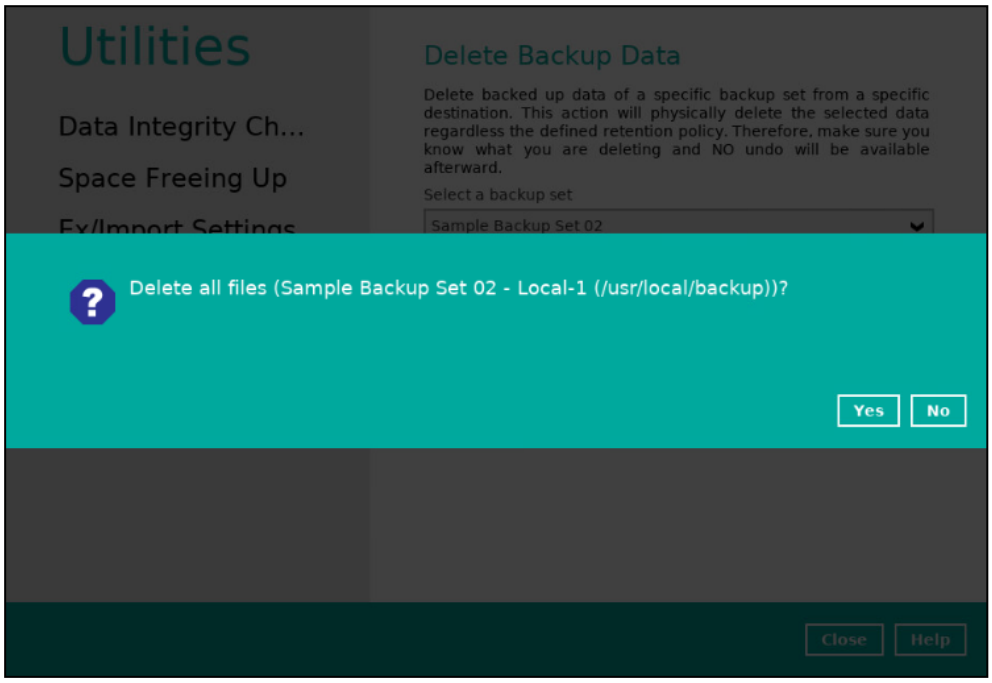
2. If you select **ALL** backup sets, you will not have to choose a specific destination.

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

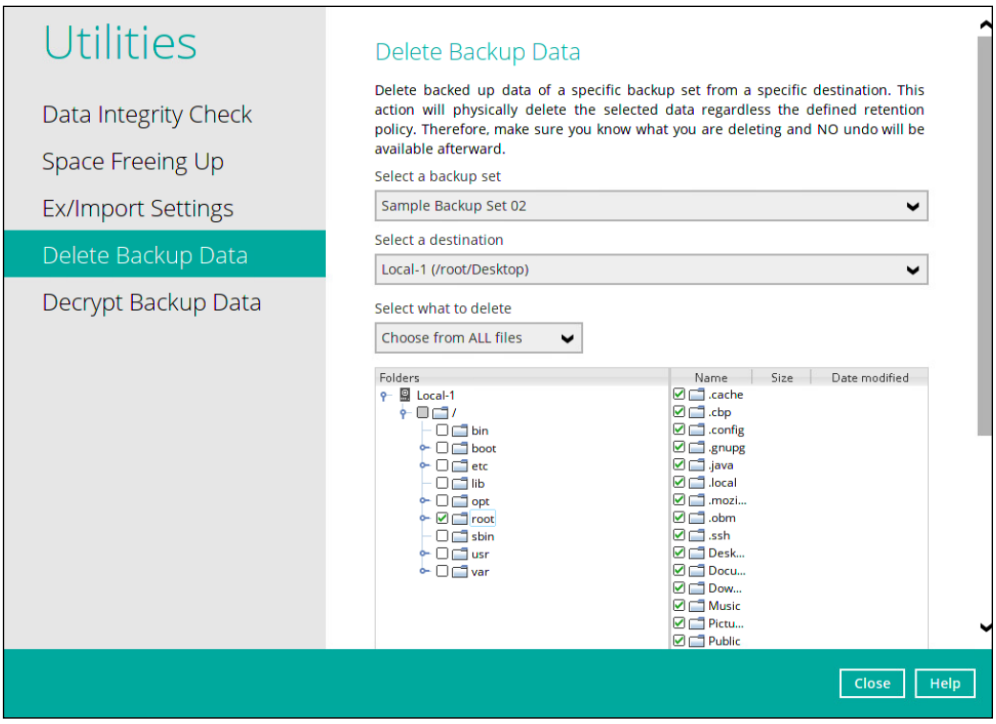
   - Delete all backed-up data
   - Choose from ALL files



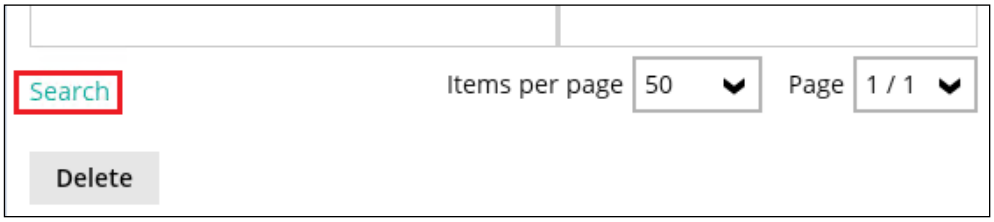
All backed-up files from the chosen backup set and selected destination will be deleted if you choose "**Delete all backed up data"**. Click **Yes** to confirm.



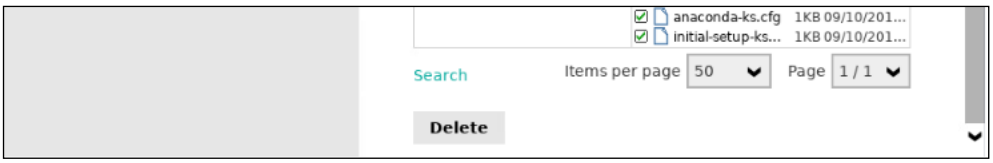
If you select "**Choose from ALL files**", you can select any file(s) in the backup set.

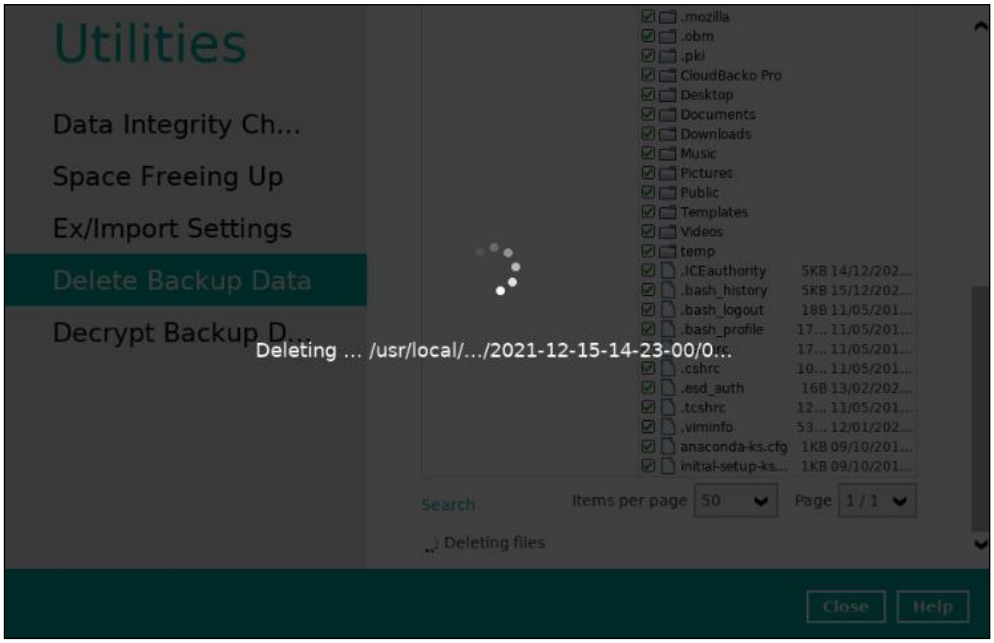


You also have the option to click the **Search** link to do an advance search.

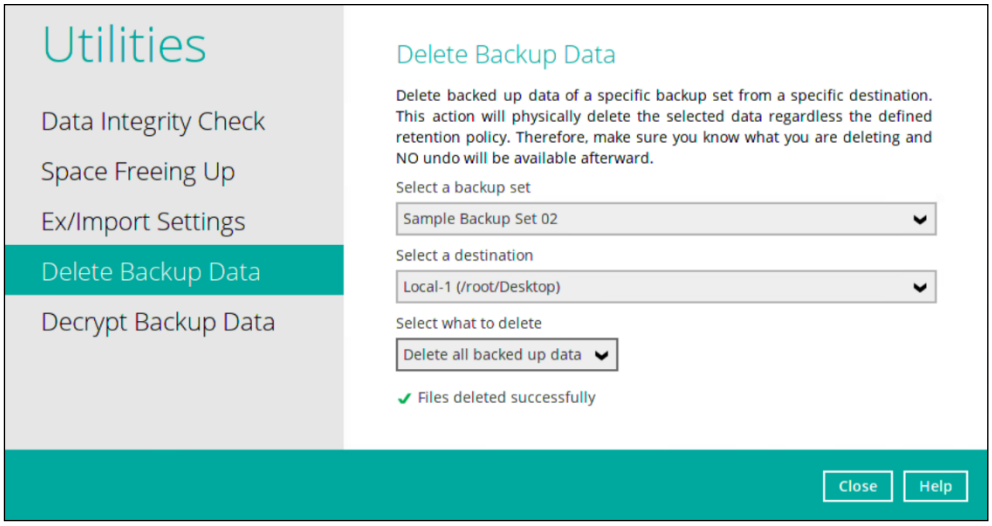


3. Click **Delete** to start the deletion of file(s).



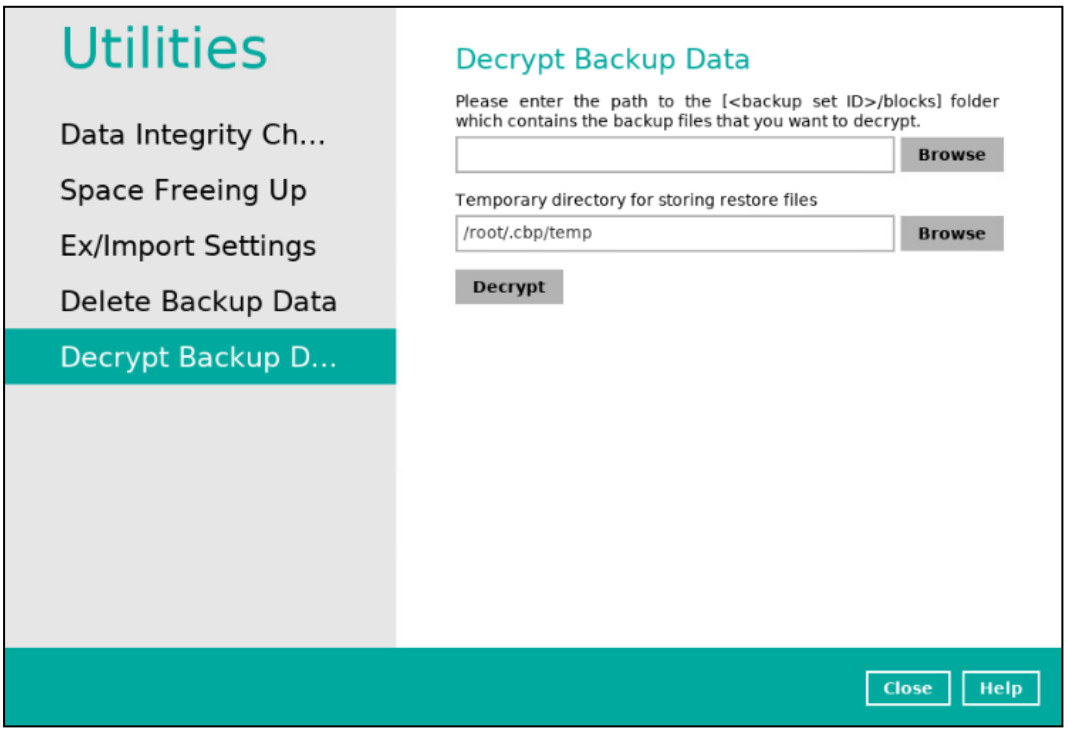


4. Files deleted successfully.

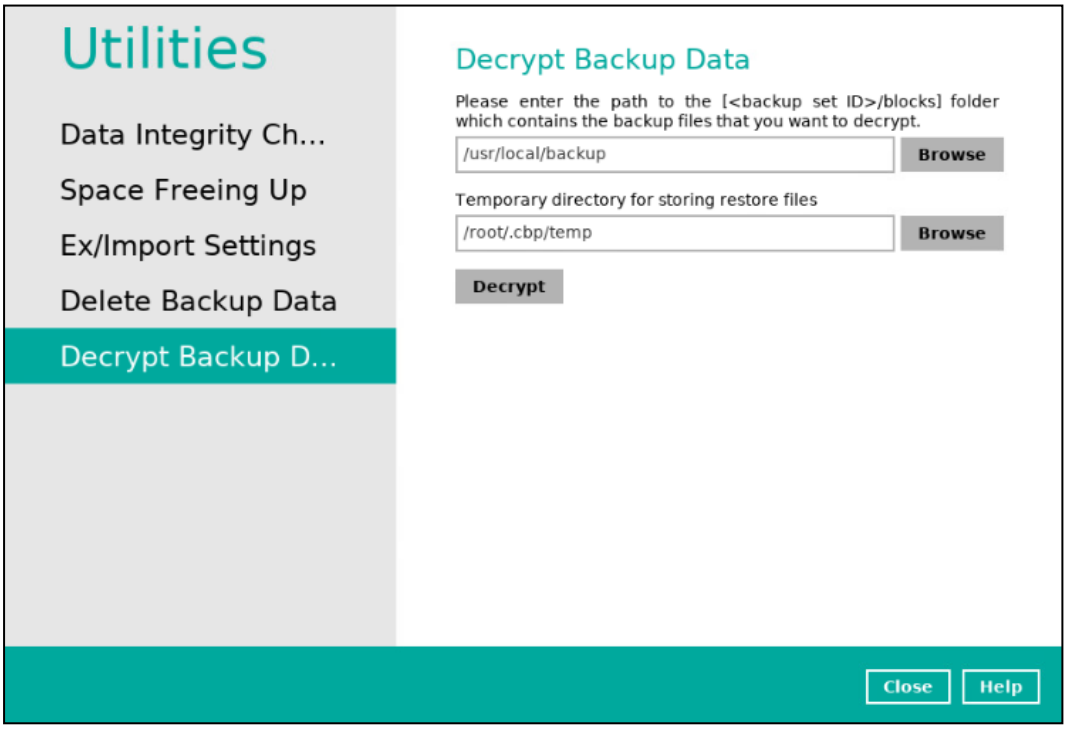


7.8.5 Decrypt Backup Data

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



Enter the path of the folder which contains the backup files you want to decrypt. Click the **Decrypt** button to start decrypting backup data.

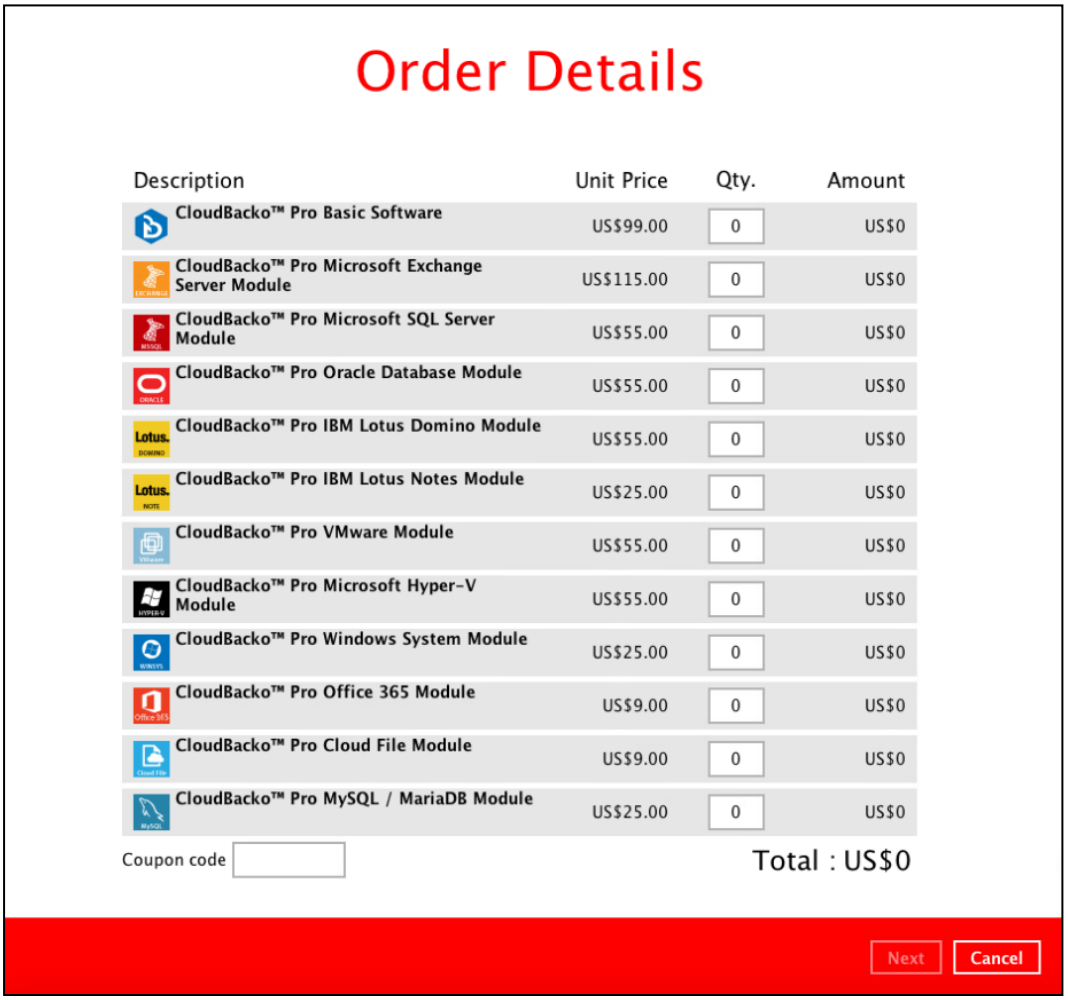


7.9 Buy

This feature allows,

- new customers who are evaluating the product using a trial key to purchase a license key and/or module.
- existing customers to purchase additional software license and/or module.

Please refer to the CloudBacko forum article for the details on the license purchase instructions: How to Buy CloudBacko Pro



To purchase additional software license and/or modules, follow the instructions below:

1. Select the software license and/or modules by adding a number on the **Qty** field then click the **Update Total** button to show the updated cost

   If Coupon code is available, input it in the “Coupon code” field.

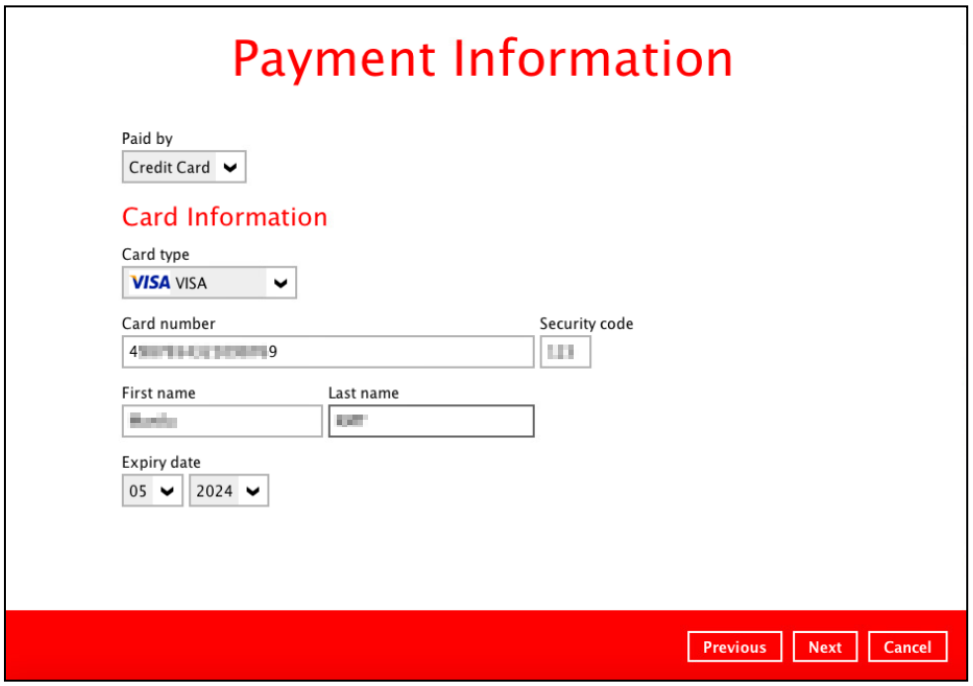
   Click the **Next** button to proceed.

2. The Payment Information screen will be displayed. Select the payment mode, Credit Card or TT (Telegraphic Transfer), by clicking the dropdown **Paid by**.

7.9.1 Credit Card

Payment through online via a Credit Card is the quickest way to purchase a software license or additional add-on modules. The only requirements are a valid Credit Card and Contact Information. Once the payment is confirmed, purchased software license or add-on modules will be available immediately.

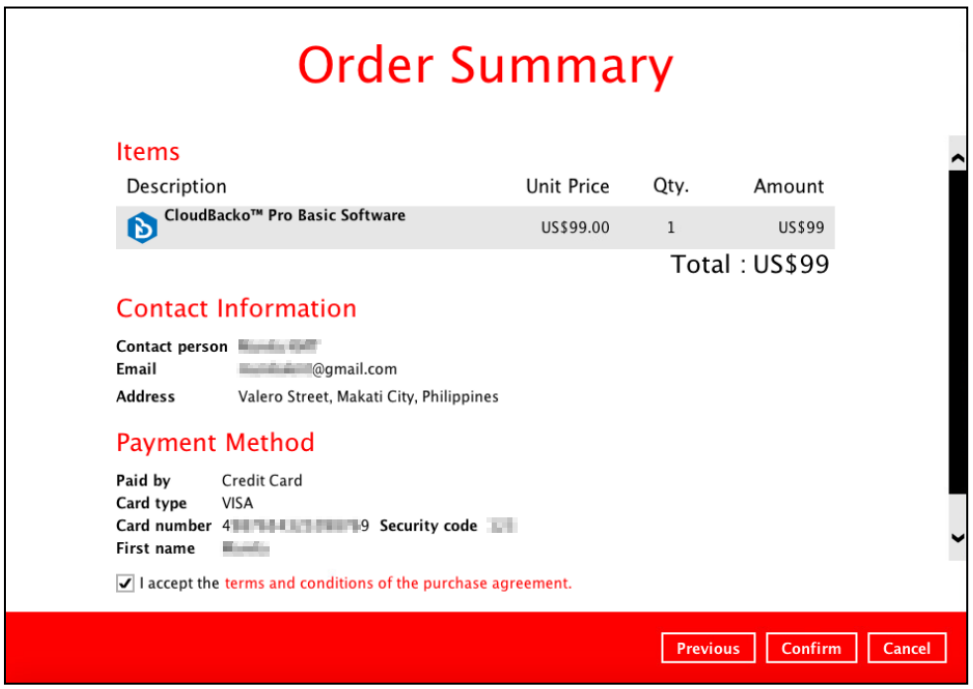
1. Complete the following fields then click the **Next** button to proceed.
   - Card type
     - VISA
     - Master Card
   - Card number
   - Security code
   - First name
   - Last name
   - Expiry date



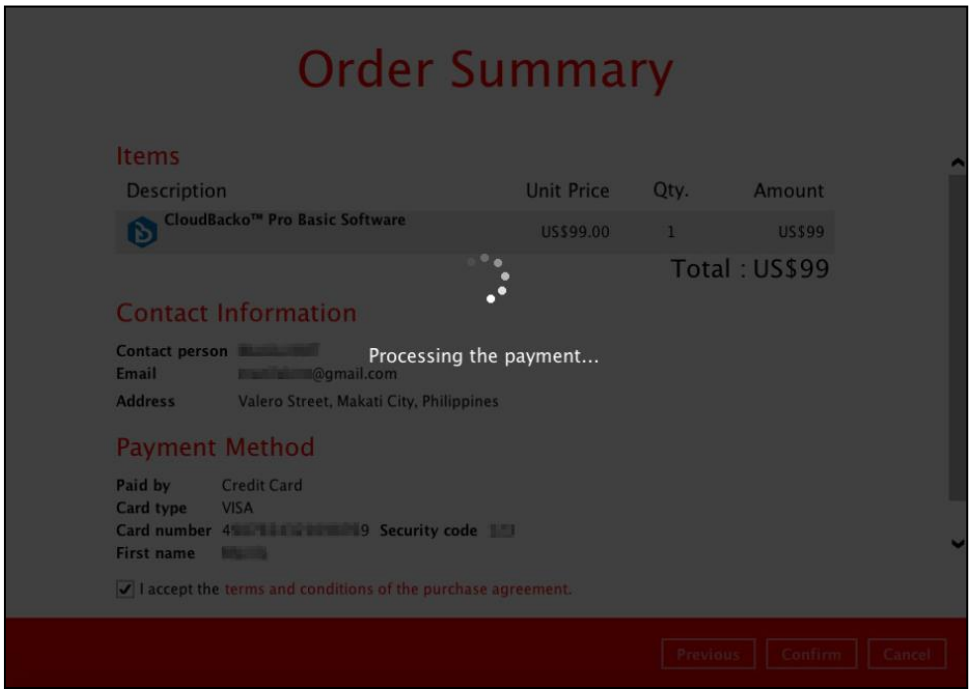
2. Complete the following fields for the Contact Information then click the **Next** button to proceed.
   - Contact person
   - Email for receiving receipt
   - Company name (optional)
   - VAT number (optional)
   - Street line 1
   - Street line 2 (optional)
   - City
   - State / Province / Territory (optional)
   - Postal / Zip code (optional)
   - Country

3. In the Order Summary screen, order Items, Contact Information, and Payment Method are displayed.

   Tick the **"I accept the terms and conditions of the purchase agreement"** and click the **Confirm** button to proceed with the payment.

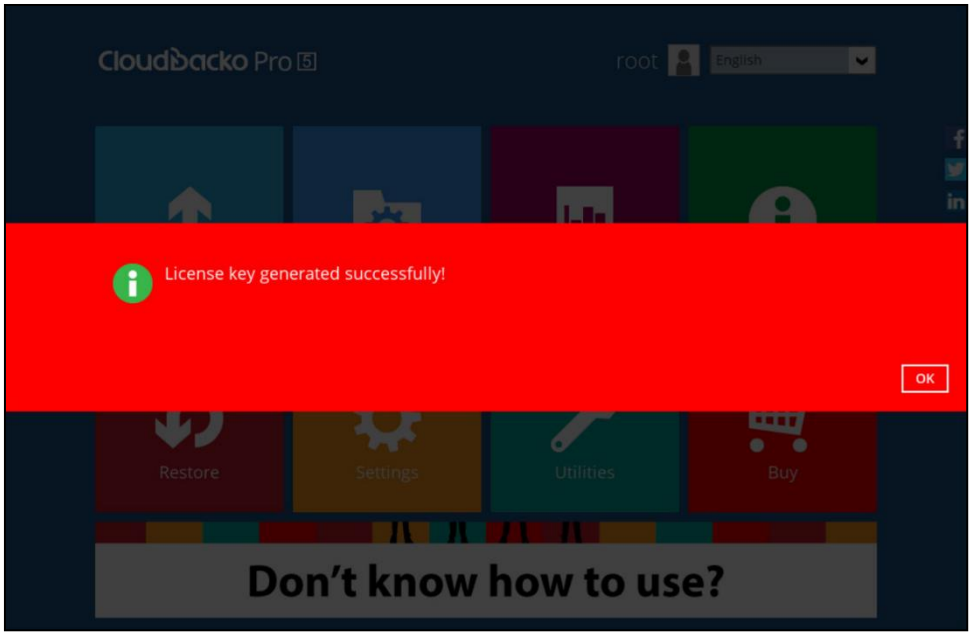


4. The payment will be processed.

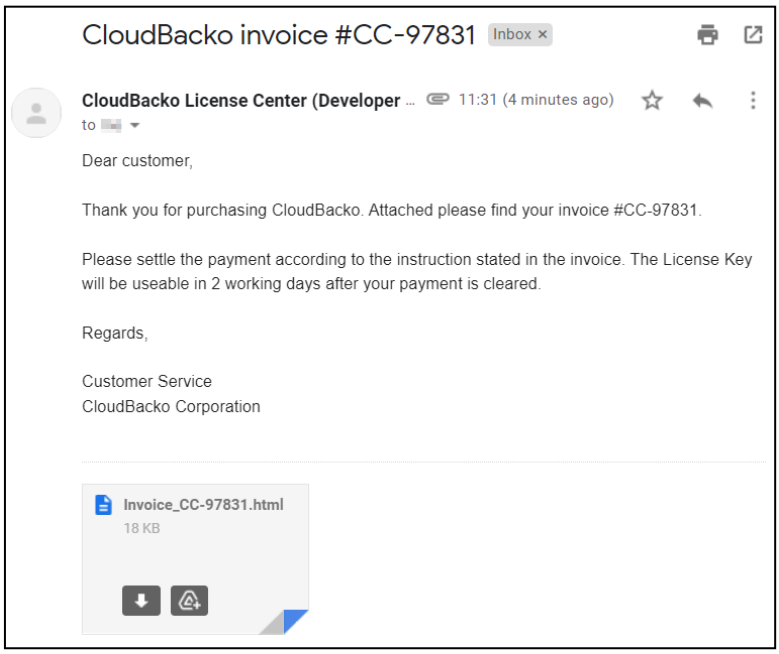


If the payment is successful, an official receipt will be displayed.

The license key on the CloudBacko Pro is now successfully applied.



These are sample emails for the copies of Invoice and Official Receipt.



CloudBacko invoice #CC-97831 Inbox ×

CloudBacko License Center (Developer ... 11:31 (4 minutes ago)
to

Dear customer,

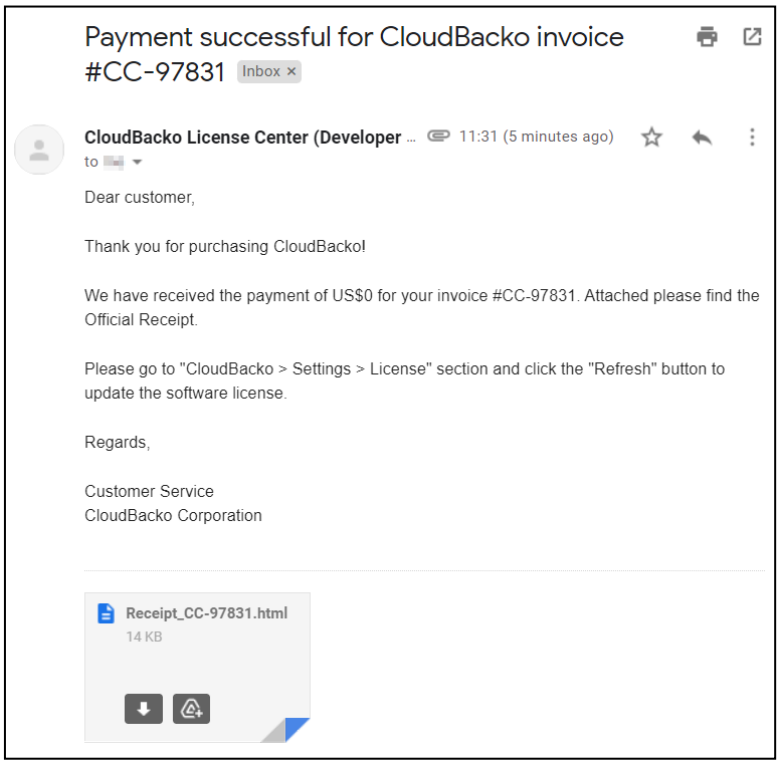
Thank you for purchasing CloudBacko. Attached please find your invoice #CC-97831.

Please settle the payment according to the instruction stated in the invoice. The License Key will be useable in 2 working days after your payment is cleared.

Regards,

Customer Service
CloudBacko Corporation

Invoice_CC-97831.html
18 KB



Payment successful for CloudBacko invoice #CC-97831 Inbox ×

CloudBacko License Center (Developer ... 11:31 (5 minutes ago)
to

Dear customer,

Thank you for purchasing CloudBacko!

We have received the payment of US$0 for your invoice #CC-97831. Attached please find the Official Receipt.

Please go to "CloudBacko > Settings > License" section and click the "Refresh" button to update the software license.

Regards,

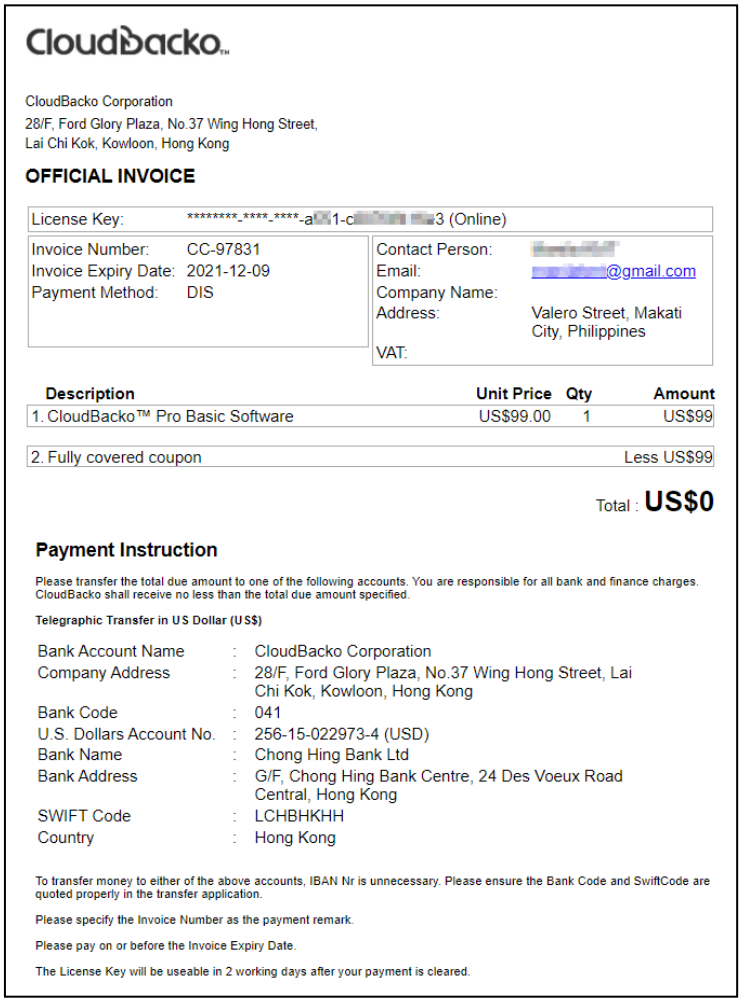
Customer Service
CloudBacko Corporation

Receipt_CC-97831.html
14 KB

Please keep the copy of your invoice as it contains half of your license key. The other half of the license key can be found on CloudBacko Pro. Both parts of the license key is required if you need to reinstall CloudBacko Pro or apply the license to another installation.

Please check this article for more information:

Where can I find my CloudBacko Pro/Lite purchase license key?



CloudBacko™

CloudBacko Corporation
28/F, Ford Glory Plaza, No.37 Wing Hong Street,
Lai Chi Kok, Kowloon, Hong Kong

OFFICIAL INVOICE

License Key: ********-****-****-a[illegible]1-c[illegible]3 (Online)

Invoice Number:	CC-97831	Contact Person:	[illegible]
Invoice Expiry Date:	2021-12-09	Email:	[illegible]@gmail.com
Payment Method:	DIS	Company Name:	
		Address:	Valero Street, Makati City, Philippines
		VAT:	

Description	Unit Price	Qty	Amount
1. CloudBacko™ Pro Basic Software	US$99.00	1	US$99
2. Fully covered coupon			Less US$99

Total : **US$0**

Payment Instruction

Please transfer the total due amount to one of the following accounts. You are responsible for all bank and finance charges. CloudBacko shall receive no less than the total due amount specified.

Telegraphic Transfer in US Dollar (US$)

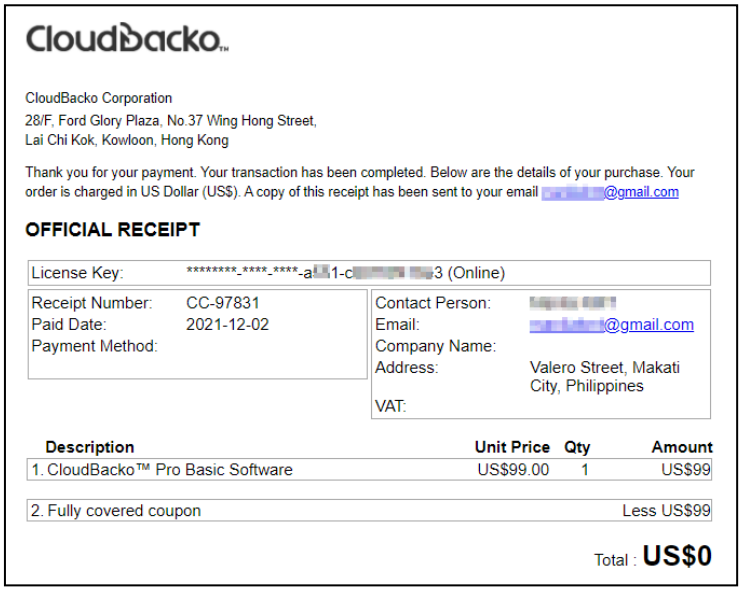
Bank Account Name	:	CloudBacko Corporation
Company Address	:	28/F, Ford Glory Plaza, No.37 Wing Hong Street, Lai Chi Kok, Kowloon, Hong Kong
Bank Code	:	041
U.S. Dollars Account No.	:	256-15-022973-4 (USD)
Bank Name	:	Chong Hing Bank Ltd
Bank Address	:	G/F, Chong Hing Bank Centre, 24 Des Voeux Road Central, Hong Kong
SWIFT Code	:	LCHBHKHH
Country	:	Hong Kong

To transfer money to either of the above accounts, IBAN Nr is unnecessary. Please ensure the Bank Code and SwiftCode are quoted properly in the transfer application.

Please specify the Invoice Number as the payment remark.

Please pay on or before the Invoice Expiry Date.

The License Key will be useable in 2 working days after your payment is cleared.



CloudBacko™

CloudBacko Corporation
28/F, Ford Glory Plaza, No.37 Wing Hong Street,
Lai Chi Kok, Kowloon, Hong Kong

Thank you for your payment. Your transaction has been completed. Below are the details of your purchase. Your order is charged in US Dollar (US$). A copy of this receipt has been sent to your email [illegible]@gmail.com

OFFICIAL RECEIPT

License Key: ********-****-****-a[illegible]1-c[illegible]3 (Online)

Receipt Number:	CC-97831	Contact Person:	[illegible]
Paid Date:	2021-12-02	Email:	[illegible]@gmail.com
Payment Method:		Company Name:	
		Address:	Valero Street, Makati City, Philippines
		VAT:	

Description	Unit Price	Qty	Amount
1. CloudBacko™ Pro Basic Software	US$99.00	1	US$99
2. Fully covered coupon			Less US$99

Total : **US$0**

However, if the payment is not successful, this prompt message will appear.

It will state the reason and four (4) options for the failed transaction:

- Retry

  This will process the payment again.

- Try another card

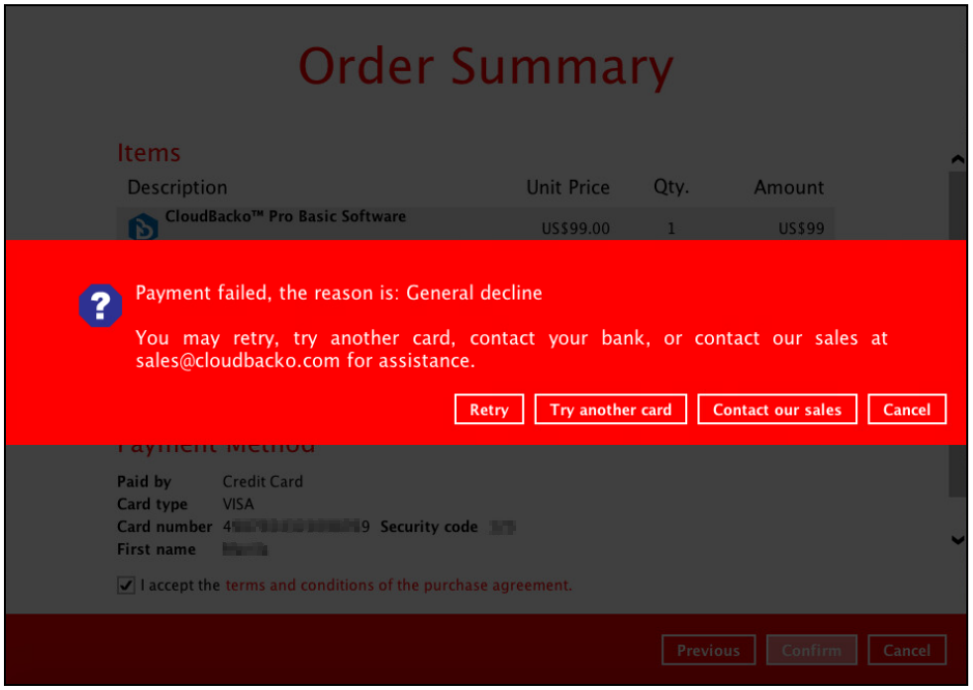
  This will redirect you to the Credit Card Information and input another Credit Card details.

- Contact our sales

  This will redirect you to the CloudBacko website.

- Cancel

  This will cancel the transaction and exit from the Buy module.

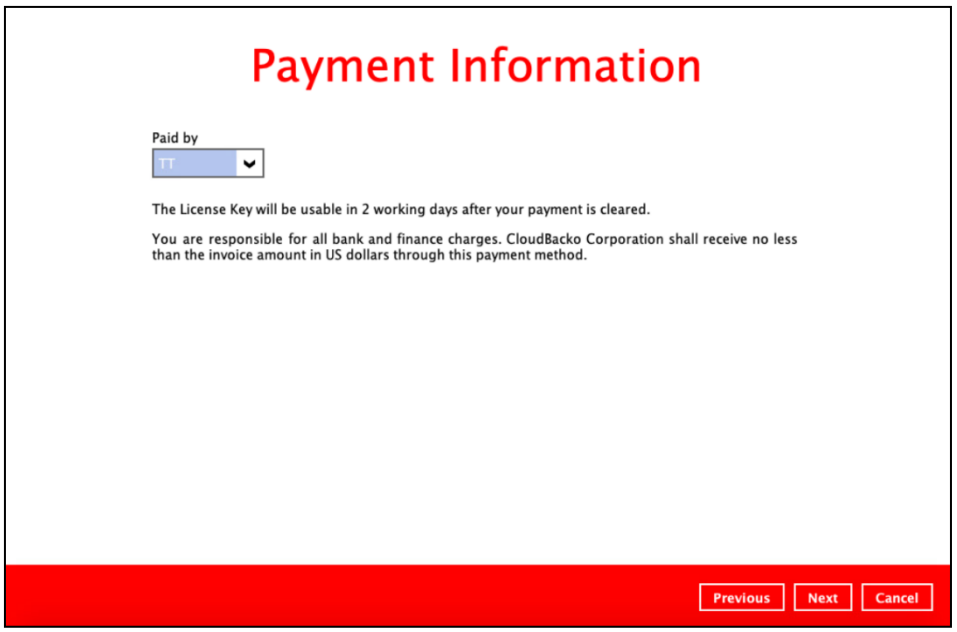


7.9.2 TT (Telegraphic Transfer)

TT (Telegraphic Transfer) is an electronic mode of transferring funds from bank to bank. Processing time can take up to one to two weeks to settle, depending on the origin, destination, and individual bank.

This payment mode can be used to purchase software licenses and/or additional add-on modules for trial users and for paid license users who want to avail add-on modules.

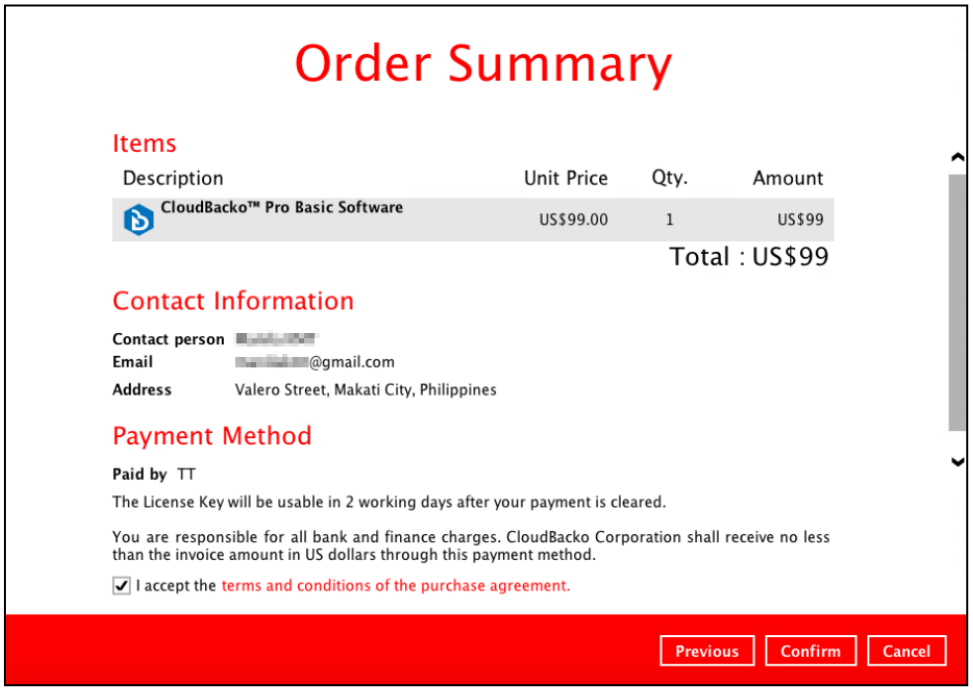
1. Click the **Next** button to proceed.



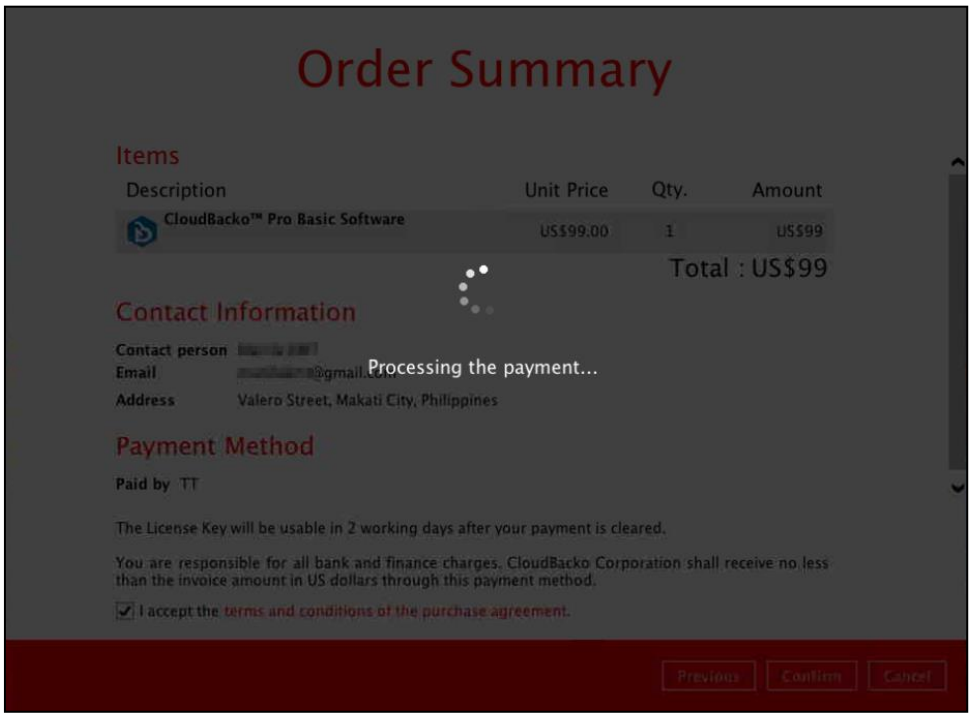
2. Complete the following fields for the Contact Information then click the **Next** button to proceed.
   - Contact person
   - Email for receiving receipt
   - Company name (optional)
   - VAT number (optional)
   - Street line 1
   - Street line 2 (optional)
   - City
   - State / Province / Territory (optional)
   - Postal / Zip code (optional)
   - Country

3. In the Order Summary screen, order Items, Contact Information, and Payment Method are displayed.

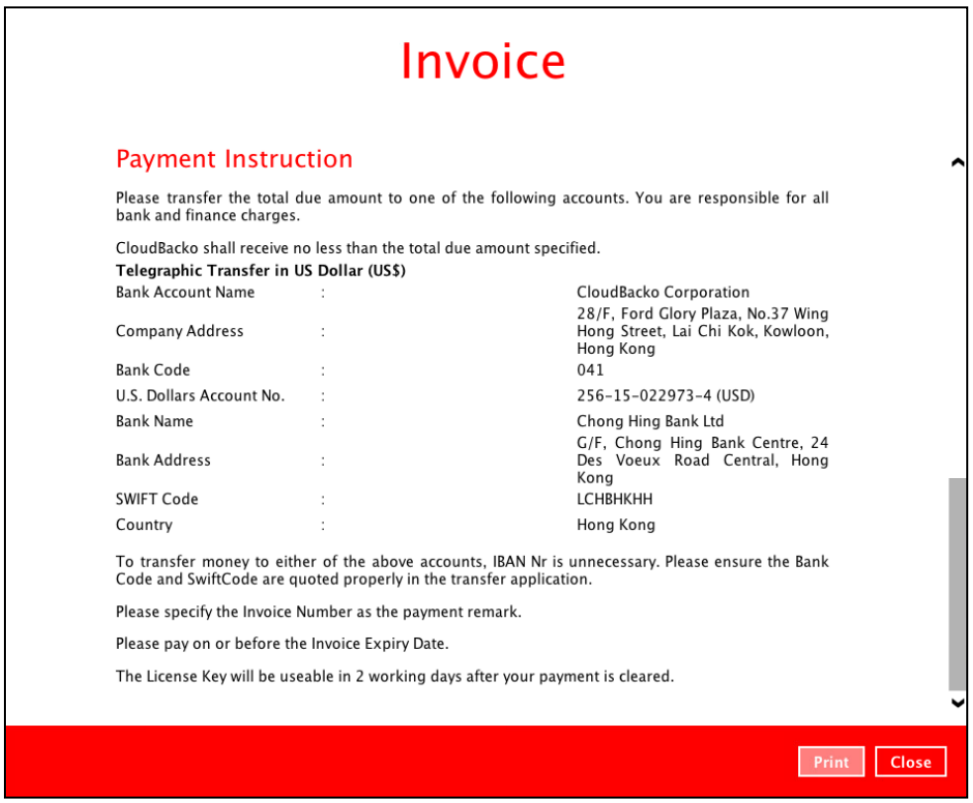
   Tick the **"I accept the terms and conditions of the purchase agreement"** and click the **Confirm** button to proceed with the payment.



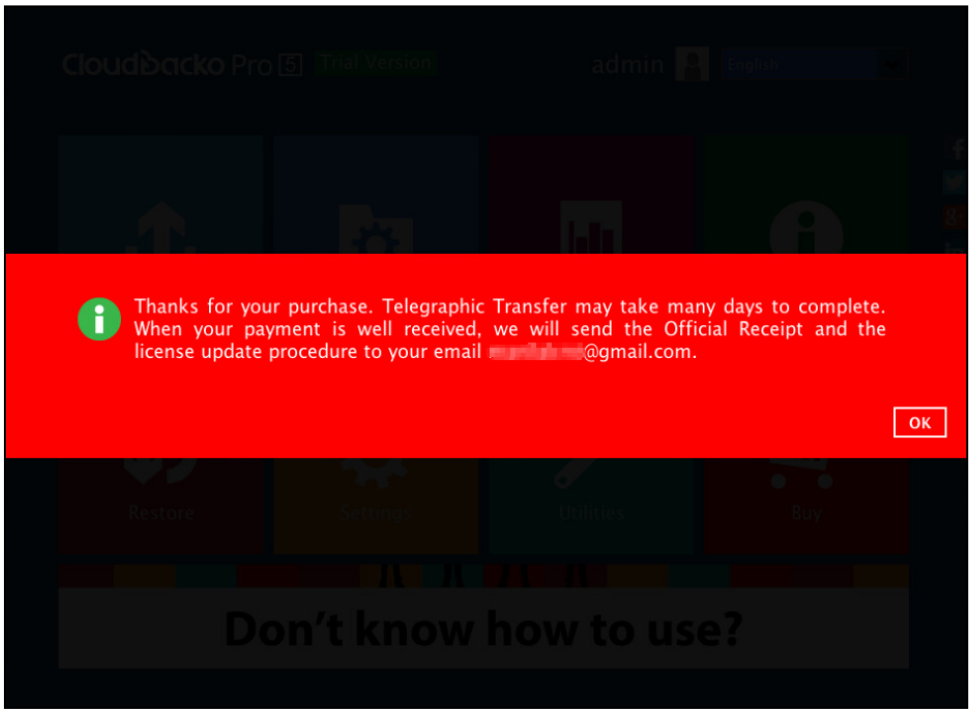
4. The invoice for the license purchase will be generated.



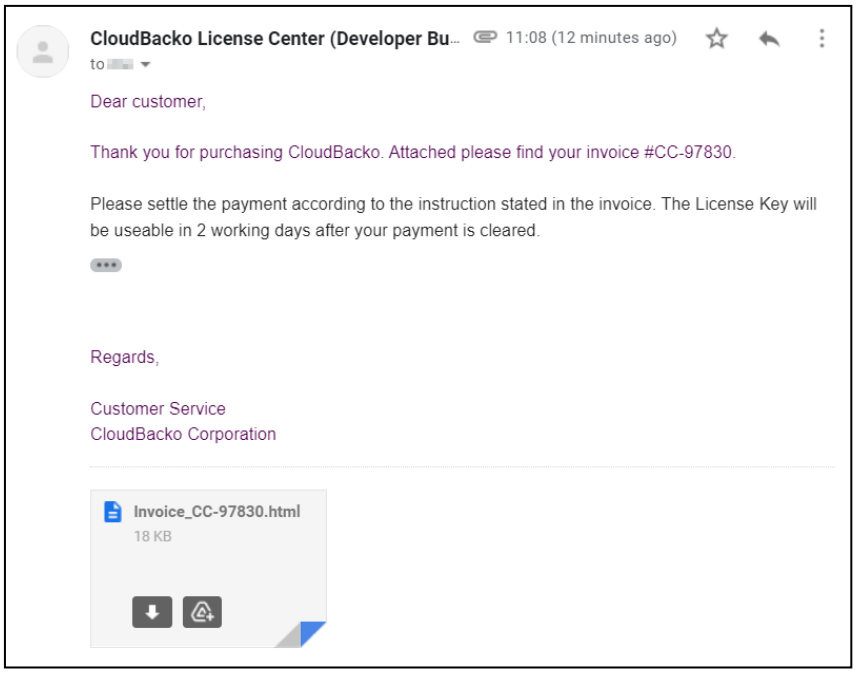
The Invoice will be displayed. Click the **Print** button to print out the invoice and bring it to your bank to arrange TT payment.



This prompt message will appear to inform customer that if the payment through telegraphic transfer is successful, the official receipt, software license, and license update procedure will be sent to the email address indicated in the Contact Information.



These are sample email for the copy of Invoice.



CloudBacko License Center (Developer Bu... 11:08 (12 minutes ago)

to [redacted]

Dear customer,

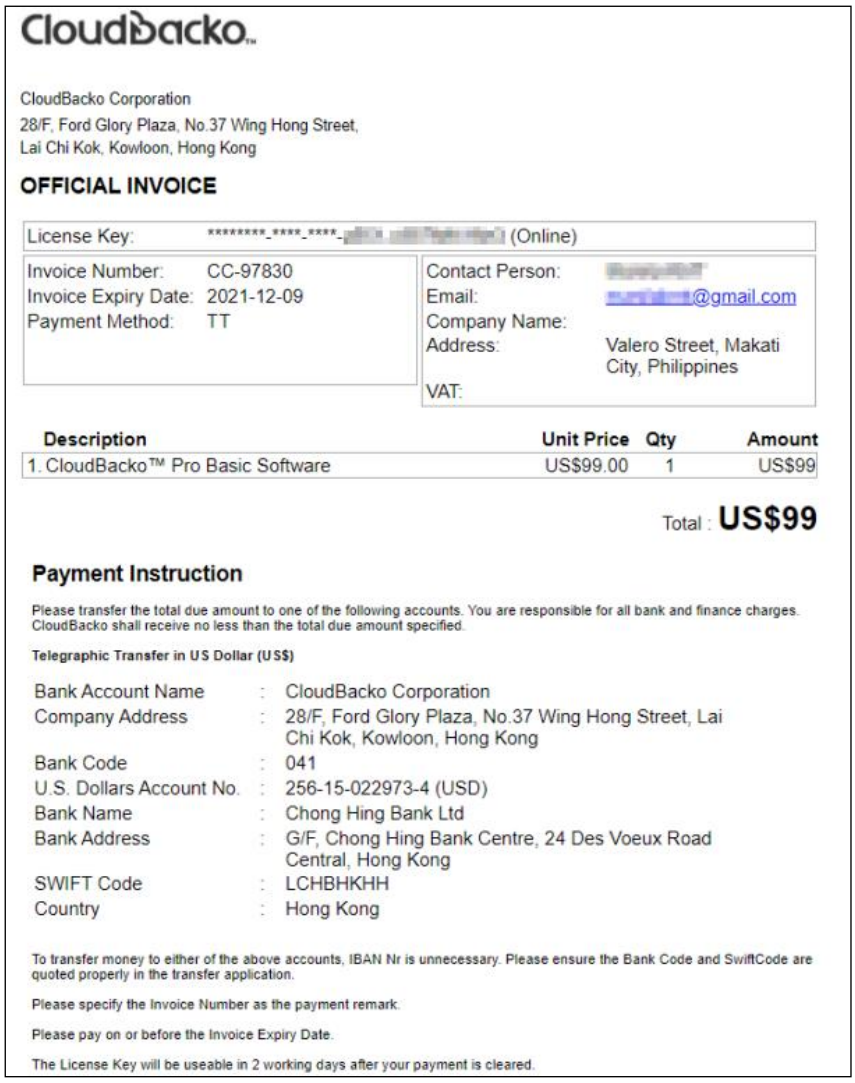
Thank you for purchasing CloudBacko. Attached please find your invoice #CC-97830.

Please settle the payment according to the instruction stated in the invoice. The License Key will be useable in 2 working days after your payment is cleared.

Regards,

Customer Service
CloudBacko Corporation

Invoice_CC-97830.html
18 KB



CloudBacko™

CloudBacko Corporation
28/F, Ford Glory Plaza, No.37 Wing Hong Street,
Lai Chi Kok, Kowloon, Hong Kong

OFFICIAL INVOICE

License Key: ********_****_****_[redacted] (Online)

Invoice Number:	CC-97830	Contact Person:	[redacted]
Invoice Expiry Date:	2021-12-09	Email:	[redacted]@gmail.com
Payment Method:	TT	Company Name:	
		Address:	Valero Street, Makati City, Philippines
		VAT:	

Description	Unit Price	Qty	Amount
1. CloudBacko™ Pro Basic Software	US$99.00	1	US$99

Total : **US$99**

Payment Instruction

Please transfer the total due amount to one of the following accounts. You are responsible for all bank and finance charges. CloudBacko shall receive no less than the total due amount specified.

Telegraphic Transfer in US Dollar (US$)

Bank Account Name	:	CloudBacko Corporation
Company Address	:	28/F, Ford Glory Plaza, No.37 Wing Hong Street, Lai Chi Kok, Kowloon, Hong Kong
Bank Code	:	041
U.S. Dollars Account No.	:	256-15-022973-4 (USD)
Bank Name	:	Chong Hing Bank Ltd
Bank Address	:	G/F, Chong Hing Bank Centre, 24 Des Voeux Road Central, Hong Kong
SWIFT Code	:	LCHBHKHH
Country	:	Hong Kong

To transfer money to either of the above accounts, IBAN Nr is unnecessary. Please ensure the Bank Code and SwiftCode are quoted properly in the transfer application.

Please specify the Invoice Number as the payment remark.

Please pay on or before the Invoice Expiry Date.

The License Key will be useable in 2 working days after your payment is cleared.

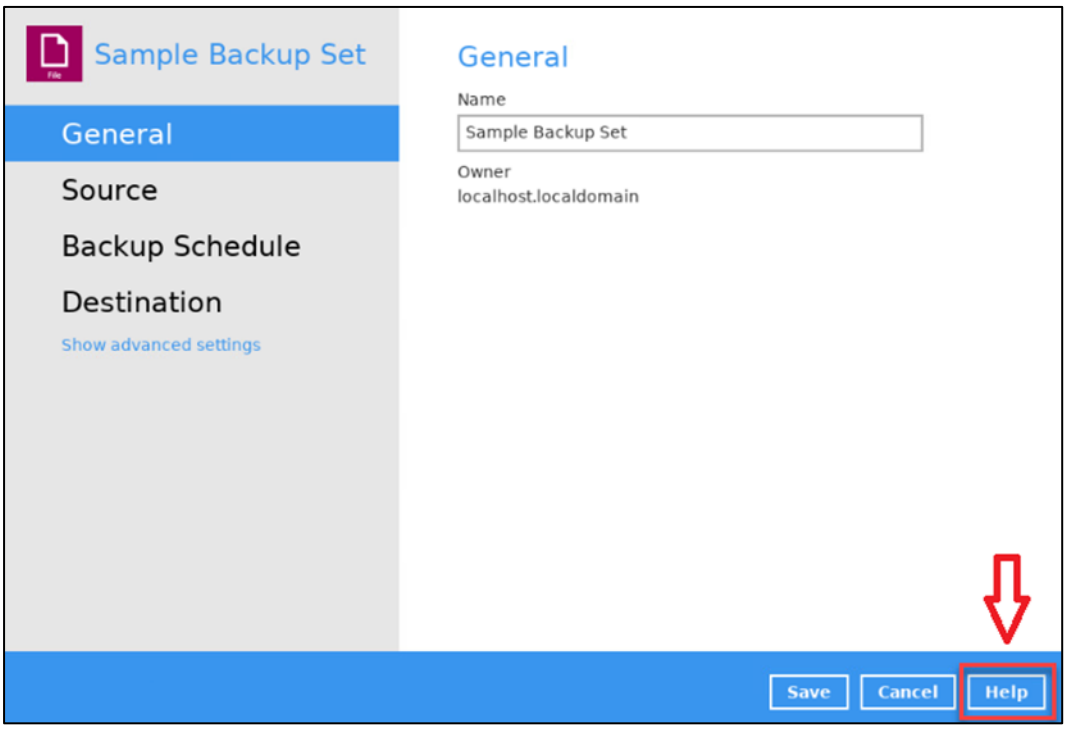
7.10 Social Media Icons

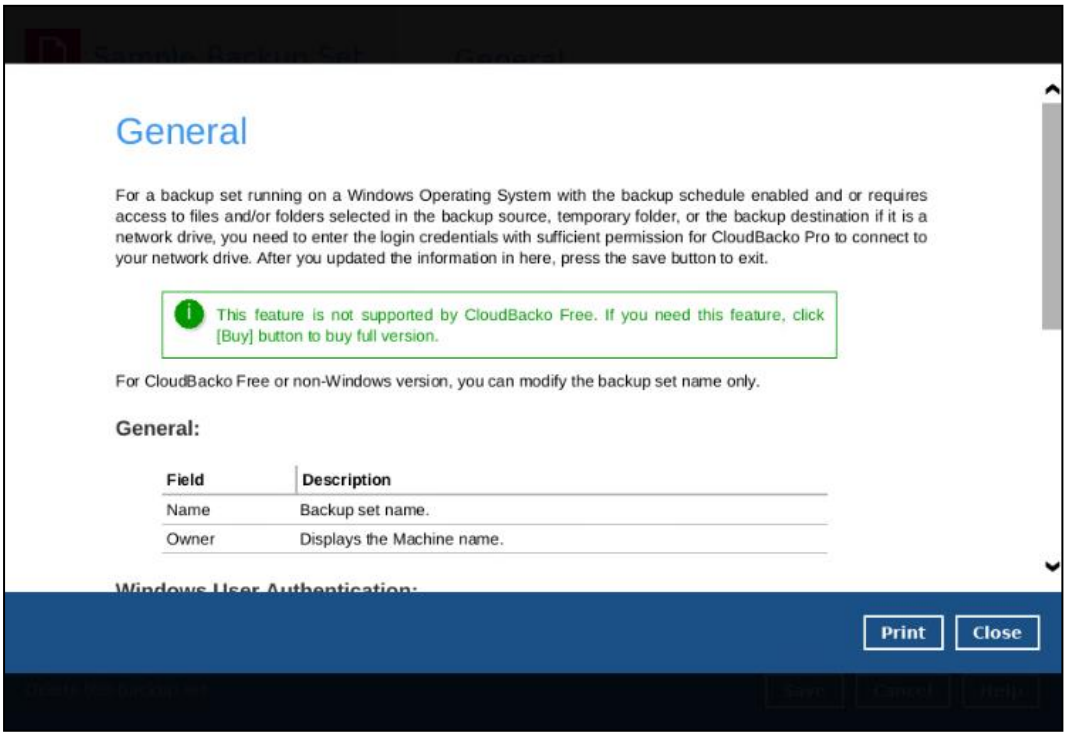
These are the social media accounts of CloudBacko. Each icon links to the CloudBacko page or channel.

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

7.11 Online Help

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

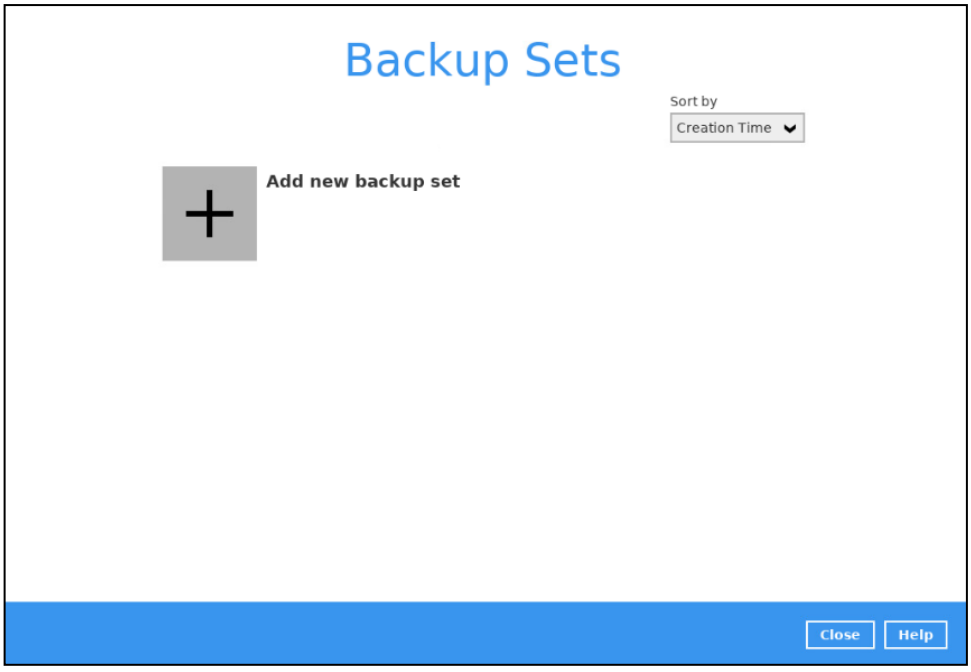




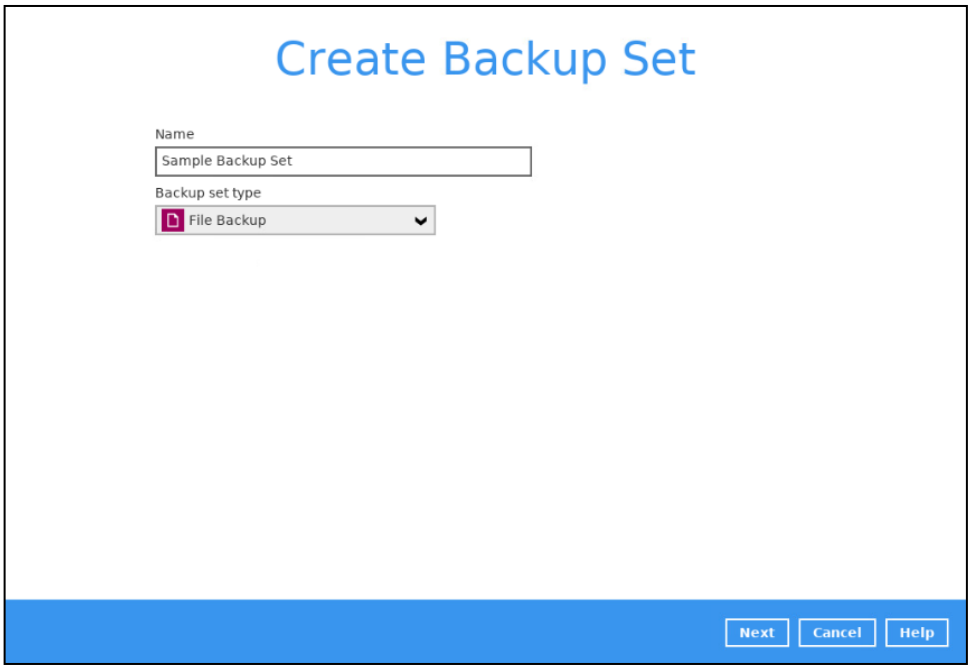
8 Create a Backup Set

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

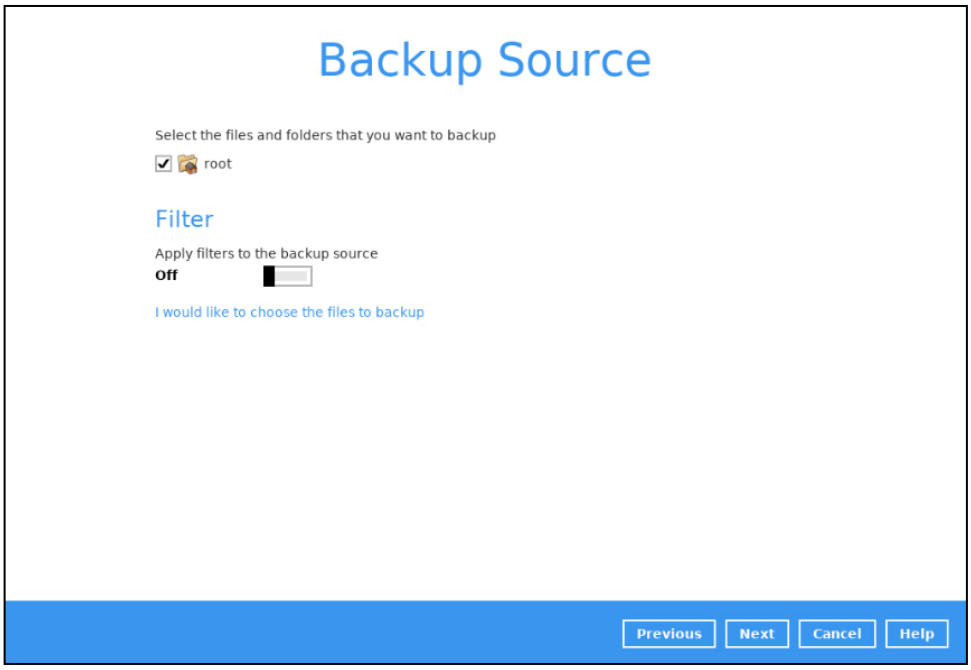
2. Create a new backup set by clicking  next to **Add new backup set**.



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

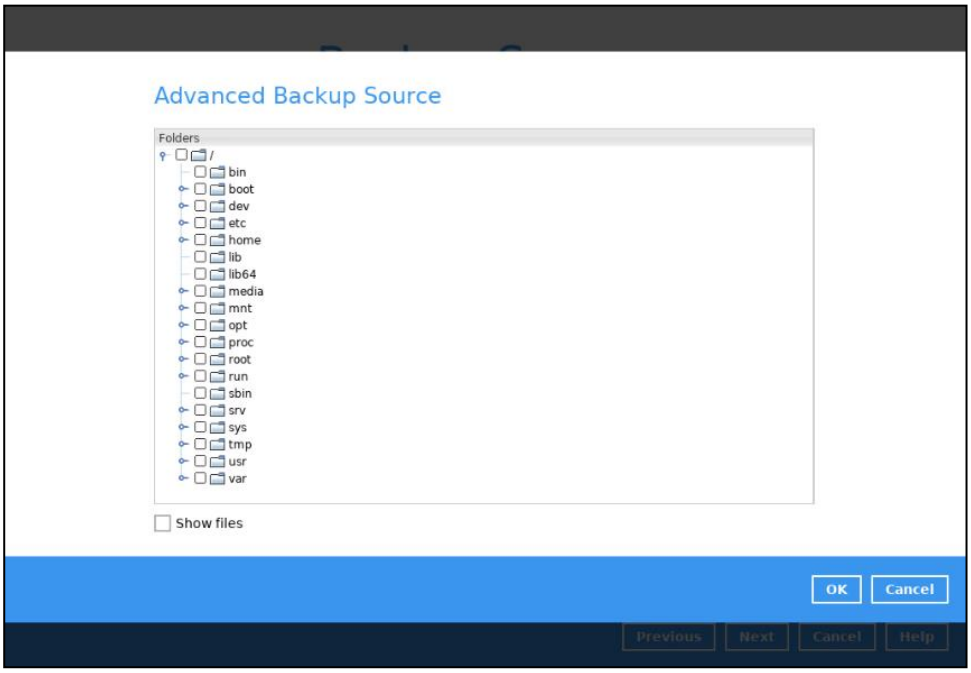


4. In the Backup Source window, select the source files and folders for backup. Click **I would like to choose the files to backup** to select individual files for backup.

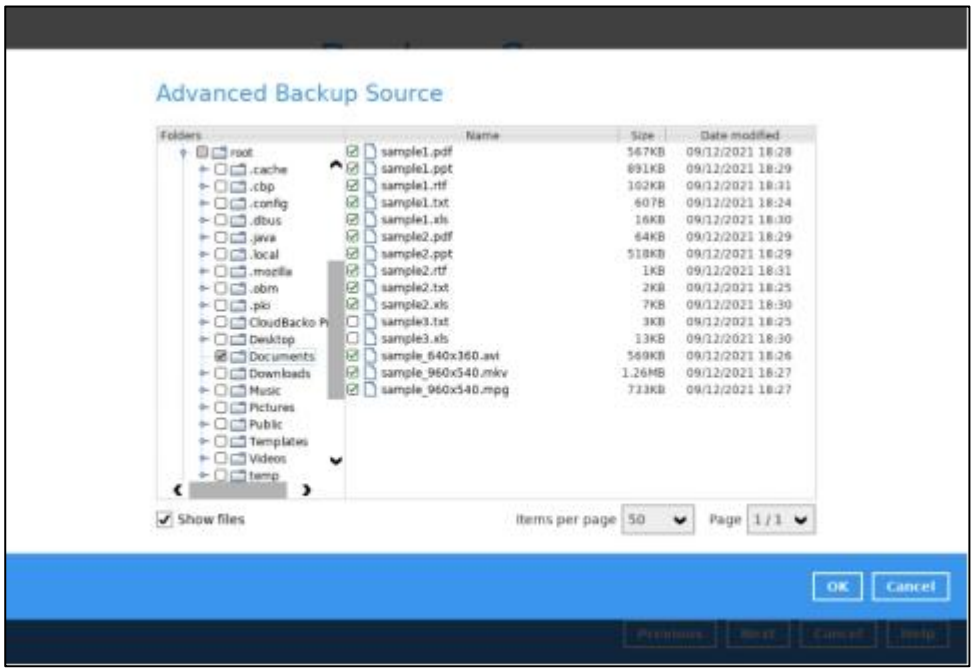


5. In the **Advanced Backup Source** window, select folder(s) to back up all files in the folder(s).

   i. Select folder(s) to back up all files in the folder(s). Click **OK** to save the selection and close the Advanced Backup Source window.



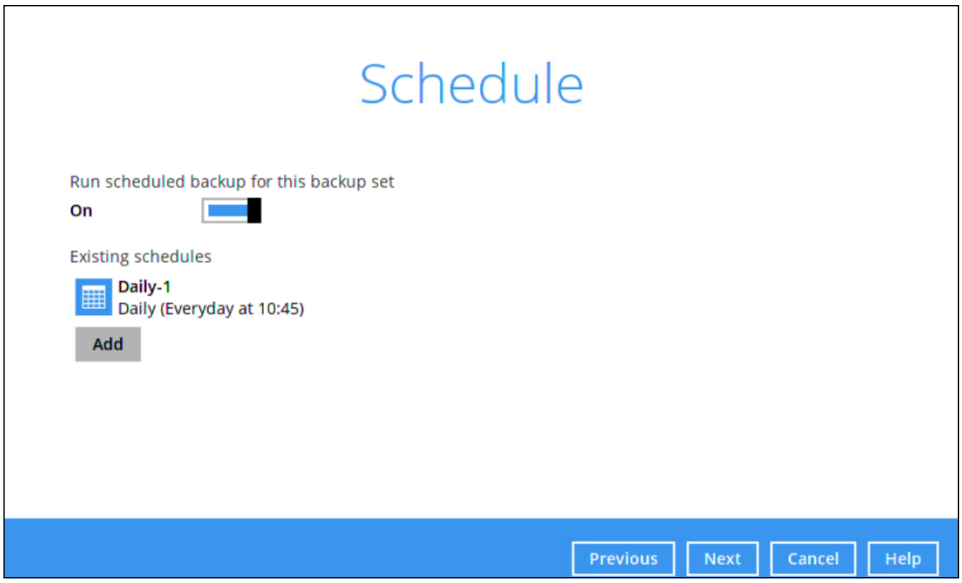
ii. Alternatively, if you want to back up only specific files instead of all files in your selected folder(s), select the **Show files** checkbox at the bottom of the screen. A list of files will appear on the right-hand side. Select the checkbox(es) next to the file(s) to back up. Then, click **OK**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



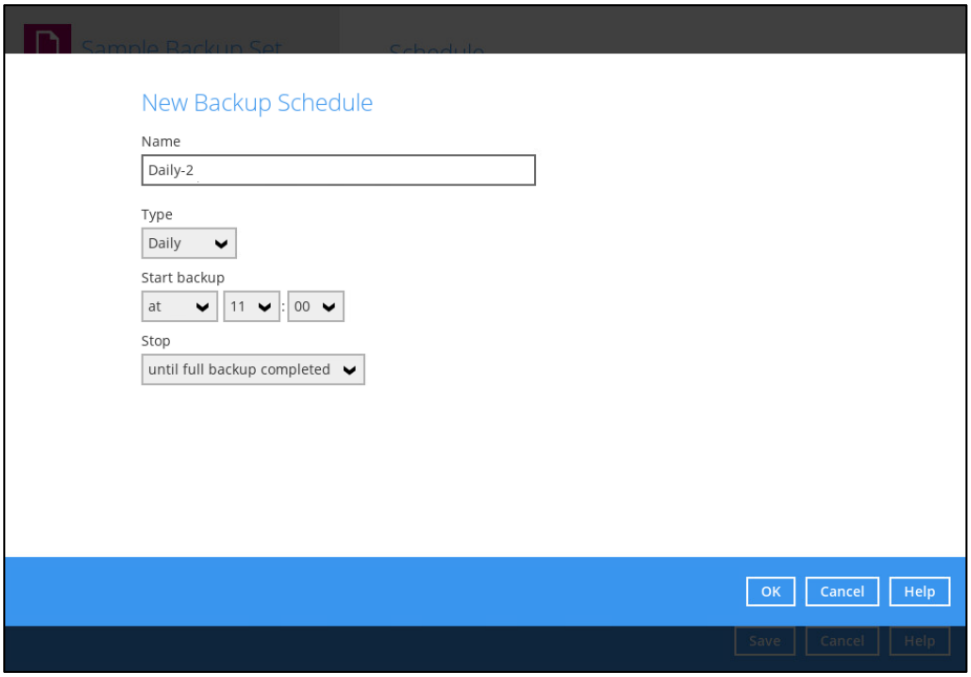
6. In the Backup Source window, click **Next** to proceed.

7. When the Schedule window appears, you can configure a backup schedule to automatically run a backup job at your specified time interval. In the Schedule window, the Run scheduled backup for this backup set is **Off** by default.

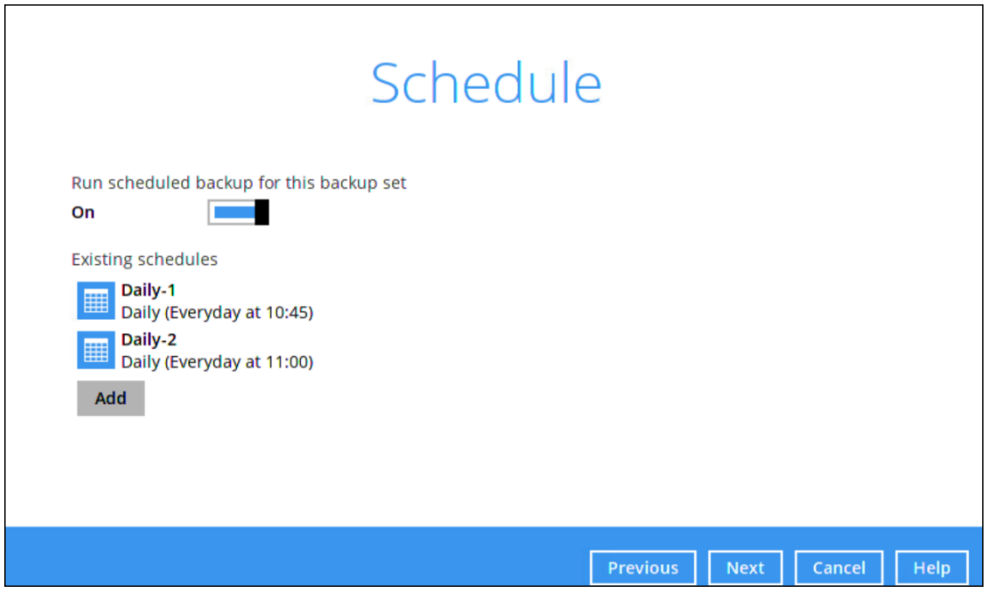
   - In the default backup schedule, there will be a daily schedule performed at the time you created the schedule. You can leave it as is or you can modify it by clicking on the existing backup schedule.



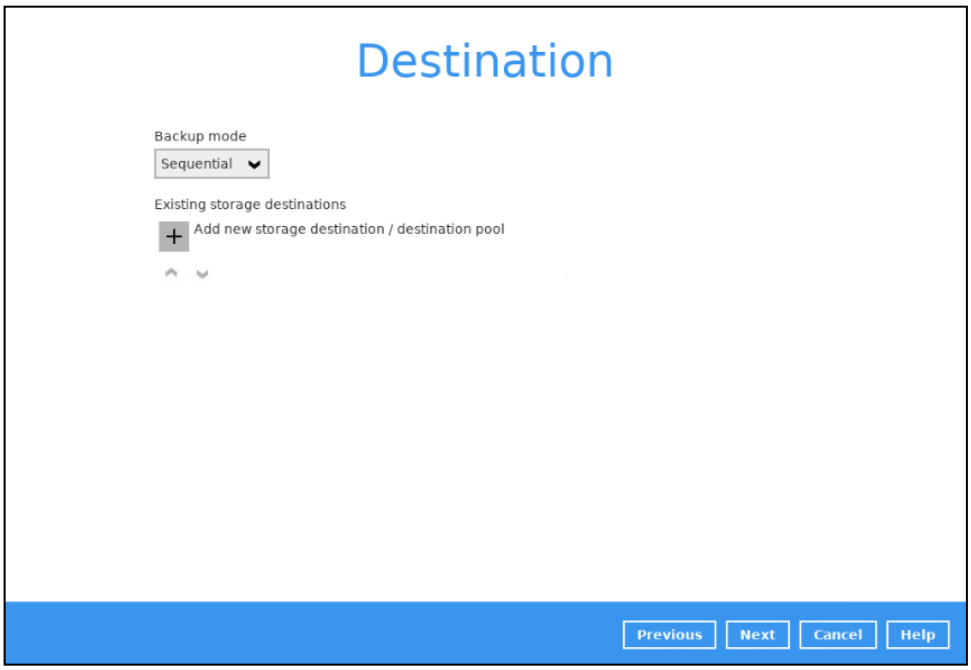
- If you want to add another schedule, click the **Add** button. When the New Backup Schedule window appears, specify your backup schedule. Then, click **OK** to save your changes and close the New Backup Schedule window.



8. In case you have added a schedule, it will be shown in the Schedule window. Click **Next** to proceed when you are done setting.



9. The **Destination** window will appear.

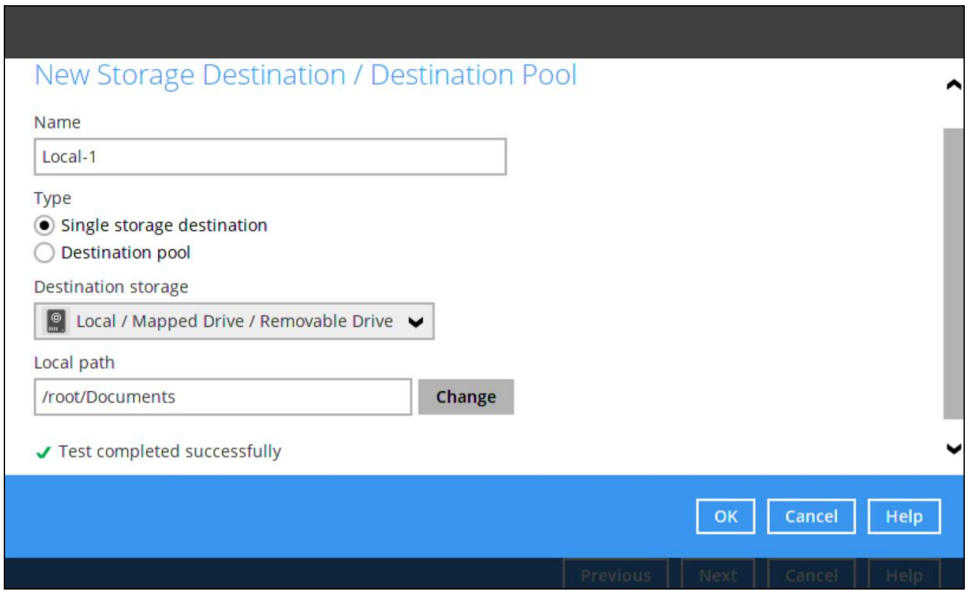


Select the appropriate option from the **Backup mode** dropdown menu.

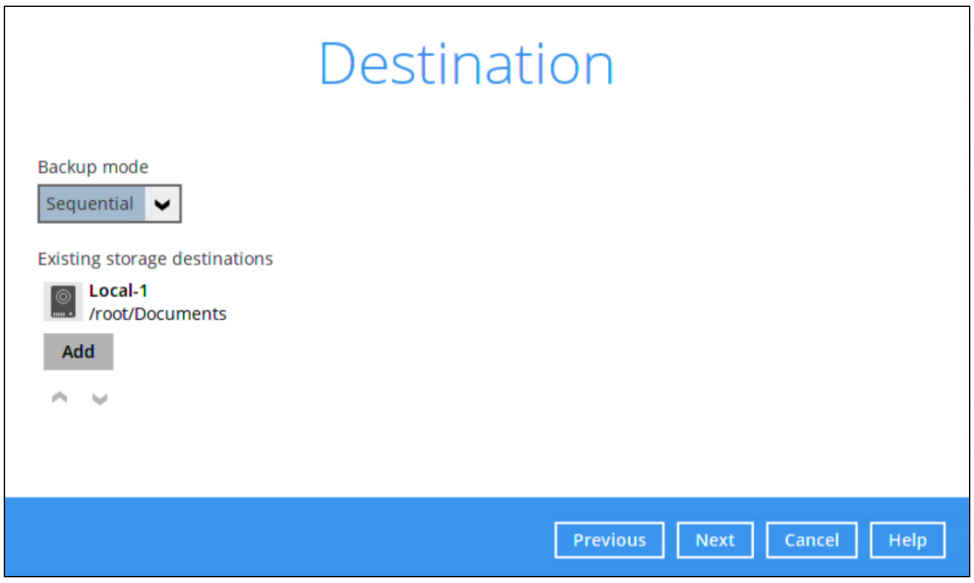
- **Sequential** (default value) – run backup jobs to each backup destination one by one
- **Concurrent** – run backup jobs to all backup destinations at the same time

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

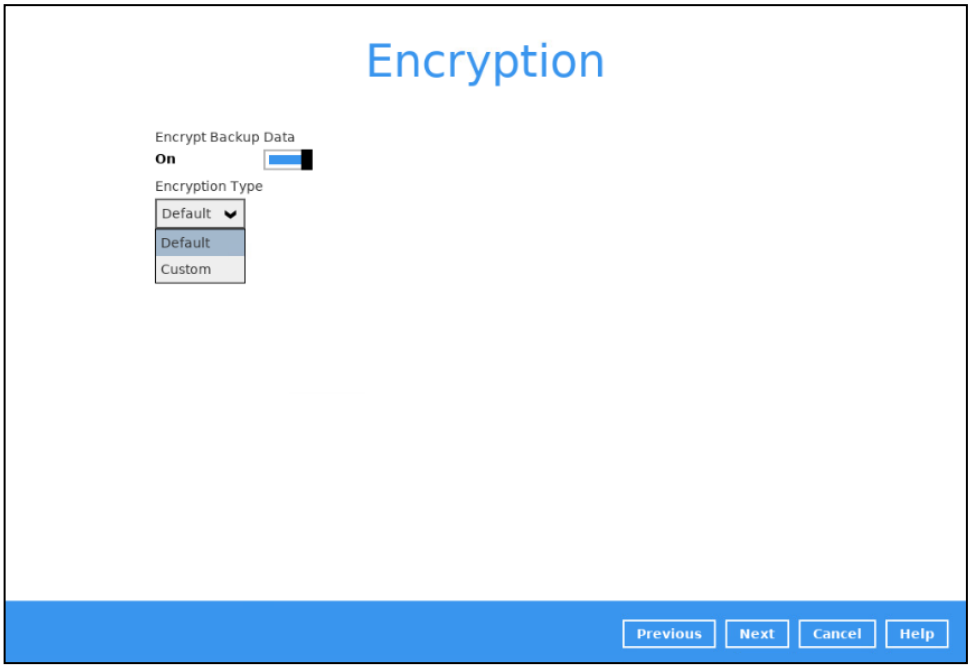
10. In the New Storage Destination / Destination Pool window, select the destination type and destination storage. Then, click **OK** to confirm your selection.



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

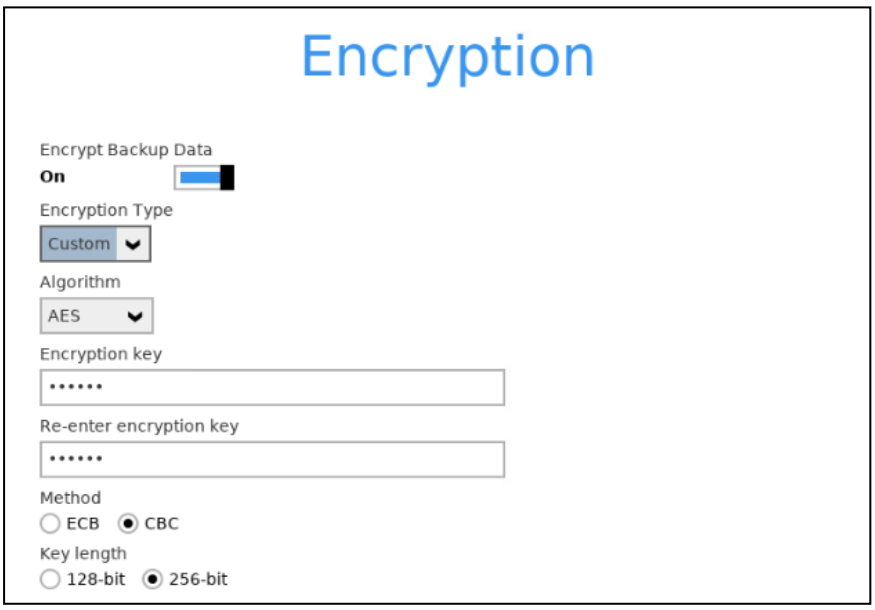


12. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



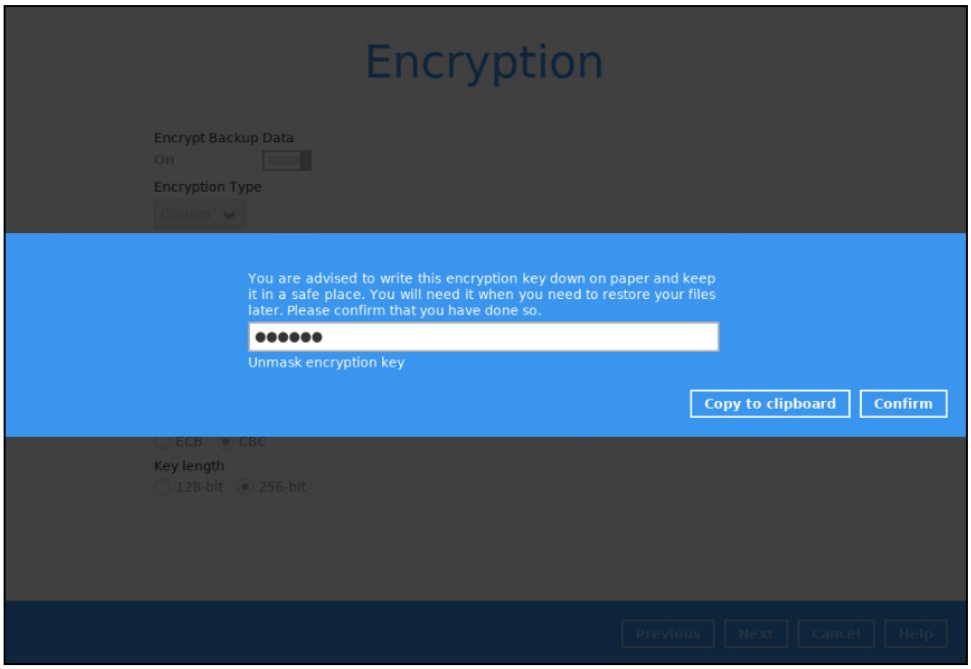
You can choose from one of the following two Encryption Type options:

- **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.



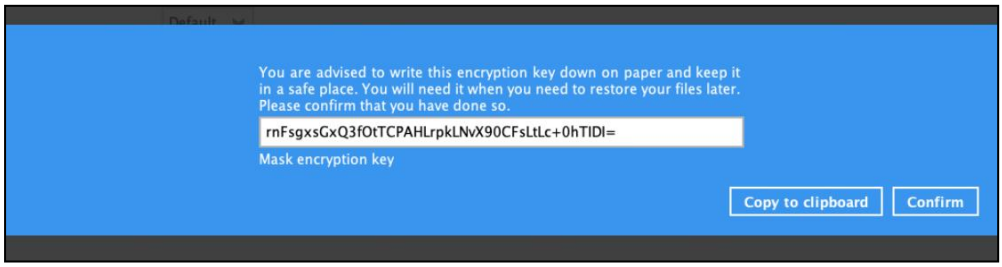
Click **Next** when you are done setting.

13. 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:

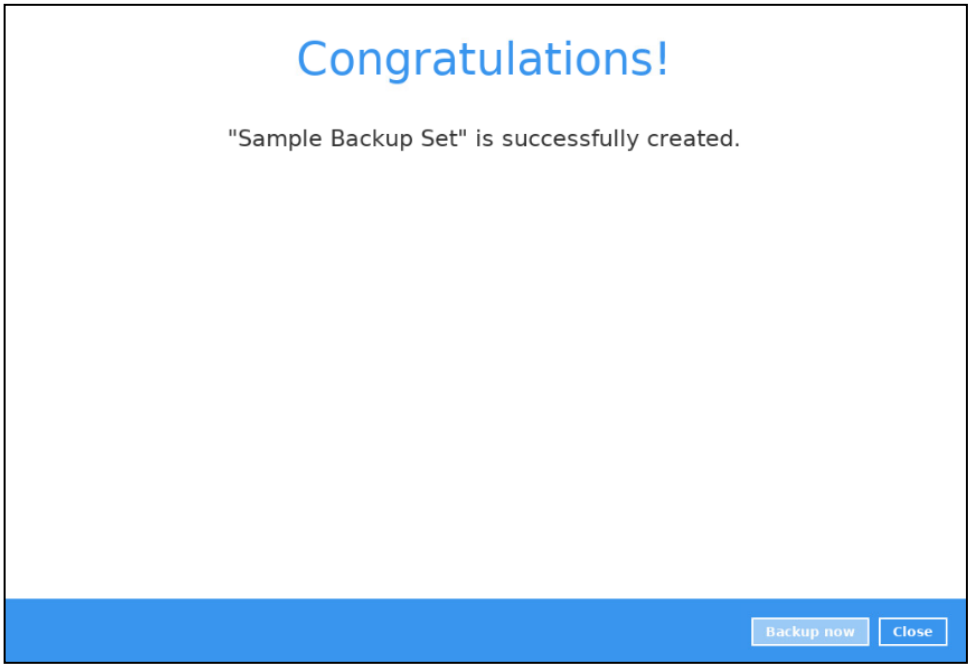
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



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

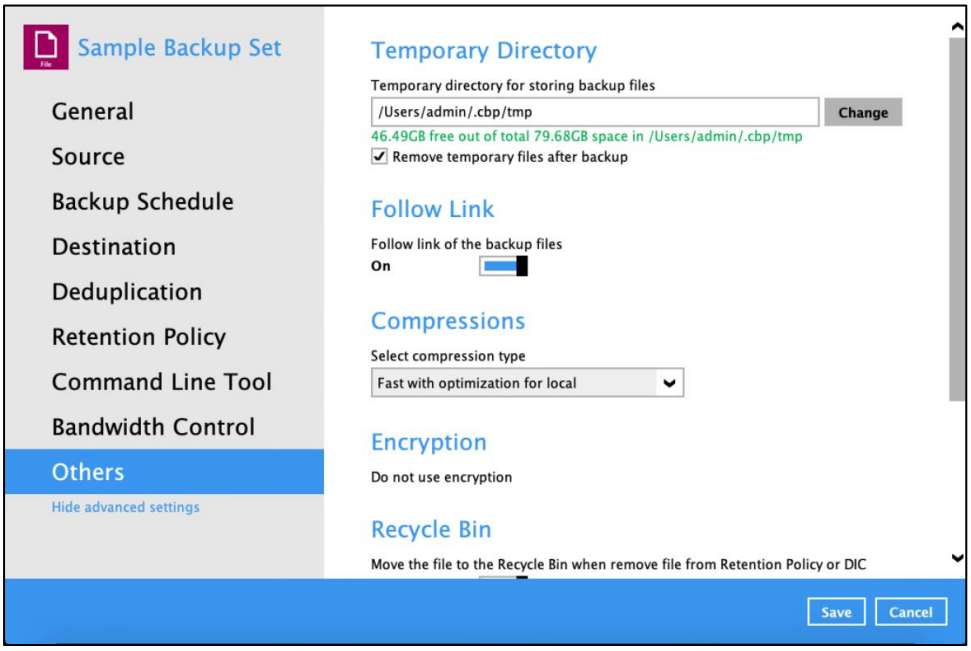
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

14. 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.



15. It is highly recommended to change the Temporary Directory. Select another location with sufficient free disk space other than **/tmp/CloudBacko Pro**.

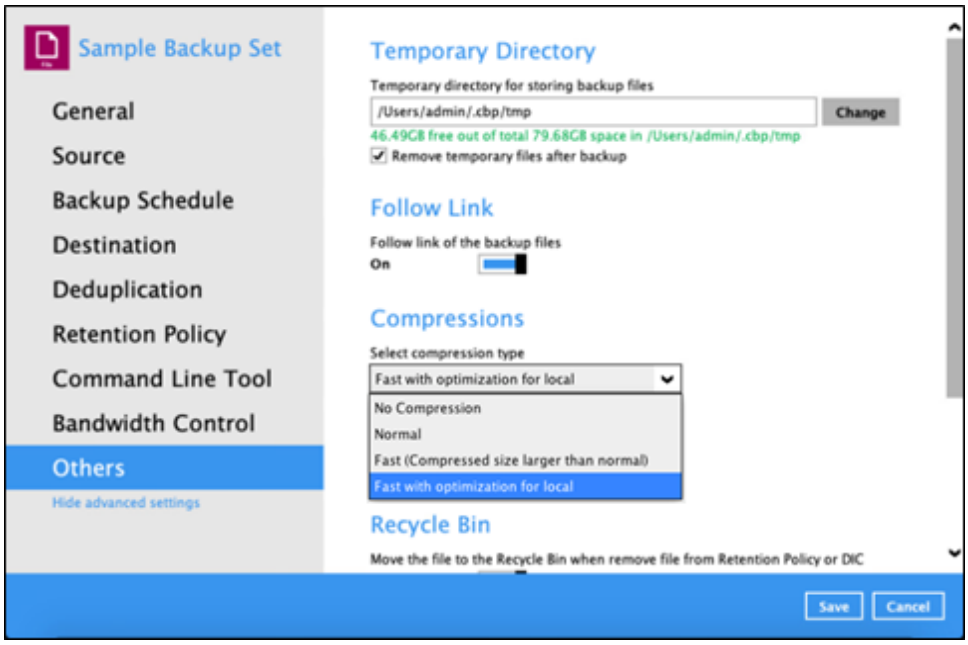
    Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



16. 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 list:

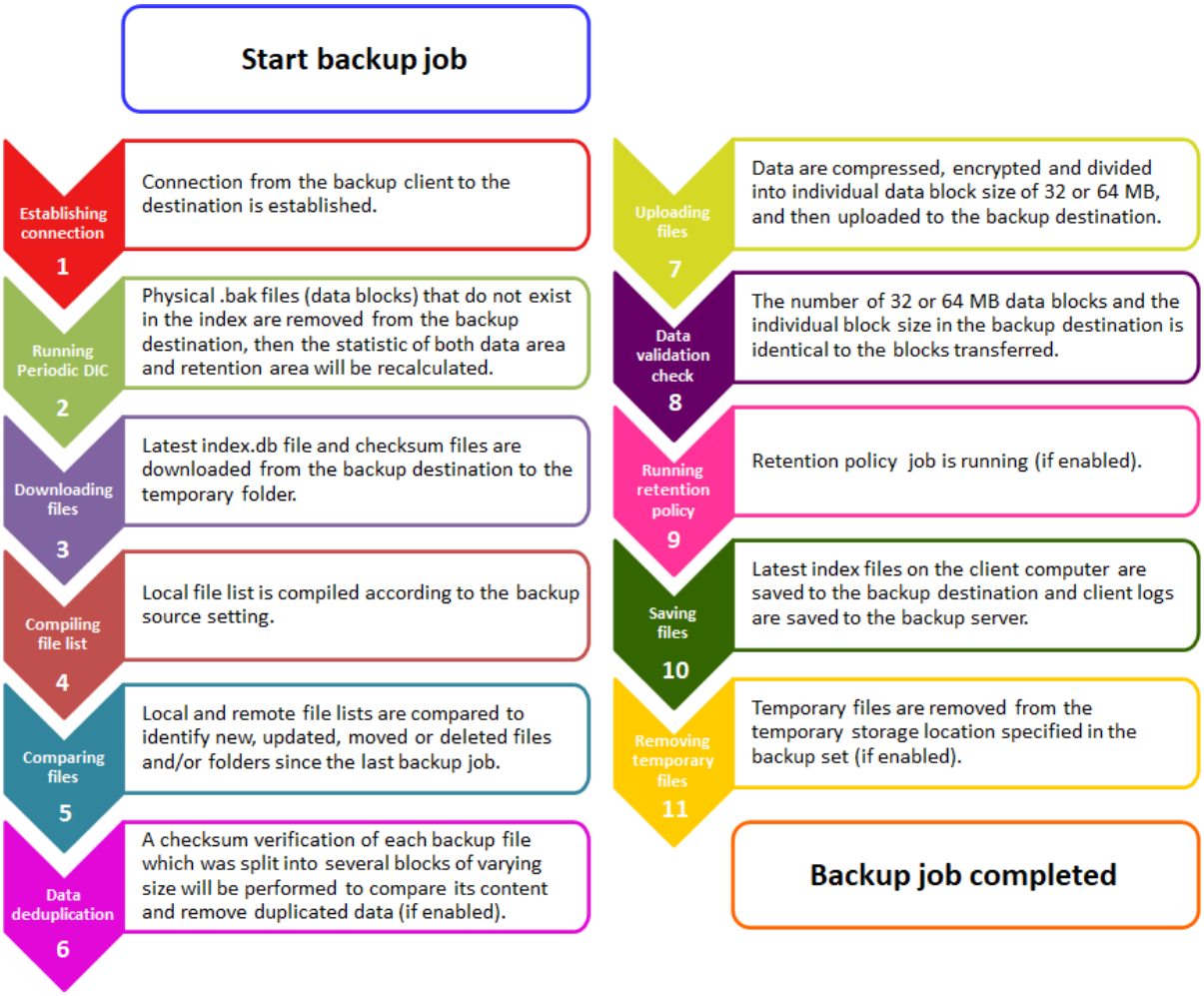
    - No Compression
    - Normal
    - Fast
    - Fast with optimization for local



9 Overview on the Backup Process

The following steps are performed during a backup job. For an overview of the detailed process for Steps **2**, **4**,**10**, and **12,** refer to the following chapters:

- Periodic Data Integrity Check (PDIC) Process **(Step 2)**
- Backup Set Index Handling Process
  - Start Backup Job **(Step 4)**
  - Completed Backup Job **(Step12)**
- Data Validation Check **(Step 10)**



9.1 Periodic Data Integrity Check (PDIC) Process

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:

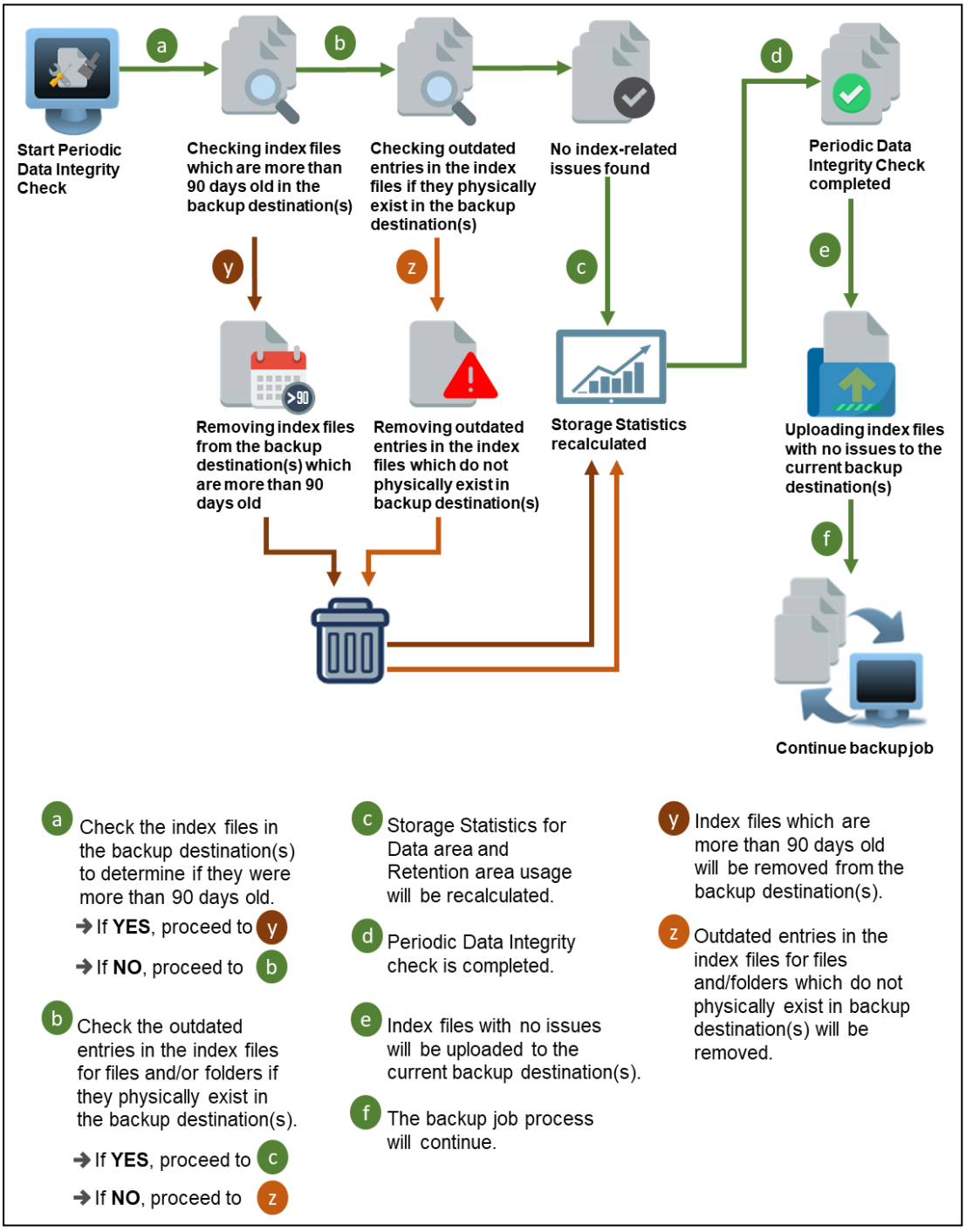
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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.

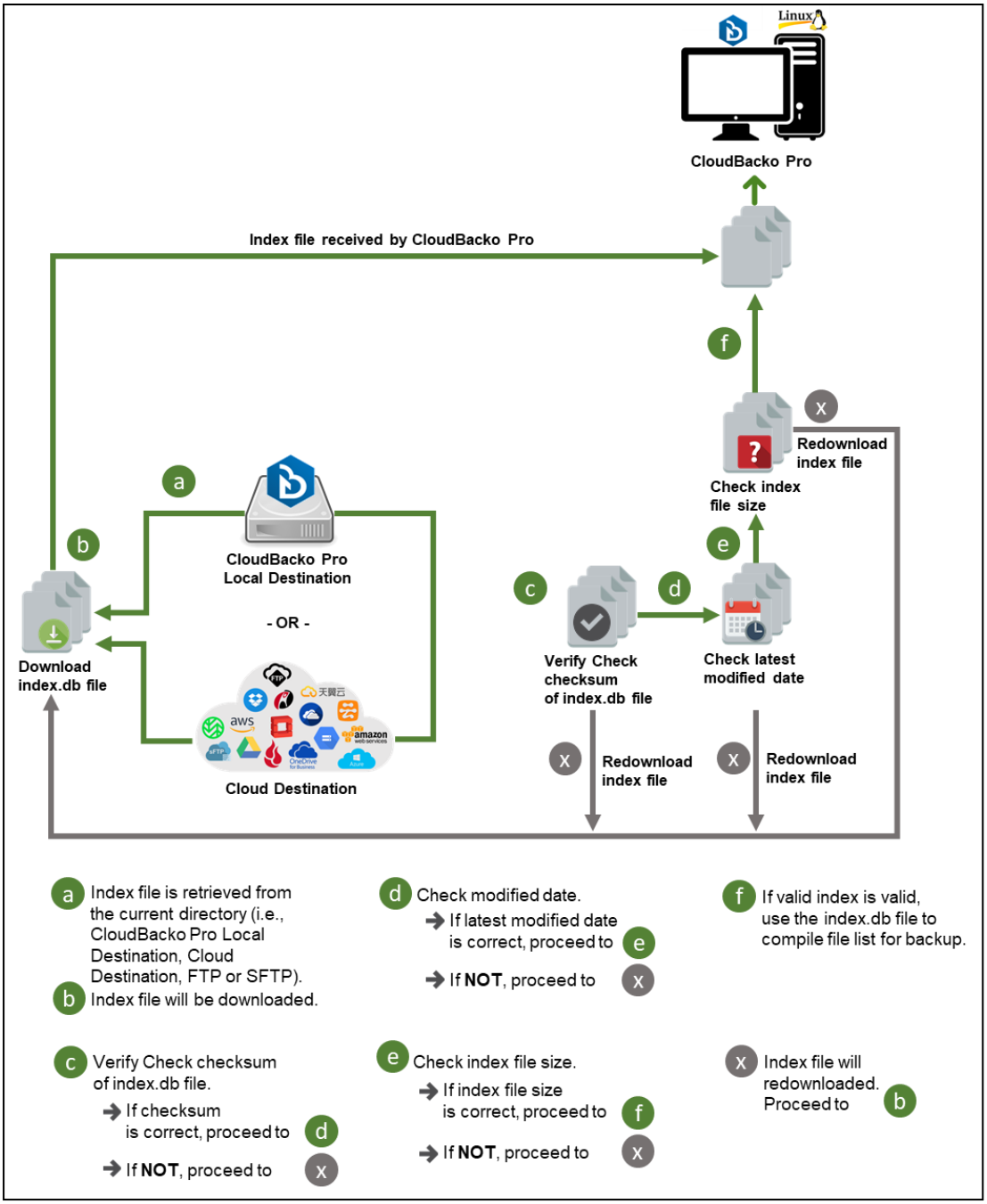
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

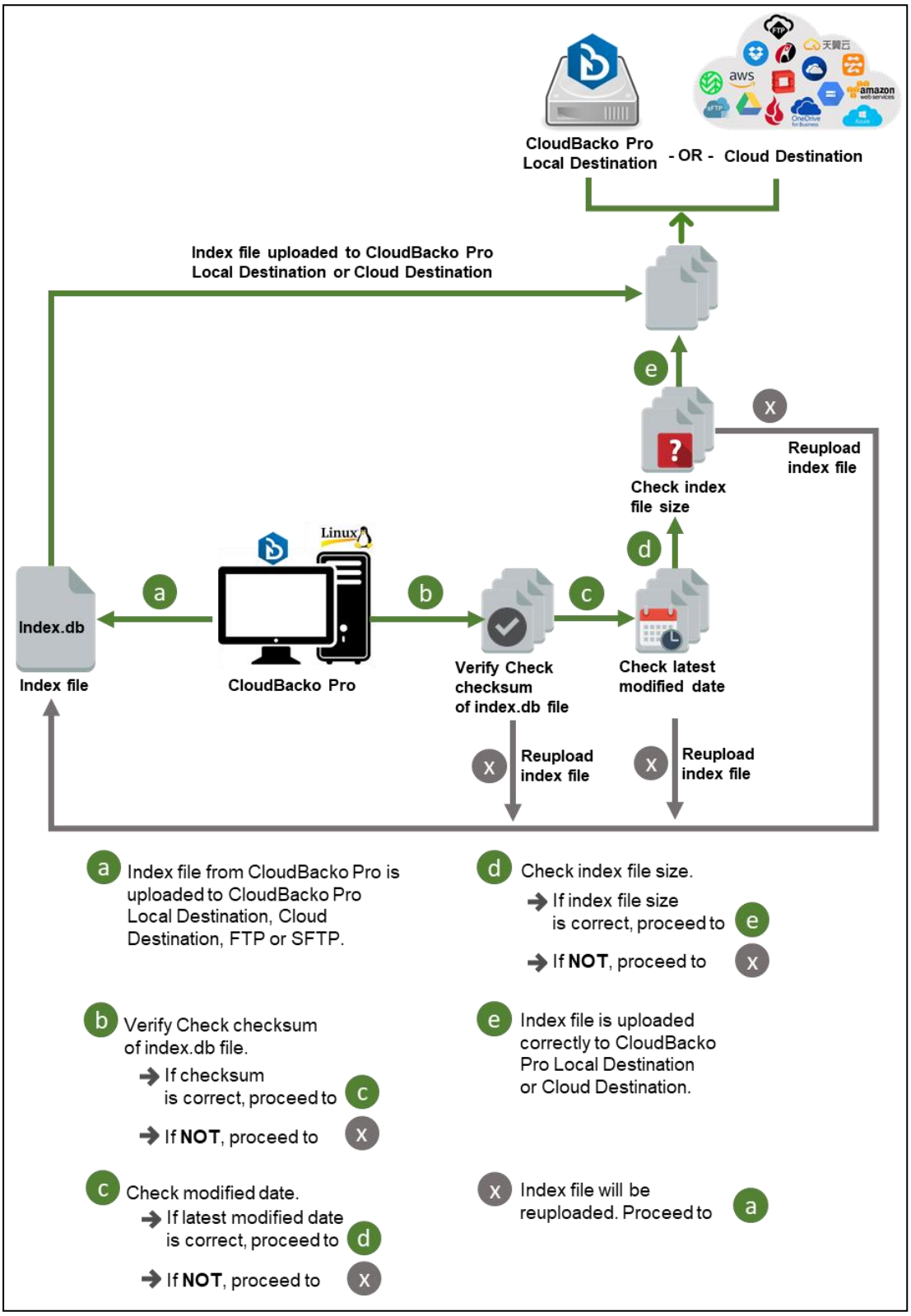
9.2 Backup Set Index Handling Process

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

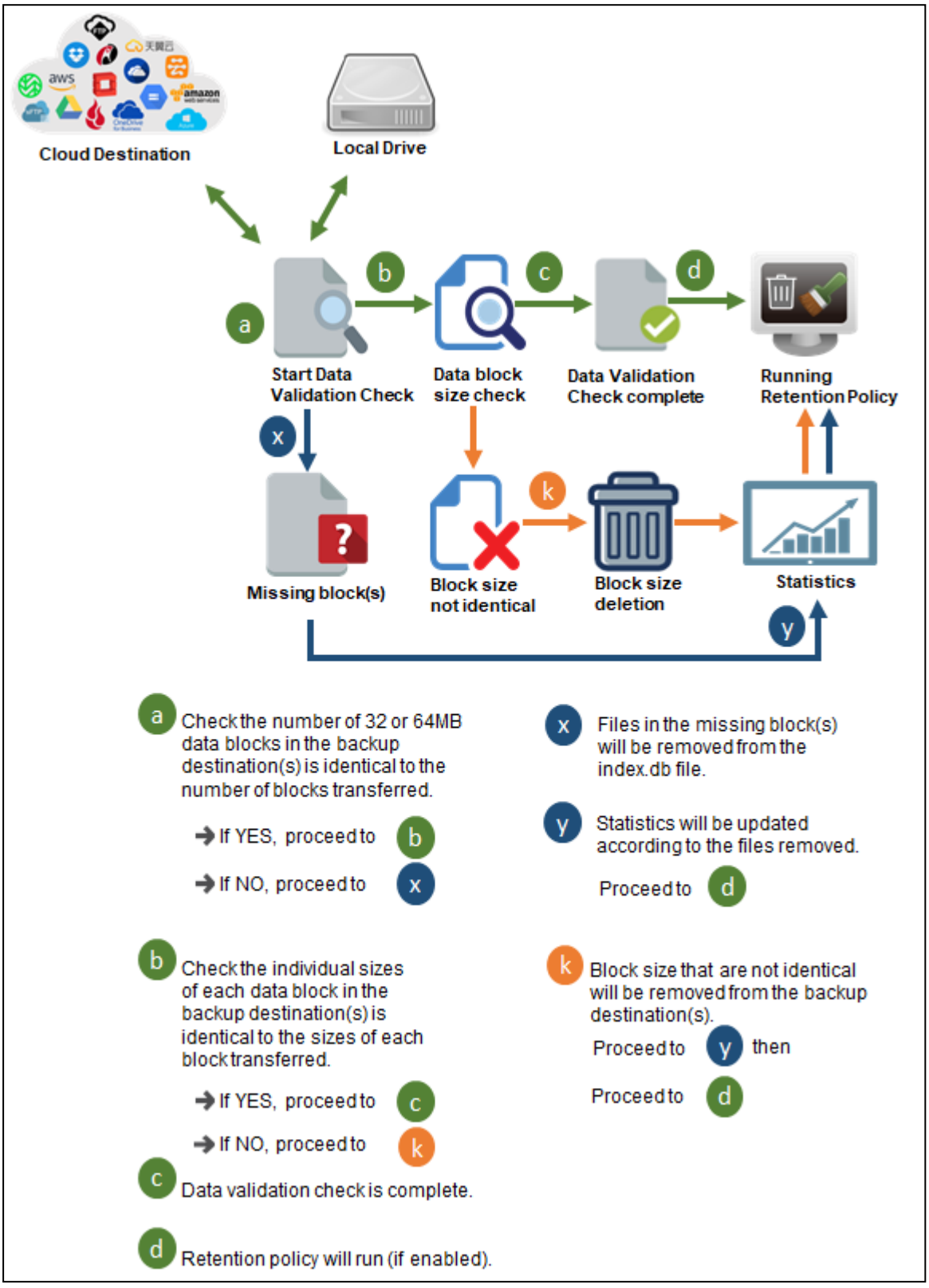


9.2.2 Completed Backup Job



9.3 Data Validation Check Process

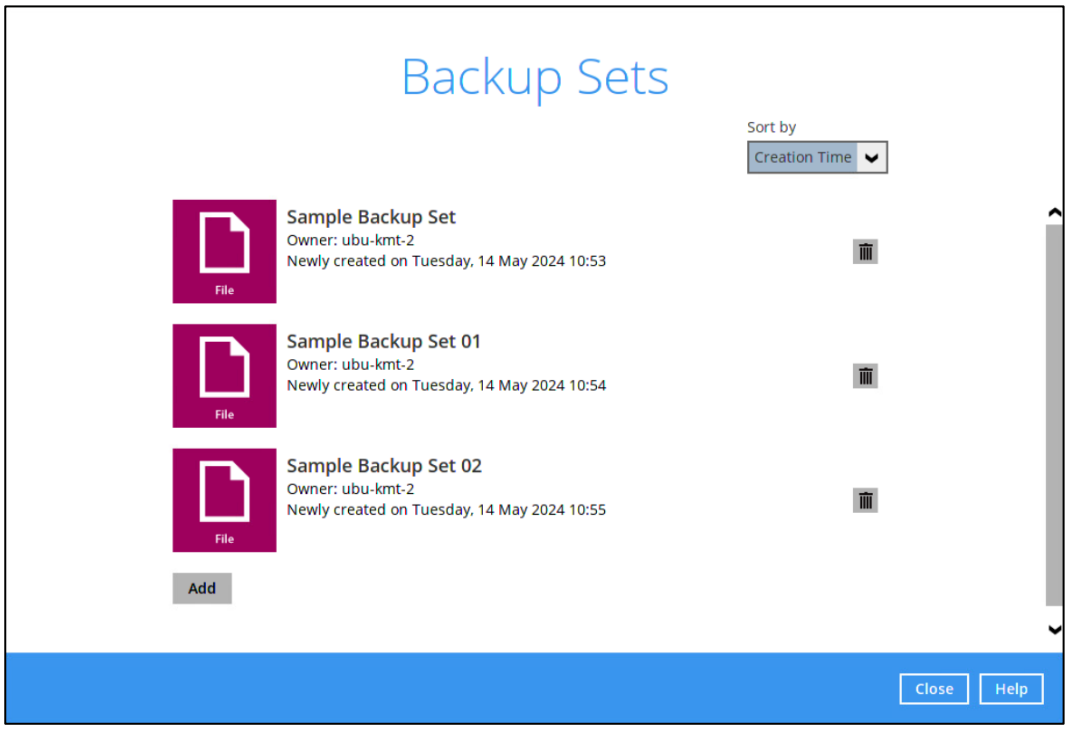
As an additional measure to ensure that all files transferred to the backup destination(s) are received and saved correctly, both the number of 16 or 32 MB data block files and the size of each block file are checked again after the files are transferred.



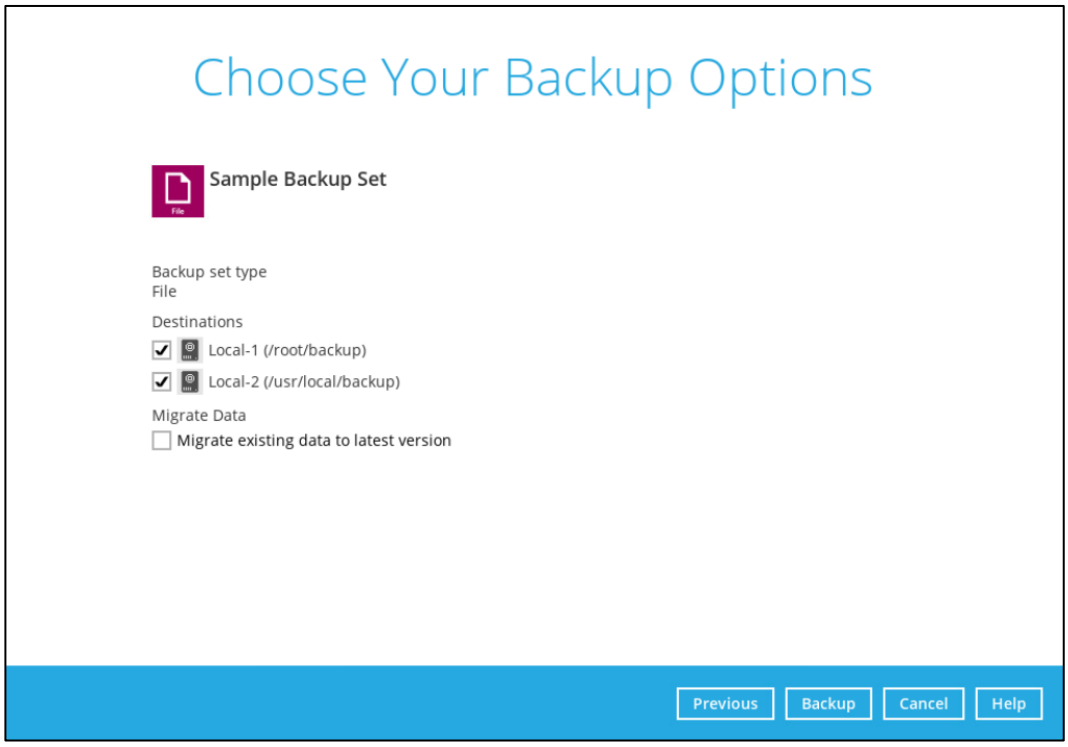
10 Running Backup Jobs

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

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



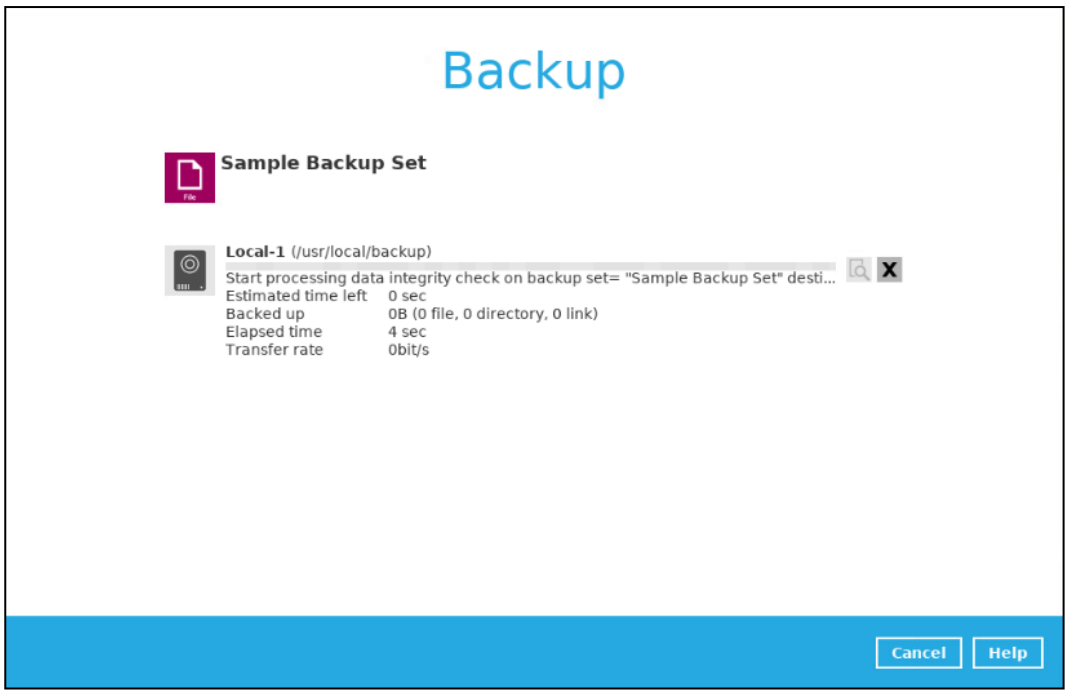
3. You can modify the Destinations and Migrate Data options. Once done with the settings, click the **Backup** button to start the backup job.



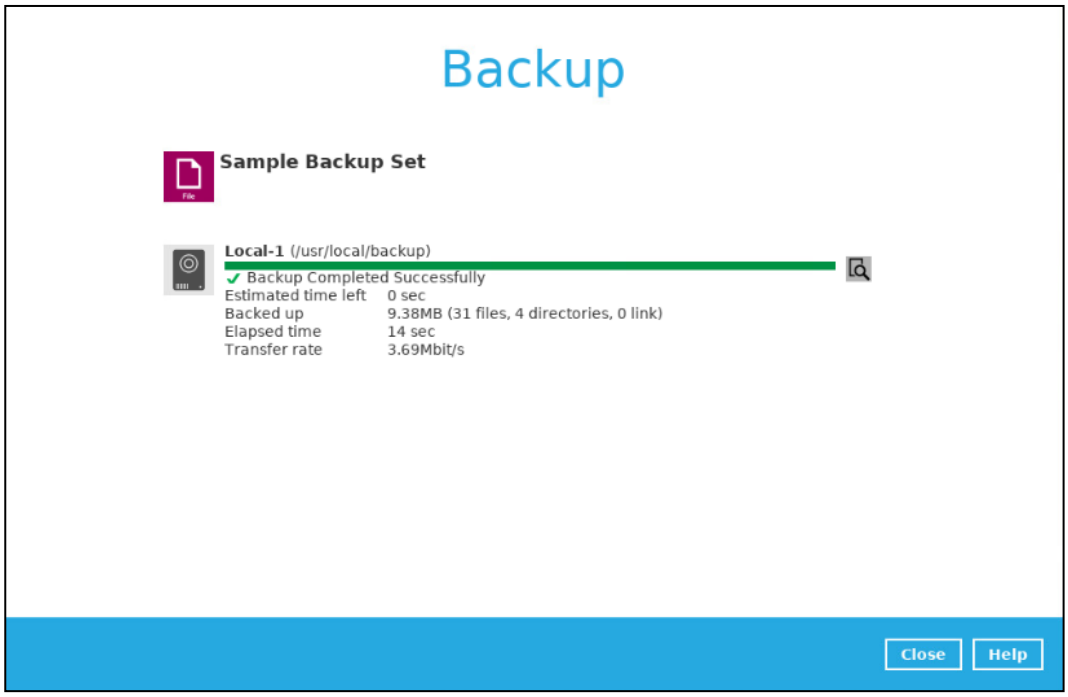
NOTE

The Migrate Data option will only be displayed if Deduplication is enabled for the backup set. Backup job(s) for backup sets with Migrate Data enabled may take longer to finish.

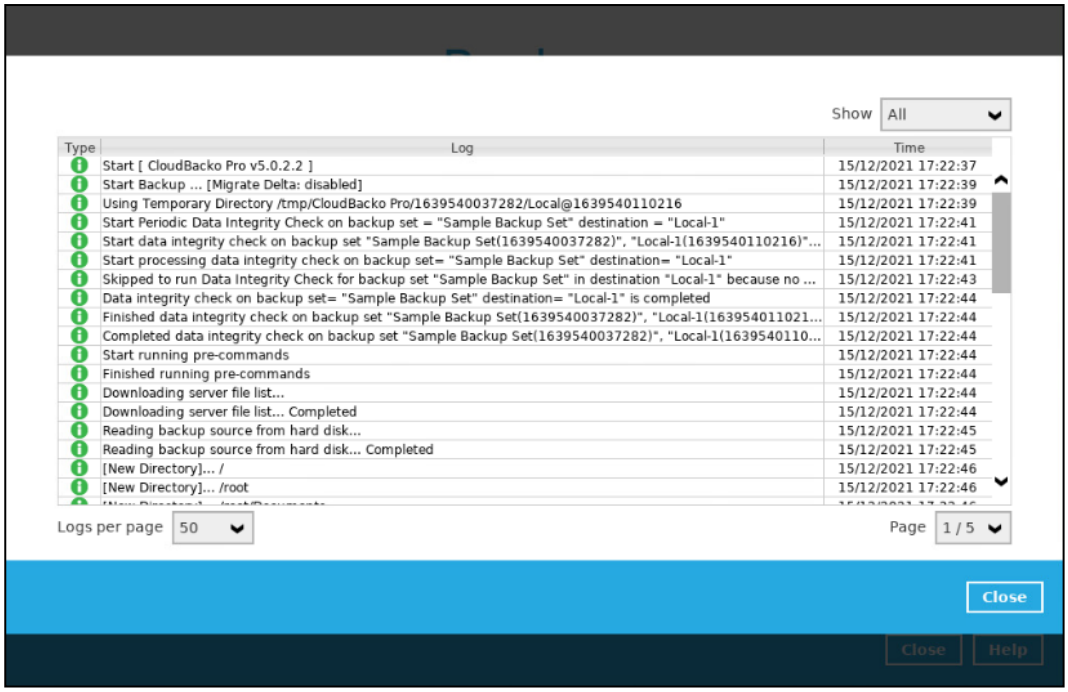
4. Click **Backup** to start the backup job. The status will be shown.



5. When the backup is completed, the progress bar will be green in color and the message "Backup Completed Successfully" will appear.



6. You can click the **View** icon on the right-hand side to check the log. A window will pop up to show the log. Close the pop-up window when you finish reading it.



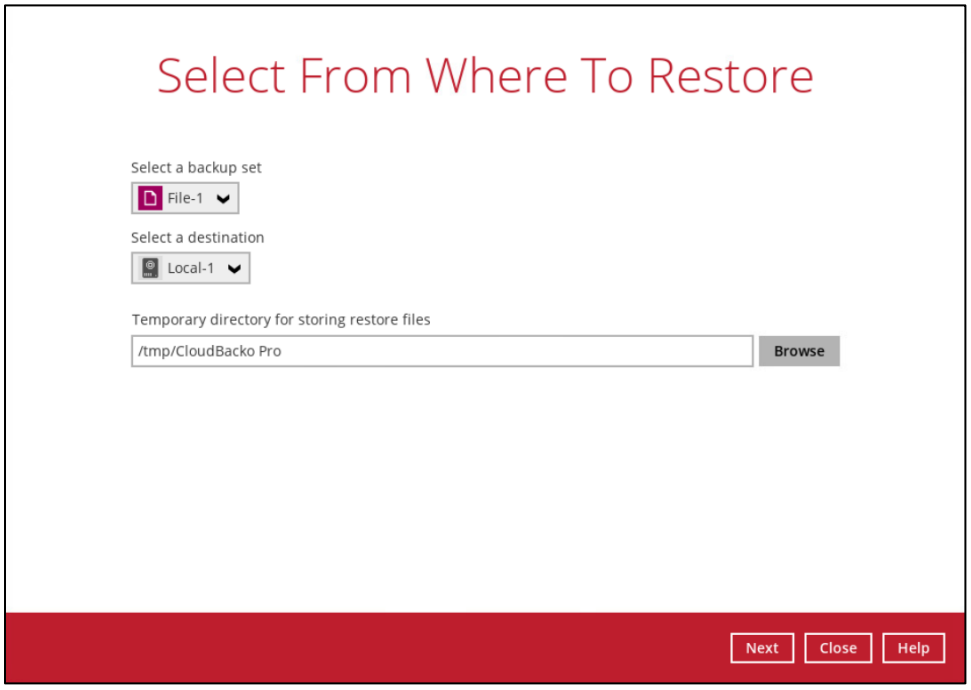
11 Restoring Data

11.1 Restore Method

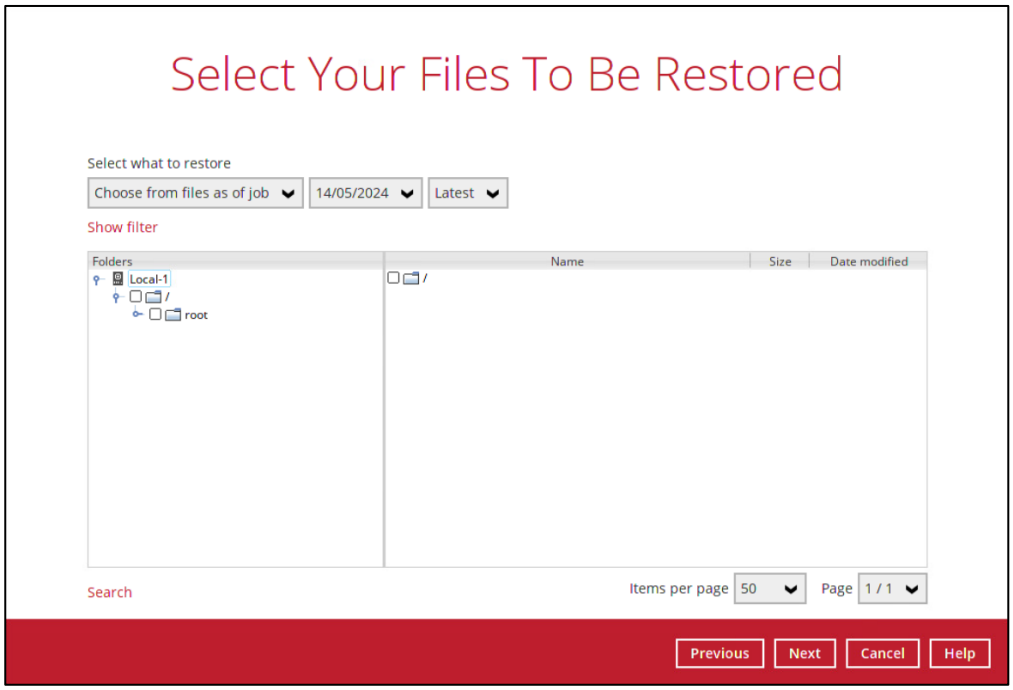
1. Login to CloudBacko Pro application according to the instructions in Chapter 6 Start CloudBacko Pro.
2. Click the **Restore** icon on the main interface of CloudBacko Pro.

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 choosing a directory under **Temporary directory for storing restore files**.

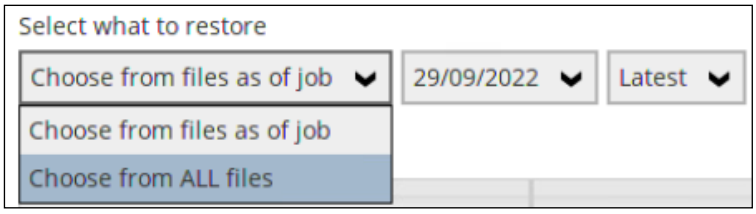


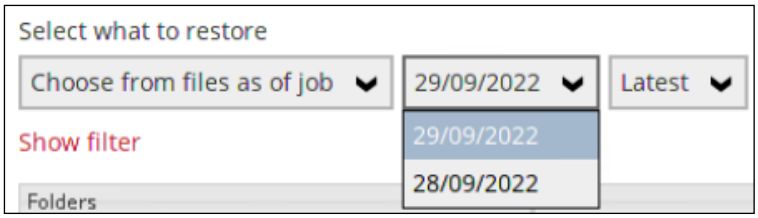
4. Select to restore files from a specific backup job, or from all files available. Then, select the files or folders that you would like to restore.



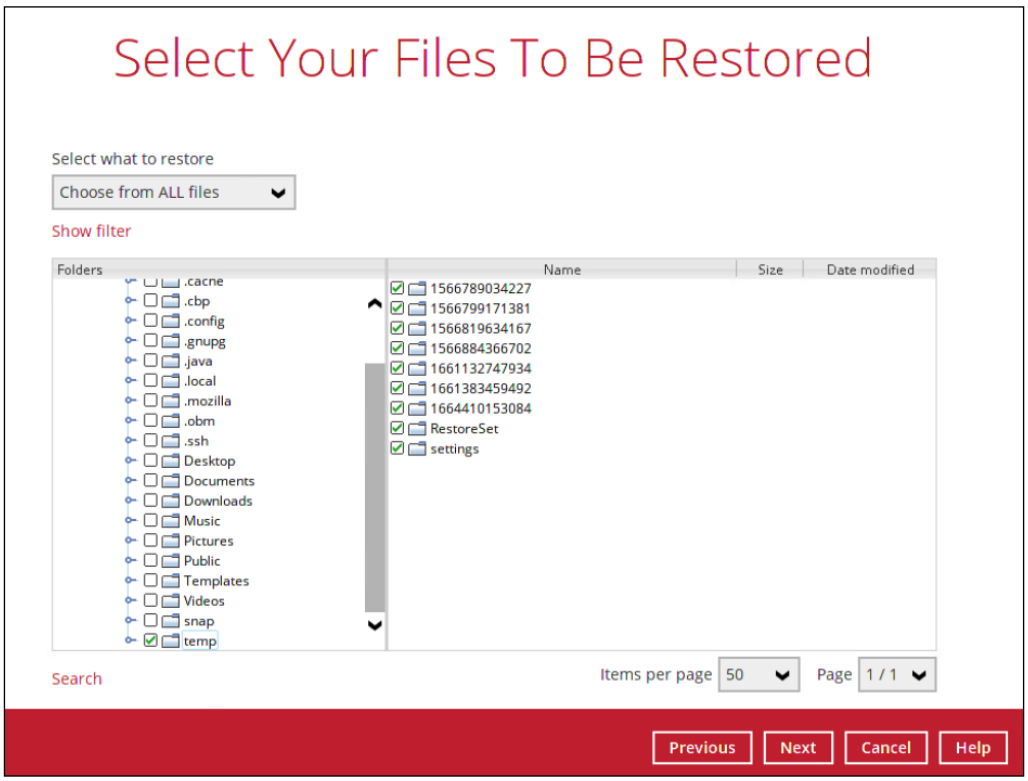
There are two options from the **Select what to restore** dropdown menu:

- **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.

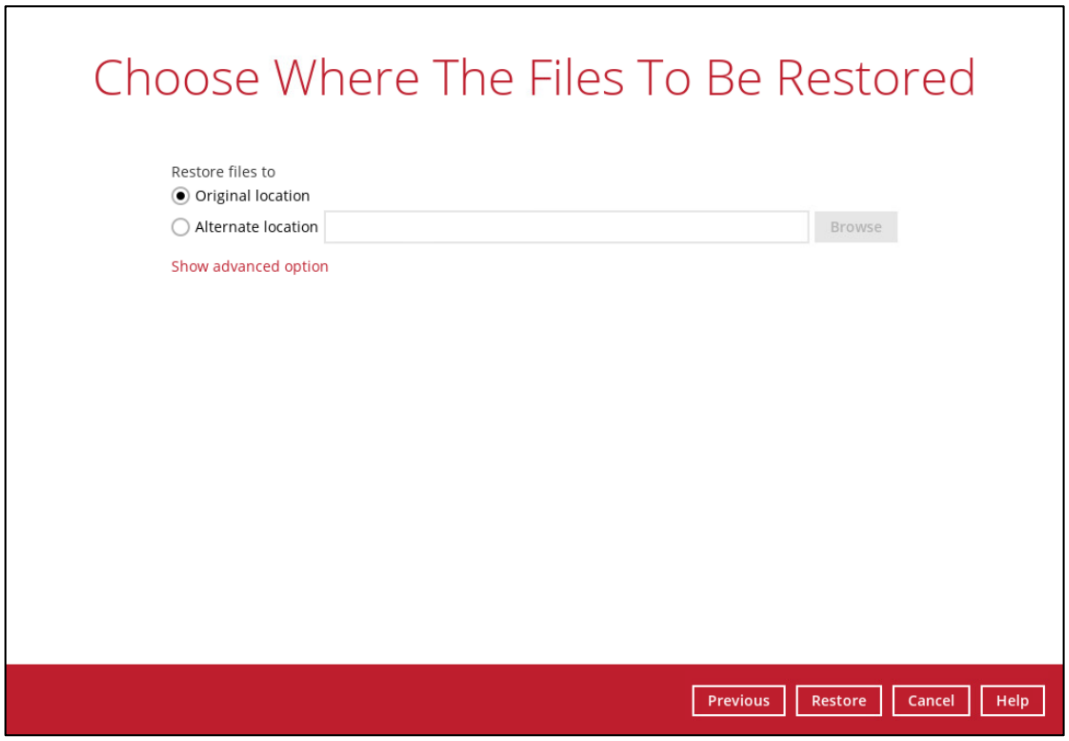


5. Click **Next** to proceed when you are done with the selections.

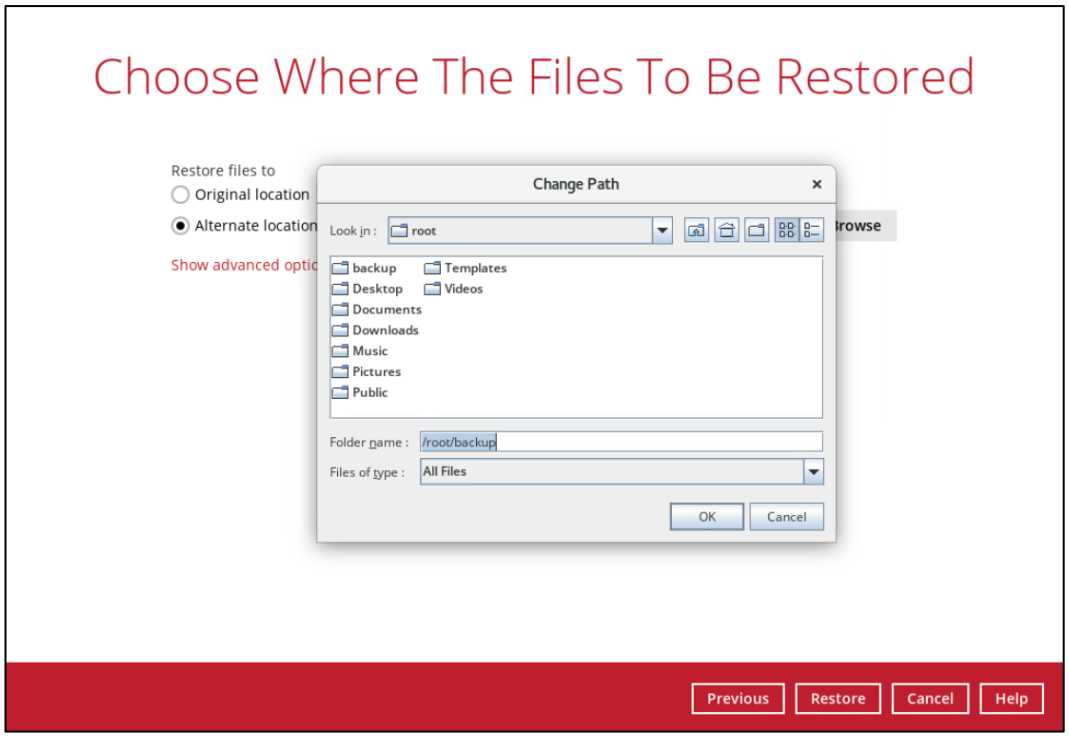
6. Select to restore the files to their **Original location**, or to an **Alternate location**. Then, click **Next** to proceed.

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

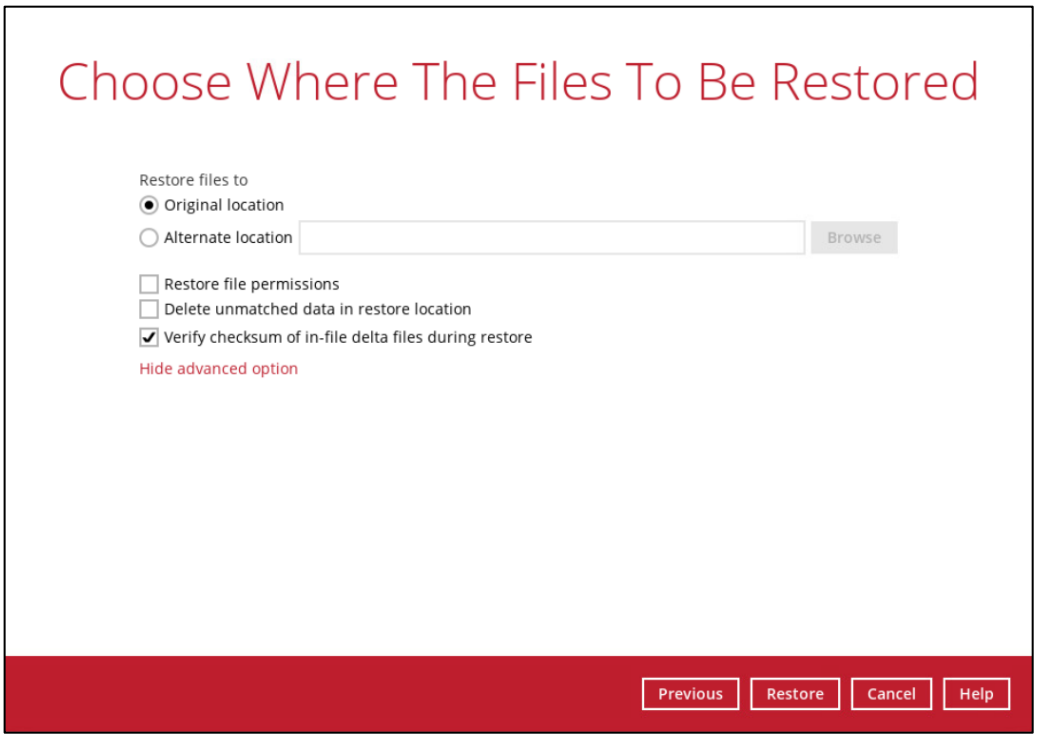
For example, if the backup source files are stored under **/root/Documents** folder, the data will be restored to **/root/Documents** as well on the computer running CloudBacko Pro.



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



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



- **Restore file permissions**

  Restore file permissions are disabled by default. When you perform a file restore on shared files or folders using a shared computer, it is recommended that you enable Restore file permissions by ticking the checkbox so that the files restored will not be fully accessible to everyone using the shared computer.

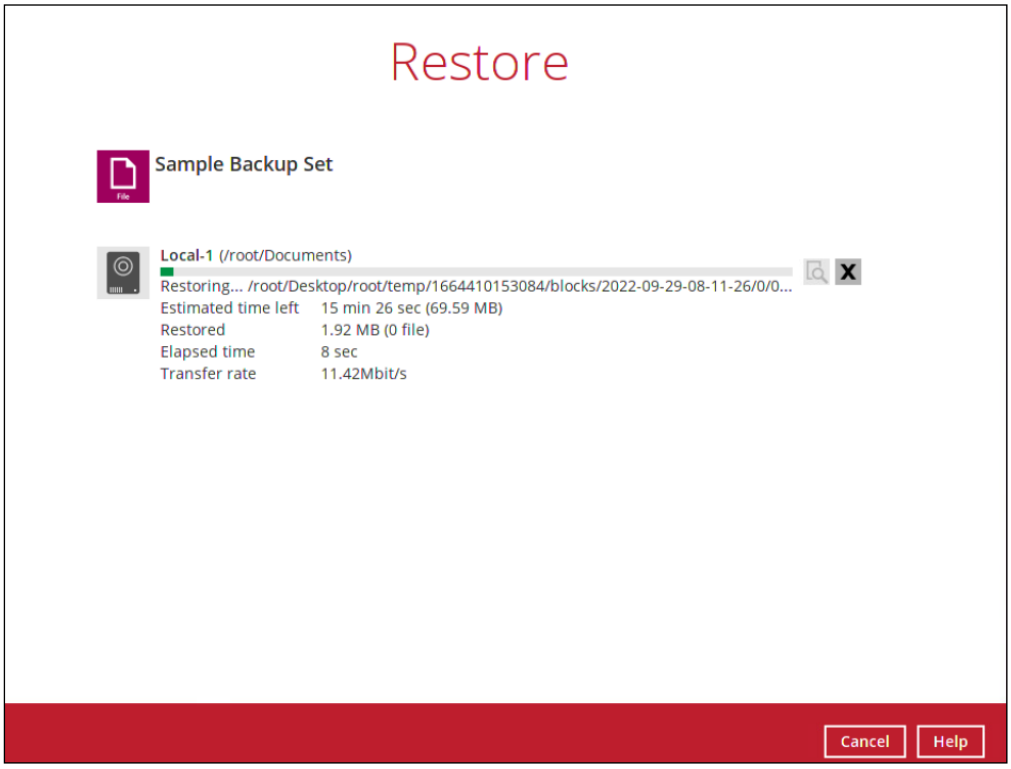
- **Delete unmatched data in restore location**

  The restore process will synchronize the selected restore source with the restore destination by removing unmatched data.

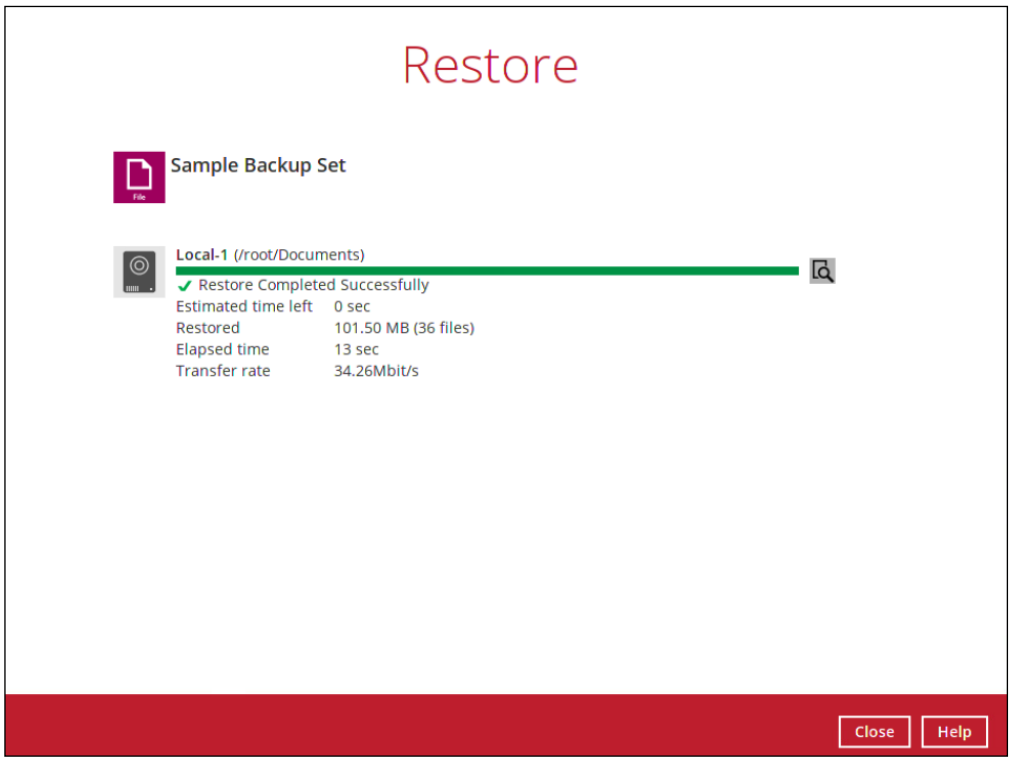
- **Verify checksum of in-file delta files during restore**

  Verify checksum of in-file delta files during restore is disabled by default. You can enable the feature by ticking the checkbox so that 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.

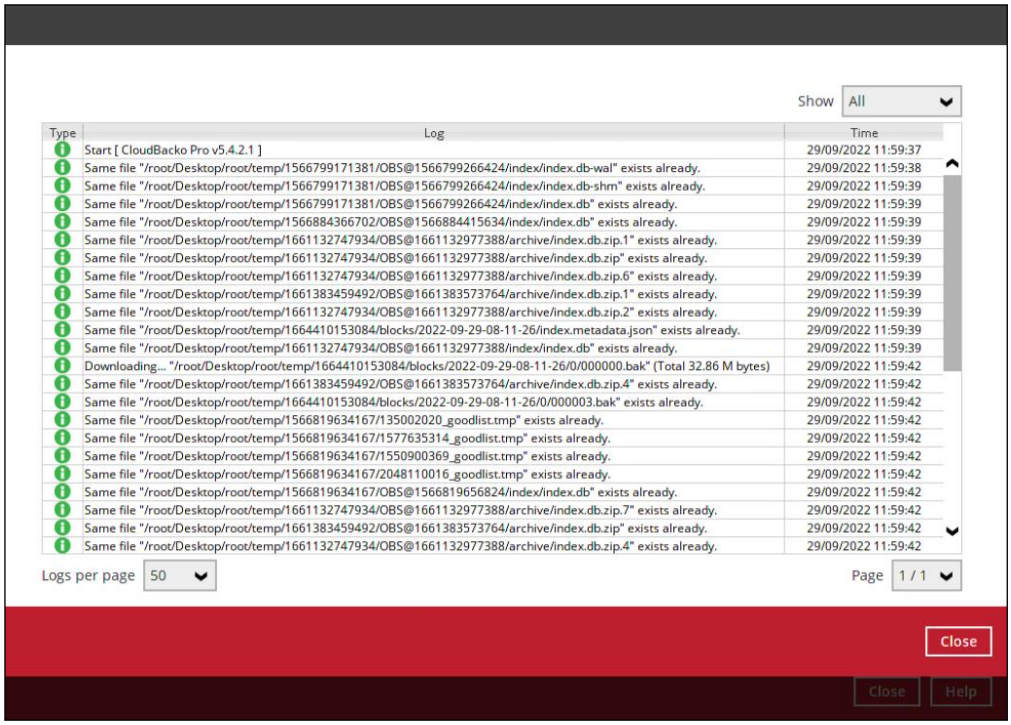
8. Click **Restore** to start the restore. The status will be shown.



9. When the restore is completed, the progress bar will be green in color and the message "Restore Completed Successfully" will appear.



10. You can click the **View** icon on the right-hand side to check the log. A window will pop up to show the log. Close the pop-up window when you finish reading it.



11. In the Restore window, click **Cancel** to close the Restore window.

12. To exit CloudBacko Pro, click the "**x**" on the top right corner. A message will appear to ask for your confirmation. Click **Yes** to close the application. If you wish to use CloudBacko Pro again, you will then have to launch it again.

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:

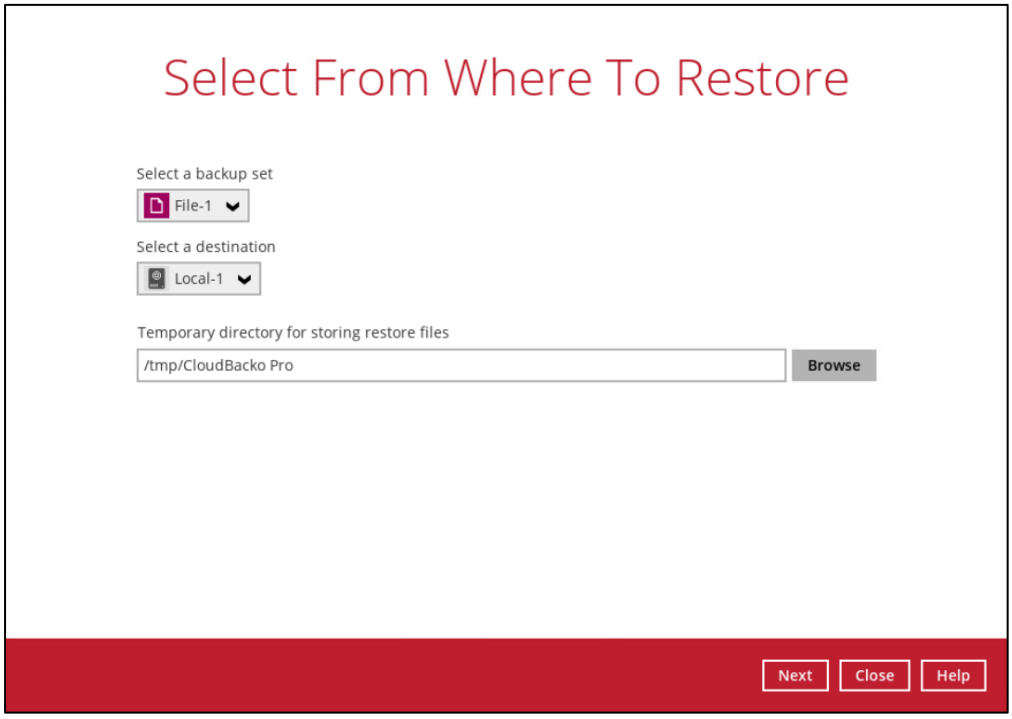
- **Contains**
  These are Directories, Files, and Folders with the name **containing** the specific letter or word.
- **Exact**
  These are Directories, Files, and Folders with the **exact** or **accurate** name.
- **Start With**
  These are Directories, Files, and Folders with the name **starting**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

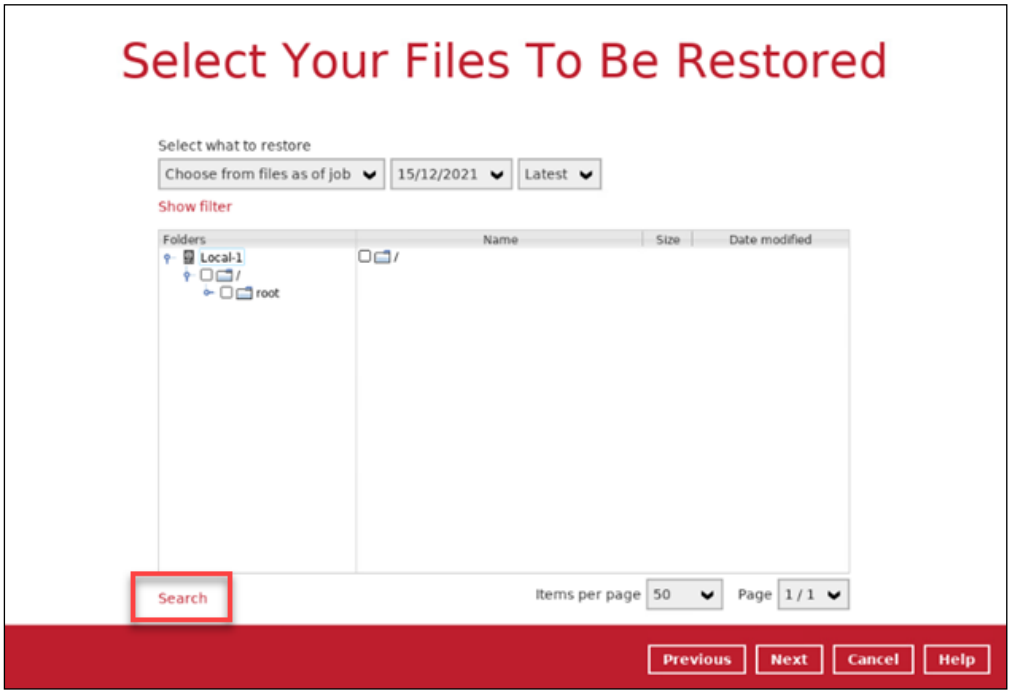
For more detailed examples using the restore filter on CloudBacko Pro, refer to Appendix F: Example Scenarios for Restore Filter.

1. Login to CloudBacko Pro application according to the instructions in Chapter 6 Start CloudBacko Pro.
2. Click the **Restore** icon on the main interface of CloudBacko Pro.
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.

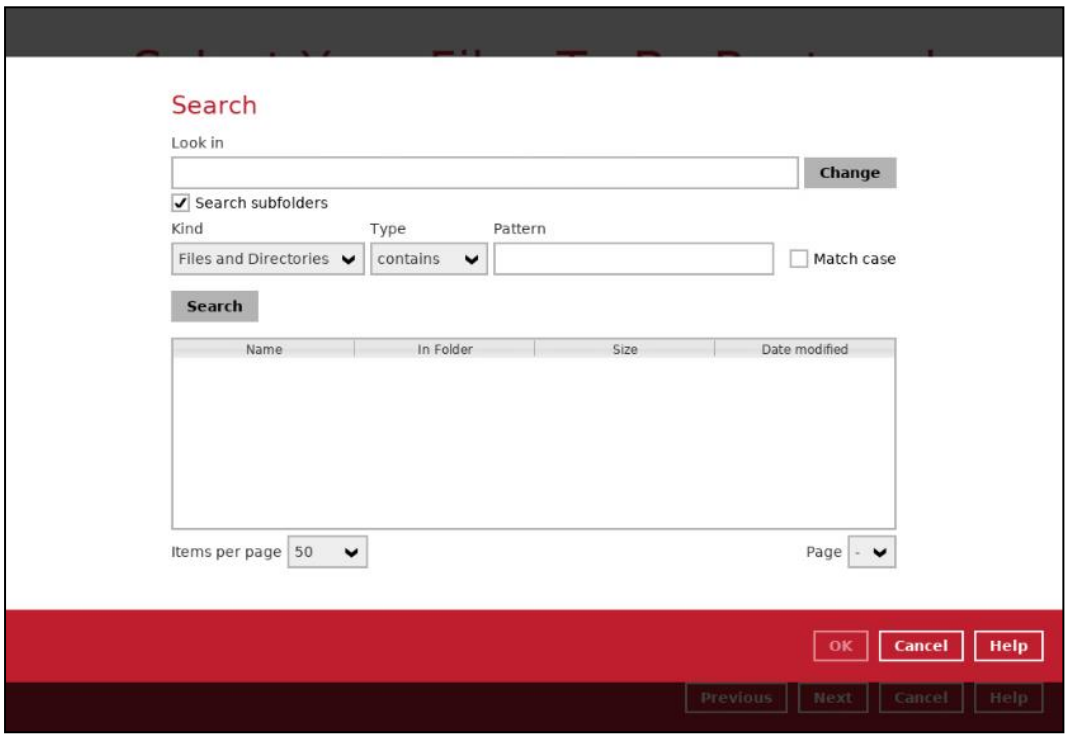
   You may also choose the temporary directory for restoring files by choosing a directory under **Temporary directory for storing restore files**.

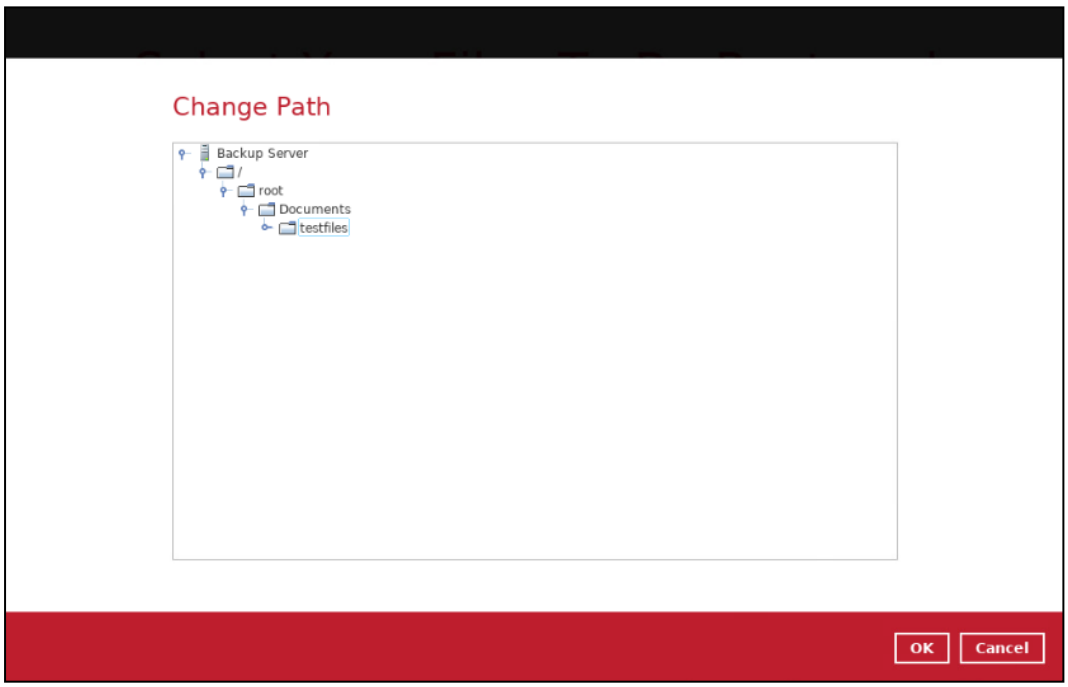


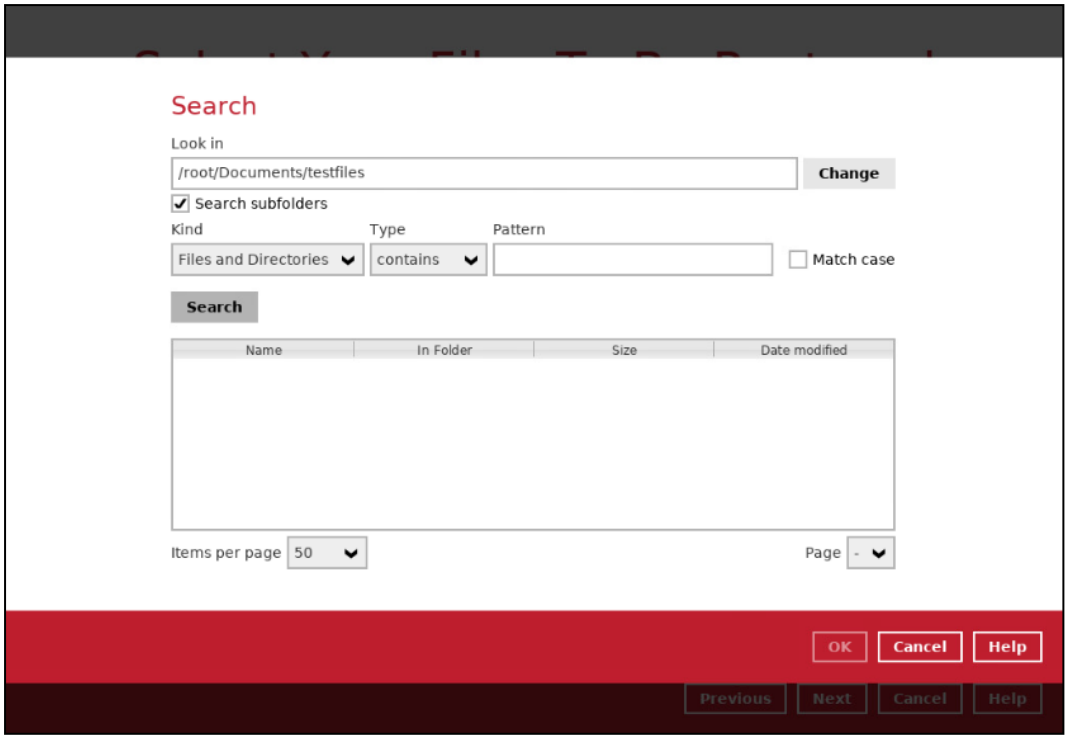
4. Click the **Search** located on the lower left side of the screen.



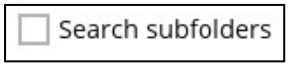
5. Click the **Change** button to change the path of the restore items from other location.

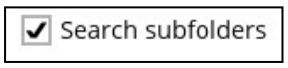






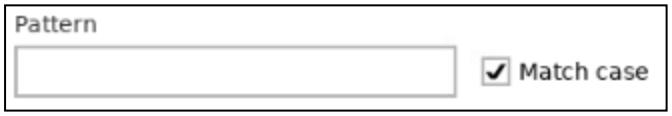
6. Tick the Search subfolders to include available subfolders upon searching.





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 box 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 you will return to the restore main screen.

12 Mobile Backup and Restore to Cloud

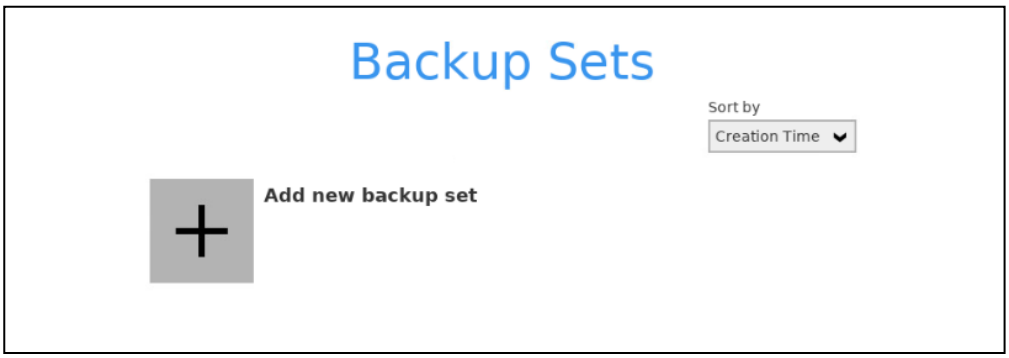
To do a mobile backup and restore to Cloud, follow these steps:

- Backup photos, videos, documents and 2FA accounts from CloudBacko app to CloudBacko Pro local destination. For more detailed information, check the CloudBacko app guide.
- Create a File Backup Set on CloudBacko Pro and follow these steps:
  - Backup source should be photos, videos, documents and 2FA accounts backed up in CloudBacko Pro local destination. Example: D:\Backup\Redmi.
  - Backup destination should be a Cloud destination. Examples: Google Drive, OneDrive, Wasabi, etc.
- Run a Backup Job on CloudBacko Pro.
- Restore Data on CloudBacko Pro. This can be from Original or Alternate location.

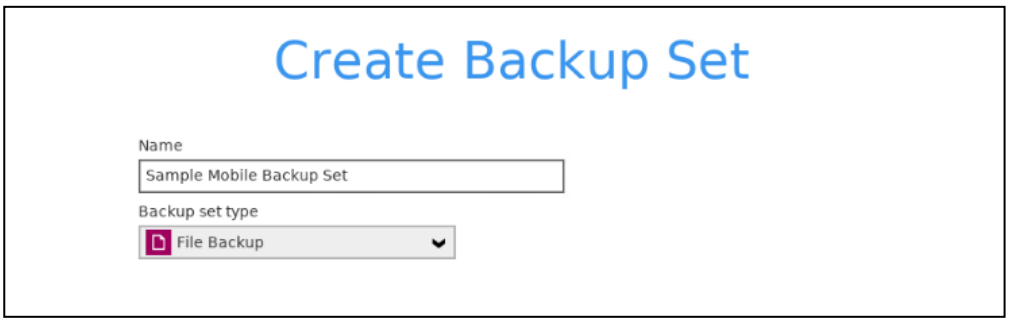
12.1 Create a File Backup Set

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

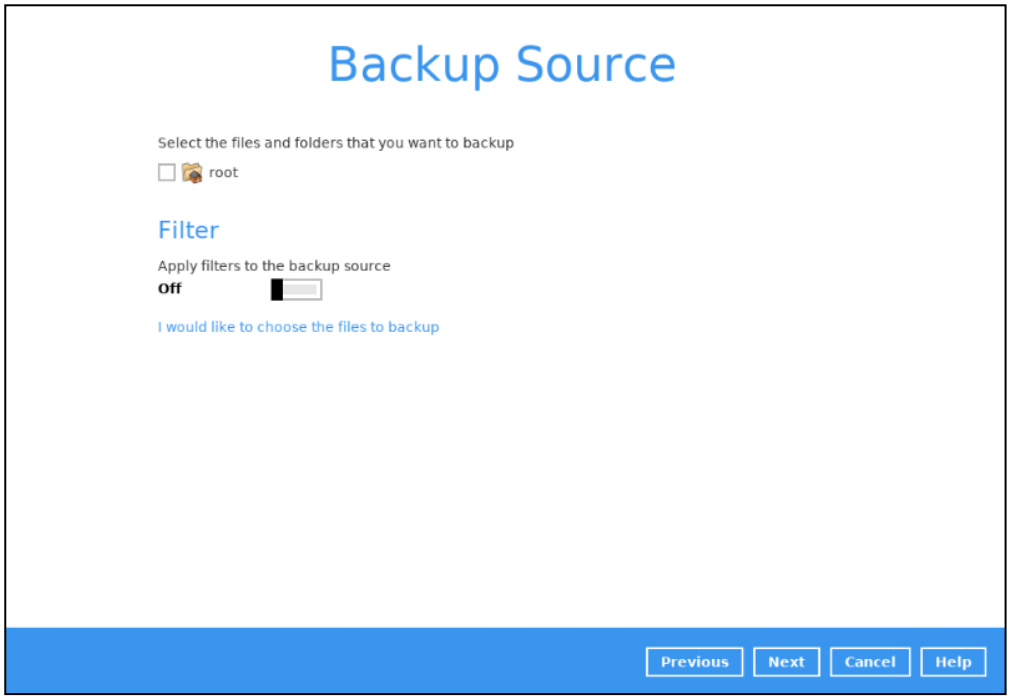
2. Create a new backup set by clicking + next to **Add new backup set**.



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

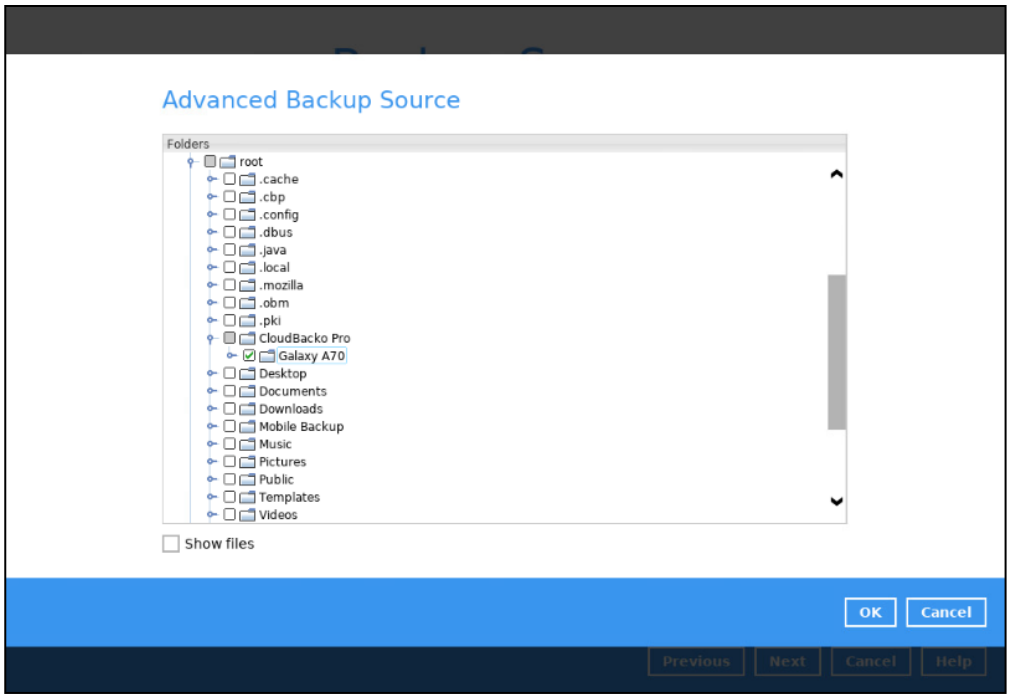


4. In the Backup Source window, select the mobile backup source for backup. Click **I would like to choose the files to backup**.

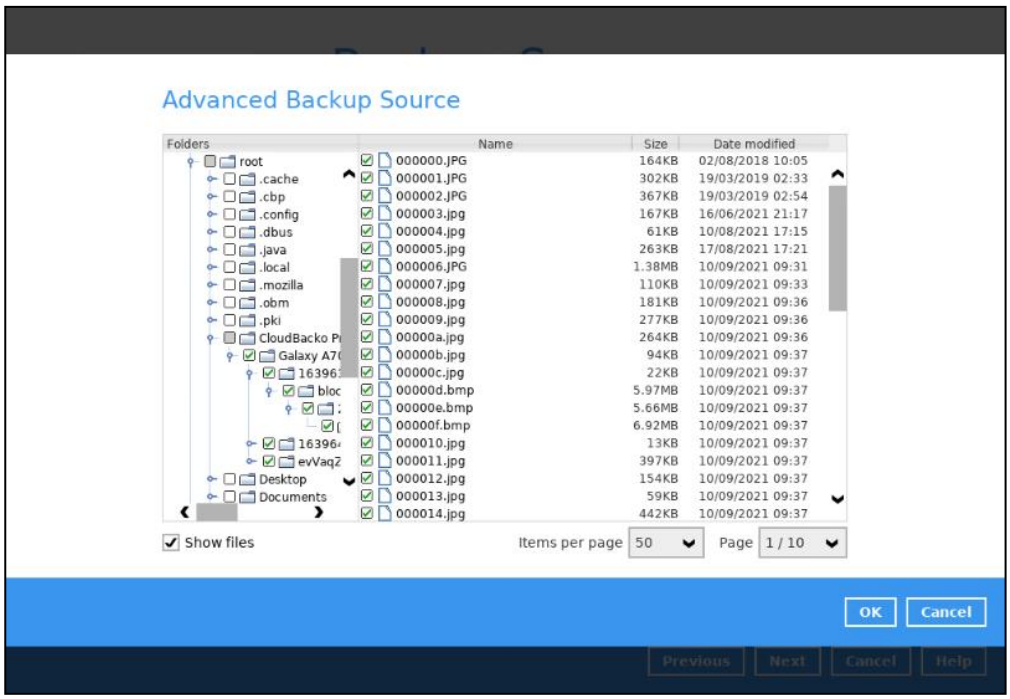


In the **Advanced Backup Source** window, select the mobile backup source.

In this example, Galaxy A70 folder is selected. The mobile backup source is in **/root/CloudBacko Pro**.



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.



In the Backup Source window, click **Next** to proceed.

5. Follow steps 8 – 17 discussed in Chapter 8 to finish creating the backup set.

12.2 Run a Backup Job

To backup your mobile data to the cloud please refer to the instructions in Chapter 10 and select the backup set that you created in Chapter 12.1.

12.3 Restore Data

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 restored on an alternate location which can be setup anywhere in the CloudBacko Pro 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:

  - 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.

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

Examples:

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

Restore to alternate location is not supported on another CloudBacko Pro 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 Pro 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 devices were not originally paired with the new installation or machine, the mobile devices will not be able to restore the photos, videos, documents and 2FA accounts from the CloudBacko Pro.

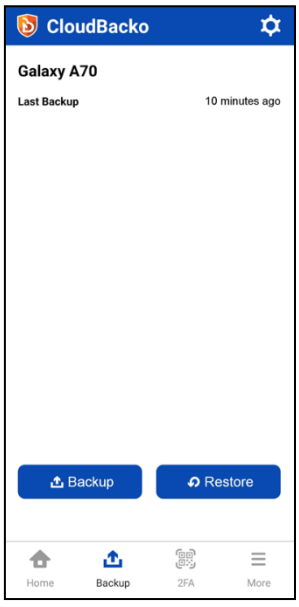
12.3.1 Original Location

To restore data from the Cloud storage to the mobile device using Original location, please refer to instructions in Chapter 11.1.

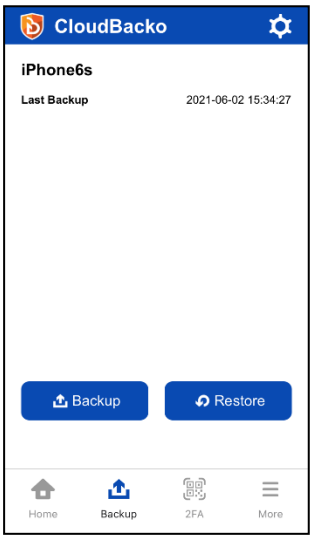
Then you can restore the restored data from the original location to your mobile device by using the CloudBacko app.

Example: Original location is in /root/CloudBacko Pro

Android device



iOS device



12.3.2 Alternate Location

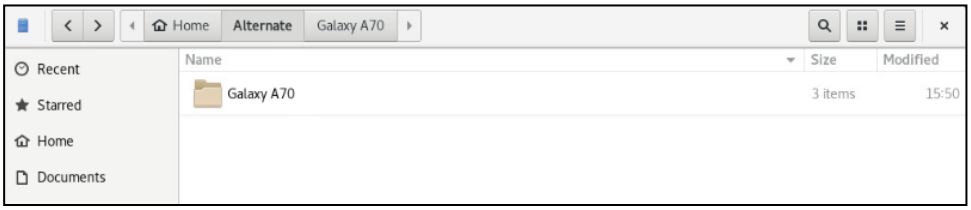
To restore data from the Cloud storage to the mobile device using Alternate location, please refer to instructions in Chapter 11.1.

Then follow these steps to restore the restored data from the alternate location to your mobile device. To do this there are two (2) options:

Option 1: Copy the restored data from alternate location to original location which is the **backup destination for your mobile device**.

Example:

Alternate location is in /root/Alternate



Original location is in /root/CloudBacko Pro

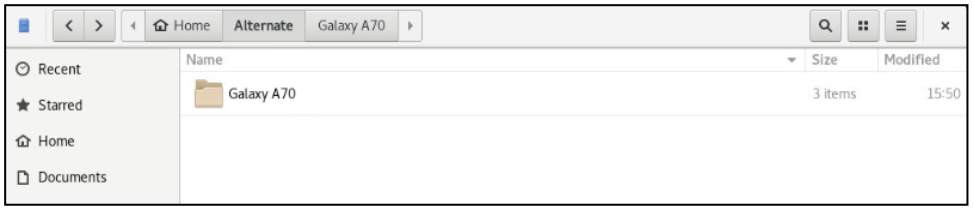
You can now use the CloudBacko app to restore the photos, videos, documents and 2FA accounts back to your mobile device.

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

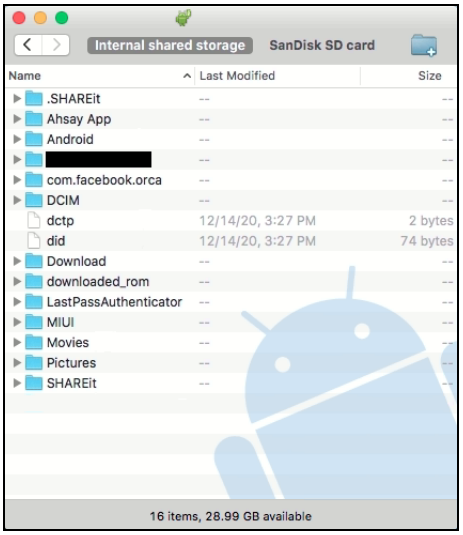
Examples:

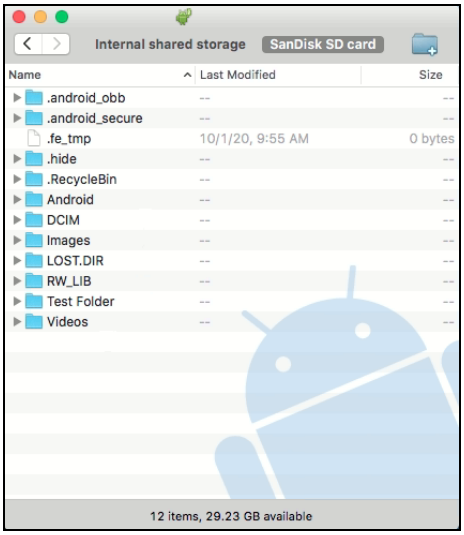
- For an Android device, you need to plug your cable and transfer the restored data from the alternate location to your mobile device storage.

  Alternate location is in /root/Alternate



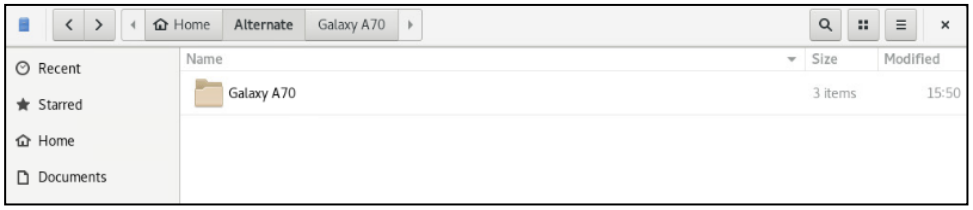
Mobile device storage: Internal shared storage and SD Card



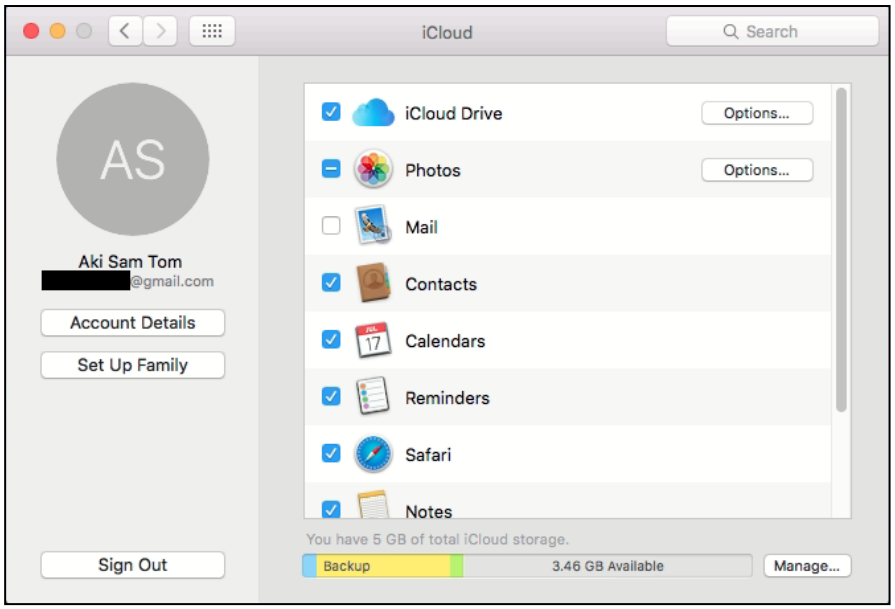


- For an iOS device, you need to transfer the restored data from the alternate location to iCloud.

  Alternate location is in /root/Alternate



  Upload to iCloud.



13 Contacting CloudBacko

Technical Assistance

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

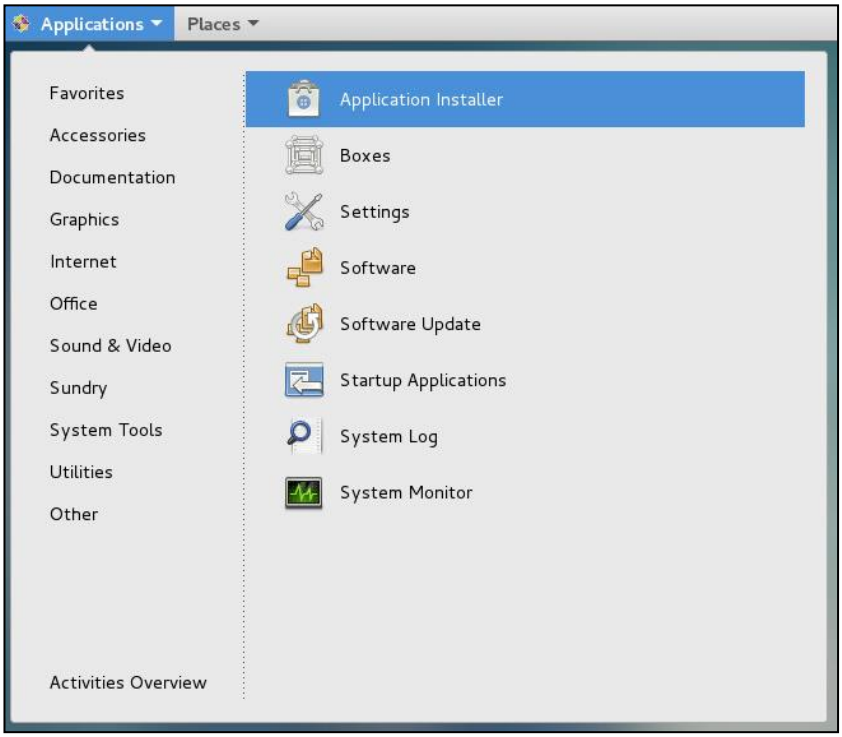
https://www.cloudbacko.com/support

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.

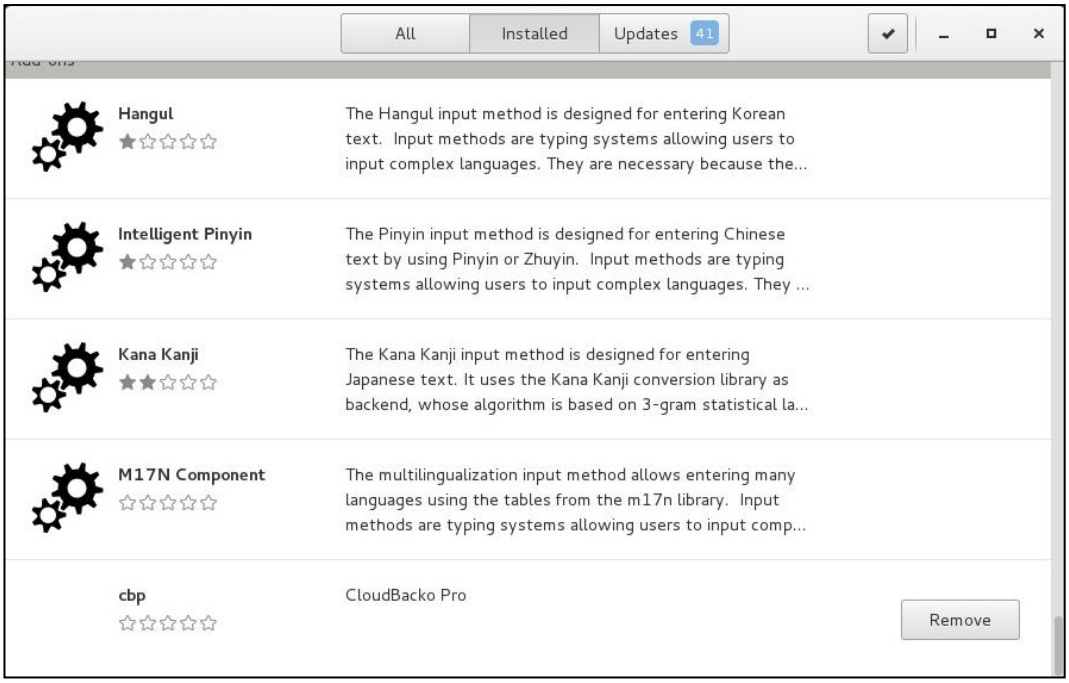
Appendix

Appendix A: Uninstall CloudBacko Pro (rpm)

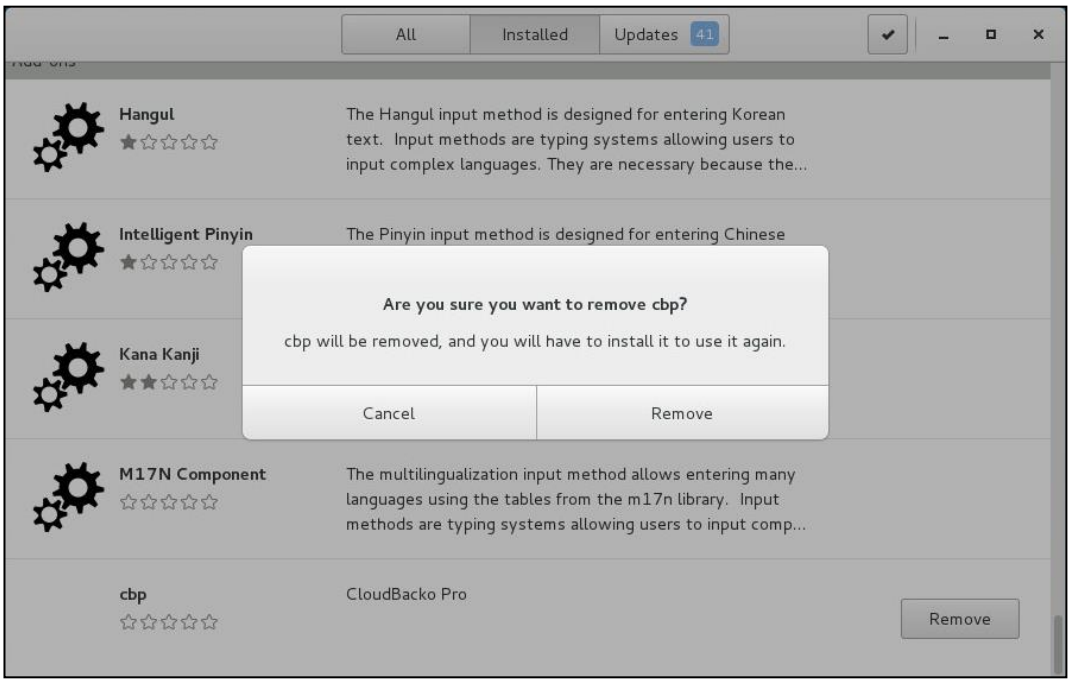
1. Under the **Applications** menu bar on the top of the screen, select **System Tools > Application Installer** option.



2. Go to the **Installed** tab and locate **cbp**, click the **Remove** button to proceed.



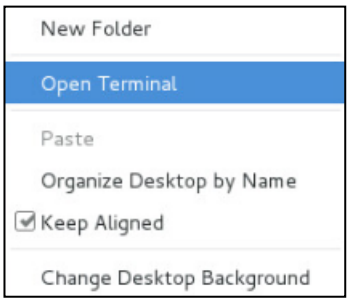
3. Click the **Remove** button to uninstall the cbp package.



4. Upon successful uninstallation, the CloudBacko Pro icon will disappear from the desktop.

Appendix B: Uninstall CloudBacko Pro (sh)

1. Right-click on the desktop and click **Open Terminal** to launch the application.



2. Go to the `# cd /usr/local/cbp/bin` directory.

```
# cd /usr/local/cbp/bin
```

3. Uninstall CloudBacko Pro with the `# sh uninstall.sh` command.

```
# sh uninstall.sh
```

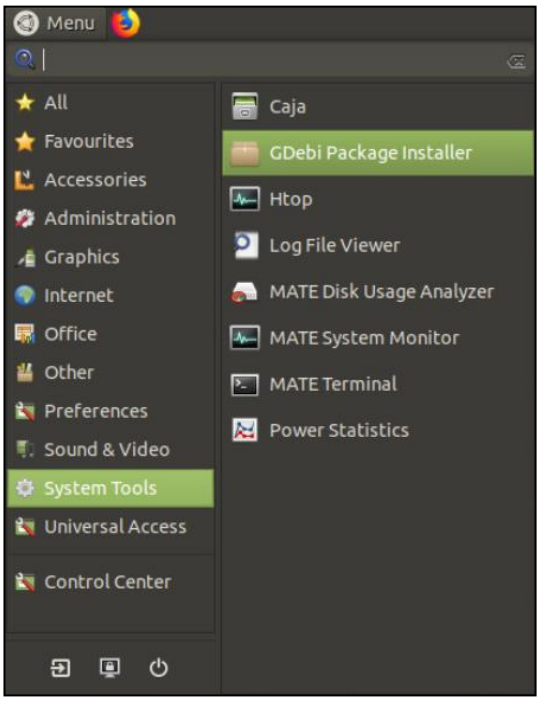
4. The uninstallation is completed when "**`CloudBacko Pro uninstall procedure is complete!`**" shows at the end of the script.

```
Log Time: Thu Dec 9 10:34:45 HKT 2021

Verifying current user privilege ...
Current user has enough privilege to "uninstall".

Uninstall CloudBacko Pro from /usr/local/cbp

Shutting down Scheduler
Wait 5 seconds before Scheduler exits
Kill running CloudBacko Pro
Kill Process by Image Name: /usr/local/cbp/jvm/bin/bJW
Ignore Process by Image Name:
Kill Process by Image Name: /usr/local/cbp/jvm/bin/bschJW
Ignore Process by Image Name:
Kill Process by Image Name: /usr/local/cbp/jvm/bin/java
Ignore Process by Image Name:
Removing Scheduler script cbpscheduler from service
Uninstall Service for NIX type OS
Using init script path /etc/init.d
Using run level script path /etc/rc.d
Removing symbolic link from run levels
Removing script file cbpscheduler from /etc/init.d
Remove shortcut /usr/share/applications/cbp.desktop
Remove shortcut /root/Desktop/cbp.desktop
CloudBacko Pro uninstall procedure is complete!
It is now safe to remove files from /usr/local/cbp
```

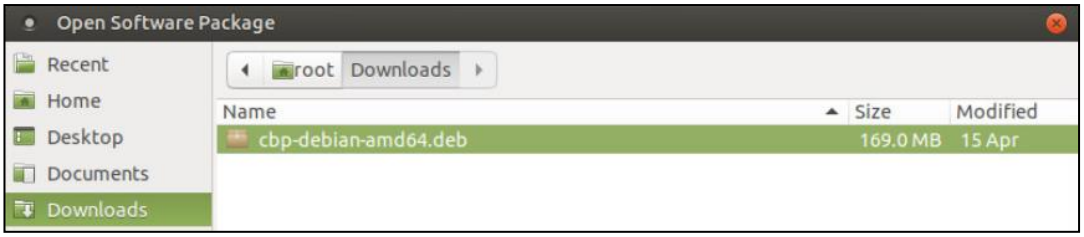
5. Upon successful uninstallation, the CloudBacko Pro icon will disappear from the desktop.

Appendix C: Uninstall CloudBacko Pro (deb)

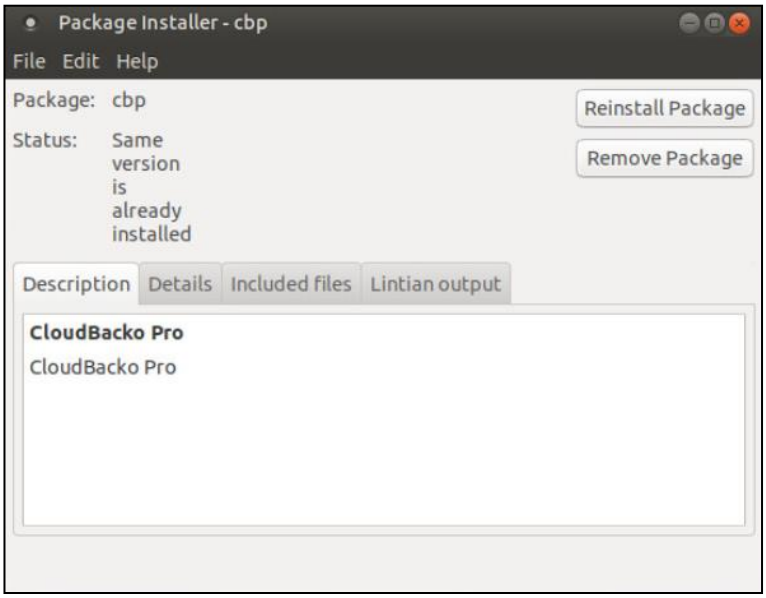
1. Go to your Package Installer.

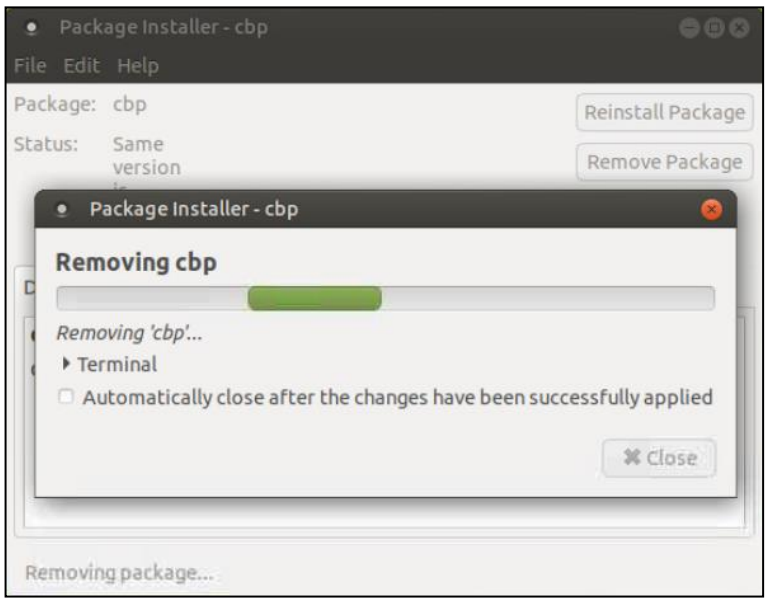


2. Click on **File** > **Open** > **Downloads** and select the CloudBacko Pro deb file you downloaded.

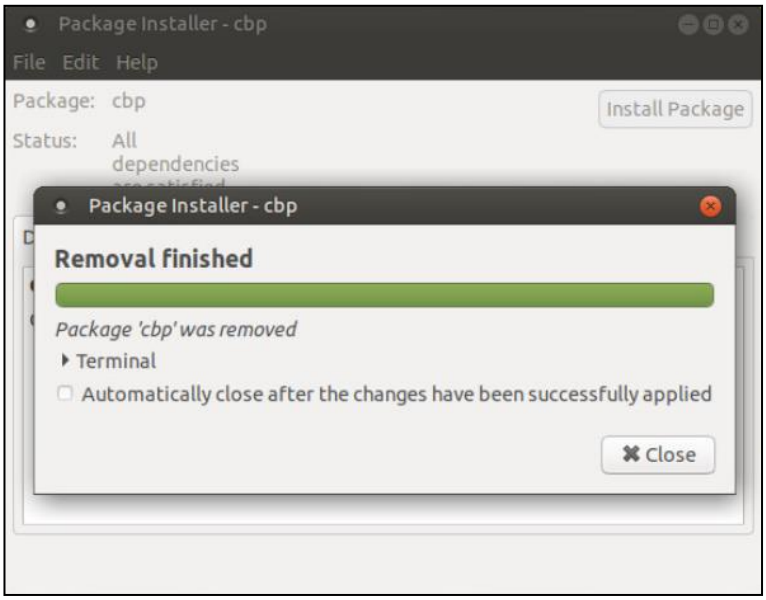


3. When the following message appears, click **Remove Package** to proceed.





4. Upon successful uninstallation, this will be the message and the CloudBacko icon will disappear from the menu.



Appendix D: Handling of Non-regular Files

The following non-regular files/folders such as device files, block files, virtual files systems, pseudo file systems etc will be automatically ignored if selected for backup. Backup log entries of these files/folders will not appear in the backup logs.

Example:
/proc
/dev
/sys
/run

For CloudBacko Pro installations on Linux GUI, these devices will not be shown on the backup source screen.

Appendix E: Script Files

These are the following script files for CloudBacko Pro:

- RunCB.sh
- ListBackupSet.sh
- ListBackupJob.sh
- RunBackupSet.sh
- Restore.sh
- Decrypt.sh
- RunDataIntegrityCheck.sh

RunCB.sh

This script file is used to run CloudBacko Pro. To configure the parameters, open the script file in a text editor like vi.

```
# cd /usr/local/cbp/bin
# vi RunCB.sh
```

Configure the following parameters:

- **SETTING_HOME** – this is the directory to your setting home. If not set, the default directory is "${HOME}/.cbp".

  e.g. SETTING_HOME="/root/.cbp"

- **DEBUG_MODE** – this parameter is used to enable or disable the debug mode when opening CloudBacko Pro.

  e.g. DEBUG_MODE="- -debug" or DEBUG_MODE=""

```
# cd /usr/local/cbp/bin
# vi RunCB.sh

#!/bin/sh

################################## RunCB.sh
###################################
# You can use this shell to run the application
#
#########################################################################
##########

########################## START: User Defined Section
#########################

# ------------------------------ SETTING_HOME -----------------------
----------
# | Directory to your setting home.
|
# | Default to ${HOME}/.cbp when not set.
|
# | e.g. SETTING_HOME="${HOME}/.cbp"
|
```

```
# ------------------------------------------------------------------
----------
SETTING_HOME=""

# ------------------------------- DEBUG_MODE -----------------------
----------
# | Enable/Disable debug mode
|
# | e.g. DEBUG_MODE="--debug"
|
# |  or  DEBUG_MODE=""
|
# ------------------------------------------------------------------
----------
DEBUG_MODE=""

########################## END: User Defined Section
############################


#########################################################################
##########
#          R E T R I E V E     A P _ H O M E     P A T H
#
#########################################################################
##########

EXE_DIR=`pwd`
SCRIPT_HOME=`dirname "$0"`
cd "$SCRIPT_HOME"
APP_BIN=`pwd`
APP_HOME=`dirname "$APP_BIN"`
xhost +SI:localuser:root
#########################################################################
##########
#          R E T R I E V E     J A V A _ H O M E     P A T H
#
#########################################################################
##########

if [ "Darwin" = `uname` ]; then
    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "'$APP_HOME/jvm' does not exist!"
    if [ ! -n "$JAVA_HOME" ]; then
        echo "Please set JAVA_HOME!"
        exit 0
    else
        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"
        echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"
    fi
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"
    exit 0
fi
```

```
JAVA_HOME="$APP_HOME/jvm"

# Use alternative executable name to define the GUI execution
if [ "Darwin" = `uname` ]; then
    JAVA_EXE="$JAVA_HOME/bin/java"
else
    JAVA_EXE="$JAVA_HOME/bin/bJW"
fi

# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.
STRING_JAVA_VERSION="java version,openjdk version"
OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`
OUTPUT_JVM_SUPPORT=0
BACKUP_IFS=$IFS
IFS=","
for word in $STRING_JAVA_VERSION; do
    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]
    then
      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
      continue;
    else
      OUTPUT_JVM_SUPPORT=1
      break;
    fi
done
IFS=$BACKUP_IFS
if [ $OUTPUT_JVM_SUPPORT -eq 0 ]
then
    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
    exit 1
fi

###########################################################################
##########
#                                 S T A R T - U P
#
###########################################################################
##########


# Set LD_LIBRARY_PATH for Lotus Notes on Linux
if [ "Linux" = `uname` ]; then
    NOTES_PROGRAM=`cat "$APP_HOME/bin/notesenv"`
    LD_LIBRARY_PATH="$APP_HOME/bin:$NOTES_PROGRAM:$LD_LIBRARY_PATH"
    export NOTES_PROGRAM
else
    LD_LIBRARY_PATH="$APP_HOME/bin:$LD_LIBRARY_PATH"
fi

DEP_LIB_PATH="X64"
case "`uname -m`" in
    i[3-6]86)
        DEP_LIB_PATH="X86"
    ;;
esac
LD_LIBRARY_PATH="${APP_BIN}/${DEP_LIB_PATH}":".":"${LD_LIBRARY_PATH}"

SHLIB_PATH="$LD_LIBRARY_PATH"
```

```
export LD_LIBRARY_PATH SHLIB_PATH

# Change to APP_BIN for JAVA execution
cd "${APP_BIN}"

# Reference path will be used to avoid empty space in the parent
directory
LIB_HOME=.
JAVA_OPTS="-Xrs -Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -client
-Dsun.nio.PageAlignDirectMemory=true"
JNI_PATH="-Djava.library.path=$LIB_HOME"
CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"
MAIN_CLASS=Gui

# Execute Java VM Runtime for BackupManager
echo "Startup CloudBacko Pro ... "
"${JAVA_EXE}" $JAVA_OPTS $JNI_PATH -cp $CLASSPATH $MAIN_CLASS
"${DEBUG_MODE}" "${APP_HOME}" "${SETTING_HOME}"

##########################################################################
##########
#                   R E S E T          A N D          E X I T
#
##########################################################################
##########

cd "${EXE_DIR}"
exit 0
```

ListBackupSet.sh

This script file is used to display the list of backup set under your backup account. To configure the parameters, open the script file in a text editor like vi.

```
# cd /usr/local/cbp/bin
# vi ListBackupSet.sh
```

Configure the following parameters:

- **SETTING_HOME** – this is the directory to your setting home. If not set, the default directory is "${HOME}/.cbp".

  e.g. SETTING_HOME="/root/.cbp"

```
# cd /usr/local/cbp/bin
# vi ListBackupSet.sh

#!/bin/sh

##############################  ListBackupSet.sh
##############################
# You can use this shell script to list all backup sets available
under        #
# your backup account.
#
#########################################################################
##########

########################  Start: User Defined Section
#########################

# ----------------------------  SETTING_HOME  ----------------------
----------
# | Directory to your setting home.
|
# | Default to ${HOME}/.cbp when not set.
|
# | e.g. SETTING_HOME="${HOME}/.cbp"
|
# -------------------------------------------------------------------
----------
SETTING_HOME=""

#########################  END: User Defined Section
#########################

#########################################################################
##########
#          R E T R I E V E     A P P _ H O M E     P A T H
#
#########################################################################
##########

EXE_DIR=`pwd`
SCRIPT_HOME=`dirname "$0"`
cd "$SCRIPT_HOME"
APP_BIN=`pwd`
APP_HOME=`dirname "$APP_BIN"`

#########################################################################
##########
```

```
#          R E T R I E V E     J A V A _ H O M E     P A T H
#
#########################################################################
##########

if [ "Darwin" = `uname` ]; then
    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "'$APP_HOME/jvm' does not exist!"
    if [ ! -n "$JAVA_HOME" ]; then
        echo "Please set JAVA_HOME!"
        exit 0
    else
        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"
        echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"
    fi
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"
    exit 0
fi

JAVA_HOME="$APP_HOME/jvm"
JAVA_EXE="$JAVA_HOME/bin/java"

# Verify the JAVA_EXE whether it can be executed or not.
if [ ! -x "${JAVA_EXE}" ]
then
    echo "The Java Executable file \"${JAVA_EXE}\" cannot be executed.
Exit \""`basename "$0"`"\" now."
    exit 1
fi

# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.
STRING_JAVA_VERSION="java version,openjdk version"
OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`
OUTPUT_JVM_SUPPORT=0
BACKUP_IFS=$IFS
IFS=","
for word in $STRING_JAVA_VERSION; do
    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]
    then
      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
      continue;
    else
      OUTPUT_JVM_SUPPORT=1
      break;
    fi
done
IFS=$BACKUP_IFS
if [ $OUTPUT_JVM_SUPPORT -eq 0 ]
then
    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
```

```
    exit 1
fi

###################################################################
##########
#                         J A V A     E X E C U T I O N
#
###################################################################
##########

# Change to APP_BIN for JAVA execution
cd "${APP_BIN}"

# Reference path will be used to avoid empty space in the parent
directory
LIB_HOME=.
JAVA_OPTS="-Xrs -Xms128m -Xmx768m -client -
Dsun.nio.PageAlignDirectMemory=true"
JNI_PATH="-Djava.library.path=$LIB_HOME"
CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"
MAIN_CLASS=ListBackupSet

echo "Using APP_HOME     : ${APP_HOME}"
echo "Using SETTING_HOME : ${SETTING_HOME}"

# API Arguments: ListBackupSet [APP_HOME] [SETTING_HOME]

# Do not include double-quote for java options, jni path, classpath
and main class
# Only apply double-quote for path to java executable and execution
arguments
"${JAVA_EXE}" $JAVA_OPTS $JNI_PATH -cp $CLASSPATH $MAIN_CLASS
"${APP_HOME}" "${SETTING_HOME}"

###################################################################
##########
#                   R E S E T          A N D          E X I T
#
###################################################################
##########

cd "${EXE_DIR}"
exit 0
```

ListBackupJob.sh

This script file is used to display the list of backup jobs under a specific backup set. To configure the parameters, open the script file in a text editor like vi.

```
# cd /usr/local/cbp/bin
# vi ListBackupJob.sh
```

Configure the following parameters:

- **SETTING_HOME** – this is the directory to your setting home. If not set, the default directory is "${HOME}/.cbp".

  e.g. SETTING_HOME="/root/.cbp"

- **BACKUP_SET** – this is the name of the backup set which contains the backup job that you want to list. There are two (2) ways to specify the backup set; by using the *backup set name* or by *backup set ID*. If the backup set name is not in English, use the backup set ID. You can leave this blank if you only have one (1) backup set.

  e.g. BACKUP_SET="1119083740107" or BACKUP_SET="FileBackupSet-1"

- **BACKUP_DEST** – this is the name of the destination of the backup set. There are two (2) ways to specify the destination; by using the *destination name* or *destination ID*. If the destination name is not in English, use the DestinationID. You can leave this blank if you only have one (1) backup destination.

  e.g. BACKUP_DEST="1119083740107" or BACKUP_DEST="Destination-1"

```
# cd /usr/local/cbp/bin
# vi ListBackupJob.sh

#!/bin/sh

##############################  ListBackupJob.sh
##############################
# You can use this shell script to list all backup job which ran under
#
# this backup set.
#
#########################################################################
##########

########################  Start: User Defined Section
########################

# ------------------------------  SETTING_HOME  ----------------------
----------
# | Directory to your setting home.
|
# | Default to ${HOME}/.cbp when not set.
|
# | e.g. SETTING_HOME="${HOME}/.cbp"
|
# -------------------------------------------------------------------
----------
SETTING_HOME=""

# ------------------------------  BACKUP_SET  ----------------------
----------
# | The name or ID of the backup set that you want to run
|
```

```
# | If backup set name is not in English, please use BackupSetID
|
# | e.g. BACKUP_SET="1119083740107"
|
# | or  BACKUP_SET="FileBackupSet-1"
|
# |
|
# | You can leave this parameter blank if you have only 1 backup set.
|
# -------------------------------------------------------------------
----------
BACKUP_SET=""

# ------------------------------  BACKUP_DEST  ----------------------
----------
# | The name or ID of the destination that you want to run
|
# | If destination name is not in English, please use DestinationID
|
# | e.g. BACKUP_DEST="1119083740107"
|
# | or  BACKUP_DEST="Destination-1"
|
# |
|
# | You can leave this parameter blank if you have only 1 destination.
|
# -------------------------------------------------------------------
----------
BACKUP_DEST=""

##########################  END: User Defined Section
##########################

#########################################################################
##########
#                S C R I P T                          U S A G E
#
#########################################################################
##########

# Input Arguments will overwrite the above settings
# defined in 'User Defined Section'.
if [ $# -ge 1 ]; then


    if [ -n "$1" ]; then
        BACKUP_SET="$1"
    fi

    if [ -n "$2" ]; then
        BACKUP_DEST="$2"
    fi

fi

#########################################################################
##########
#         R E T R I E V E          A P P _ H O M E          P A T H
#
```

```
##############################################################################
##########

EXE_DIR=`pwd`
SCRIPT_HOME=`dirname "$0"`
cd "$SCRIPT_HOME"
APP_BIN=`pwd`
APP_HOME=`dirname "$APP_BIN"`

##############################################################################
##########
#         R E T R I E V E           J A V A _ H O M E           P A T
H         #
##############################################################################
##########

if [ "Darwin" = `uname` ]; then
    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "'$APP_HOME/jvm' does not exist!"
    if [ ! -n "$JAVA_HOME" ]; then
        echo "Please set JAVA_HOME!"
        exit 0
    else
        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"
        echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"
    fi
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"
    exit 0
fi

JAVA_HOME="$APP_HOME/jvm"
JAVA_EXE="$JAVA_HOME/bin/java"

# Verify the JAVA_EXE whether it can be executed or not.
if [ ! -x "${JAVA_EXE}" ]
then
    echo "The Java Executable file \"${JAVA_EXE}\" cannot be executed.
Exit \""`basename "$0"`"\" now."
    exit 1
fi

# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.
STRING_JAVA_VERSION="java version,openjdk version"
OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`
OUTPUT_JVM_SUPPORT=0
BACKUP_IFS=$IFS
IFS=","
for word in $STRING_JAVA_VERSION; do
    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]
    then
      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
```

```
      continue;
    else
      OUTPUT_JVM_SUPPORT=1
      break;
    fi
done
IFS=$BACKUP_IFS
if [ $OUTPUT_JVM_SUPPORT -eq 0 ]
then
    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
    exit 1
fi

###########################################################################
##########
#                  J A V A                  E X E C U T I O N
#
###########################################################################
##########

# Change to APP_BIN for JAVA execution
cd "${APP_BIN}"

# Reference path will be used to avoid empty space in the parent
directory
LIB_HOME=.
JAVA_OPTS="-Xrs -Xms128m -Xmx768m -client -
Dsun.nio.PageAlignDirectMemory=true"
JNI_PATH="-Djava.library.path=$LIB_HOME"
CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"
MAIN_CLASS=ListBackupJob

echo "Using APP_HOME     : ${APP_HOME}"
echo "Using SETTING_HOME : ${SETTING_HOME}"
echo "Using BACKUP_SET   : ${BACKUP_SET}"

# API Arguments: ListBackupJob [APP_HOME] [BACKUP_SET] [BACKUP_DEST]
[SETTING_HOME]

# Do not include double-quote for java options, jni path, classpath
and
# main class.
# Only apply double-quote for path to java executable and execution
arguments
"${JAVA_EXE}" $JAVA_OPTS $JNI_PATH -cp $CLASSPATH $MAIN_CLASS "--app-
home=${APP_HOME}" "--backup-set=${BACKUP_SET}" "--backup-
dest=${BACKUP_DEST}" "--setting-home=${SETTING_HOME}"

###########################################################################
##########
#                   R E S E T          A N D          E X I T
#
###########################################################################
##########

cd "${EXE_DIR}"
exit 0
```

RunBackupSet.sh

This script file is used to manually run a backup. To configure the parameters, open the script file in a text editor like vi.

```
# cd /usr/local/cbp/bin
# vi RunBackupSet.sh
```

Configure the following parameters:

- **BACKUP_SET** – this is the name of the backup set which you want to backup. There are two (2) ways to specify the backup set; by using the *backup set name* or by *backup set ID*. If the backup set name is not in English, use the backup set ID. You can leave this blank if you only have one (1) backup set.

  e.g. BACKUP_SET="1119083740107" or BACKUP_SET="FileBackupSet-1"

- **BACKUP_DESTS** – this is the name of the destination where you want your backup to be stored. There are two (2) ways to specify the destination; by using the *destination name* or *destination ID*. If the destination name is not in English, use the DestinationID. You can leave this blank if you only have one (1) backup destination.

  e.g. BACKUP_DESTS="1119083740107" or BACKUP_DEST="Destination-1"

- **BACKUP_TYPE** – this is the backup set type. You do not need to change this if you are backing up a file backup set. There are four (4) options available for this: *FILE*, *DATABASE*, *DIFFERENTIAL* and *LOG*.

  e.g. BACKUP_TYPE="FILE" for file backup

  BACKUP_TYPE="DATABASE" for full database backup

  BACKUP_TYPE="DIFFERENTIAL" for differential database backup

  BACKUP_TYPE="LOG" for log database backup

- **SETTING_HOME** – this is the directory to your setting home. If not set, the default directory is "${HOME}/.cbp".

  e.g. SETTING_HOME="/root/.cbp"

- **DELTA_MODE** – this is the In-File Delta setting. There are three (3) options available for this: *Incremental*, *Differential* and *Full*.

  e.g. DELTA_MODE="I" for Incremental In-file delta backup

  DELTA_MODE="D" for Differential In-file delta backup

  DELTA_MODE="F" for full file backup

  DELTA_MODE="" for using backup set in-file delta setting

- **CLEANUP_MODE** – this is used to remove obsolete files from your backup destination after a backup has been run. There are two (2) options available for this: *ENABLE-CLEANUP* and *DISABLE-CLEANUP*.

  e.g. CLEANUP_MODE="ENABLE-CLEANUP" or CLEANUP_MODE="DISABLE-CLEANUP"

- **DEBUG_MODE** – this is used to enable or disable debug for a backup job. There are two (2) options available for this: *ENABLE-DEBUG* and *DISABLE-DEBUG*.

  e.g. DEBUG_MODE="ENABLE-DEBUG" or DEBUG_MODE="DISABLE-DEBUG"

```
# cd /usr/local/cbp/bin
# vi RunBackupSet.sh

#!/bin/sh

##############################  RunBackupSet.sh
################################
# You can use this shell script to run any of your backup sets from
the        #
# command line. Just customize the "User Defined Section" below with
your      #
# values for your backup action.
#
#########################################################################
##########

######################### START: User Defined Section
############################

# --------------------------------- BACKUP_SET ----------------------
----------
# | The name or ID of the backup set that you want to run
|
# | If backup set name is not in English, please use ID instead.
|
# | e.g. BACKUP_SET="1119083740107"
|
# |  or  BACKUP_SET="FileBackupSet-1"
|
# |
|
# | You can leave this parameter blank if you have only 1 backup set.
|
# -------------------------------------------------------------------
----------
BACKUP_SET=""

# --------------------------------- BACKUP_DESTS ----------------------
----------
# | The list of name or ID of the backup destinations that you want to
run.    |
# | If backup destination name is not in English, please use ID
instead.       |
# | e.g. BACKUP_DESTS="1740107119083"
|
# |  or  BACKUP_DESTS="Destination-1,Destination-2"
|
# |  or  BACKUP_DESTS="ALL"
|
# |
|
# | You can specify multiple destinations in comma-separated format,
|
# | or use "ALL" to run backup for all destinations.
|
# -------------------------------------------------------------------
----------
BACKUP_DESTS="ALL"

# --------------------------------- BACKUP_TYPE ----------------------
----------
```

```
# | Set backup type. You don't need to change this if you are backing
up a     |
# | file backup set.
|
# | Options available: FILE/DATABASE/DIFFERENTIAL/LOG
|
# | e.g. BACKUP_TYPE="FILE"          for file backup
|
# |  or  BACKUP_TYPE="DATABASE"      for Full database backup
|
# |  or  BACKUP_TYPE="DIFFERENTIAL"  for Differential database backup
|
# |  or  BACKUP_TYPE="LOG"           for Log database backup
|
# ------------------------------------------------------------------
----------
BACKUP_TYPE="FILE"

# ------------------------------- SETTING_HOME ----------------------
----------
# | Directory to your setting home.
|
# | Default to ${HOME}/.cbp when not set.
|
# | e.g. SETTING_HOME="${HOME}/.cbp"
|
# ------------------------------------------------------------------
----------
SETTING_HOME=""

# -------------------------------- DELTA_MODE ----------------------
----------
# | Set In-File Delta mode.
|
# | Options available: Incremental/Differential/Full (I/D/F)
|
# | e.g. DELTA_MODE="I"   for Incremental In-file delta backup
|
# |  or  DELTA_MODE="D"   for Differential In-file delta backup
|
# |  or  DELTA_MODE="F"   for Full File backup
|
# |  or  DELTA_MODE=""    for using backup set in-file delta setting
|
# ------------------------------------------------------------------
----------
DELTA_MODE=""

# ------------------------------- CLEANUP_MODE ----------------------
----------
# | You can enable Cleanup mode to remove obsolete files from your
backup      |
# | destinations after backup.
|
# | Options available: ENABLE-CLEANUP/DISABLE-CLEANUP
|
# | e.g. CLEANUP_MODE="ENABLE-CLEANUP"
|
# |  or  CLEANUP_MODE="DISABLE-CLEANUP"
|
# ------------------------------------------------------------------
----------
```

```
CLEANUP_MODE="DISABLE-CLEANUP"

# ---------------------------------- DEBUG_MODE -----------------------
----------
# | Set Debug mode.
|
# | Options available: ENABLE-DEBUG/DISABLE-DEBUG
|
# | e.g. DEBUG_MODE="ENABLE-DEBUG"
|
# |  or  DEBUG_MODE="DISABLE-DEBUG"
|
# ---------------------------------------------------------------------
----------
DEBUG_MODE="DISABLE-DEBUG"

########################## END: User Defined Section
############################


#########################################################################
##########
#                S C R I P T                          U S A G E
#
#########################################################################
##########

# Input Arguments will overwrite the above settings
# defined in 'User Defined Section'.
if [ $# -ge 1 ]; then

    if [ -n "$1" ]; then
        BACKUP_SET="$1"
    fi

fi

#########################################################################
##########
#          R E T R I E V E     A P P _ H O M E     P A T H
#
#########################################################################
##########

EXE_DIR=`pwd`
SCRIPT_HOME=`dirname "$0"`
cd "$SCRIPT_HOME"
APP_BIN=`pwd`
APP_HOME=`dirname "$APP_BIN"`

#########################################################################
##########
#          R E T R I E V E     J A V A _ H O M E     P A T H
#
#########################################################################
##########

if [ "Darwin" = `uname` ]; then
    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"
fi

if [ ! -x "$APP_HOME/jvm" ];
```

```
then
    echo "'$APP_HOME/jvm' does not exist!"
    if [ ! -n "$JAVA_HOME" ]; then
        echo "Please set JAVA_HOME!"
        exit 0
    else
        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"
        if [ ! -x "$APP_HOME/jvm" ];
        then
            echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"
            exit 0
        else
            echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"
        fi
    fi
fi


JAVA_HOME="$APP_HOME/jvm"
JAVA_EXE="$JAVA_HOME/bin/java"

# Verify the JAVA_EXE whether it can be executed or not.
if [ ! -x "${JAVA_EXE}" ]
then
    echo "The Java Executable file \"${JAVA_EXE}\" cannot be executed.
Exit \""`basename "$0"`"\" now."
    exit 1
fi

# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.
STRING_JAVA_VERSION="java version,openjdk version"
OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`
OUTPUT_JVM_SUPPORT=0
BACKUP_IFS=$IFS
IFS=","
for word in $STRING_JAVA_VERSION; do
    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]
    then
      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
      continue;
    else
      OUTPUT_JVM_SUPPORT=1
      break;
    fi
done
IFS=$BACKUP_IFS
if [ $OUTPUT_JVM_SUPPORT -eq 0 ]
then
    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
    exit 1
fi

#################################################################################
##########
#            E X E C U T I O N     J A V A     P R O P E R T I E S
#
#################################################################################
##########
```

```
# Set LD_LIBRARY_PATH for Lotus Notes on Linux
if [ "Linux" = `uname` ];
then
    NOTES_PROGRAM=`cat "$APP_HOME/bin/notesenv"`
    LD_LIBRARY_PATH="$APP_HOME/bin:$NOTES_PROGRAM:$LD_LIBRARY_PATH"
    export NOTES_PROGRAM
else
    LD_LIBRARY_PATH="$APP_HOME/bin:$LD_LIBRARY_PATH"
fi
DEP_LIB_PATH="X64"
case "`uname -m`" in
    i[3-6]86)
        DEP_LIB_PATH="X86"
    ;;
esac
LD_LIBRARY_PATH="${APP_BIN}/${DEP_LIB_PATH}":".":"${LD_LIBRARY_PATH}"

SHLIB_PATH="$LD_LIBRARY_PATH"
export LD_LIBRARY_PATH SHLIB_PATH

###########################################################################
##########
#                          J A V A     E X E C U T I O N
#
###########################################################################
##########

# Change to APP_BIN for JAVA execution
cd "${APP_BIN}"

# Reference path will be used to avoid empty space in the parent
directory
LIB_HOME=.
JAVA_OPTS="-Xrs -Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -client
-Dsun.nio.PageAlignDirectMemory=true"
JNI_PATH="-Djava.library.path=$LIB_HOME"
CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"
MAIN_CLASS=RunBackupSet

echo "-"
echo "Using APP_HOME       : $APP_HOME"
echo "Using SETTING_HOME   : $SETTING_HOME"
echo "Using JAVA_HOME      : $JAVA_HOME"
echo "Using JAVA_EXE       : $JAVA_EXE"
echo "Using JAVA_OPTS      : $JAVA_OPTS"
echo "Using JNI_PATH       : $JNI_PATH"
echo "Using CLASSPATH      : $CLASSPATH"
echo "-"

echo "Running Backup Set - '$BACKUP_SET' ..."

# API Arguments: RunBackupSet [APP_HOME] [BACKUP_SET] [BACKUP_DESTS]
[BACKUP_TYPE] [SETTING_HOME] [DELTA_MODE] [CLEANUP_MODE] [DEBUG_MODE]

# Do not include double-quote for java options, jni path, classpath
and
# main class.
# Only apply double-quote for path to java executable and execution
arguments
```

```
"${JAVA_EXE}" $JNI_PATH -cp $CLASSPATH $JAVA_OPTS $MAIN_CLASS
"${APP_HOME}" "${BACKUP_SET}" "${BACKUP_DESTS}" "${BACKUP_TYPE}"
"${SETTING_HOME}" "${DELTA_MODE}" "${CLEANUP_MODE}" "${DEBUG_MODE}"

##########################################################################
##########
#                   R E S E T          A N D          E X I T
#
##########################################################################
##########

cd "${EXE_DIR}"
exit 0
```

Restore.sh

This script file is used to restore backup files to its original or alternate location. To configure the parameters, open the script file in a text editor like vi.

```
# cd /usr/local/cbp/bin
# vi Restore.sh
```

Configure the following parameters:

- **BACKUP_SET** – this is the name of the backup set which you want to restore. There are two (2) ways to specify the backup set; by using the *backup set name* or by *backup set ID*. If the backup set name is not in English, use the backup set ID. You can leave this blank if you only have one (1) backup set.

  e.g. BACKUP_SET="1119083740107" or BACKUP_SET="FileBackupSet-1"

- **DESTINATION** – this is the name of the destination where the backup set was stored. There are two (2) ways to specify the destination; by using the *destination name* or *destination ID*. If the destination name is not in English, use the DestinationID. You can leave this blank if you only have one (1) backup destination.

  e.g. DESTINATION="1119083740107" or DESTINATION="Destination-1"

- **RESTORE_TO** – this is the directory where you want to restore the backup file. You do not need to change this if you want the backup file to be restored to its original location.

  e.g. RESTORE_TO="" or RESTORE_TO-"/tmp"

- **RESTORE_FROM** – this is the file or directory that you would like to restore.

  e.g. RESTORE_FROM="/Data"

- **POINT_IN_TIME** – this is the specific successful backup that you want to restore. You can use *Current* if you want to use the latest backup snapshot. You can see the point in time snapshot by using the *ListBackupJob.sh* script file.

  e.g. POINT_IN_TIME="Current" or POINT_IN_TIME="2006-10-04-12-57-13"

- **RESTORE_PERMISSION** – you can set the file permission here.

  e.g. RESTORE_PERMISSION="N" or RESTORE_PERMISSION="Y"

- **SKIP_INVALID_KEY** – you can set here if you want to skip restoring the backup file with an invalid key. There are two (2) options for this: *Y* or *N*.

  e.g. SKIP_INVALID_KEY="N"

- **SYNC_OPTION** – this is the sync options if you want to delete extra files.

  e.g. SYNC_OPTIONS="Y" if you want to enable sync options

  SYNC_OPTIONS="N" if you do not want to enable sync options

  SYNC_OPTIONS="" if you want to prompt for selection

- **REPLACE_EXISTING_FILE** – you can set here if you want files with the same filename to be replaced. There are three (3) options for this: *--all, --none* or blank.

  e.g. REPLACE_EXISTING_FILE="—all" if you want to replace existing files with the same filename

  REPLACE_EXISTING_FILE="—none" if you want to keep all existing files with the same filename

  REPLACE_EXISTING_FILE="" if you want to be prompted for selection

- **SETTING_HOME** – this is the directory to your setting home. If not set, the default directory is "${HOME}/.cbp".

  e.g. SETTING_HOME="/root/.cbp"

- **FILTER** – you can filter the files that you want to be restored. You can use this format to set the filter *-Pattern=xxx-Type=yyy-Target=zzz.*

  xxx is the filter pattern

  yyy is the filter type, you have eight (8) options available for this: *exact, exactMatchCase, contains, containsMatchCase, startWith*, *startWithMatchCase*, *endWith* and *endWithMatchCase*.

  zzz is the filter target, you have three (3) options available for this: *toFile, toFileDir* and *toDir*.

  e.g. FILTER="-Pattern=.txt-Type=exact-Target=toFile"

- **TEMP_DIR** – this is the directory where the restore files will be stored temporarily. If set to "" the temporary directory in the backup set will be used.

  e.g. TEMP_DIR="/tmp"

- **VERIFY_CHKSUM** – you can set here if you want the in-file delta file checksum to be verified during restore. There are two (2) options available for this: *Y* or *N*.

  e.g. VERIFY_CHKSUM="N" or VERIFY_CHKSUM="Y"

```
# cd /usr/local/cbp/bin
# vi Restore.sh

#!/bin/sh

################################  Restore.sh
################################
# You can use this shell script to restore backup files using command-
line.    #
# Just customize the "User Define Section" below with values for your
restore  #
# action.
#
#########################################################################
##########

########################  Start: User Defined Section
########################

# ----------------------------  BACKUP_SET  ----------------------
----------
# | The name or ID of the backup set that you want to restore.
|
```

```
# | If backup set name is not in English, please use ID instead.
|
# | e.g. BACKUP_SET="1119083740107"
|
# |  or  BACKUP_SET="FileBackupSet-1"
|
# |
|
# | You can leave this parameter blank if you have only 1 backup set.
|
# ------------------------------------------------------------------
----------
BACKUP_SET=""

# ------------------------------  DESTINATION  ----------------------
----------
# | The name or ID of the backup destination that you want to restore
from.    |
# | If backup destination name is not in English, please use ID
instead.       |
# | e.g. DESTINATION="1740107119083"
|
# |  or  DESTINATION="Destination-1"
|
# |
|
# | You can leave this parameter blank if you have only 1 destination.
|
# ------------------------------------------------------------------
----------
DESTINATION=""

# ------------------------------  RESTORE_TO  -----------------------
----------
# | Directory to where you want files to be restored
|
# | set to "" to restore files to original location
|
# | e.g. RESTORE_TO="/tmp"
|
# ------------------------------------------------------------------
----------
RESTORE_TO=""

# ------------------------------  RESTORE_FROM  ---------------------
----------
# | File/Directory on the backup server that you would like to restore
|
# | e.g. RESTORE_FROM="/Data"
|
# ------------------------------------------------------------------
----------
RESTORE_FROM=""

# ------------------------------  POINT_IN_TIME  --------------------
----------
# | The point-in-time snapshot (successful backup) that you want to
restore    |
# | from the backup server. Use "Current" for the latest backup
snapshot       |
# | e.g. POINT_IN_TIME="2006-10-04-12-57-13"
|
```

```
# |  or  POINT_IN_TIME="Current"
|
# |
|
# | You can retrieve the point in time by using the ListBackupJob.sh
|
# ------------------------------------------------------------------
----------
POINT_IN_TIME="Current"

# -------------------------  RESTORE_PERMISSION  --------------------
----------
# | set to "Y" if you want to restore file permissions
|
# | set to "N" if you do NOT want to restore file permissions
|
# ------------------------------------------------------------------
----------
RESTORE_PERMISSION="N"

# ---------------------------  SKIP_INVALID_KEY  --------------------
----------
# | set to "Y" if you want to skip restore file with invalid key
|
# | set to "N" if you want to prompt user to input a correct key
|
# ------------------------------------------------------------------
----------
SKIP_INVALID_KEY="N"

# ------------------------------  SYNC_OPTION  ----------------------
----------
# | Delete extra files
|
# | set to "Y" if you want to enable sync option
|
# | set to "N" if you do NOT want to enable sync option
|
# | set to "" to prompt for selection
|
# ------------------------------------------------------------------
----------
SYNC_OPTION="N"

# -------------------------  REPLACE_EXISTING_FILE  ------------------
----------
# | set to "--all" to replace all existing file(s) of the same
filename        |
# | set to "--none" to skip all existing file(s) with the same
filename        |
# | set to "" to prompt for selection
|
# ------------------------------------------------------------------
----------
REPLACE_EXISTING_FILE="--all"

# ------------------------------  SETTING_HOME  ---------------------
----------
# | Directory to your setting home.
|
# | Default to ${HOME}/.cbp when not set.
|
```

```
# | e.g. SETTING_HOME="${HOME}/.cbp"
|
# ------------------------------------------------------------------
----------
SETTING_HOME=""
# --------------------------------  FILTER  ------------------------
----------
# | Filter out what files you want to restore
|
# | -Pattern=xxx-Type=yyy-Target=zzz
|
# | where xxx is the filter pattern,
|
# |       yyy is the filter type, whice can be one of the following:
|
# |           [exact | exactMatchCase | contains | containsMatchCase|
|
# |            startWith | startWithMatchCase | endWith |
endWithMatchCase]    |
# |       zzz is the filter target, which can be one of the following:
|
# |           [toFile | toFileDir | toDir]
|
# |
|
# | e.g. FILTER="-Pattern=.txt-Type=exact-Target=toFile"
|
# ------------------------------------------------------------------
----------
FILTER=""

# --------------------------------  TEMP_DIR  ------------------------
----------
# | Directory to where you want to store restore files temporarily
|
# | set to "" to use the temporary directory in the backup set
|
# | e.g. TEMP_DIR="/tmp"
|
# ------------------------------------------------------------------
----------
TEMP_DIR=""

# ----------------------------  VERIFY_CHKSUM  ---------------------
----------
# | set to "Y" if you want to verify in-file delta file checksum
during restore|
# | set to "N" if you do NOT want to verify in-file delta file
checksum during |
# | restore
|
# ------------------------------------------------------------------
----------
VERIFY_CHKSUM="N"

##########################  END: User Defined Section
##########################

#########################################################################
##########
#      R E T R I E V E           A P P _ H O M E          P A T H
#
```

```
###############################################################################
##########

EXE_DIR=`pwd`
SCRIPT_HOME=`dirname "$0"`
cd "$SCRIPT_HOME"
APP_BIN=`pwd`
APP_HOME=`dirname "$APP_BIN"`
###############################################################################
##########
#      R E T R I E V E          J A V A _ H O M E          P A T H
#
###############################################################################
##########

if [ "Darwin" = `uname` ]; then
    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "'$APP_HOME/jvm' does not exist!"
    if [ ! -n "$JAVA_HOME" ]; then
        echo "Please set JAVA_HOME!"
        exit 0
    else
        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"
        echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"
    fi
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"
    exit 0
fi

JAVA_HOME="$APP_HOME/jvm"
JAVA_EXE="$JAVA_HOME/bin/java"

# Verify the JAVA_EXE whether it can be executed or not.
if [ ! -x "${JAVA_EXE}" ]
then
    echo "The Java Executable file \"${JAVA_EXE}\" cannot be executed.
Exit \""`basename "$0"`"\" now."
    exit 1
fi

# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.
STRING_JAVA_VERSION="java version,openjdk version"
OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`
OUTPUT_JVM_SUPPORT=0
BACKUP_IFS=$IFS
IFS=","
for word in $STRING_JAVA_VERSION; do
    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]
    then
      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
      continue;
```

```
    else
      OUTPUT_JVM_SUPPORT=1
      break;
    fi
done
IFS=$BACKUP_IFS
if [ $OUTPUT_JVM_SUPPORT -eq 0 ]
then
    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \"`basename "$0"`"\" now."
    exit 1
fi


#########################################################################
##########
#                  J A V A                  E X E C U T I O N
#
#########################################################################
##########

# Set LD_LIBRARY_PATH for Lotus Notes on Linux
if [ "Linux" = `uname` ];
then
    NOTES_PROGRAM=`cat "$APP_BIN/notesenv"`
    LD_LIBRARY_PATH="$APP_BIN:$NOTES_PROGRAM:$LD_LIBRARY_PATH"
    export NOTES_PROGRAM
else
    LD_LIBRARY_PATH="$APP_BIN:$LD_LIBRARY_PATH"
fi

# The Restore Action must be execute at path $APP_HOME/bin
cd "${APP_BIN}"

DEP_LIB_PATH="X64"
case "`uname -m`" in
    i[3-6]86)
        DEP_LIB_PATH="X86"
    ;;
esac
LD_LIBRARY_PATH="${APP_BIN}/${DEP_LIB_PATH}":".":"${LD_LIBRARY_PATH}"

SHLIB_PATH="$LD_LIBRARY_PATH"
export LD_LIBRARY_PATH SHLIB_PATH

# Reference path will be used to avoid empty space in the parent
directory
LIB_HOME=.
JAVA_OPTS="-Xrs -Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -client
-Dsun.nio.PageAlignDirectMemory=true"
JNI_PATH="-Djava.library.path=$LIB_HOME"
CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"
MAIN_CLASS=Restore

echo "Using APP_HOME:          : ${APP_HOME}"
echo "Using BACKUP_SET         : ${BACKUP_SET}"
echo "Using RESTORE_FROM       : ${RESTORE_FROM}"
echo "Using RESTORE_TO         : ${RESTORE_TO}"
echo "Using POINT_IN_TIME      : ${POINT_IN_TIME}"
echo "Using RESTORE_PERMISSION : ${RESTORE_PERMISSION}"
echo "Using TEMP_DIR           : ${TEMP_DIR}"
```

```
# Do not include double-quote for java options, jni path, classpath
and
# main class.
# Only apply double-quote for path to java executable and execution
arguments
"${JAVA_EXE}" $JAVA_OPTS $JNI_PATH -cp $CLASSPATH $MAIN_CLASS --
to="${RESTORE_TO}" --from="${RESTORE_FROM}" --backup-
set="${BACKUP_SET}" --backup-dest="${DESTINATION}"
"${REPLACE_EXISTING_FILE}" --date="${POINT_IN_TIME}" --set-
permission="${RESTORE_PERMISSION}" --skip-invalid-
key="${SKIP_INVALID_KEY}" --sync="${SYNC_OPTION}" --filter="${FILTER}"
--temp-dir="${TEMP_DIR}" --verify-delta-file-chksum="${VERIFY_CHKSUM}"
--app-home="${APP_HOME}" --setting-home="${SETTING_HOME}"

##########################################################################
##########
#                   R E S E T          A N D          E X I T
#
##########################################################################
##########

cd "${EXE_DIR}
```

Decrypt.sh

This script file is used to decrypt backup files. To configure the parameters, open the script file in a text editor like vi.

```
# cd /usr/local/cbp/bin
# vi Decrypt.sh
```

Configure the following parameters:

- **SOURCE_DIR** – this is the path of the folder that contains the backup files that you want to decrypt.

  e.g. SOURCE_DIR="/Users/john/backupdata/1498444438340/blocks"

- **ENCRYPT_KEY** – this is the encryption key the backup set. You can leave this blank if you backup set is not encypted.

  e.g. ENCRYPT_KEY="RU5DUllQVF9LRVk="

- **DECRYPT_TO** – this is the directory where you want to store the decrypted backup file.

  e.g. DECRYPT_TO="/tmp"

- **DECRYPT_FROM** – this is the file or directory that you would like to decrypt.

  e.g. RESTORE_FROM="/Data"

- **POINT_IN_TIME** – this is the specific successful backup that you want to decrypt. You can use *Current* if you want to use the latest backup snapshot. You can see the point in time snapshot by using the *ListBackupJob.sh* script file.

  e.g. POINT_IN_TIME="Current" or POINT_IN_TIME="2006-10-04-12-57-13"

- **RESTORE_PERMISSION** – you can set the file permission here.

  e.g. RESTORE_PERMISSION="N" or RESTORE_PERMISSION="Y"

- **SKIP_INVALID_KEY** – you can set here if you want to skip decrypting the backup file with an invalid key. There are two (2) options for this: *Y* or *N*.

  e.g. SKIP_INVALID_KEY="N"

- **SYNC_OPTION** – this is the sync options if you want to delete extra files.

  e.g. SYNC_OPTIONS="Y" if you want to enable sync options

  SYNC_OPTIONS="N" if you do not want to enable sync options

  SYNC_OPTIONS="" if you want to prompt for selection

- **REPLACE_EXISTING_FILE** – you can set here if you want files with the same filename to be replaced. There are three (3) options for this: *--all, --none* or blank.

  e.g. REPLACE_EXISTING_FILE="—all" if you want to replace existing files with the same filename

  REPLACE_EXISTING_FILE="—none" if you want to keep all existing files with the same filename

  REPLACE_EXISTING_FILE="" if you want to be prompted for selection

- **SETTING_HOME** – this is the directory to your setting home. If not set, the default directory is "${HOME}/..cbp".

  e.g. SETTING_HOME="/root/.cbp"

- **FILTER** – you can filter the files that you want to be restored. You can use this format to set the filter *-Pattern=xxx-Type=yyy-Target=zzz.*

  xxx is the filter pattern

  yyy is the filter type, you have eight (8) options available for this: *exact, exactMatchCase, contains, containsMatchCase, startWith*, *startWithMatchCase*, *endWith* and *endWithMatchCase*.

  zzz is the filter target, you have three (3) options available for this: *toFile, toFileDir* and *toDir*.

  e.g. FILTER="-Pattern=.txt-Type=exact-Target=toFile"

- **TEMP_DIR** – this is the directory where the restore files will be stored temporarily. If set to "" the temporary directory in the backup set will be used.

  e.g. TEMP_DIR="/tmp"

- **VERIFY_CHKSUM** – you can set here if you want the in-file delta file checksum to be verified during restore. There are two (2) options available for this: *Y* or *N*.

  e.g. VERIFY_CHKSUM="N" or VERIFY_CHKSUM="Y"

```
# cd /usr/local/cbp/bin
# vi Decrypt.sh

#!/bin/sh

##################################  Decrypt.sh
##################################
# You can use this shell script to decrypt backup files using command-
line.    #
# Just customize the "User Define Section" below with values for your
decrypt  #
# action.
#
#########################################################################
##########

#########################  Start: User Defined Section
########################

# ------------------------------  SOURCE_DIR  ----------------------
----------
# | The path to the [<backup set ID>/blocks] folder which contains
|
# | the backup files that you want to decrypt.
|
# | This folder should located under backup destination physically.
|
# | e.g. SET SOURCE_DIR="/Users/john/backupdata/1498444438340/blocks"
|
# |      where directory "/Users/john/backupdata" is path of local
destination |
# ------------------------------------------------------------------
----------
SOURCE_DIR=""

# ------------------------------  ENCRYPT_KEY  ---------------------
----------
# | The encrypting key of the backup data.
|
```

```
# | e.g. SET ENCRYPT_KEY="RU5DUllQVF9LRVk="
|
# |
|
# | You can leave this parameter blank if backup data is not
encrypted.        |
# ------------------------------------------------------------------
----------
ENCRYPT_KEY=""

# ------------------------------  DECRYPT_TO  ----------------------
----------
# | Directory to where you want files to be decrypted
|
# | e.g. DECRYPT_TO="/tmp"
|
# ------------------------------------------------------------------
----------
DECRYPT_TO=""

# ------------------------------  DECRYPT_FROM  --------------------
----------
# | File/Directory on the backup data that you would like to decrypt
|
# | e.g. DECRYPT_FROM="/Data"
|
# ------------------------------------------------------------------
----------
DECRYPT_FROM=""
# ------------------------------  POINT_IN_TIME  -------------------
----------
# | The point-in-time snapshot (successful backup) that you want to
decrypt    |
# | from the backup data. Use "Current" for the latest backup snapshot
|
# | e.g. POINT_IN_TIME="2006-10-04-12-57-13"
|
# |  or  POINT_IN_TIME="Current"
|
# |
|
# | You can retrieve the point in time by using the ListBackupJob.sh
|
# ------------------------------------------------------------------
----------
POINT_IN_TIME="Current"

# --------------------------  RESTORE_PERMISSION  --------------------
----------
# | set to "Y" if you want to restore file permissions
|
# | set to "N" if you do NOT want to restore file permissions
|
# ------------------------------------------------------------------
----------
RESTORE_PERMISSION="N"

# ----------------------------  SKIP_INVALID_KEY  --------------------
----------
# | set to "Y" if you want to skip decrypt file with invalid key
|
```

```
# | set to "N" if you want to prompt to input a correct key
|
# ------------------------------------------------------------------
----------
SKIP_INVALID_KEY="N"

# ------------------------------  SYNC_OPTION  ----------------------
----------
# | Delete extra files
|
# | set to "Y" if you want to enable sync option
|
# | set to "N" if you do NOT want to enable sync option
|
# | set to "" to prompt for selection
|
# ------------------------------------------------------------------
----------
SYNC_OPTION="N"

# -------------------------  REPLACE_EXISTING_FILE  ------------------
----------
# | set to "--all" to replace all existing file(s) of the same
filename        |
# | set to "--none" to skip all existing file(s) with the same
filename        |
# | set to "" to prompt for selection
|
# ------------------------------------------------------------------
----------
REPLACE_EXISTING_FILE="--all"

# ------------------------------  SETTING_HOME  ---------------------
----------
# | Directory to your setting home. Log files will be located inside.
|
# | Default to ${HOME}/.cbp when not set.                          |
# | e.g. SETTING_HOME="/Users/john/.cbp"                           |
# ------------------------------------------------------------------
----------
SETTING_HOME=""
# ---------------------------------  FILTER  -------------------------
----------
# | Filter out what files you want to decrypt
|
# | -Pattern=xxx-Type=yyy-Target=zzz
|
# | where xxx is the filter pattern,
|
# |       yyy is the filter type, whice can be one of the following:
|
# |           [exact | exactMatchCase | contains | containsMatchCase|
|
# |            startWith | startWithMatchCase | endWith |
endWithMatchCase]    |
# |       zzz is the filter target, which can be one of the following:
|
# |           [toFile | toFileDir | toDir]
|
# |
|
```

```
# | e.g. FILTER="-Pattern=.txt-Type=exact-Target=toFile"
|
# ------------------------------------------------------------------------
----------
FILTER=""

# --------------------------------  TEMP_DIR  ------------------------
----------
# | Directory to where you want to store decrypt files temporarily
|
# | e.g. TEMP_DIR="/tmp"
|
# ------------------------------------------------------------------------
----------
TEMP_DIR=""

# ----------------------------  VERIFY_CHKSUM  ----------------------
----------
# | set to "Y" if you want to verify in-file delta file checksum
during decrypt|
# | set to "N" if you do NOT want to verify in-file delta file
checksum during |
# | decrypt
|
# ------------------------------------------------------------------------
----------
VERIFY_CHKSUM="N"

##########################  END: User Defined Section
##########################

#########################################################################
##########
#      R E T R I E V E           A P P _ H O M E          P A T H
#
#########################################################################
##########

EXE_DIR=`pwd`
SCRIPT_HOME=`dirname "$0"`
cd "$SCRIPT_HOME"
APP_BIN=`pwd`
APP_HOME=`dirname "$APP_BIN"`
#########################################################################
##########
#      R E T R I E V E          J A V A _ H O M E          P A T H
#
#########################################################################
##########

if [ "Darwin" = `uname` ]; then
    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "'$APP_HOME/jvm' does not exist!"
    if [ ! -n "$JAVA_HOME" ]; then
        echo "Please set JAVA_HOME!"
        exit 0
    else
        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"
```

```
        echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"
    fi
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"
    exit 0
fi

JAVA_HOME="$APP_HOME/jvm"
JAVA_EXE="$JAVA_HOME/bin/java"

# Verify the JAVA_EXE whether it can be executed or not.
if [ ! -x "${JAVA_EXE}" ]
then
    echo "The Java Executable file \"${JAVA_EXE}\" cannot be executed.
Exit \""`basename "$0"`"\" now."
    exit 1
fi

# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.
STRING_JAVA_VERSION="java version,openjdk version"
OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`
OUTPUT_JVM_SUPPORT=0
BACKUP_IFS=$IFS
IFS=","
for word in $STRING_JAVA_VERSION; do
    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]
    then
      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
      continue;
    else
      OUTPUT_JVM_SUPPORT=1
      break;
    fi
done
IFS=$BACKUP_IFS
if [ $OUTPUT_JVM_SUPPORT -eq 0 ]
then
    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
    exit 1
fi


##########################################################################
##########
#                  J A V A                 E X E C U T I O N
#
##########################################################################
##########

# Set LD_LIBRARY_PATH for Lotus Notes on Linux
if [ "Linux" = `uname` ];
then
    NOTES_PROGRAM=`cat "$APP_BIN/notesenv"`
    LD_LIBRARY_PATH="$APP_BIN:$NOTES_PROGRAM:$LD_LIBRARY_PATH"
    export NOTES_PROGRAM
```

```
else
    LD_LIBRARY_PATH="$APP_BIN:$LD_LIBRARY_PATH"
fi

# The Decrypt Action must be execute at path $APP_HOME/bin
cd "${APP_BIN}"

DEP_LIB_PATH="X64"
case "`uname -m`" in
    i[3-6]86)
        DEP_LIB_PATH="X86"
    ;;
esac
LD_LIBRARY_PATH="${APP_BIN}/${DEP_LIB_PATH}":".":"${LD_LIBRARY_PATH}"

SHLIB_PATH="$LD_LIBRARY_PATH"
export LD_LIBRARY_PATH SHLIB_PATH

# Reference path will be used to avoid empty space in the parent
directory
LIB_HOME=.
JAVA_OPTS="-Xrs -Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -client
-Dsun.nio.PageAlignDirectMemory=true"
JNI_PATH="-Djava.library.path=$LIB_HOME"
CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"
MAIN_CLASS=Decrypt

echo "Using APP_HOME:          : ${APP_HOME}"
echo "Using SETTING_HOME:      : ${SETTING_HOME}"
echo "Using SOURCE_DIR         : ${SOURCE_DIR}"
echo "Using DECRYPT_FROM       : ${DECRYPT_FROM}"
echo "Using DECRYPT_TO         : ${DECRYPT_TO}"
echo "Using POINT_IN_TIME      : ${POINT_IN_TIME}"
echo "Using RESTORE_PERMISSION : ${RESTORE_PERMISSION}"
echo "Using TEMP_DIR           : ${TEMP_DIR}"

# Do not include double-quote for java options, jni path, classpath
and
# main class.
# Only apply double-quote for path to java executable and execution
arguments
"${JAVA_EXE}" $JAVA_OPTS $JNI_PATH -cp $CLASSPATH $MAIN_CLASS --
to="${DECRYPT_TO}" --from="${DECRYPT_FROM}" --source-
dir="${SOURCE_DIR}" --key="${ENCRYPT_KEY}" "${REPLACE_EXISTING_FILE}"
--date="${POINT_IN_TIME}" --set-permission="${RESTORE_PERMISSION}" --
skip-invalid-key="${SKIP_INVALID_KEY}" --sync="${SYNC_OPTION}" --
filter="${FILTER}" --temp-dir="${TEMP_DIR}" --verify-delta-file-
chksum="${VERIFY_CHKSUM}" --app-home="${APP_HOME}" --setting-
home="${SETTING_HOME}"

##########################################################################
##########
#                   R E S E T          A N D          E X I T
#
##########################################################################
##########

cd "${EXE_DIR}"
exit 0
```

RunDataIntegrityCheck.sh

This script file is used to run data integrity check on your backup set. To configure the parameters, open the script file in a text editor like vi.

```
# cd /usr/local/cbp/bin
# vi RunDataIntegrityCheck.sh
```

Configure the following parameters:

- **SETTING_HOME** – this is the directory to your setting home. If not set, the default directory is "${HOME}/.cbp".

  e.g. SETTING_HOME="/root/.cbp"

- **BACKUP_SET** – this is the name of the backup set which you want to run data integrity check on. There are two (2) ways to specify the backup set; by using the *backup set name* or by *backup set ID*. If the backup set name is not in English, use the backup set ID. You can leave this blank if you only have one (1) backup set. You can also run the data integrity check on all backup sets by using "*ALL*".

  e.g. BACKUP_SET="1119083740107", BACKUP_SET="FileBackupSet-1" or BACKUP_SET="ALL"

- **BACKUP_DEST** – this is the name of the destination where the backup set was stored. There are two (2) ways to specify the destination; by using the *destination name* or *destination ID*. If the destination name is not in English, use the DestinationID. You can leave this blank if you only have one (1) backup destination. This will be disregarded if BACKUP_SET="ALL".

  e.g. DESTINATION="1119083740107" or DESTINATION="Destination-1"

- **CRC_MODE** – you can set here if you want to run cyclic redundancy check while doing the data integrity check. There are two (2) options available: *ENABLE-CRC* or *DISABLE-CRC*

  e.g. CRC_MODE="DISABLE-CRC" or CRC_MODE="ENABLE-CRC"

```
# cd /usr/local/cbp/bin
# vi RunDataIntegrityCheck.sh

#!/bin/sh

##########################  RunDataIntegrityCheck.sh
##########################
# You can use this shell script to run any of your backup sets from
the        #
# command line. Just customize the "User Defined Section" below with
your      #
# values for your backup action.
#
#########################################################################
##########

########################  START: User Defined Section
########################

# ------------------------- SETTING_HOME (Optional) -----------------
----------
# | Directory to your setting home.
|
# | Default to ${HOME}/.cbp when not set.
|
# | e.g. SETTING_HOME="${HOME}/.cbp"
|
```

```
# ------------------------------------------------------------------
----------
SETTING_HOME=""

# --------------------------------- BACKUP_SET ----------------------
----------
# | The name or ID of the backup set that you want to run.
|
# | If backup set name is not in English, please use ID instead.
|
# | e.g. BACKUP_SET="1119083740107"
|
# |  or  BACKUP_SET="FileBackupSet-1"
|
# | You can use "ALL" to run data integrity check for all backup sets.
|
# | i.e. BACKUP_SET="ALL"
|
# |
|
# | You can leave this parameter blank if you have only 1 backup set.
|
# ------------------------------------------------------------------
----------
BACKUP_SET="ALL"

# --------------------------------- BACKUP_DEST ---------------------
----------
# | The name or ID of the backup destination that you want to run.
|
# | If backup destination name is not in English, please use ID
instead.       |
# | e.g. BACKUP_DEST="1740107119083"
|
# |  or  BACKUP_DEST="Destination-1"
|
# | You can use "ALL" to run data integrity check for all
destinations.        |
# | i.e. BACKUP_DEST="ALL"
|
# |
|
# | You can leave this parameter blank if you have only 1 destination.
|
# | Remark: This option is ignored if BACKUP_SET="ALL"
|
# ------------------------------------------------------------------
----------
BACKUP_DEST="ALL"
# ---------------------------------- CRC_MODE ----------------------
----------
# | You can run Cyclic Redundancy Check (CRC) during data integrity
check      |
# | Options available: ENABLE-CRC/DISABLE-CRC
|
# | i.e. CRC_MODE="ENABLE-CRC"
|
# |  or  CRC_MODE="DISABLE-CRC"
|
# ------------------------------------------------------------------
----------
CRC_MODE="DISABLE-CRC"
```

```
########################## END: User Defined Section
############################


#########################################################################
##########
#                S C R I P T                          U S A G E
#
#########################################################################
##########

# Input Arguments will overwrite the above settings
# defined in 'User Defined Section'.
if [ $# -ge 1 ]; then

    if [ -n "$1" ]; then
        BACKUP_SET="$1"
    fi

fi

#########################################################################
##########
#          R E T R I E V E     A P P _ H O M E     P A T H
#
#########################################################################
##########

EXE_DIR=`pwd`
SCRIPT_HOME=`dirname "$0"`
cd "$SCRIPT_HOME"
APP_BIN=`pwd`
APP_HOME=`dirname "$APP_BIN"`
#########################################################################
##########
#          R E T R I E V E     J A V A _ H O M E     P A T H
#
#########################################################################
##########

if [ "Darwin" = `uname` ]; then
    JAVA_HOME="/System/Library/Frameworks/JavaVM.framework/Home"
fi

if [ ! -x "$APP_HOME/jvm" ];
then
    echo "'$APP_HOME/jvm' does not exist!"
    if [ ! -n "$JAVA_HOME" ]; then
        echo "Please set JAVA_HOME!"
        exit 0
    else
        ln -sf "$JAVA_HOME" "$APP_HOME/jvm"
        if [ ! -x "$APP_HOME/jvm" ];
        then
            echo "Please create symbolic link for '$JAVA_HOME' to
'$APP_HOME/jvm'"
            exit 0
        else
            echo "Created JAVA_HOME symbolic link at '$APP_HOME/jvm'"
        fi
    fi
```

```
fi

JAVA_HOME="$APP_HOME/jvm"
JAVA_EXE="$JAVA_HOME/bin/java"

# Verify the JAVA_EXE whether it can be executed or not.
if [ ! -x "${JAVA_EXE}" ]
then
    echo "The Java Executable file \"${JAVA_EXE}\" cannot be executed.
Exit \""`basename "$0"`"\" now."
    exit 1
fi

# Verify the JAVA_EXE whether it is a valid JAVA Executable or not.
STRING_JAVA_VERSION="java version,openjdk version"
OUTPUT_JAVA_VERSION=`"${JAVA_EXE}" -version 2>&1`
OUTPUT_JVM_SUPPORT=0
BACKUP_IFS=$IFS
IFS=","
for word in $STRING_JAVA_VERSION; do
    if [ `echo "${OUTPUT_JAVA_VERSION}" | grep "${word}" | grep -cv
"grep ${word}"` -le 0 ]
    then
      #echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
      continue;
    else
      OUTPUT_JVM_SUPPORT=1
      break;
    fi
done
IFS=$BACKUP_IFS
if [ $OUTPUT_JVM_SUPPORT -eq 0 ]
then
    echo "The Java Executable \"${JAVA_EXE}\" is not a valid Java
Executable. Exit \""`basename "$0"`"\" now."
    exit 1
fi

#########################################################################
##########
#            E X E C U T I O N     J A V A     P R O P E R T I E S
#
#########################################################################
##########

# Set LD_LIBRARY_PATH for Lotus Notes on Linux
if [ "Linux" = `uname` ];
then
    NOTES_PROGRAM=`cat "$APP_HOME/bin/notesenv"`
    LD_LIBRARY_PATH="$APP_HOME/bin:$NOTES_PROGRAM:$LD_LIBRARY_PATH"
    export NOTES_PROGRAM
else
    LD_LIBRARY_PATH="$APP_HOME/bin:$LD_LIBRARY_PATH"
fi

DEP_LIB_PATH="X64"
case "`uname -m`" in
    i[3-6]86)
        DEP_LIB_PATH="X86"
    ;;
esac
```

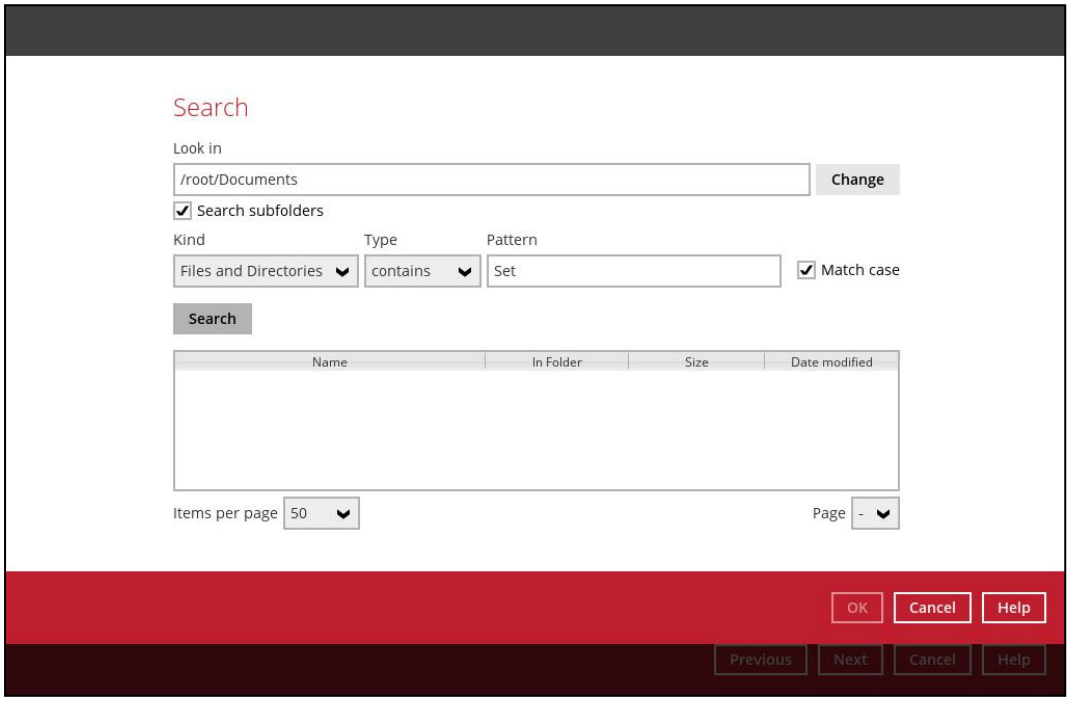
```
LD_LIBRARY_PATH="${APP_BIN}/${DEP_LIB_PATH}":".":"${LD_LIBRARY_PATH}"

SHLIB_PATH="$LD_LIBRARY_PATH"
export LD_LIBRARY_PATH SHLIB_PATH

#########################################################################
##########
#                          J A V A     E X E C U T I O N
#
#########################################################################
##########

# Change to APP_BIN for JAVA execution
cd "${APP_BIN}"

# Reference path will be used to avoid empty space in the parent
directory
LIB_HOME=.
JAVA_OPTS="-Xrs -Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -client
-Dsun.nio.PageAlignDirectMemory=true"
JNI_PATH="-Djava.library.path=$LIB_HOME"
CLASSPATH="$LIB_HOME:$LIB_HOME/cb.jar"
MAIN_CLASS=RunDataIntegrityCheck

echo "-"
echo "Using APP_HOME       : $APP_HOME"
echo "Using SETTING_HOME   : $SETTING_HOME"
echo "Using JAVA_HOME      : $JAVA_HOME"
echo "Using JAVA_EXE       : $JAVA_EXE"
echo "Using JAVA_OPTS      : $JAVA_OPTS"
echo "Using JNI_PATH       : $JNI_PATH"
echo "Using CLASSPATH      : $CLASSPATH"
echo "-"

echo "Running data integrity check for backup set - '$BACKUP_SET',
destination - '$BACKUP_DEST' ..."

# API Arguments: RunDataIntegrityCheck [APP_HOME] [SETTING_HOME]
[BACKUP_SET] [BACKUP_DEST] [CRC_MODE]

# Do not include double-quote for java options, jni path, classpath
and
# main class.
# Only apply double-quote for path to java executable and execution
arguments
"${JAVA_EXE}" $JNI_PATH -cp $CLASSPATH $JAVA_OPTS $MAIN_CLASS
"${APP_HOME}" "${SETTING_HOME}" "${BACKUP_SET}" "${BACKUP_DEST}"
"${CRC_MODE}"

#########################################################################
##########
#                    R E S E T          A N D          E X I T
#
#########################################################################
##########

cd "${EXE_DIR}"
exit 0
```

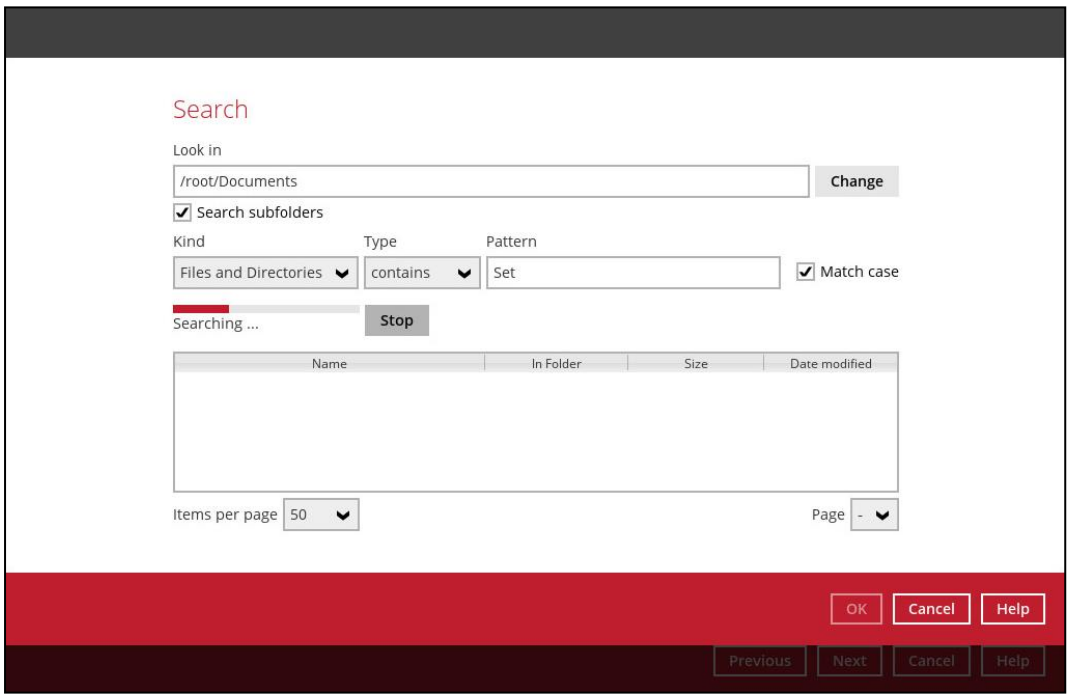
Appendix F: Example Scenarios for Restore Filter

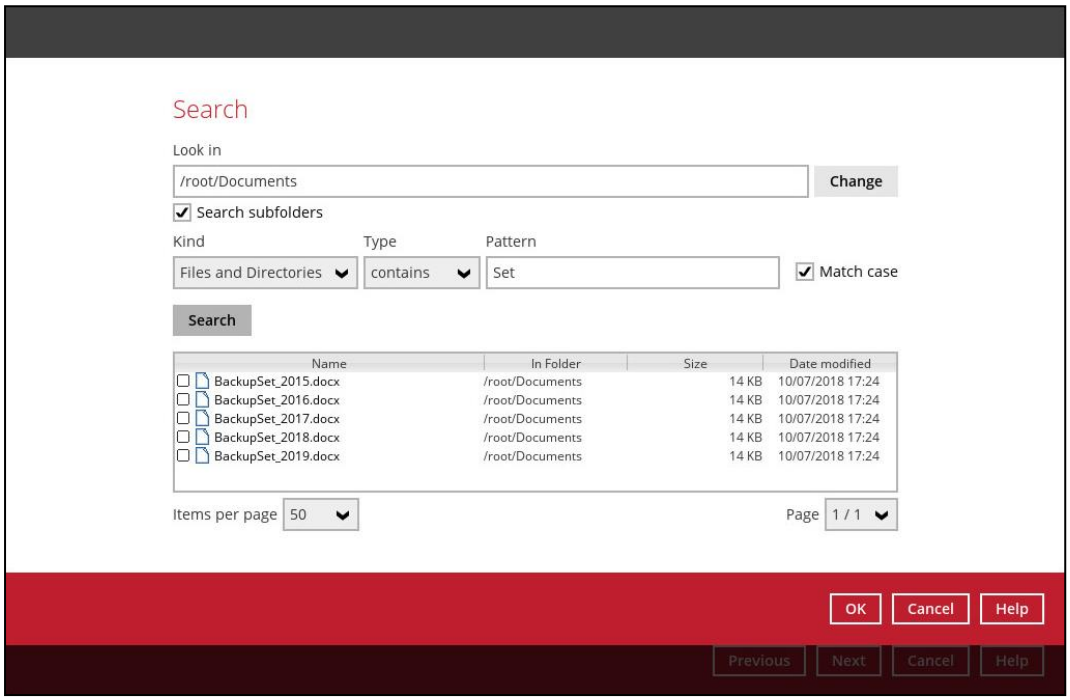
Example No.1: Restore filter setting from /root/Documents with filter type Contains

Location:	/root/Documents
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 \root\Documents that has the pattern that contains with ‘Set’ with match case set to true will be included upon performing search.

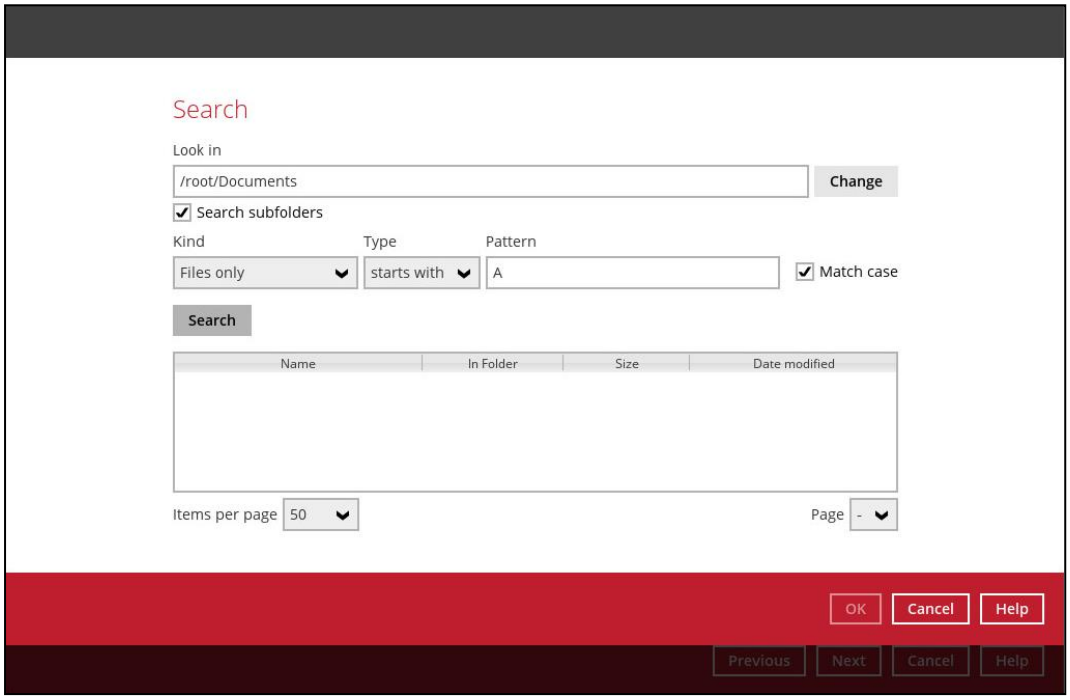
As you can see on the screen shot above, the result panel contains the Name of the file or directory, Directory which are indicated In-Folder column, Size, and Date Modified.

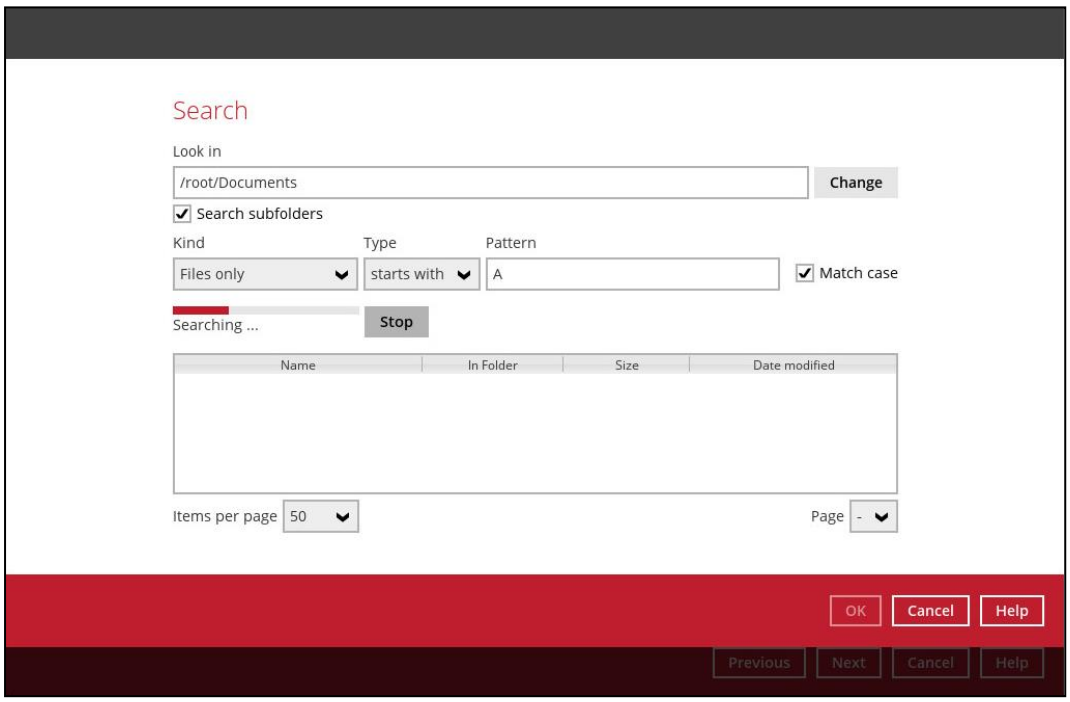
The restore filter setting includes the Search subfolder and Match case set to true. Meaning, the filter will include all available subfolders in \Documents upon searching. And it will strictly search only the specified pattern and case which starts with ‘Set’.

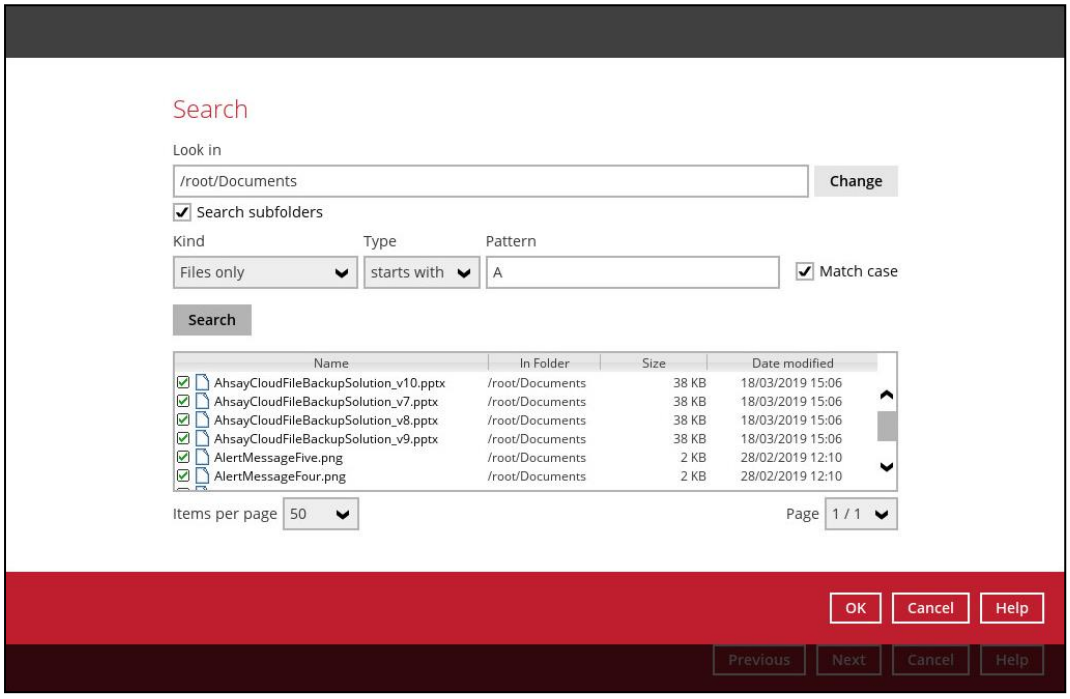
Example No.2: Restore filter setting from /root/Documents with filter type Starts With

Location:	/root/Documents
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 \root\Documents that has the pattern that starts with ‘A’ with match case set to true will be included upon performing search.

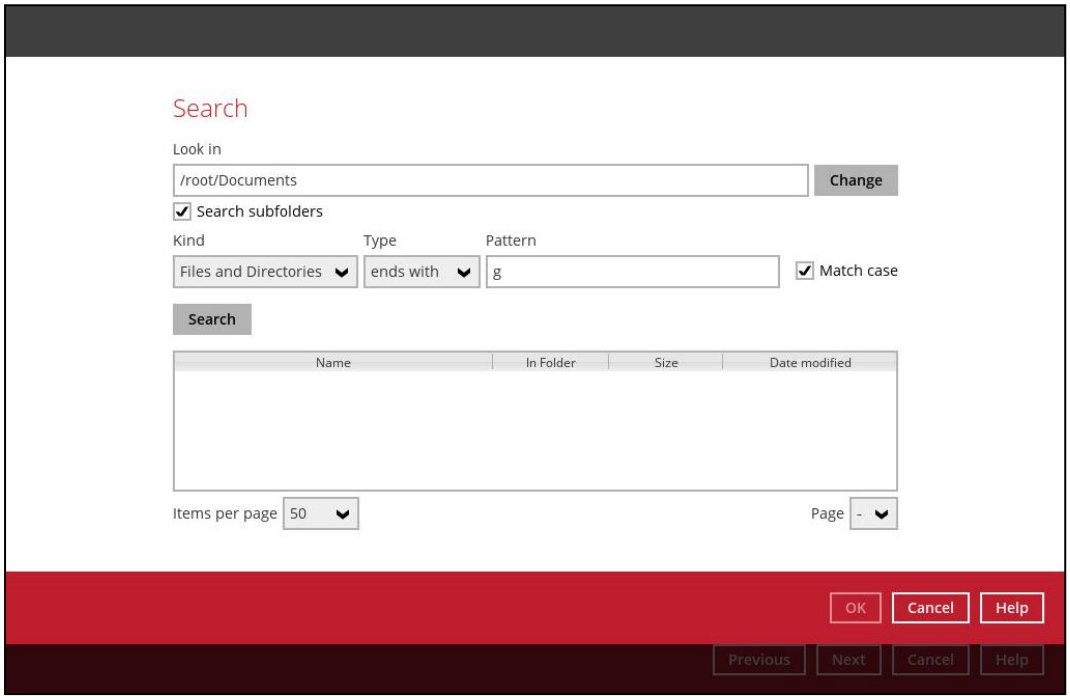
As you can see on the screen shot above, the result panel contains the Name of the file, Directory which are indicated In-Folder column, Size, and Date Modified.

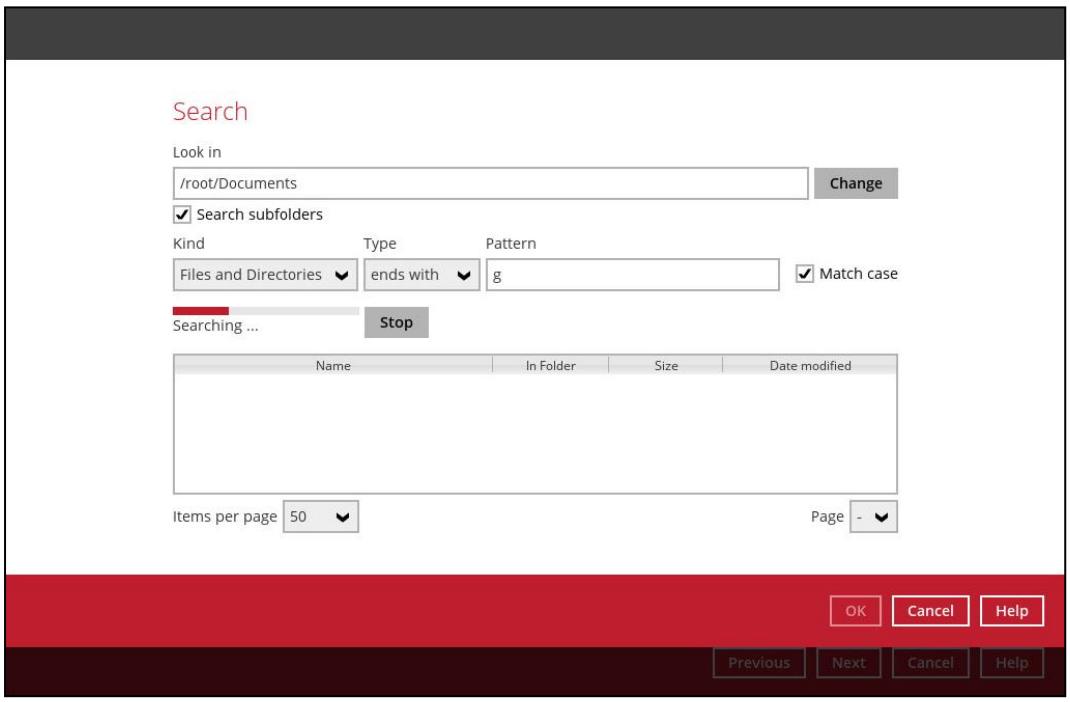
The restore filter setting includes the Search subfolder and Match case set to true. Meaning, the filter will include all available subfolders in \Documents upon searching. And it will strictly search only the specified pattern and case which starts with ‘A’.

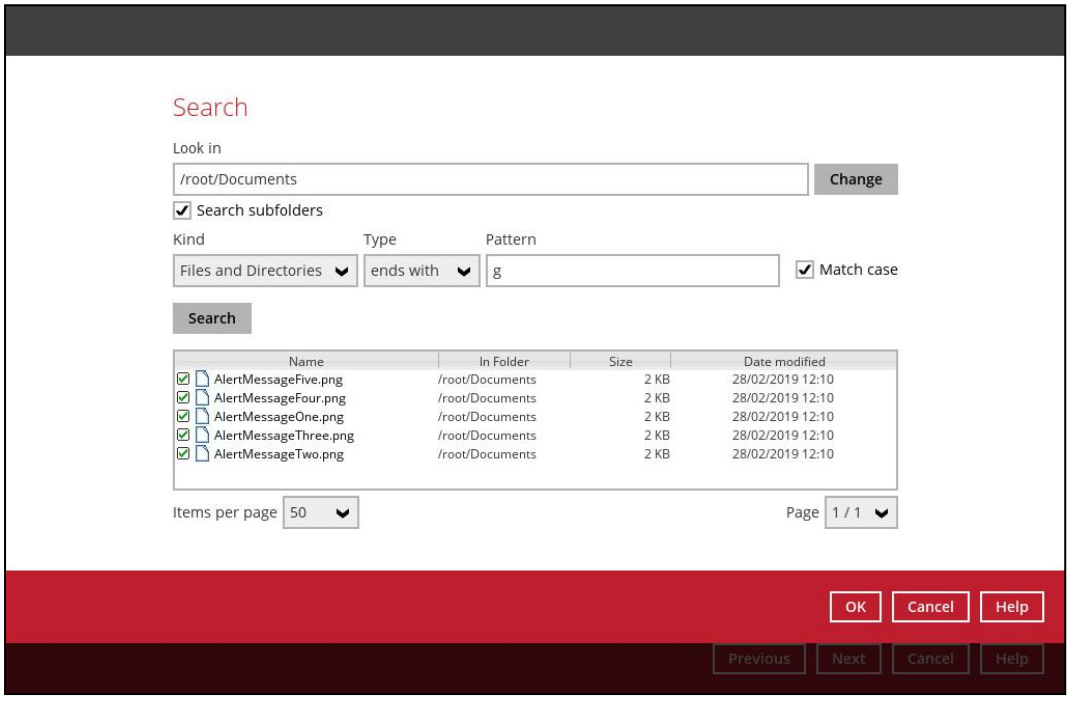
Example No.3: Restore filter setting from /root/Documents with filter type Ends With

Location:	/root/Documents
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 \root\Documents that has the pattern that ends with ‘g’ with match case set to true will be included upon performing search.

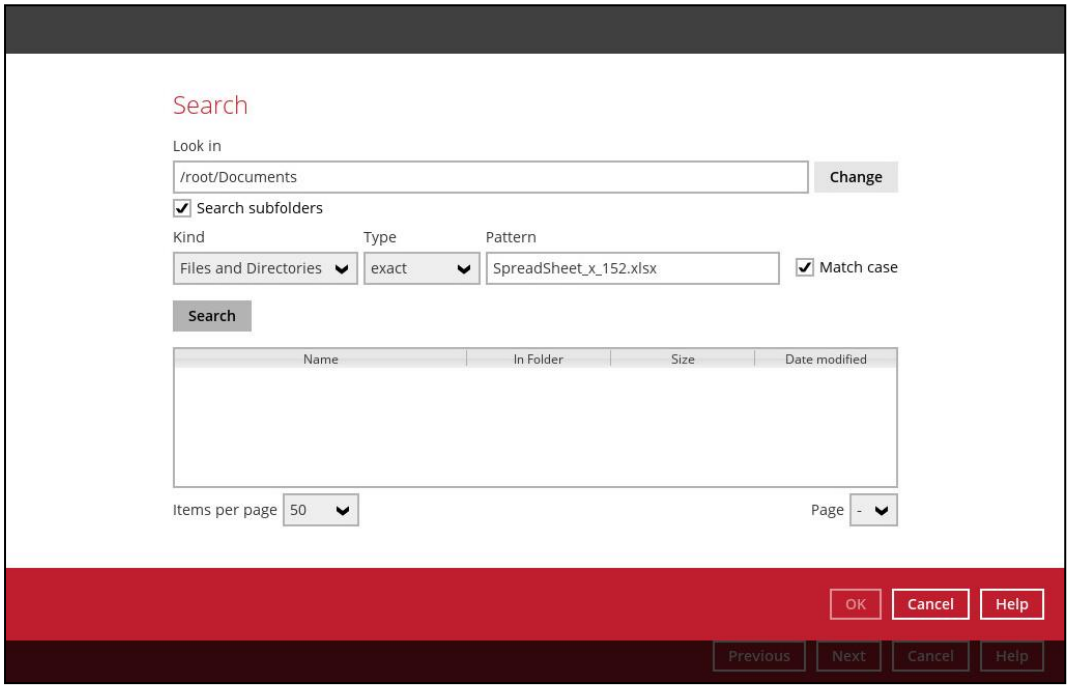
As you can see on the screen shot above, the result panel contains the Name of the files and directories, Directory which are indicated In-Folder column, Size, and Date Modified.

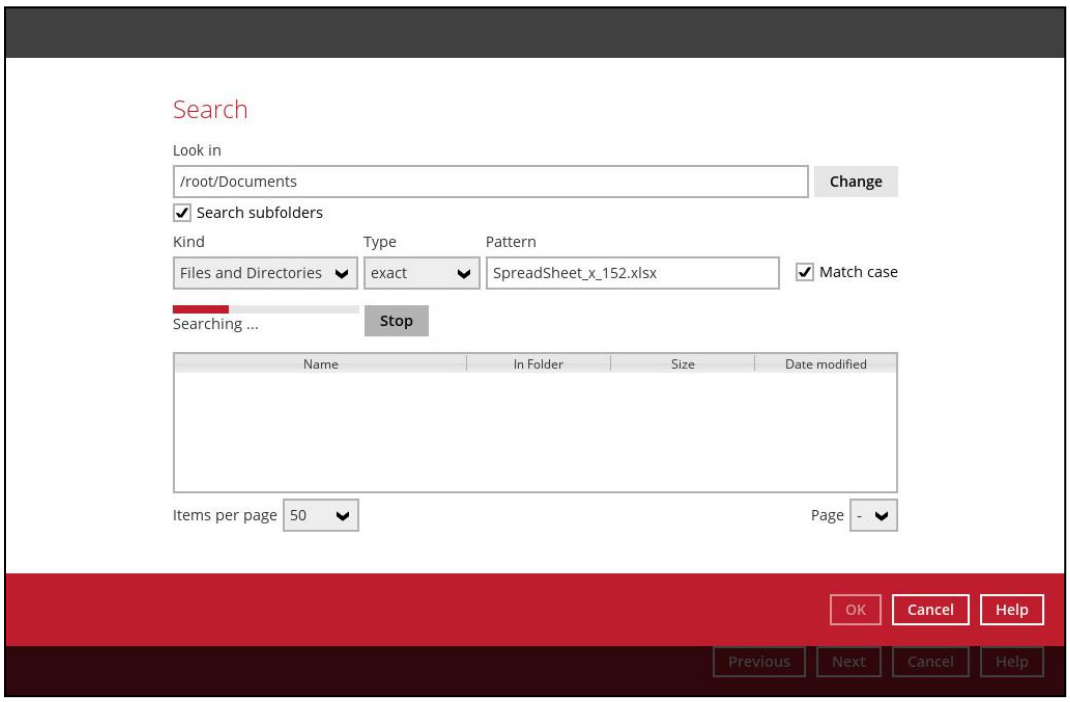
The restore filter setting includes the Search subfolder and Match case set to true. Meaning, the filter will include all available subfolders in \Documents upon searching. And it will strictly search only the specified pattern and case which starts with ‘g’.

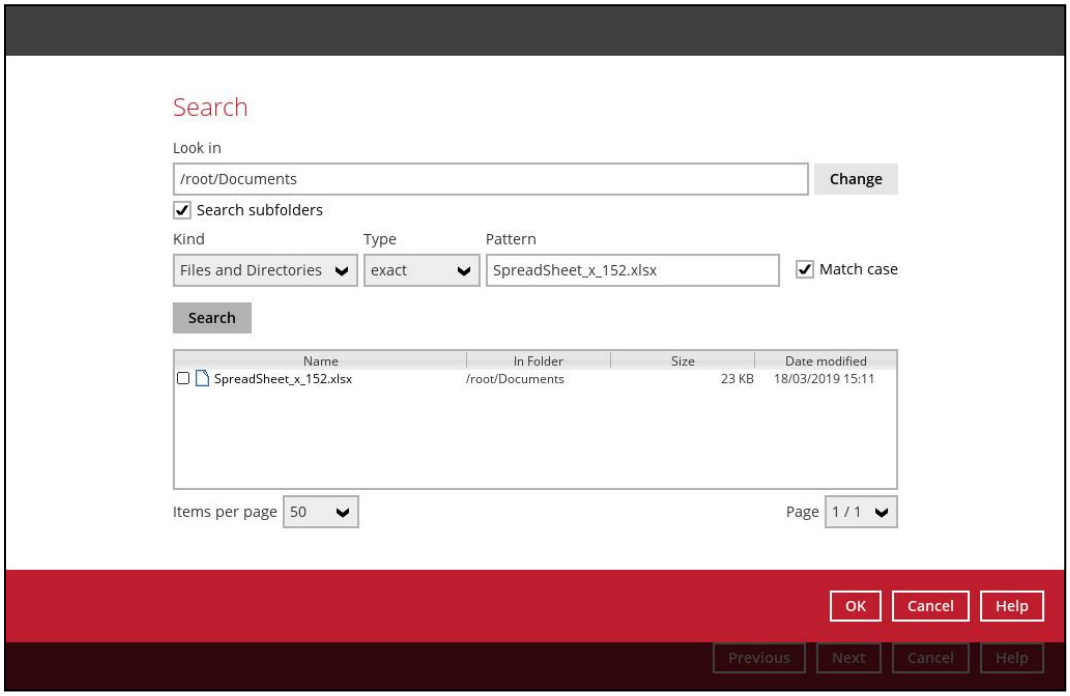
Example No.4: Restore filter setting from /root/Documents with filter type Exact

Location:	/root/Documents
Search subfolders:	True
Kind:	Files and Directories
Type:	Exact
Pattern:	SpreadSheet_x_152.xlsx
Match Case:	True

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







Explanation:

All files and directories under \root\Documents that has the pattern that has the exact pattern 'SpreadSheet_x_152.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. Meaning, the filter will include all available subfolders in \Documents upon searching. And it will strictly search only the specified pattern and case which starts with 'SpreadSheet_x_152.xlsx'.

Appendix G: Pre-installation Check

Follow the instructions below to perform a pre-installation check to verify if there is a pre-existing version remaining or was not uninstalled properly. Otherwise, CloudBacko Pro may not be installed properly.

```
# dpkg -l |grep cbp
```

Example:

There's an existing CloudBacko Pro.

```
# dpkg -l |grep cbp
#ii  cbp                                          3.7.0.0
amd64        CloudBacko Pro
```

Need to perform uninstall first.

```
# cd /usr/local/cbp/bin
# dpkg -r cbp
(Reading database ... 200210 files and directories currently
installed.)
Removing cbp (3.7.0.0) ...
Log Time: Tue May 26 02:50:22 UTC 2020

Verifying current user privilege ...
Current user has enough privilege to "uninstall".

Uninstall CloudBacko Pro from /usr/local/cbp

Shutting down Scheduler
Wait 5 seconds before Scheduler exits
Kill running CloudBacko Pro
Kill Process by Image Name: /usr/local/cbp/jvm/bin/bJW
Ignore Process by Image Name:
Kill process of PID 3355
Kill Process by Image Name: /usr/local/cbp/jvm/bin/bschJW
Ignore Process by Image Name:
Kill Process by Image Name: /usr/local/cbp/jvm/bin/java
Ignore Process by Image Name:
Removing Scheduler script cbpscheduler from service
Uninstall Service for NIX type OS
Using init script path /etc/init.d
Using run level script path /etc
Removing symbolic link from run levels
Removing script file cbpscheduler from /etc/init.d
Remove shortcut /usr/share/applications/cbp.desktop
Remove shortcut /root/Desktop/cbp.desktop
CloudBacko Pro uninstall procedure is complete!
It is now safe to remove files from /usr/local/cbp
    Remove files in /usr/local/cbp
```

Remove files and or folder from /usr/local/cbp

```
# cd /usr/local/
# rm -fr cbp
```

Appendix H: Exclude Filter System Files

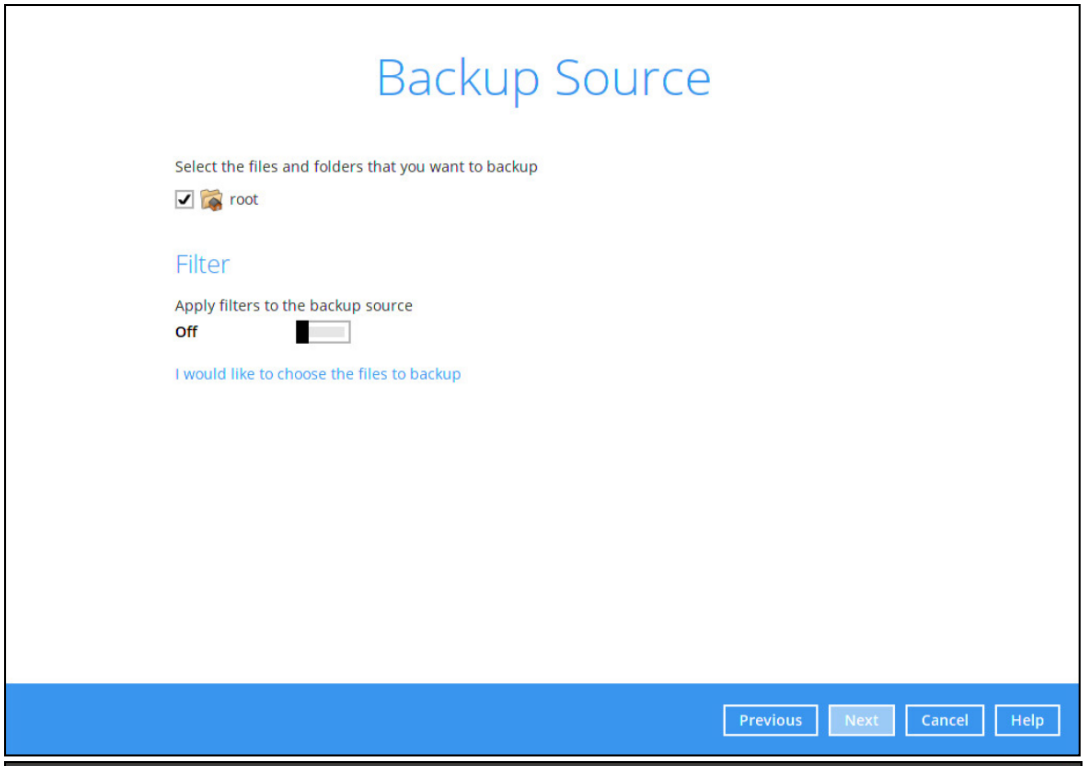
If root is selected, all files and/or folders located in **/root** is recommended to include these folders to exclude from the backup source using the Exclude Filter.

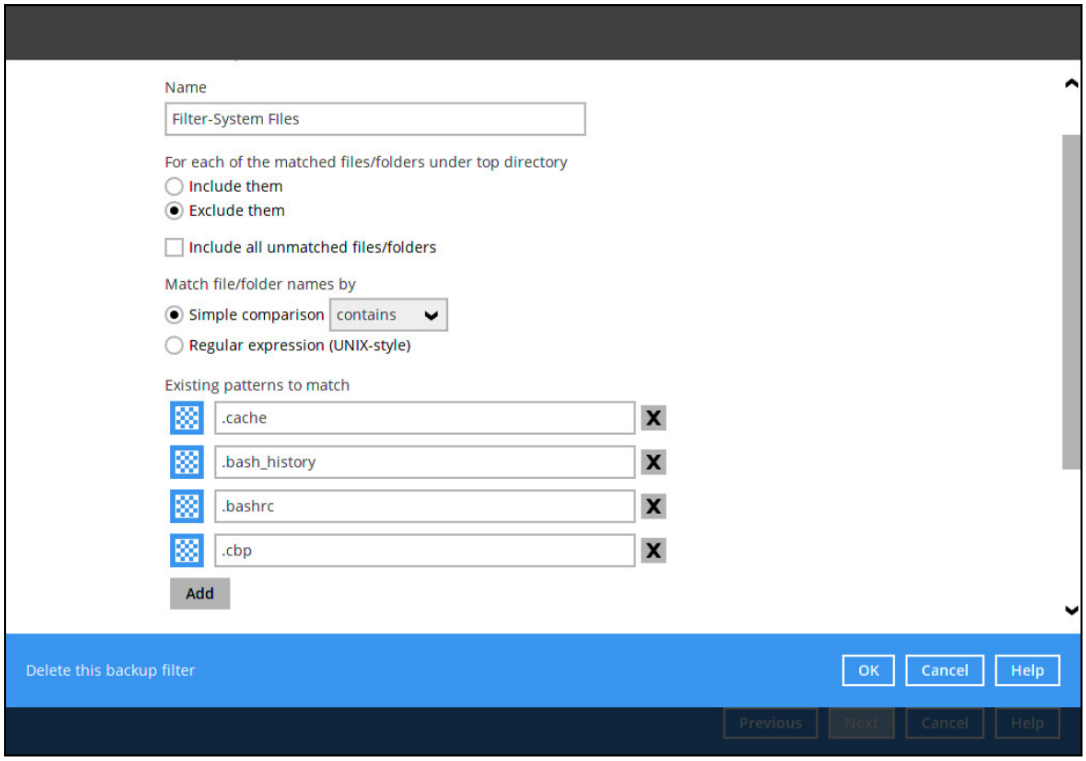
/root/.cache

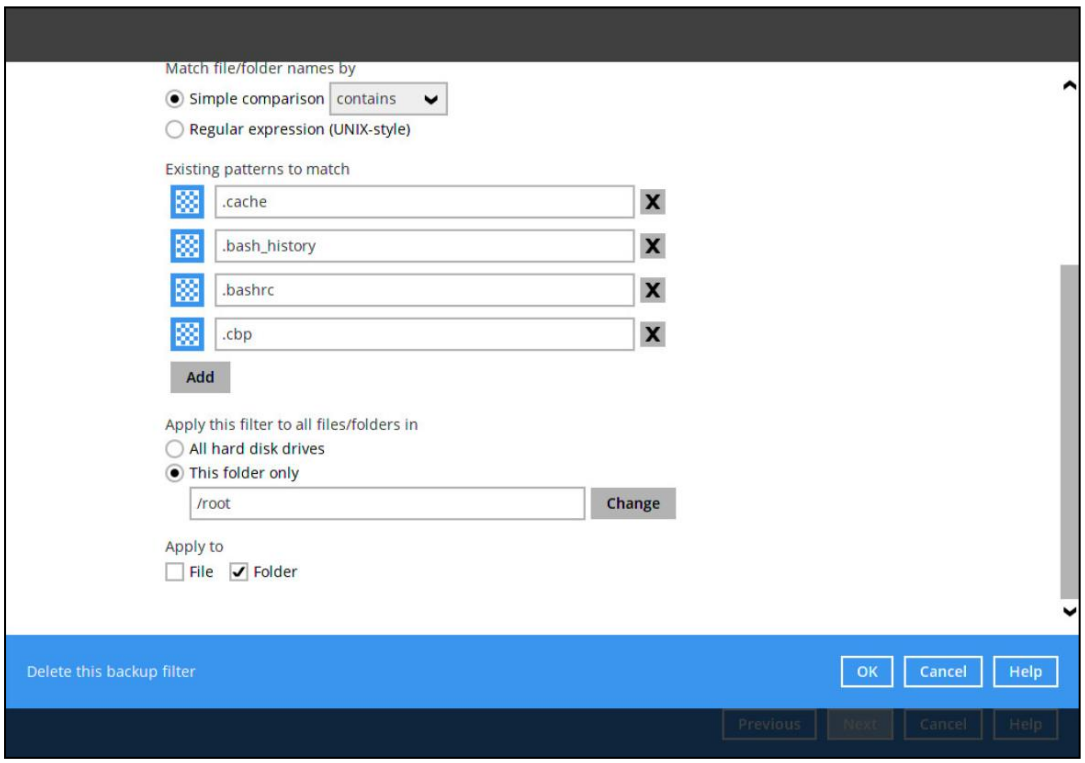
/root/.bash_history

/root/.bashrc

/root/.cbp

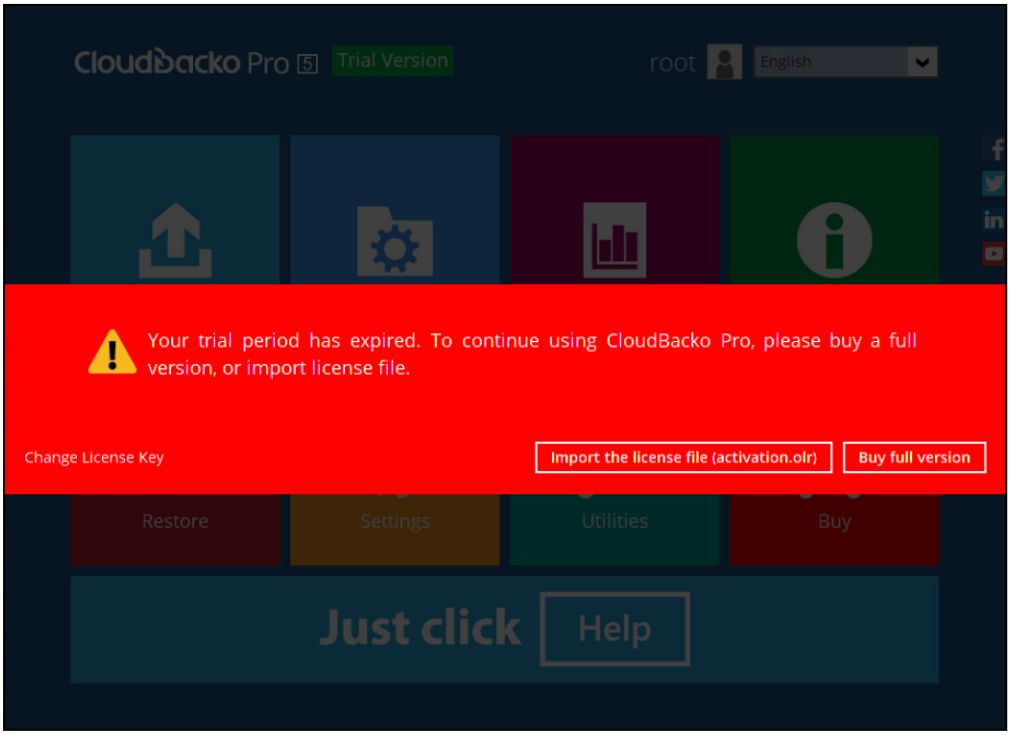




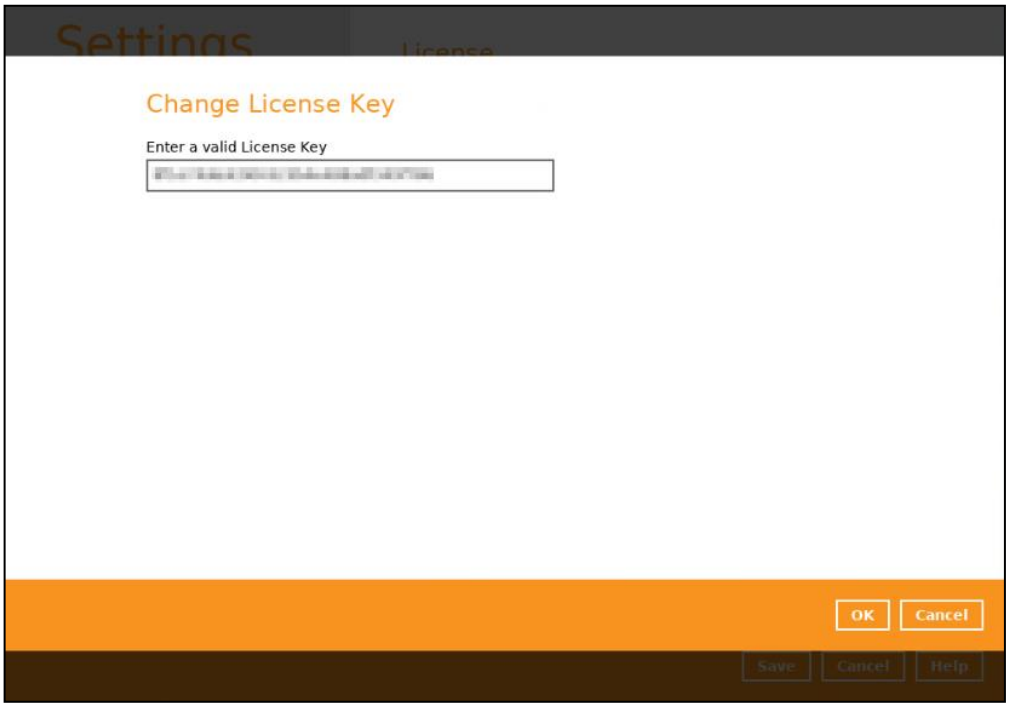

Match file/folder names by
Simple comparison
contains
Regular expression (UNIX-style)
Existing patterns to match
.cache
.bash_history
.bashrc
.cbp
Add
Apply this filter to all files/folders in
All hard disk drives
This folder only
/root
Change
Apply to
File
Folder
Delete this backup filter
OK
Cancel
Help
Previous
Next
Cancel
Help

Appendix I: How to apply a license key to a CloudBacko Pro installation with an expired trial license?

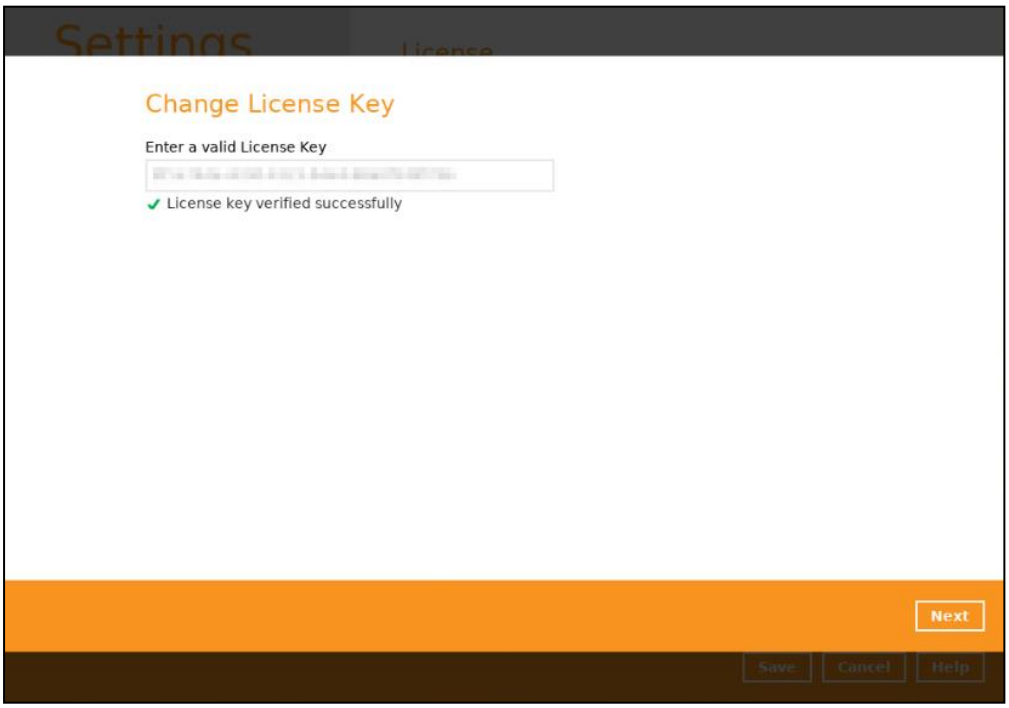
1. Open CloudBacko Pro and click on **Change License Key**.



2. Enter your new license key and click **OK** to continue.

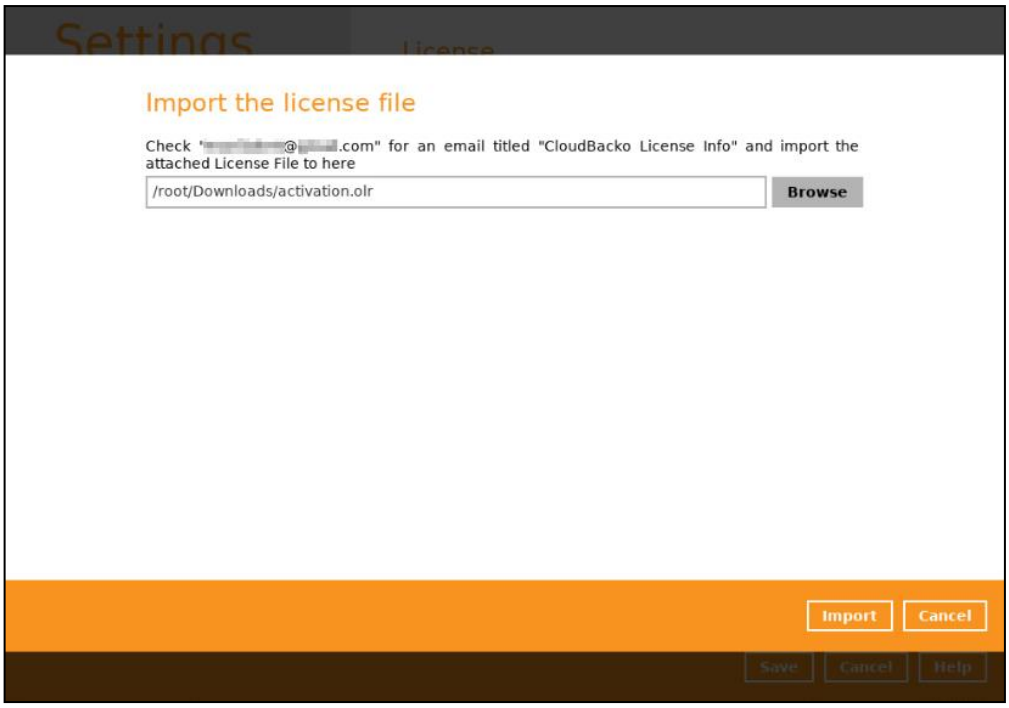


3. Once the new license key has been verified, click **Next** to continue.

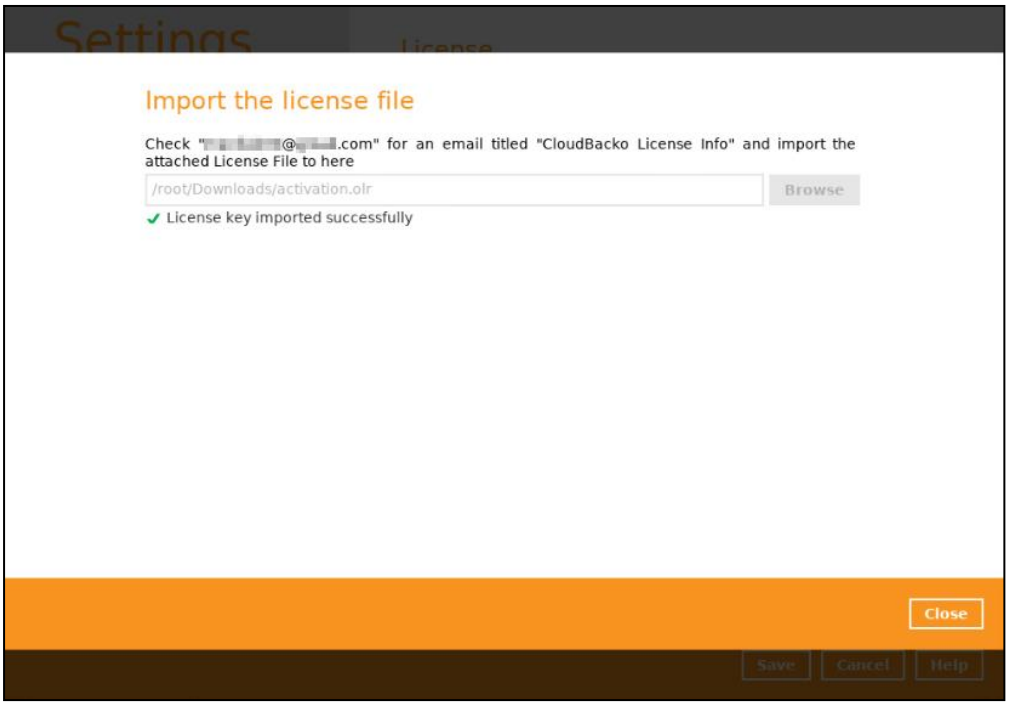


An activation file will be sent to the email address registered during the license purchase immediately containing the license activation file.

4. Copy the “activation.olr” file to the CloudBacko machine. Click **Browse** to locate the “activation.olr” file and click **Import** to continue.

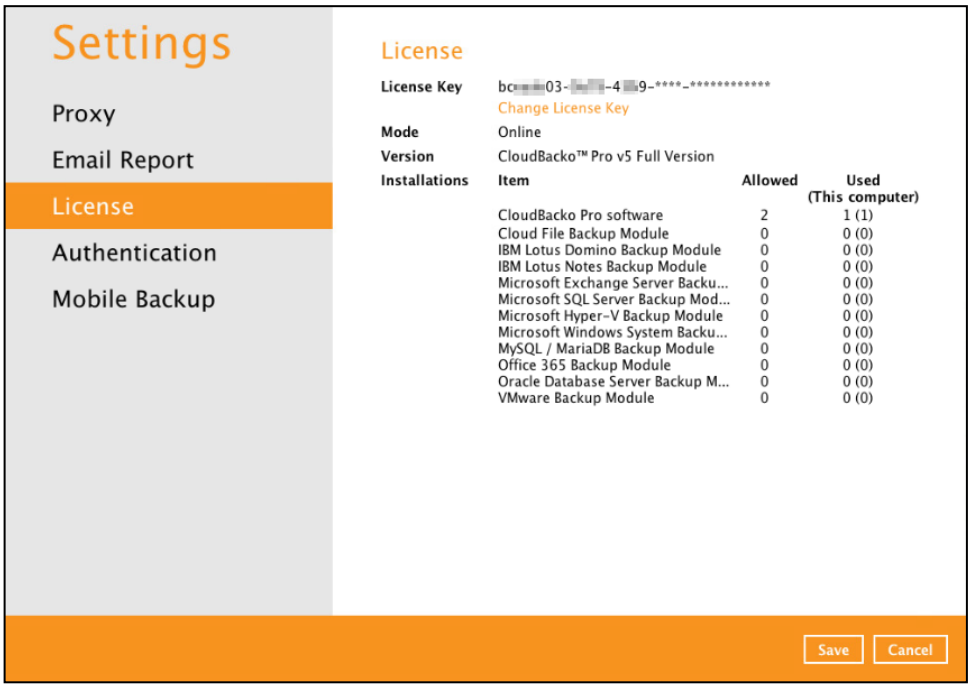


5. Your new license key has now been successfully imported to your CloudBacko Pro installation and is ready to use.

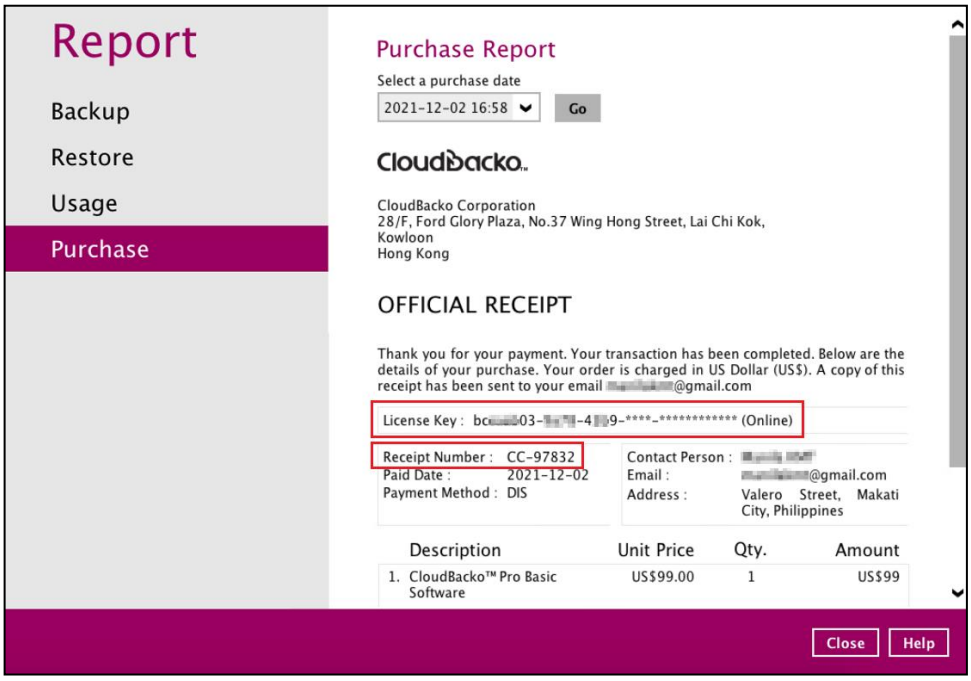


Appendix J: Where to find the CloudBacko Pro purchase license key?

1. Your CloudBacko Pro purchase license key is shown in the **Settings** > **License** page. For security reasons the CloudBacko Pro license key is only partially displayed on the application.

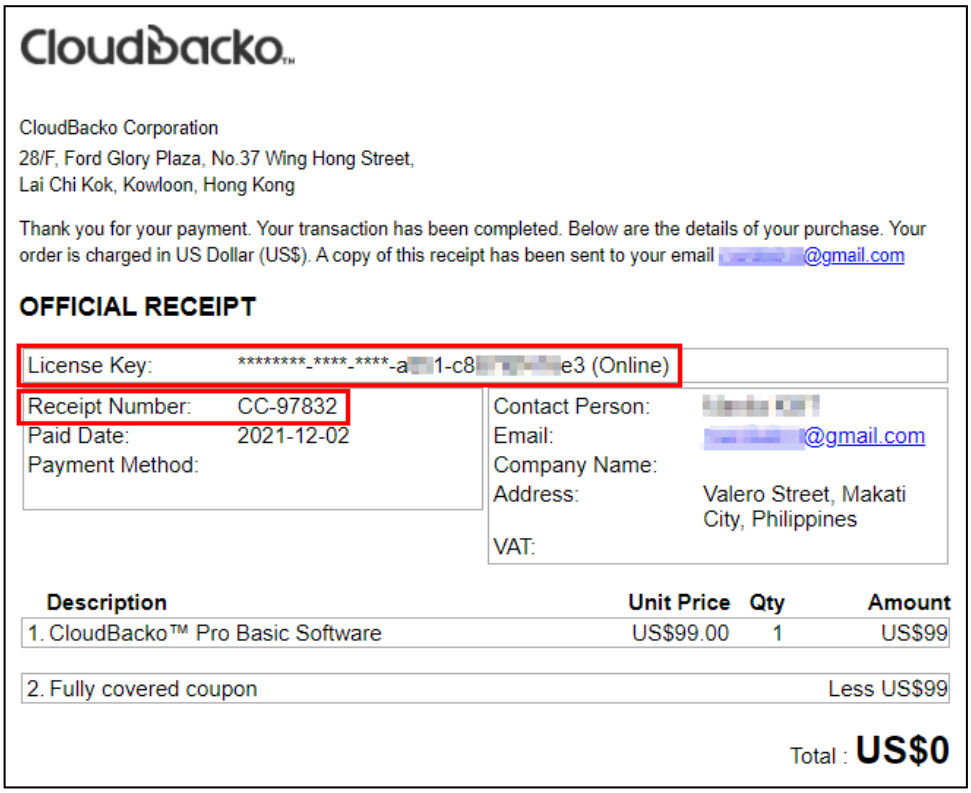


2. You can verify the license key displayed is our purchase key by comparing it with the details of the license key and receipt no. in CloudBacko Pro under the **Report** > **Purchase** page. It is recommended to print a copy of the receipt for your records (If there is no purchase record then current license key is an evaluation key).



3. The remaining part of the license key is email to you along with your official receipt at the time of purchase.

   Please print a copy of the receipt and keep it in a safe place along with a copy of the invoice. In case you have to re-install CloudBacko Pro on another machine.



CloudBacko™

CloudBacko Corporation
28/F, Ford Glory Plaza, No.37 Wing Hong Street,
Lai Chi Kok, Kowloon, Hong Kong

Thank you for your payment. Your transaction has been completed. Below are the details of your purchase. Your order is charged in US Dollar (US$). A copy of this receipt has been sent to your email [redacted]@gmail.com

OFFICIAL RECEIPT

License Key: ********-****-****-a[redacted]1-c8[redacted]e3 (Online)

Receipt Number: CC-97832
Paid Date: 2021-12-02
Payment Method:

Contact Person: [redacted]
Email: [redacted]@gmail.com
Company Name:
Address: Valero Street, Makati City, Philippines
VAT:

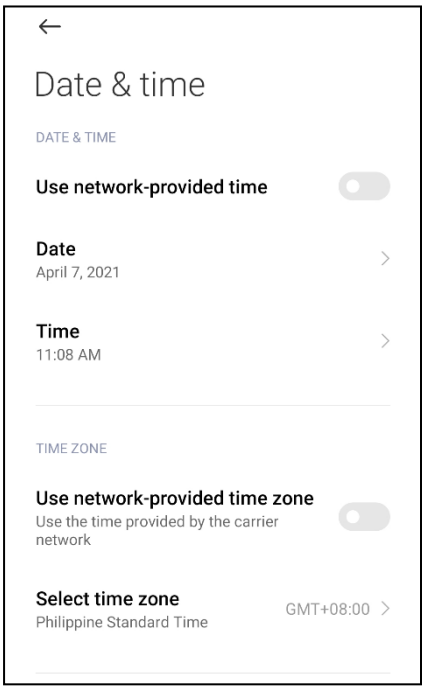
Description	Unit Price	Qty	Amount
1. CloudBacko™ Pro Basic Software	US$99.00	1	US$99
2. Fully covered coupon			Less US$99

Total : **US$0**

Appendix K: Different Date, Time, and Time zone with CloudBacko Pro machine and mobile device

1. Check the date, time, and time zone in mobile device.

   Example: Time zone settings of a mobile device used in the Philippines (time zone GMT+08:00).



2. Check the date, time, and time zone in CloudBacko Pro machine.

   Example: Time zone settings of a Linux machine used in the Philippines (time zone UTC+08:00). However, the set time zone in the CloudBacko Lite machine is set incorrectly in (Asia/Tokyo) JST+09:00.

```
[root@centos73 ~]# timedatectl
      Local time: Wed 2021-04-07 11:00:10 JST
  Universal time: Wed 2021-04-07 03:00:10 UTC
        RTC time: Wed 2021-04-07 03:00:58
       Time zone: Asia/Tokyo (JST, +0900)
     NTP enabled: no
NTP synchronized: no RTC in local TZ: no
      DST active: n/a
```

3. Stop the scheduler service.

```
[root@centos73 bin]# sh StopScheduler.sh
[root@centos73 bin]# ps -ef|grep java
root      8673  8612  0 11:06 pts/0    00:00:00 grep --color=auto java
```

4. Change the time zone in CloudBacko Pro, follow the command in red.

```
[root@centos73 ~]# timedatectl set-timezone Asia/Manila
```

5. Check the changed timezone in CloudBacko Pro, follow the command in red:

```
[root@centos73 ~]# timedatectl
      Local time: Wed 2021-04-07 11:10:15 +08
  Universal time: Wed 2021-04-07 03:10:15 UTC
        RTC time: Wed 2021-04-07 03:10:28
       Time zone: Asia/Manila (+08, +0800)
     NTP enabled: no
NTP synchronized: no RTC in local TZ: no
      DST active: n/a
```

6. Start the scheduler service.

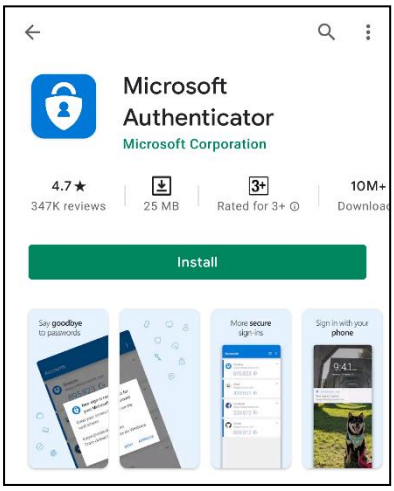
```
[root@centos73 bin]# sh Scheduler.sh
[root@centos73 bin]# ps -ef|grep java
root      8709     1 99 11:06 pts/0    00:00:03
/usr/local/cbp/jvm/bin/bschJW -Xms128m -Xmx768m -
Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=.:./LinX64 -cp
.:./cbs.jar cbs /usr/local/cbp
root      8730  8612  0 11:06 pts/0    00:00:00 grep --color=auto java
```

Appendix L: Example Registration of Time-base One-time Password (TOTP) Authenticator app in CloudBacko app

The following are examples of how to register a TOTP authenticator app in the CloudBacko app.

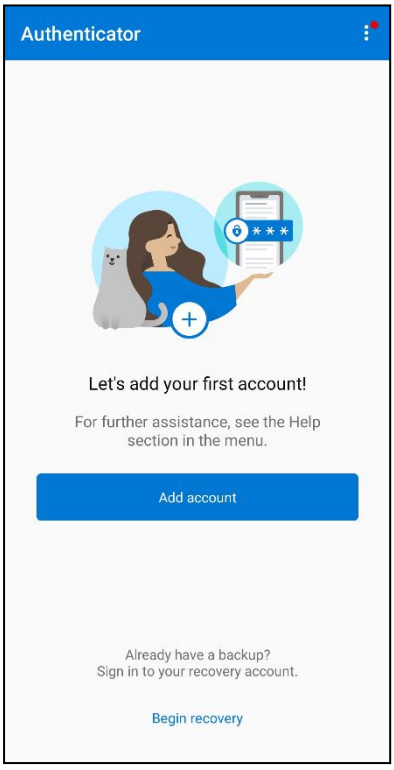
Microsoft Authenticator app

1. Download and install the Microsoft Authenticator from the Play Store for Android devices or the App Store for iOS devices.

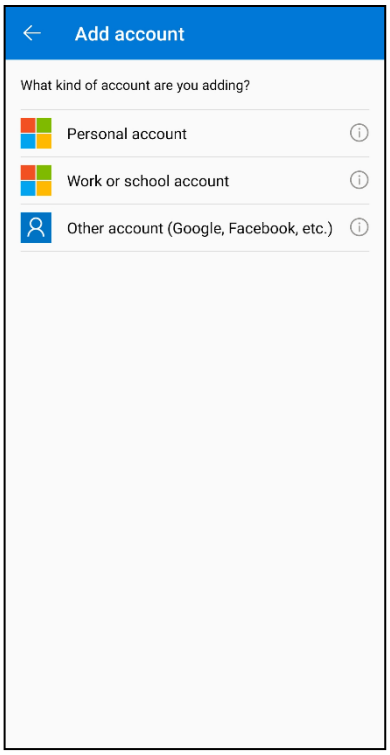


2. Launch the Microsoft Authenticator app.

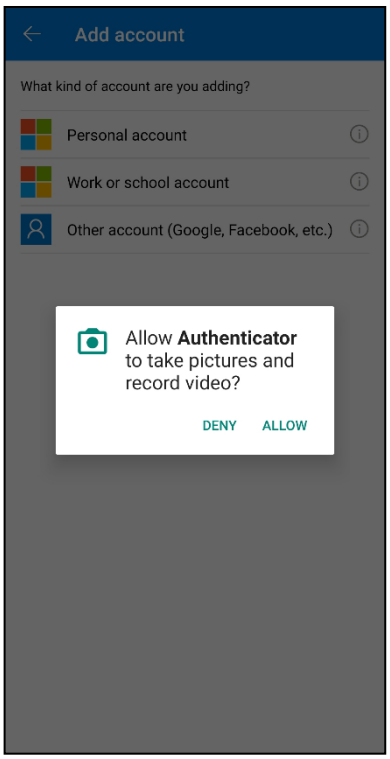
3. Tap **Add account**.



4. Select **Other account (Google, Facebook, etc.)**.



5. Allow permission to take pictures and record video.

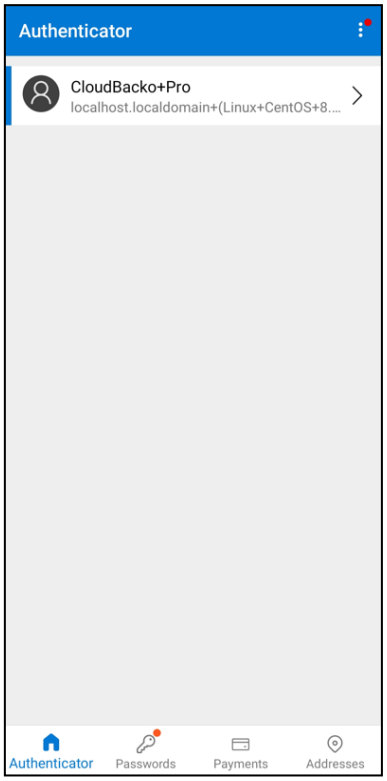


6. Setup the account. Select from the following methods: Scan the QR code or Enter a setup key.

   Method 1: Scan the QR code

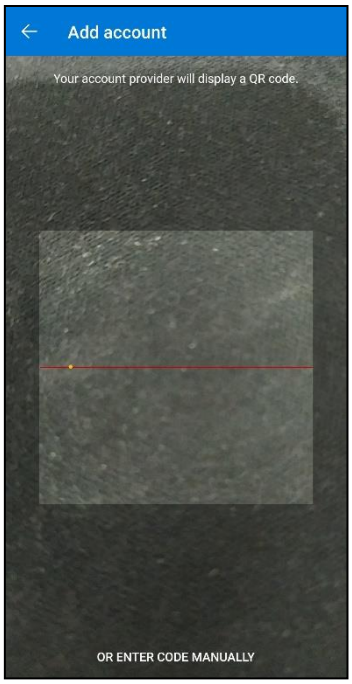
   i. Scan the QR code on CloudBacko Pro.

   ii. Account is successfully added to Microsoft Authenticator and registered the mobile device on CloudBacko Pro.

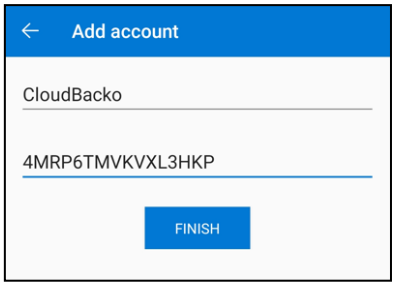


   Method 2: Enter Code Manually

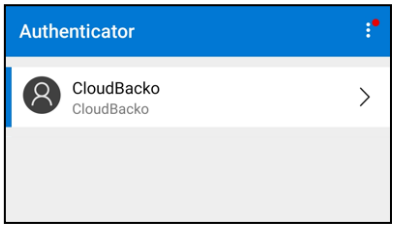
i. Tap **OR ENTER CODE MANUALLY**.



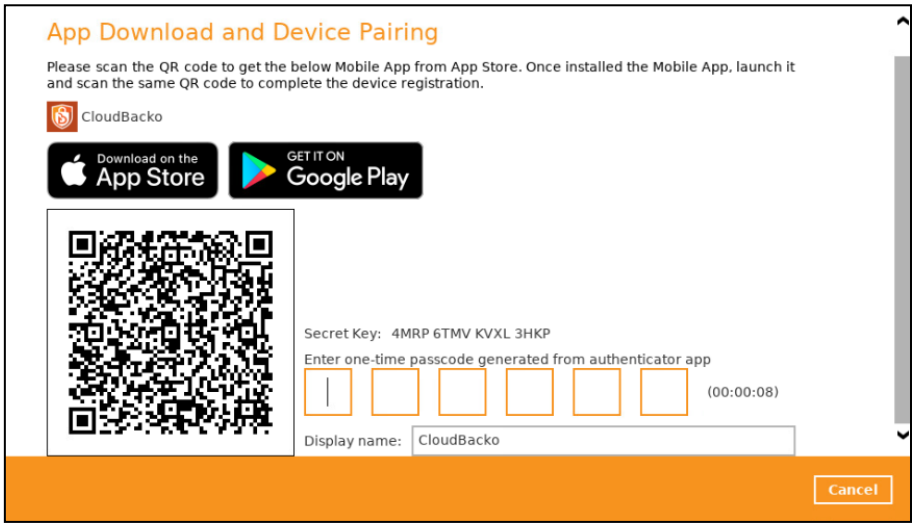
ii. Enter the account name and the key which is the Secret Key that is provided by CloudBacko Pro then tap **FINISH**.



iii. Account is successfully added to Microsoft Authenticator.



iv. In CloudBacko Pro, enter the display name and one-time password generated by the Microsoft Authenticator app.



7. Mobile device is successfully registered on CloudBacko Pro.