

Ahsay Online Backup Manager v8

Quick Start Guide for MacOS

Ahsay Systems Corporation Limited

30 April 2021

Copyright Notice

© 2021 Ahsay Systems Corporation Limited. All rights reserved.

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

This product includes software developed by the Apache Software Foundation (<https://www.apache.org/>).

Trademarks

Ahsay, Ahsay Cloud Backup Suite, Ahsay Online Backup Suite, Ahsay Offsite Backup Server, Ahsay Online Backup Manager, Ahsay A-Click Backup, Ahsay Replication Server, Ahsay BackupBox Firmware, Ahsay Universal Backup System and Ahsay NAS Client Utility, Ahsay Mobile are trademarks of Ahsay Systems Corporation Limited.

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 Office 365 are registered trademarks of Microsoft Corporation.

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

Oracle 11g, Oracle 12c, Oracle 18c, Oracle 19c, and MySQL are registered trademarks of Oracle Corporation.

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.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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

Disclaimer

Ahsay Systems Corporation Limited 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 Ahsay Systems Corporation Limited without prior notice to you.

Revision History

Date	Descriptions	Type of modification
25 January 2021	Updated Ch. 1.2 System Architecture; Added Ch. 1.3 Mobile Backup Server (MBS); Added Ch. 1.4 Two-Factor Authentication; Added Ch. 2.1 Requirements for Ahsay Mobile app; Added Ch. 3.5 Two-Factor Authentication Requirements; Added Ch. 3.6 Mobile Backup Requirements; Updated Ch 5.3 AhsayOBM Services; Added Ch. 5.5 Mobile Backup Server (MBS) Health Check and Ahsay Mobile app Connection Check; Added Ch. 6.1 Login to AhsayOBM without 2FA; Added Ch. 6.2 Login to AhsayOBM with 2FA using Android or iOS mobile device; Added Ch. 6.3 Login to AhsayOBM with 2FA using Twilio; Updated Ch. 7.1 Profile; Updated Ch. 7.1.5 Password; Updated Ch. 7.1.6 Authentication; Updated Ch. 7.1.7 Mobile Backup; Updated Ch. 7.1.8 Security Settings; Updated Ch. 7.3 Language; Added Ch. 13 Mobile Backup and Restore to AhsayOBM and Predefined Destinations; Added Appendix E: Example Registration of Time-base One-time Password (TOTP) Authenticator app in Ahsay Mobile app;	New / Modifications
29 January 2021	Updated Ch. 6.3.1, 6.3.2, and 6.3.3;	Modifications
25 March 2021	Updated Ch. 6.3 and Ch. 9;	Modifications
7 April 2021	Updated Ch. 9; added sub-chapters for the detailed process diagrams in Ch. 9.1, 9.2, 9.2.1, 9.2.2 and 9.3	Modifications
30 April 2021	Added new diagrams for the detailed process of Data Integrity Check (DIC) and updated screenshots for the Rebuild index option in Ch. 7.9.1; Updated description of Space Freeing Up in Ch. 7.9.2; Updated description of Delete Backup Data in Ch. 7.9.3; Added notes for Periodic Data Integrity Check (PDIC) in Ch. 9.1	New / Modifications

Table of Contents

1	Overview	1
1.1	What is this software?	1
1.2	System Architecture	1
1.3	Mobile Backup Server	2
1.4	Two-Factor Authentication	5
2	Requirements for Ahsay Mobile	7
2.1	Backup Software Version Requirement	7
2.2	Network Connection	7
2.3	Android and iOS Version Requirement	7
3	Requirements for AhsayOBM on MacOS	8
3.1	Hardware Requirements	8
3.2	Software Requirements	8
3.3	Full Disk Access Permission	8
3.4	Installation on Root Drive	8
3.5	Two-Factor Authentication Requirements	8
3.6	Mobile Backup Requirements	9
3.1	Firewall Settings	9
3.7	Limitations	9
3.8	Best Practices and Recommendations	9
4	Get Started with AhsayOBM	11
5	Download and Install AhsayOBM	12
5.1	Download AhsayOBM	13
5.2	Install AhsayOBM	14
5.2.1	Option 1: Online Installation Option	14
5.2.2	Option 2: Offline Installation Option	18
5.3	AhsayOBM Services	22
5.3.1	Option 1: Stop and Start	24
5.3.2	Option 2: Stop and Start	24
5.4	RunLevel Symlink Check	25
5.5	Mobile Backup Server (MBS) Status Check and Ahsay Mobile app Connection Check	26
6	Start AhsayOBM	29
6.1	Add an AhsayOBM Shortcut Icon to the Desktop	29
6.2	Login to AhsayOBM without 2FA	30

6.2.1	Initial login to AhsayOBM with no 2FA and no Mobile Add-on Module	30
6.2.2	Initial login to AhsayOBM with no 2FA and with Mobile Add-on Module ..	32
6.2.3	Subsequent login to AhsayOBM with no 2FA.....	40
6.3	Login to AhsayOBM with 2FA using Android or iOS mobile device	41
6.3.1	Initial login to AhsayOBM with 2FA and with no Mobile Add-on Module..	41
6.3.2	Initial login to AhsayOBM with 2FA and with Mobile Add-on Module.....	49
6.3.3	Subsequent login to AhsayOBM with 2FA.....	54
6.4	Login to AhsayOBM with 2FA using Twilio	58
7	AhsayOBM Overview.....	60
7.1	Profile	61
7.1.1	General.....	61
7.1.2	Contacts	63
7.1.3	Time Zone	65
7.1.4	Encryption Recovery.....	66
7.1.5	Password.....	67
7.1.6	Authentication.....	69
7.1.7	Mobile Backup	78
7.1.8	Security Settings.....	80
7.2	Language.....	82
7.3	Information.....	82
7.4	Backup.....	83
7.5	Backup Sets	83
	Backup Set Settings.....	83
7.6	Report.....	124
7.6.1	Backup	124
7.6.2	Restore.....	127
7.7	Restore	128
7.8	Settings.....	130
7.9	Utilities	130
7.9.1	Data Integrity Check	131
7.9.2	Space Freeing Up.....	147
7.9.3	Delete Backup Data.....	150
7.9.4	Decrypt Backup Data.....	156
8	Create a Backup Set	157
9	Overview on Backup Process.....	165
9.1	Periodic Data Integrity Check Process	166
9.2	Backup Set Index Handling Process	168

9.2.1 Start Backup Job	168
9.2.2 Completed Backup Job.....	169
9.3 Data Validation Check Process.....	170
10 Run Backup Jobs	171
10.1 Login to AhsayOBM	171
10.2 Start a Manual Backup.....	171
11 Restore Data.....	174
11.1 Login to AhsayOBM	174
11.2 Restore Data.....	174
11.3 Restore Filter	181
12 Mobile Backup and Restore to AhsayCBS and Predefined Destination ...	186
12.1 Create a File Backup Set	186
12.2 Run a Backup Job	195
12.3 Restore Data.....	198
12.3.1 Original Location.....	199
12.3.2 Alternate Location.....	206
13 Contact Ahsay.....	216
13.1 Technical Assistance	216
13.2 Documentation.....	216
Appendix.....	217
Appendix A: Uninstall AhsayOBM	217
Appendix B: Example Scenarios for Restore Filter	219
Appendix C: Setting up Full Disk Access Permission	227
Appendix D: Example Registration of Time-based One-Time Password (TOTP)	
Authenticator app in Ahsay Mobile app	231

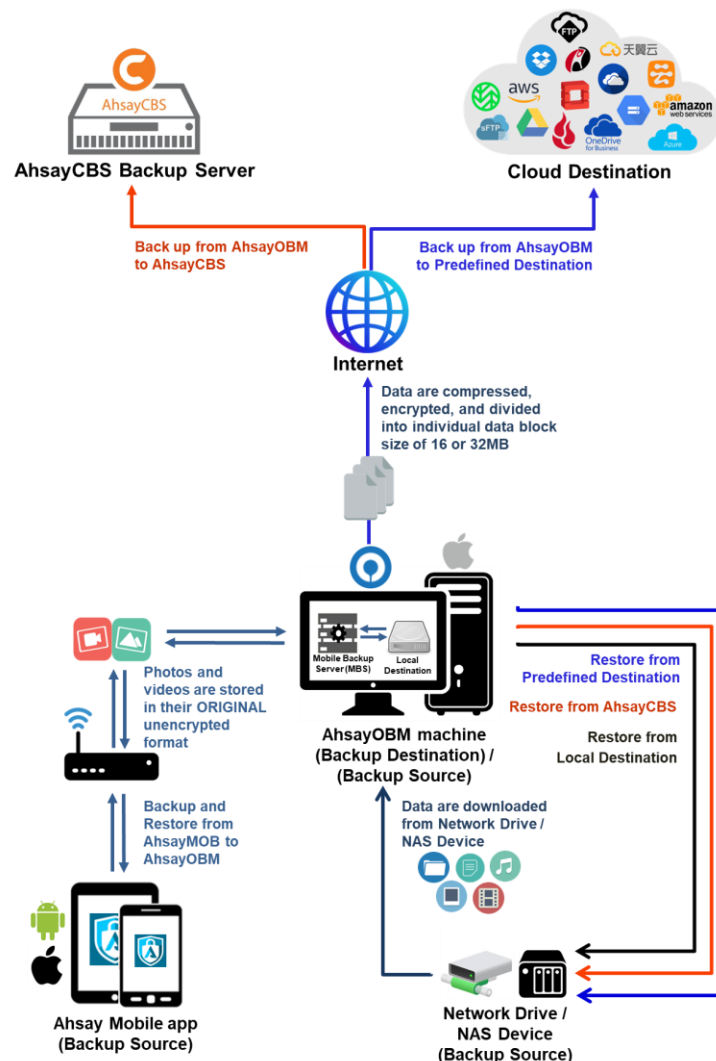
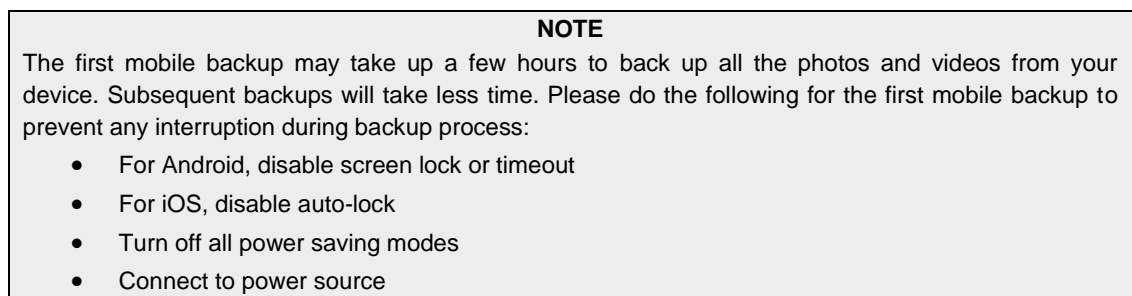
1 Overview

1.1 What is this software?

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

1.2 System Architecture

Below is the system architecture diagram illustrating the major elements involved in the backup process among the backup machine AhsayOBM, Ahsay Mobile app and AhsayCBS.



1.3 Mobile Backup Server

Starting with AhsayOBM v8.5.0.0, the Mobile Backup Server (MBS) will be utilized to handle mobile backup and restore of Ahsay Mobile app. It is an integral part of AhsayOBM.

System Diagram

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


The MBS will use the following port ranges, **TCP Port:** 54000 to 54099, **UDP Port:** 54200 to 54299, **Protocol:** Http, for the request of Ahsay Mobile app.


The default TCP and UDP ports are **54000** and **54200**, 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 AhsayOBM when pairing a mobile device for mobile backup.

Mobile Backup Setup

Please scan the QR code to register your mobile device with your backup account for following feature:

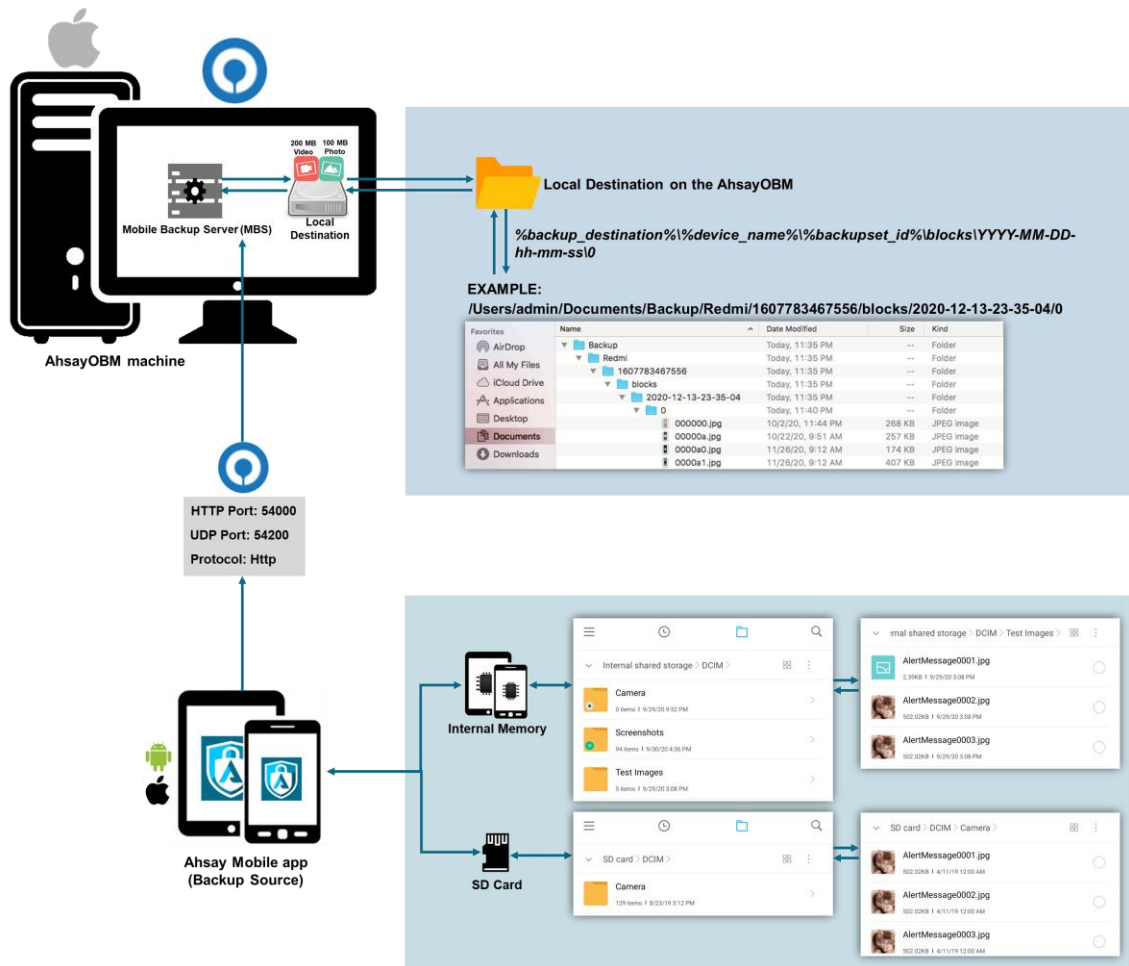
 Mobile Backup



Please make sure below 2 ports are not blocked by any Firewall settings before pairing your mobile device for backup

TCP Port: 54000
UDP Port: 54200

Photos and videos are stored either in mobile device's internal memory or SD Card. These are selected as backup source using the Ahsay Mobile app and will be backed up to the local destination of a Ahsay 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.

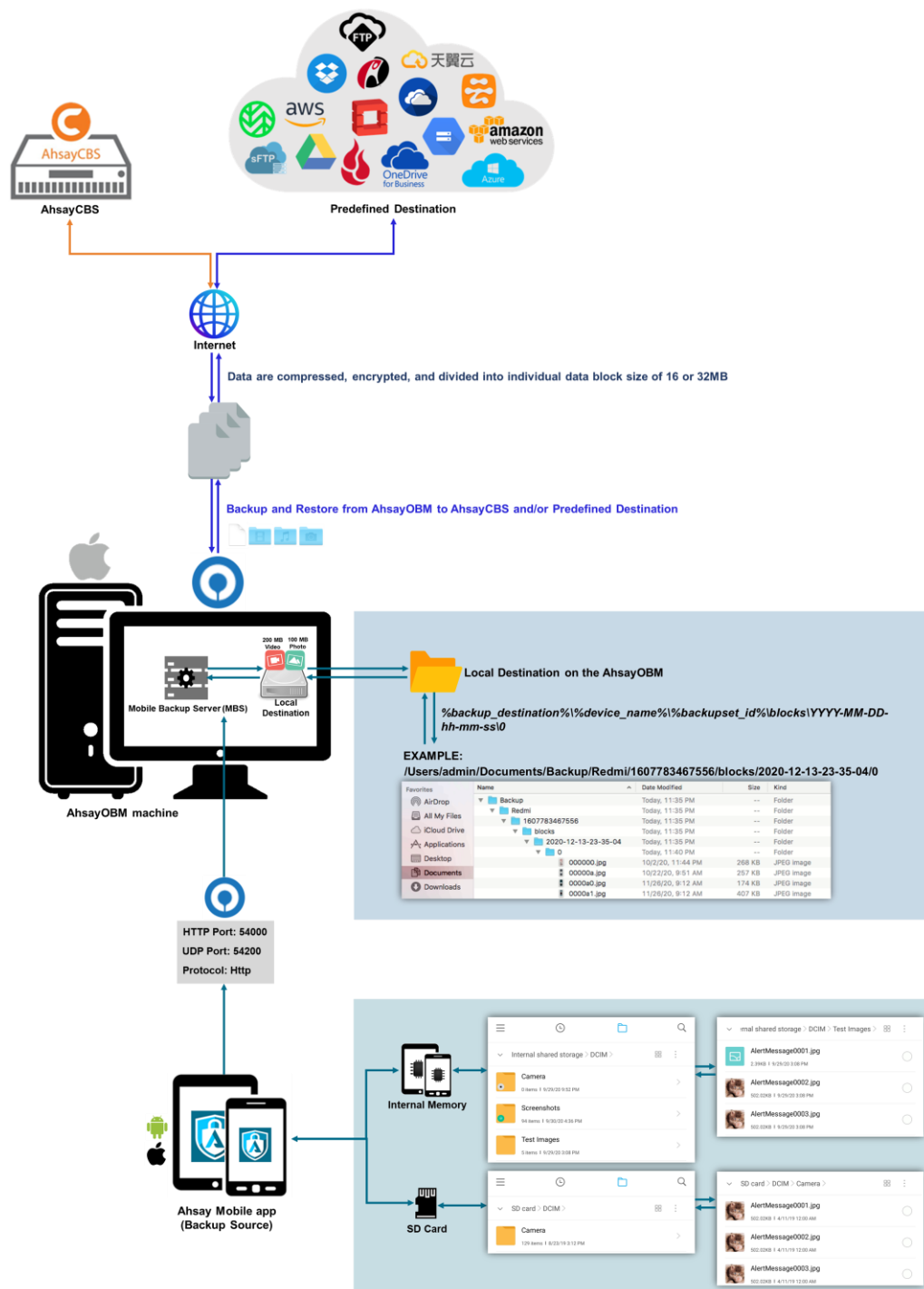


If storage of photos and videos to a predefined destination is required, then this can be done using AhsayOBM to perform a secondary backup and restore of the photos and videos on the local drive to the predefined destination.

To backup and restore photos and/or videos from the Ahsay Mobile app to AhsayOBM then AhsayCBS and/or Predefined Destination is a two-step process.

1st: Backup of photos and/or videos from Ahsay Mobile app to AhsayOBM local destination.

2nd: Create a File backup set using AhsayOBM, using the local backup destination as the backup source, and then backup this backup set to AhsayCBS and/or Predefined Destination.

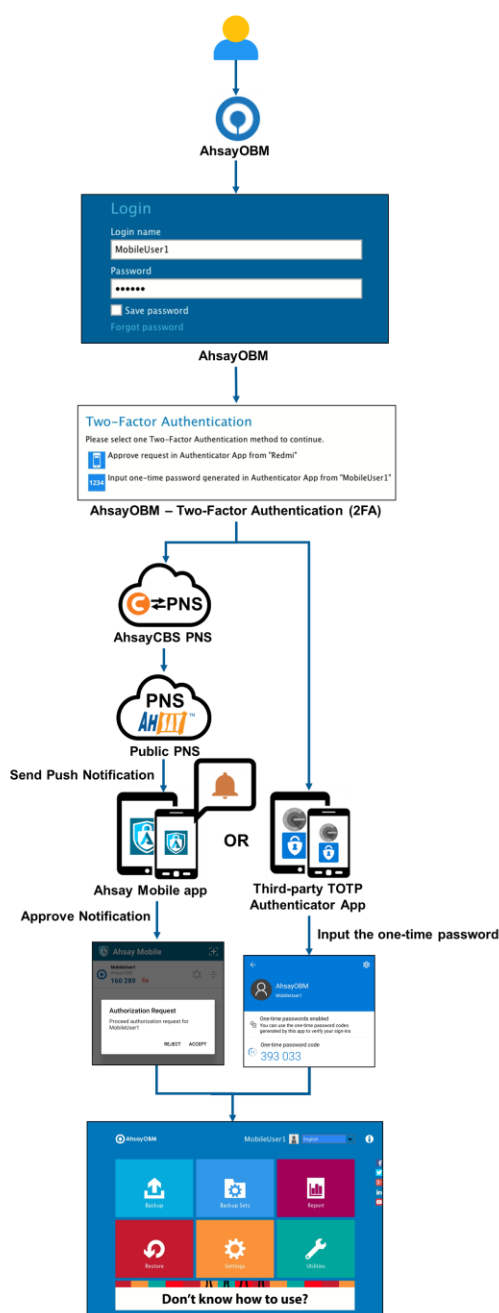


1.4 Two-Factor Authentication

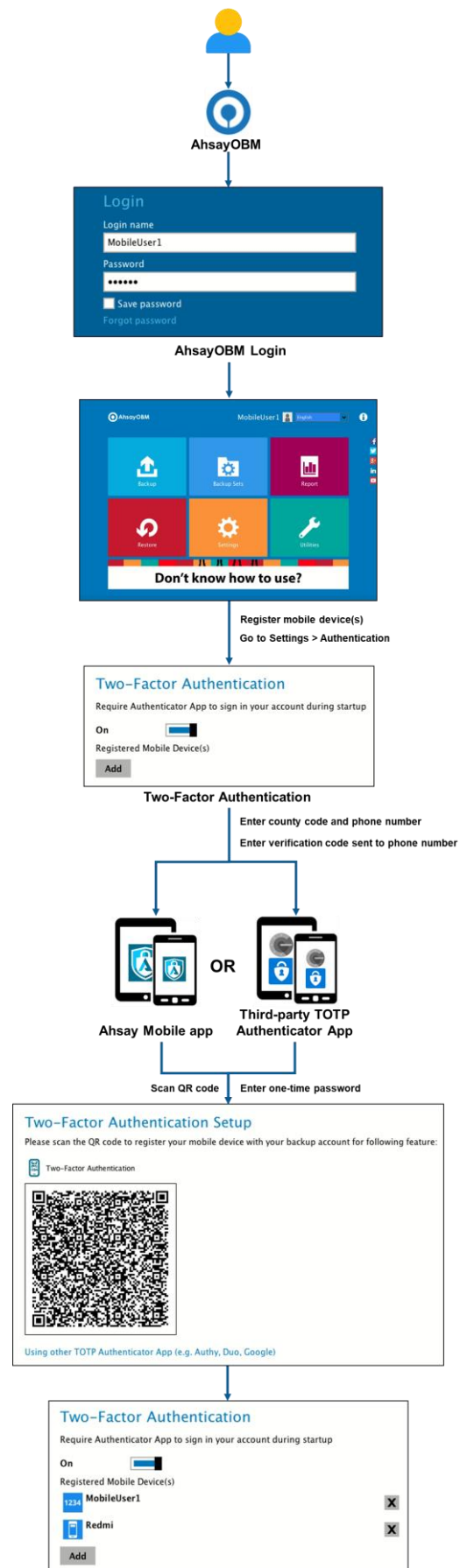
New two-factor authentication implemented on AhsayOBM v8.5.0.0 onwards, to include support for TOTP (Time-based One-time Password) and Push notification authentication using the Ahsay Mobile app to provide additional security for the user login process. Since aside from logging in with just a username and password, if two-factor authentication is enabled for the account, there will be an added step that is needed to be able to login.

Upon initial login to AhsayOBM, you will have an option to setup two-factor authentication or skip the setup and do it later. If you continue the setup of two-factor authentication, it will be automatically enabled for your account. Several mobile devices may be added for authentication.

For logins with two-factor authentication enabled, you will be asked to select the method that you would like to use. This depends on the authenticator app used, you will either accept the login request in the Ahsay Mobile app or enter a one-time password generated in the third-party TOTP authenticator app such as Google Authenticator, Microsoft Authenticator, LastPass etc.



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



2 Requirements for Ahsay Mobile

2.1 Backup Software Version Requirement

- Download and install the latest version of AhsayOBM v8.5.0.0 or above.
- Download and install the latest version of Ahsay Mobile app on the Play Store for android mobile devices and on the App Store for iOS mobile devices.

2.2 Network Connection

Ensure that the Ahsay Mobile app is connected to the same local network as the AhsayOBM machine. Failure to do so will prevent you from performing backup and/or restore.

2.3 Android and iOS Version Requirement

- For android device, android version must be 8 or above.
- For apple device, iOS version must be 12.0.0 or above.

3 Requirements for AhsayOBM on MacOS

3.1 Hardware Requirements

Refer to the link below for details of the minimum and recommended requirements for installing AhsayOBM:

[FAQ: Ahsay Hardware Requirement List \(HRL\) for version 8.1 or above](#)

3.2 Software Requirements

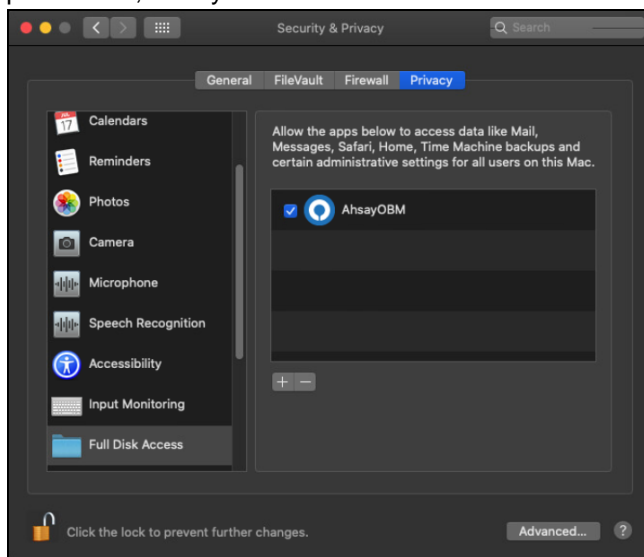
Refer to the following link for details of the operating systems, applications and databases supported by AhsayOBM:

[FAQ: Ahsay Software Compatibility List \(SCL\) for version 8.1 or above](#)

3.3 Full Disk Access Permission

MacOS 10.15 or higher "Full Disk Access" permission needs to be granted in, **System Preferences > Security & Privacy > Privacy tab to AhsayOBM**

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



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

3.4 Installation on Root Drive

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

3.5 Two-Factor Authentication Requirements

Please refer to the [Ahsay Mobile App User Guide for Android and iOS – Chapter 2.4](#) for details of the minimum and recommended requirements for using Two-Factor Authentication on Ahsay Mobile app.

3.6 Mobile Backup Requirements

Please refer to the [Ahsay Mobile App User Guide for Android and iOS – Chapter 2.5](#) for details of the minimum and recommended requirements for installing the Ahsay Mobile app.

3.1 Firewall Settings

Make sure that your firewall settings allows network traffic through the following domain and/or ports:

- For AhsayOBM to function correctly must allow outbound connections to *.ahsay.com via port 80 and 443.
- For mobile backup inbound / outbound network traffic must be allowed through the following default ports: HTTP port: 54000 and UDP port: 54200.

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

3.7 Limitations

- Resource Fork Files – Resource fork files cannot be restored with AhsayOBM installation on Mac OS 10.8 above.
- Case-Insensitive File System – For volume with a case-insensitive file system, target file of a symbolic link will be backed up twice (in both upper case and in lower case), hence, doubling the backup quota storage requirement.

3.8 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 back up.

- 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.

4 Get Started with AhsayOBM

This quick start guide will walk you through the following 6 major parts to get you started with using AhsayOBM.

Download and Install

Download and Install
AhsayOBM on your Mac

Launch the App

Launch and log in to AhsayOBM

Setup 2FA and/or Mobile Backup

Register mobile device for 2FA and/or
mobile backup (optional)

Create File Backup Set

Create backup set according to
your preferences

Run Backup Jobs

Run the backup jobs to back up
data

Restore Data

Restore backed up data to your
system

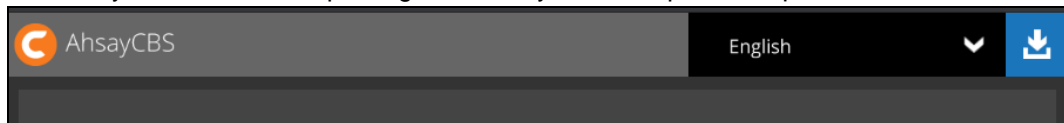
5 Download and Install AhsayOBM

There are two installation modes of AhsayOBM, online installation and offline installation. Below is the table of comparison between online installation and offline installation.

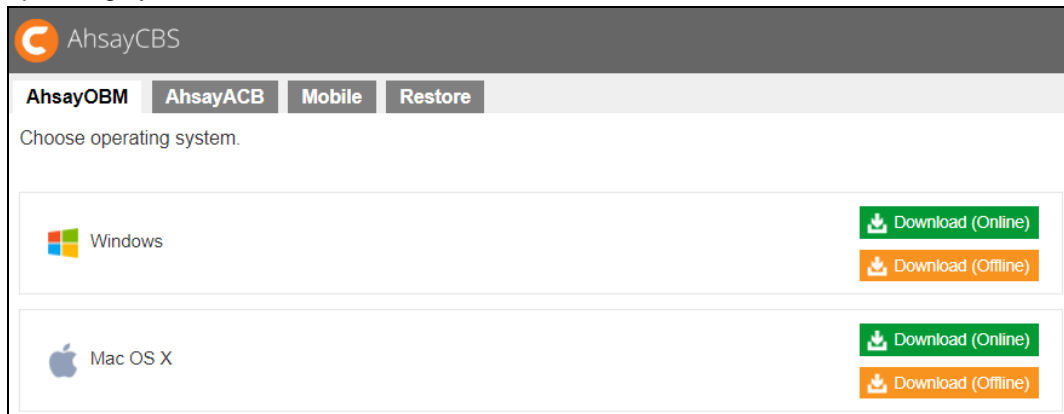
	Online Installation	Offline Installation
Installation Time	<ul style="list-style-type: none">➤ Takes more time as it needs to download the binary and component files (80MB to 132MB depending on operating system) each time the installation is run.➤ Online installer size is 6KB to 3.5MB depending on operating system as it contains only the initial installation package files.	<ul style="list-style-type: none">➤ Takes less time as all the necessary binary and component files are already available in the offline installer and offline installer can be downloaded once but reused many times.➤ Offline installer size is 50MB to 195MB depending on operating system as it contains all the necessary binary and component files.
Deployments	<ul style="list-style-type: none">➤ Suitable for single or small amount of device installations.➤ Suitable for sites with fast and stable internet connection as internet connection is needed each time when an installation is run.➤ A slow internet connection will result in longer installation time and interrupted, or unstable internet connection may lead to unsuccessful installation.➤ Ensures the latest version of the product is installed.	<ul style="list-style-type: none">➤ Suitable for multiple or mass device installations.➤ Suitable for client sites with metered internet connections as once the offline installer is downloaded, internet connection is not needed each time when an installation is run.➤ May need to update the product version after installation if an older offline installer is used.

5.1 Download AhsayOBM

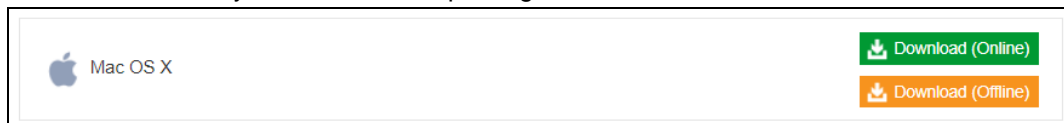
1. In a web browser, click the blue icon on the top right corner to open the download page for the AhsayOBM installation package file from your backup service provider's website.



2. In the **AhsayOBM** tab of the download page, you can choose the AhsayOBM installer by operating system.



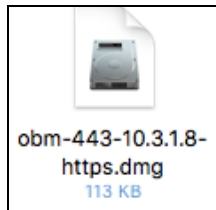
3. In the **Mac OS** section, click on the **Download (Online)** or **Download (Offline)** button to download the AhsayOBM installation package.



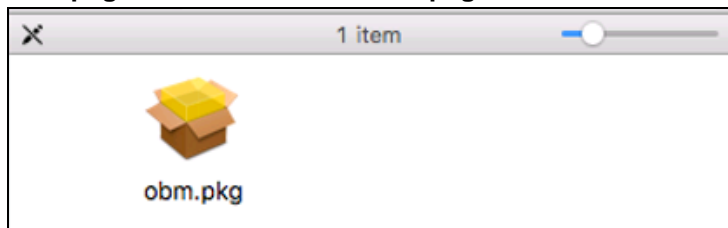
5.2 Install AhsayOBM

5.2.1 Option 1: Online Installation Option

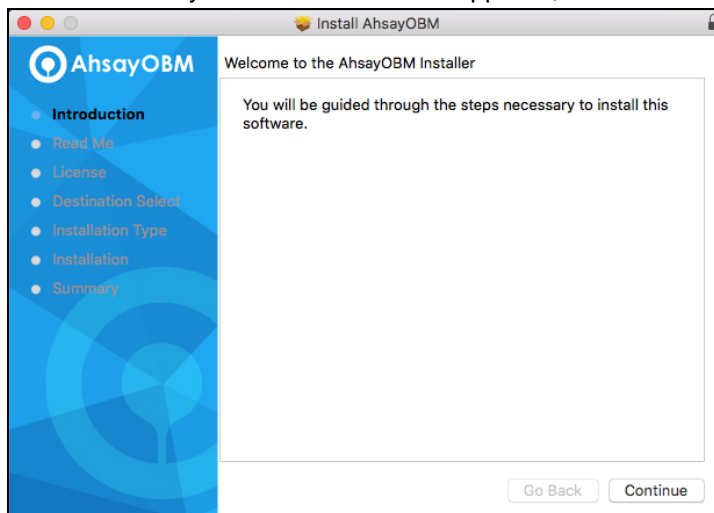
1. Double-click the icon of the AhsayOBM installation package **.dmg** file you have downloaded.



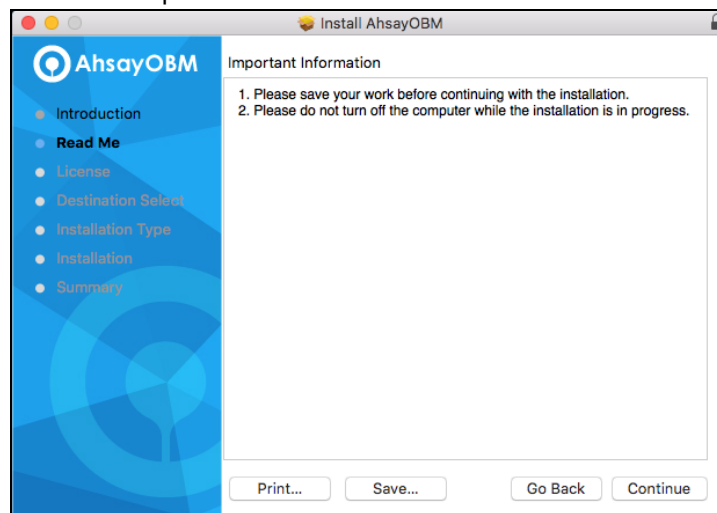
2. The Ahsay Online Backup Manager window will appear. You will see another file named **obm.pkg**. Double click on the **obm.pkg** file.




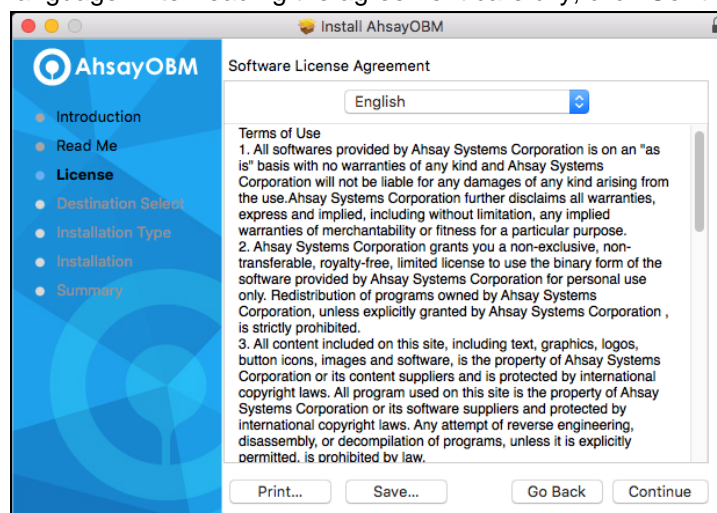
3. When the AhsayOBM Installer wizard appears, click **Continue** to proceed.



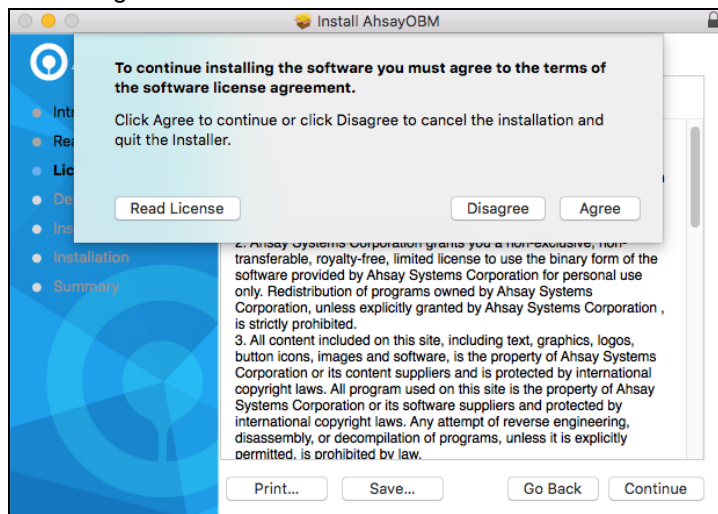
4. When the Important Information screen appears, read the information and then click **Continue** to proceed.



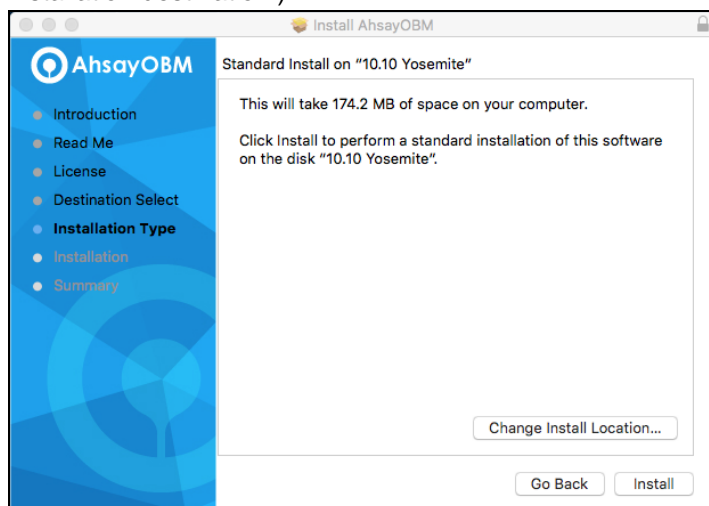
5. When the Software License Agreement appears, the agreement content will be displayed in English by default. If you prefer to read it in a different language, click  to change the language. After reading the agreement carefully, click **Continue** to proceed.



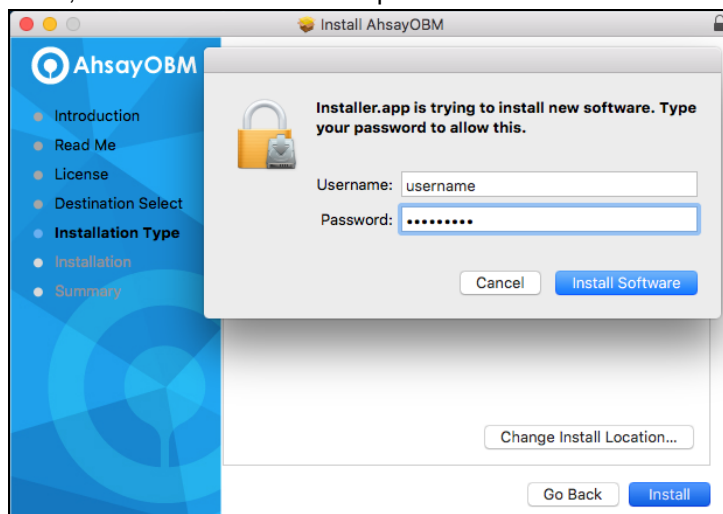
6. The following message will appear in a pop-up window. Click **Agree** to accept the software license agreement.



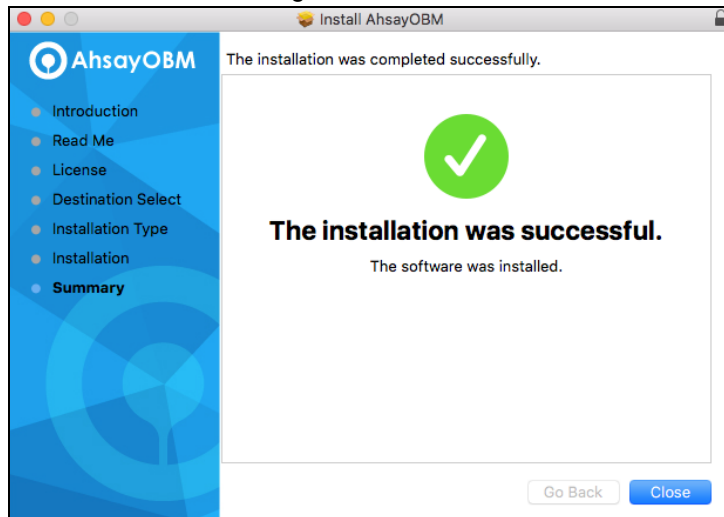
7. Click **Install** to start installing AhsayOBM to the default location, i.e. "10.10 Yosemite" in this example. (Alternatively, you can click **Change Install Location...** to choose a different installation destination.)



8. The following message will appear in a pop-up window. Enter your Mac OS login credentials. Then, click **Install Software** to proceed with the installation.



9. You will see the following screen when the installation of AhsayOBM is completed.



5.2.2 Option 2: Offline Installation Option

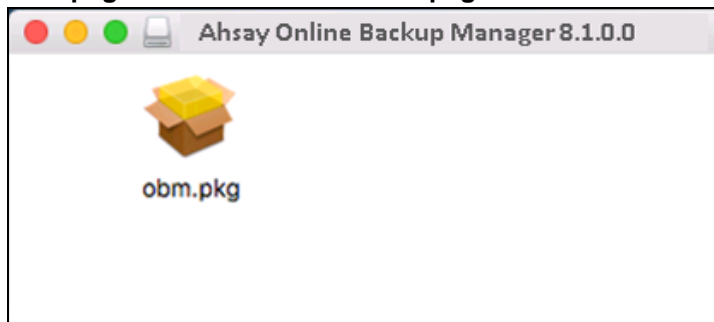
1. Double-click the icon of the AhsayOBM installation package **.gz** file you have downloaded to expand it.



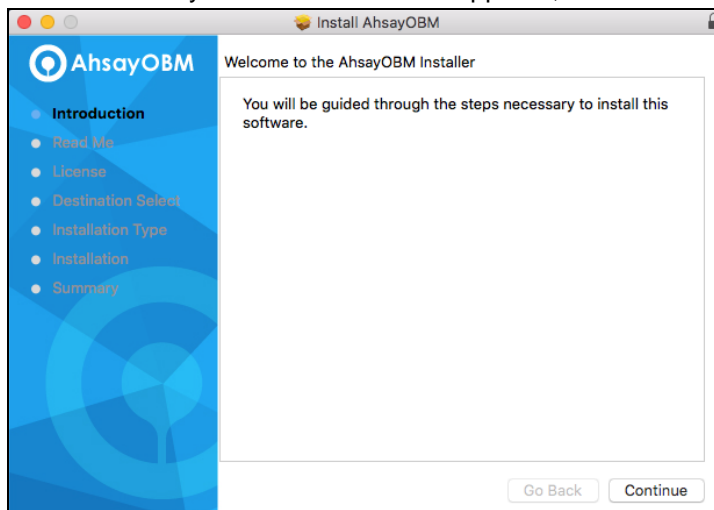
2. Double-click the icon of the AhsayOBM installation package **.dmg** file you have expanded.



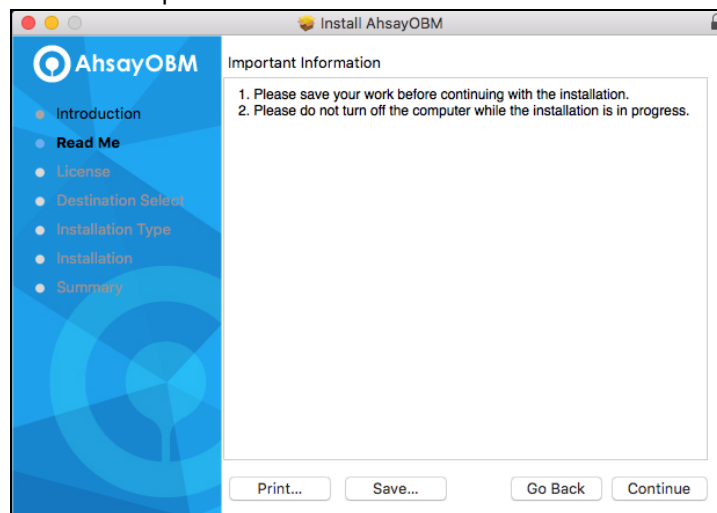
3. The Ahsay Online Backup Manager window will appear. You will see another file named **obm.pkg**. Double click on the **obm.pkg** file.




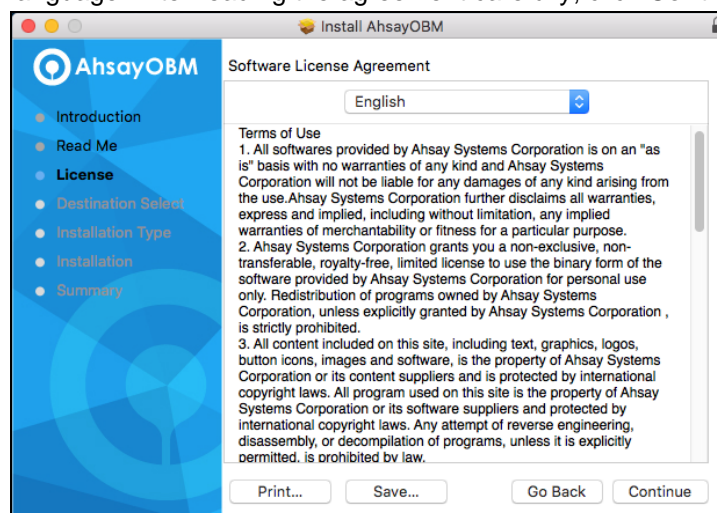
4. When the AhsayOBM Installer wizard appears, click **Continue** to proceed.



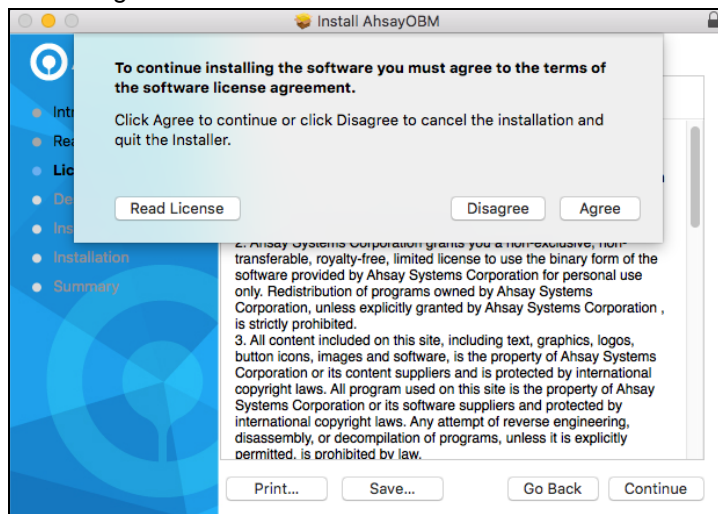
5. When the Important Information screen appears, read the information and then click **Continue** to proceed.



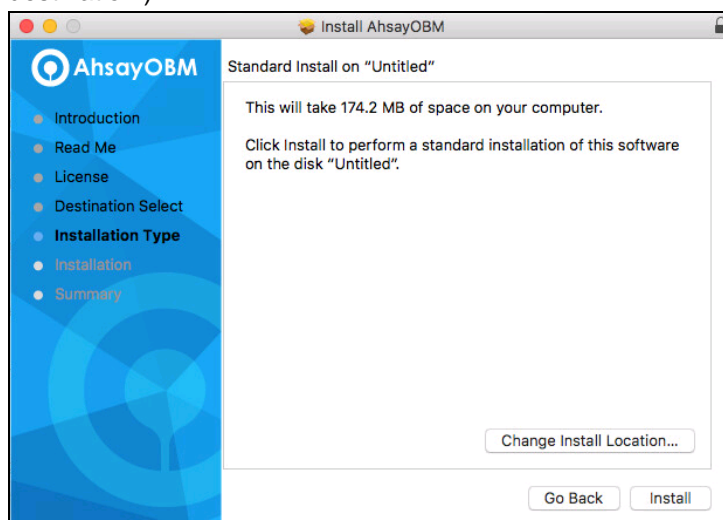
6. When the Software License Agreement appears, the agreement content will be displayed in English by default. If you prefer to read it in a different language, click  to change the language. After reading the agreement carefully, click **Continue** to proceed.



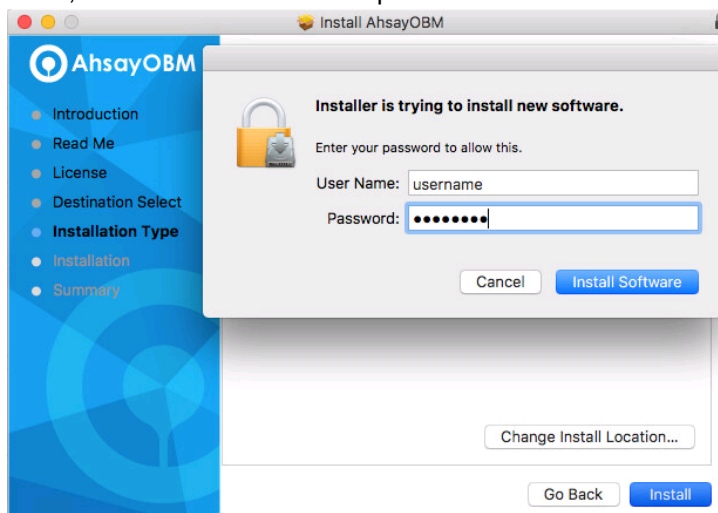
7. The following message will appear in a pop-up window. Click **Agree** to accept the software license agreement.



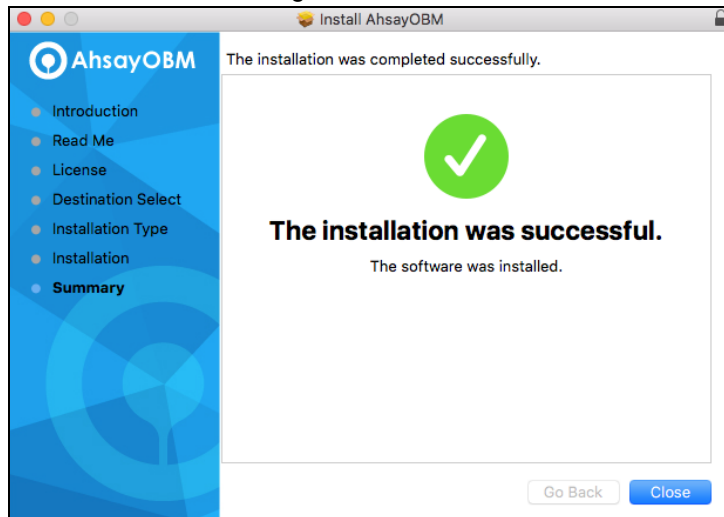
8. Click **Install** to start installing AhsayOBM to the default location, i.e. "Untitled" in this example. (Alternatively, you can click **Change Install Location...** to choose a different installation destination.)



9. The following message will appear in a pop-up window. Enter your Mac OS login credentials. Then, click **Install Software** to proceed with the installation.



10. You will see the following screen when the installation of AhsayOBM is completed.



5.3 AhsayOBM Services

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

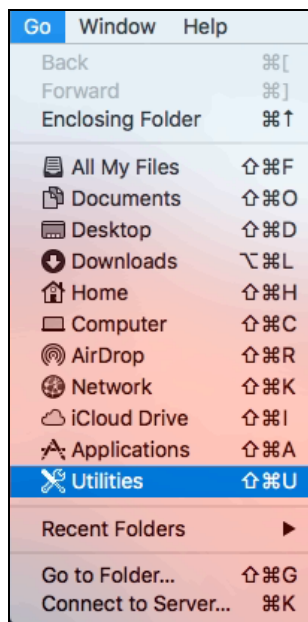
Function	Description
Continuous Backups (Windows platform only)	Ensures that Continuous backups are run according to the backup interval.
Reminder (Windows platform only)	Ensures that a reminder popup is displayed when the last time a backup was run exceeded the tolerance period.
Mobile Backup Server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

Therefore, it is very important to ensure the AhsayOBM Services are running after:

- a new AhsayOBM installation
- an AhsayOBM software update
- the machine was rebooted
- the machine is powered on
- the machine wakes up from hibernation or standby mode

Otherwise, all of the functions above will stop working.

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



Open the **Terminal** application.



Use the command highlighted in **red** to enter the AhsayOBM folder.

```
[admins-Mac:bin admin$ cd /Applications/AhsayOBM.app/bin  
[admins-Mac:bin admin$
```

To check if the scheduler service is running, use the **ps** command. You will see that the scheduler service is running, highlighted in **red**.

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

There are two (2) options to **stop** and **start** the AhsayOBM scheduler service.

5.3.1 Option 1: Stop and Start

- To **stop** the scheduler service, use the command highlighted in **red**. If you run this command for the first time, you will need to enter the login password of your local machine. To check if the scheduler service has stopped running, use the **ps** command.

```
admins-Mac:~ admin$ sudo /Applications/AhsayOBM.app/bin/StopScheduler.sh
Password:
admins-Mac:~ admin$ ps -ef|grep java
501 5721 5705 0 9:02PM ttys000 0:00.00 grep java
```

- Use the command highlighted in **red** to **start** the scheduler service then use the **ps** command. You will see that the scheduler service is running, highlighted in **red**.

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

5.3.2 Option 2: Stop and Start

- To **stop** the scheduler service, use the command highlighted in **red**. Use the **ps** command to check if the scheduler service has stopped running.

```
admins-Mac:~ admin$ sudo launchctl unload -F /Applications/AhsayOBM.app/
bin/com.cb.scheduler.plist
admins-Mac:~ admin$ ps -ef|grep java
501 5842 5793 0 9:23PM ttys000 0:00.01 grep java
admins-Mac:~ admin$
```

- Use the command highlighted in **red** to **start** the scheduler service then use the **ps** command. You will see that the scheduler service is running, highlighted in **red**.

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

5.4 RunLevel Symlink Check

During installation, the following symlinks to the scheduler startup script **/Applications/AhsayOBM.app/bin/com.cb.scheduler.plist** will be created that allows the AhsayOBM Scheduler Service to start automatically each time the machine is rebooted or restarted.

To verify if the symlinks have been created correctly, use the **ls** command. You will see the symlink, highlighted in **red**.

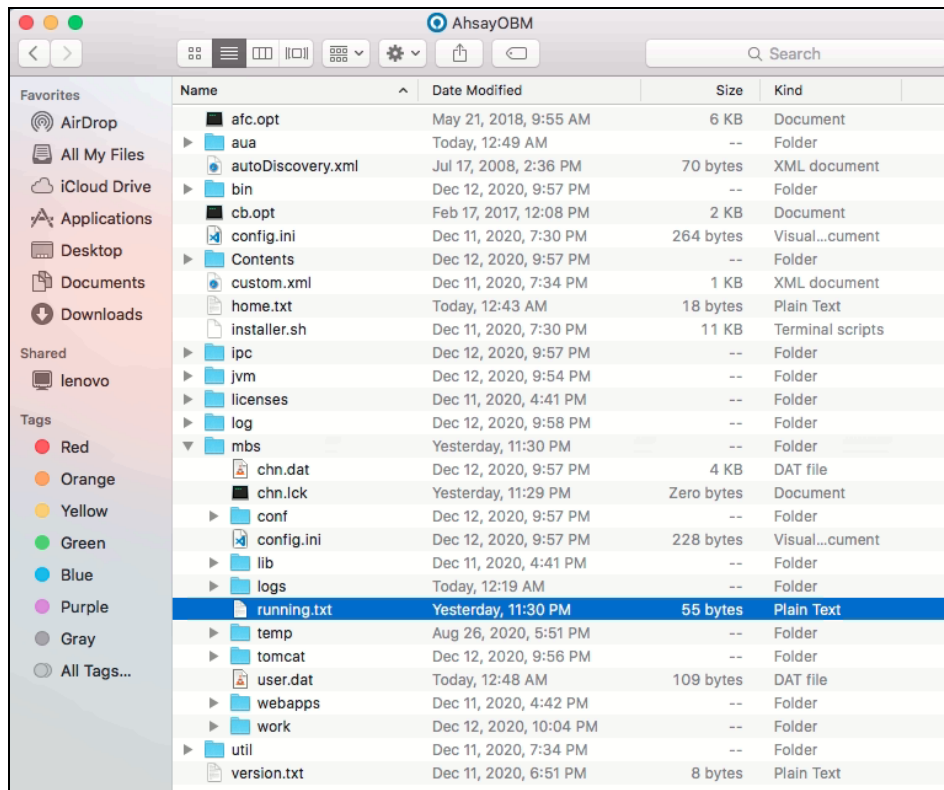
```
admins-Mac:~ admin$ ls -la /Library/LaunchDaemons/  
total 16  
drwxr-xr-x+ 62 root wheel 2108 Apr  5 01:56 ..  
lrwxr-xr-x  1 root wheel 53 May 15 03:07 com.AhsayOBM.scheduler.plist ->  
/Applications/AhsayOBM.app/bin/com.cb.scheduler.plist  
admins-Mac:~ admin$
```

5.5 Mobile Backup Server (MBS) Status Check and Ahsay Mobile app Connection Check

Although the Mobile Backup Server (MBS) will be activated automatically when a mobile device installed with the Ahsay Mobile app is successfully registered for mobile backup with AhsayOBM.

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

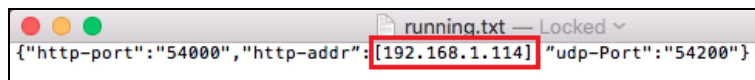
1. Check HTTP port, IP address and UDP port in the **running.txt** file. Go to mbs folder.
Example: /Applications/AhsayOBM.app/mbs



NOTE

If the "running.txt" file does not exist, then the MBS is not running. Restart the AhsayOBM services.

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



- Open the Terminal and check if the IP address captured in the running.txt file is the correct IP address of the machine where AhsayOBM is installed.

```

MacBook-Pro:~ admin$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=3<RXCSUM,TXCSUM>
    inet6 ::1 prefixlen 128
    inet 127.0.0.1 netmask 0xff000000
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=1<PERFORMNUD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=10b<RXCSUM,TXCSUM,VLAN_HWTAGGING,AV>
    ether 3c:07:54:54:86:c5
    nd6 options=1<PERFORMNUD>
    media: autoselect (none)
    status: inactive
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 68:a8:6d:29:05:8e
    inet6 fe80::6a8:6dff:fe29:58%en1 prefixlen 64 duplicated scopeid 0x5
    inet 192.168.1.114 netmask 0xffffff00 broadcast 192.168.1.255
    nd6 options=9<PERFORMNUD,IFDISABLED>
    media: autoselect
    status: active
fw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 4078
    lladdr a4:b1:97:ff:fe:eb:b7:48
    nd6 options=1<PERFORMNUD>
    media: autoselect <full-duplex>
    status: inactive
en2: flags=963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX> mtu 1500
    options=60<TS04,TS06>
    ether d2:00:1e:bb:74:80
    media: autoselect <full-duplex>
    status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    ether 0a:a8:6d:29:05:8e
    media: autoselect
    status: inactive
  
```

- To verify the actual HTTP port used by MBS, type the command:
netstat -vanp tcp \| grep 54000.

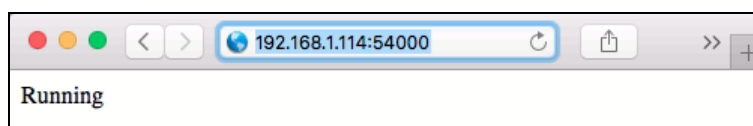
```

MacBook-Pro:~ admin$ netstat -vanp tcp \| grep 54000
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         (state)      rhiwat shiwat    pid    epid
tcp4  0      0  192.168.1.114.49342    125.5.184.164.80        CLOSE_WAIT   32768  32768    66     0
tcp4  0      0  127.0.0.1.64050       *.*                     LISTEN       131072 131072    66     0
tcp46 0      0  *.54000               *.*                     LISTEN       131072 131072    66     0
tcp4  0      0  192.168.1.114.7070    192.168.1.111.50057     ESTABLISHED  262144 311296    84     0
tcp4  0      0  *.49192               *.*                     LISTEN       131072 131072    84     0
tcp4  0      0  192.168.1.114.49192    92.223.85.120.80        ESTABLISHED  131072 131860    84     0
tcp4  0      0  192.168.1.114.49191    17.57.145.68.5223       ESTABLISHED  131072 131860    91     0
tcp4  0      0  *.7070                *.*                     LISTEN       131072 131072    84     0
  
```

- Make sure that your firewall setting allows network traffic through the following HTTP and UDP ports to ensure that the communication between your machine and mobile device is successful: HTTP Port: 54000 to 54099 and UDP Port: 54200 to 54299. Otherwise mobile backup and restore will not work.
- To perform a status check on the MBS. Open a browser on the AhsayOBM machine and type the IP address, followed by the TCP port.

For example: If the HTTP port used is 54000, <http://192.168.1.114:54000>, you should get the following result which shows “Running” status. This means the MBS is running.

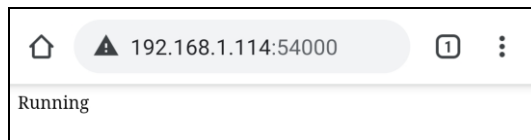
In the AhsayOBM machine



- To run a connection test between the mobile device and machine open a browser in your mobile device and type the IP address followed by the TCP port.
- For example: If the HTTP port used is 54000, <http://192.168.1.114:54000>, you should get the following result which shows “Running” status. This means the Ahsay Mobile app can

successfully connect to the MBS and both backup and restore can proceed on the mobile device.

In the mobile device

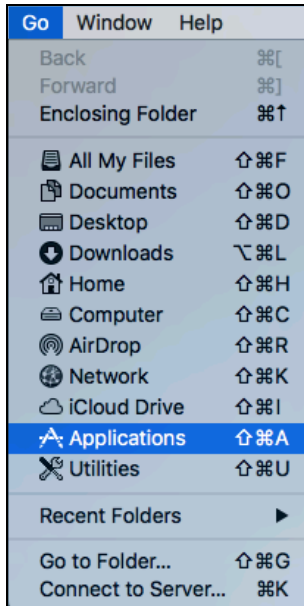


6 Start AhsayOBM

Starting with AhsayOBM v8.5.0.0, you will find two new features introduced with this latest version which are the Mobile Backup and Two-Factor Authentication. With these new features there are several scenarios that will be encountered for first time login if, Mobile Backup and/or Two-Factor Authentication are enabled on the user account. Login steps for the different scenarios will be discussed in this chapter.

6.1 Add an AhsayOBM Shortcut Icon to the Desktop

1. Under the Go menu bar on the top of the screen, click the Applications option.



2. Look for the AhsayOBM application icon as shown below.



3. Then, drag the icon to to add a shortcut to the desktop.



6.2 Login to AhsayOBM without 2FA

To login to AhsayOBM without two-factor authentication, here are the three scenarios:

- ▶ [Initial login to AhsayOBM with no 2FA and no Mobile Add-on Module](#)
- ▶ [Initial login to AhsayOBM with no 2FA and with Mobile Add-on Module](#)
- ▶ [Subsequent login to AhsayOBM with no 2FA](#)

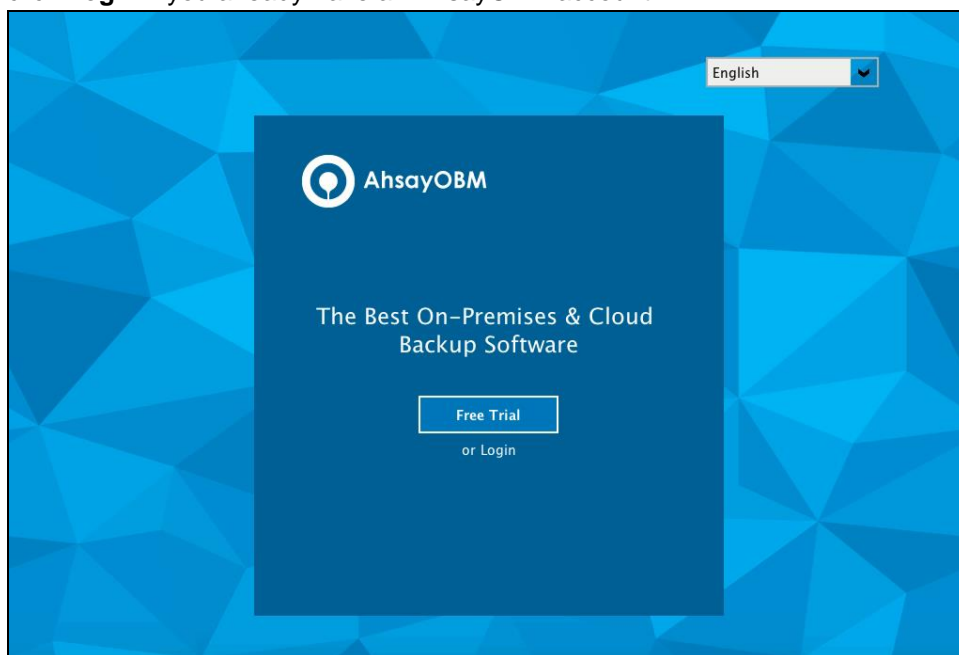
6.2.1 Initial login to AhsayOBM with no 2FA and no Mobile Add-on Module

When logging in to AhsayOBM for the first time pre-v8.5 login sequence, please follow the steps below:

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



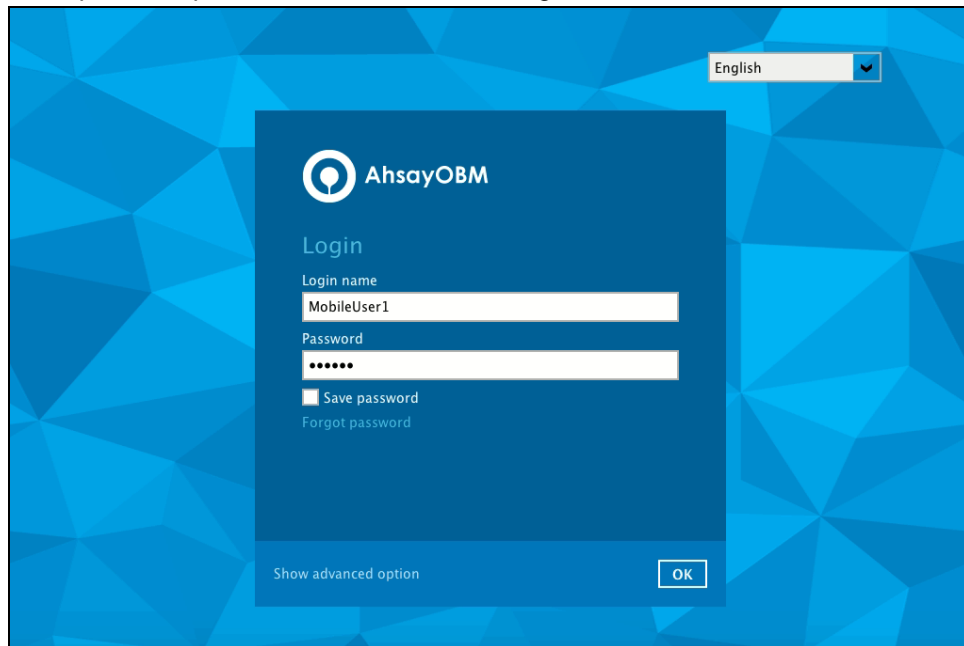
2. The Free Trial Registration menu may be displayed when you login for the first time. If you want to create a free trial account please proceed to [Appendix E](#). Otherwise, click **Login** if you already have an AhsayOBM account.



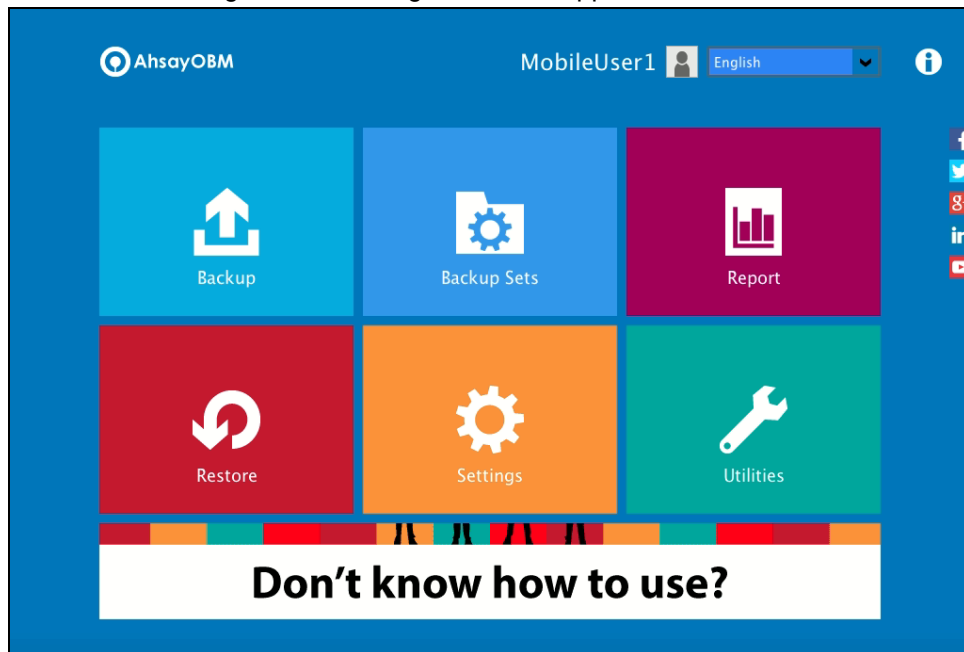
3. Click **Show advanced option** to enter the backup server settings provided by your backup service provider. Then, click **OK** to save the changes.

A dialog box titled 'Backup Server'. It contains a dropdown menu for the protocol, currently set to 'http', followed by a text input field for the server address. Below this is a section titled 'Proxy (HTTP)' with the text 'Use proxy to access the Internet' and a toggle switch currently set to 'Off'.

4. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



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



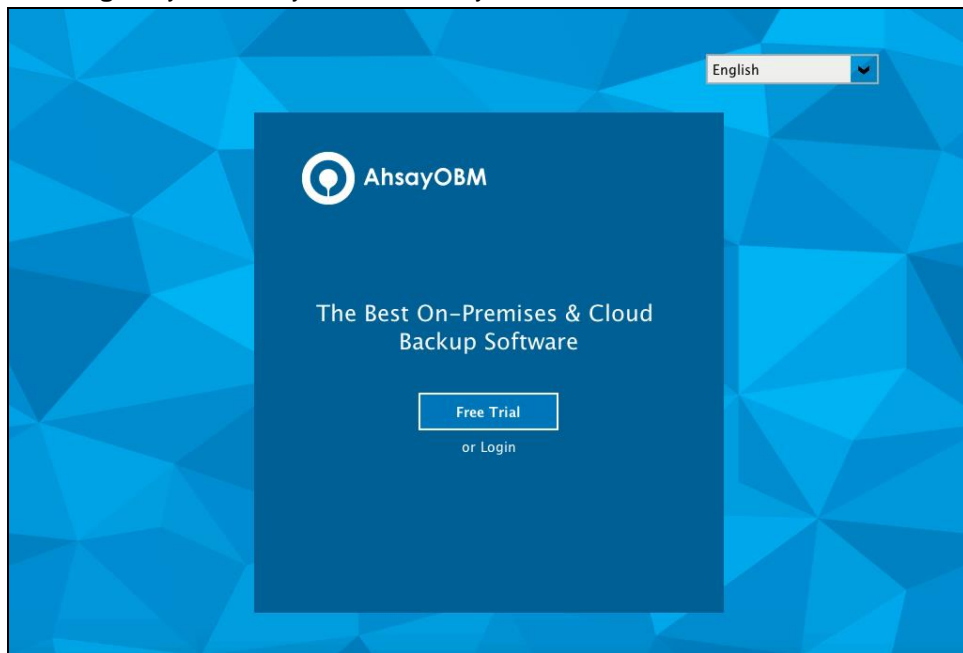
6.2.2 Initial login to AhsayOBM with no 2FA and with Mobile Add-on Module

When logging in to AhsayOBM for the first time without two-factor authentication but with Mobile Add-on Module enabled, please follow the steps below:

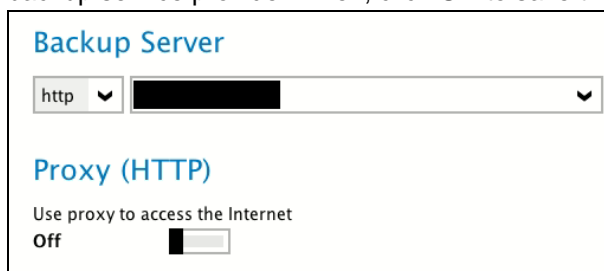
1. A shortcut icon of AhsayOBM will be available on your desktop after installation. Double-click the icon to launch the application.



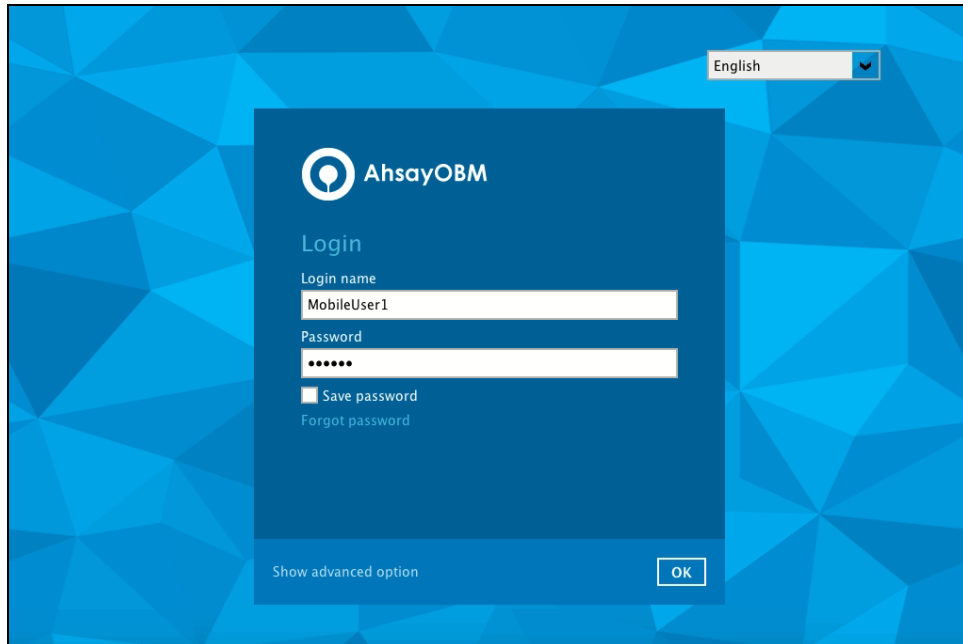
2. The Free Trial Registration menu may be displayed when you login for the first time. If you want to create a free trial account please proceed to [Appendix E](#). Otherwise, click **Login** if you already have an AhsayOBM account.



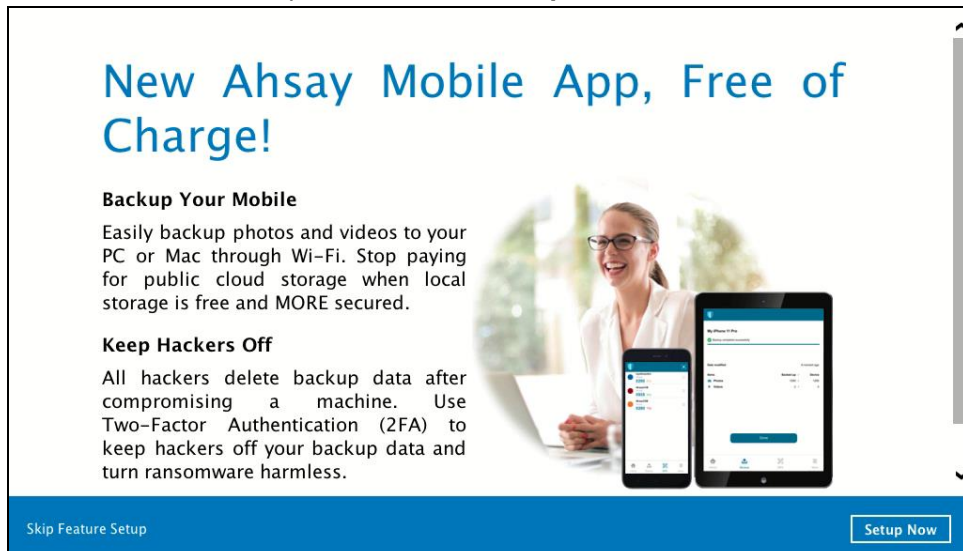
3. Click **Show advanced option** to enter the backup server settings provided by your backup service provider. Then, click **OK** to save the changes.

A dialog box titled 'Backup Server'. It contains a dropdown menu for the protocol, currently set to 'http', and a text input field for the server address. Below this is a section titled 'Proxy (HTTP)' with the text 'Use proxy to access the Internet' and a toggle switch currently set to 'Off'.

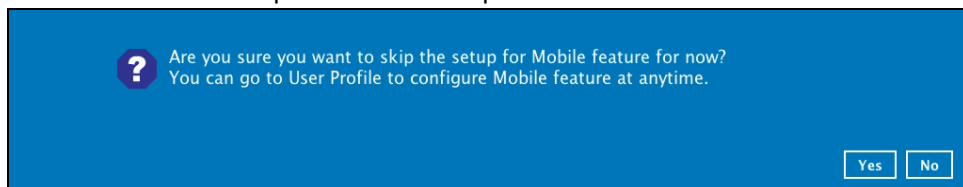
4. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.

The image shows the AhsayOBM login interface. It features a blue background with a geometric pattern. In the top right corner, there is a language dropdown menu set to 'English'. The main content area is a dark blue box with the AhsayOBM logo at the top. Below the logo, the word 'Login' is displayed. There are two input fields: 'Login name' with the text 'MobileUser1' and 'Password' with masked characters '*****'. Below the password field, there is a checkbox for 'Save password' and a link for 'Forgot password'. At the bottom of the login box, there is a link for 'Show advanced option' and an 'OK' button.

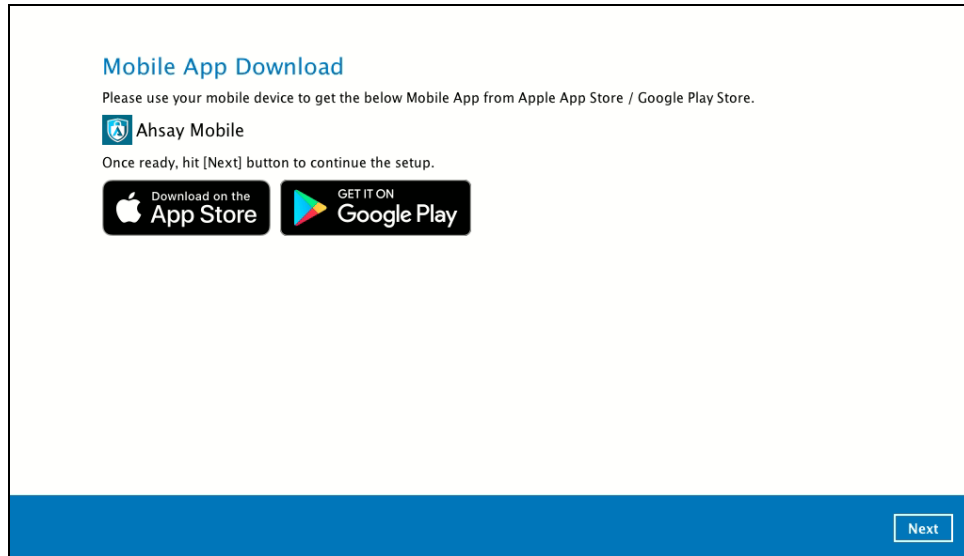
5. You will have the option to set up your mobile backup if the **Mobile Add-on Module is enabled** in the backup account. Click **Setup Now**.

The image is a promotional banner for the 'New Ahsay Mobile App, Free of Charge!'. It features a woman smiling next to a laptop and two smartphones displaying the app. The text on the banner includes: 'New Ahsay Mobile App, Free of Charge!', 'Backup Your Mobile' (Easily backup photos and videos to your PC or Mac through Wi-Fi. Stop paying for public cloud storage when local storage is free and MORE secured.), and 'Keep Hackers Off' (All hackers delete backup data after compromising a machine. Use Two-Factor Authentication (2FA) to keep hackers off your backup data and turn ransomware harmless.). At the bottom, there is a 'Skip Feature Setup' link and a 'Setup Now' button.

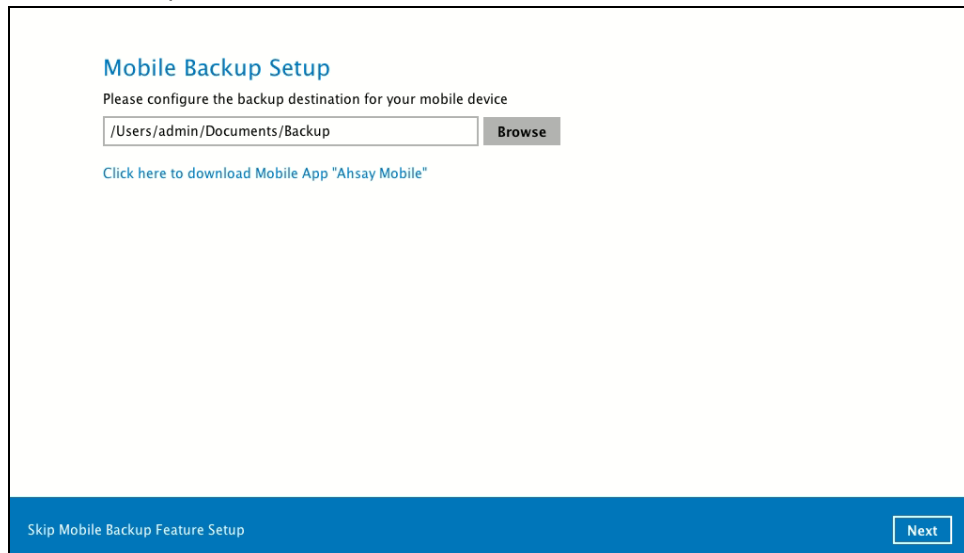
If you do not want to set up the mobile backup feature click **Skip Feature Setup** link. Click **Yes** in the pop-up message that will be displayed. Otherwise click **No** to continue with the set-up of mobile backup feature.

The image shows a blue pop-up message box. It contains a question mark icon and the text: 'Are you sure you want to skip the setup for Mobile feature for now? You can go to User Profile to configure Mobile feature at anytime.' At the bottom right, there are two buttons: 'Yes' and 'No'.

6. Download the Ahsay Mobile app from the App Store / Google Play Store. Click **Next**.



7. Click **Browse** to select the location where the backup of your device will be saved. Click **Next** to proceed.



8. Select your country code and enter your phone number. Click **Send SMS Verification code** to receive the passcode.

Two-Factor Authentication Setup

For first time activation of Two-Factor Authentication feature, mobile device needs to pair with a verified phone number for account recovery.

Phone number

Philippines (+63)

*This phone number will be used for account security and recovery only. Please be reminded that standard SMS charge will be applied.

Send SMS Verification code

[Click here to download Mobile App "Ahsay Mobile"](#)

Skip Two-Factor Authentication Feature Setup

Next

If you do not want to set up the 2FA feature click **Skip Two-Factor Authentication Feature Setup** link. Click **Yes** in the pop-up message that will be displayed to proceed with the login. Otherwise click **No** to continue with the set-up of 2FA feature.

?

Are you sure you want to skip the setup for Two-Factor Authentication feature for now?
You can go to User Profile to configure Two-Factor Authentication feature at anytime.

Yes

No

This can also be setup in the AhsayCBS User Web Console, please refer to the [AhsayCBS User's Guide](#) for more information.

9. Enter the verification code and click **Next**.

Verification Code: ANRJ-706536

Two-Factor Authentication Setup

For first time activation of Two-Factor Authentication feature, mobile device needs to pair with a verified phone number for account recovery.

Phone number

Philippines (+63)

*This phone number will be used for account security and recovery only. Please be reminded that standard SMS charge will be applied.

Verification code

ANRJ - 706536

(00:04:37)

Resend SMS Verification code

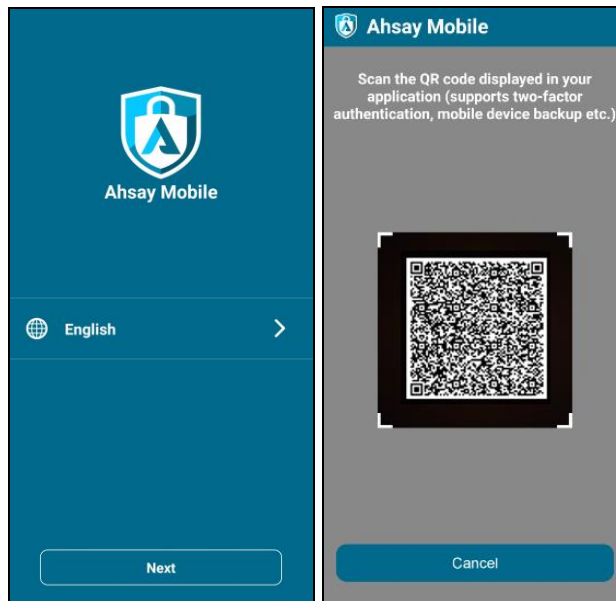
[Click here to download Mobile App "Ahsay Mobile"](#)

Skip Two-Factor Authentication Feature Setup

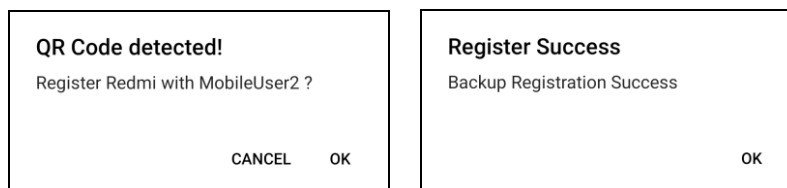
Next

10. Pair your device with the backup account. There are two ways to do this:

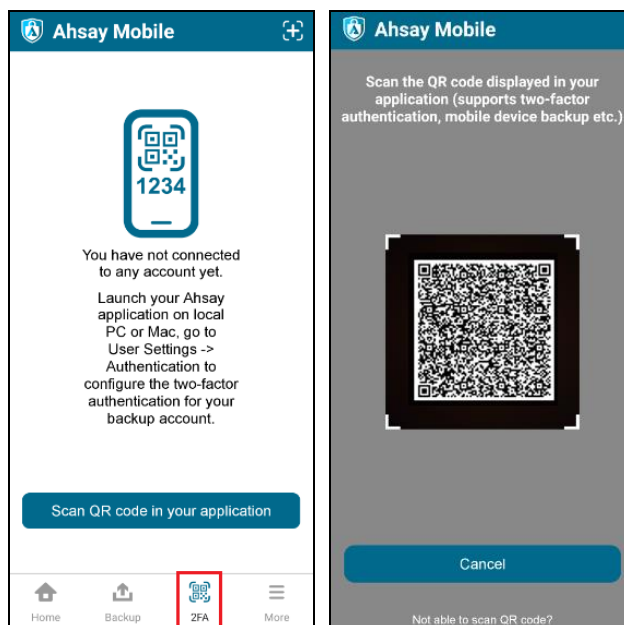
By using the Ahsay Mobile app, tap **Next** and scan the QR code displayed in AhsayOBM.



Then click **OK**.





Then go to **2FA** and tap **Scan QR code in your application**, once again scan the QR code.

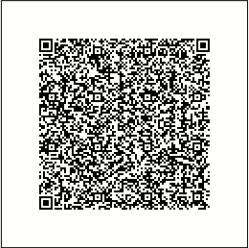


Device Pairing

Please scan the QR code to register your mobile device with your backup account for following feature:

 Mobile Backup

 Two-Factor Authentication



Please make sure below 2 ports are not blocked by any Firewall settings before pairing your mobile device for backup

TCP Port: 54000
UDP Port: 54200

[Using other TOTP Authenticator App \(e.g. Authy, Duo, Google\)](#)

Skip Device Pairing

If you do not want to pair your device with the backup account click the **Skip Device Pairing** link. Click **Yes** in the pop-up message that will be displayed to proceed with the login. Otherwise click **No** to continue with the set-up of Mobile Backup and Two-Factor Authentication feature.

Are you sure you want to skip Device Pairing now?
Once skipped, the mobile feature setup will be discarded.
You can go to User Profile to configure mobile feature at anytime.

Yes No

or

By using a third-party TOTP Authenticator App (e.g. Authy, Duo, Google), click the **Using other TOTP Authenticator App (e.g. Authy, Duo, Google)** link.

Click **Yes** if you want to use a third-party app as your authenticator. However if you use this, the Mobile Backup feature that you set up earlier will be discarded.


Are you sure you want to use other TOTP Authenticator App?
Once using other TOTP Authenticator App, Mobile Backup feature will be discarded from this setup.
You can go to User Profile to configure Mobile Backup feature at anytime.


Yes No

Either scan the QR code using the third-party authenticator app or enter the Secret Key in the third-party authenticator app. After doing so, the one-time password will be generated in the authenticator app. Enter a name and the one-time password generated in the authenticator app here and click **Next**.

Device Pairing

Please scan the QR code or input Secret Key to register your mobile device with your backup account for following feature:

 Two-Factor Authentication



Secret Key: 6FHF YRJU EUHT UKRF

Enter a display name for user profile.

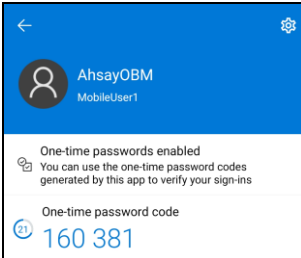
Enter the one-time password generated by Authenticator App.

 (00:00:19)

[Using Ahsay Mobile](#)

[Skip Device Pairing](#) [Next](#)

This is a sample of the one-time password generated in the third-party Authenticator App Microsoft Authenticator.



AhsayOBM
MobileUser1

One-time passwords enabled
You can use the one-time password codes generated by this app to verify your sign-ins


One-time password code
160381


11. After pairing the device, this message will be displayed. Click **OK** to proceed.

This is a sample of the message displayed when using Ahsay Mobile app.

Mobile Setup

You have registered "Redmi" for the following feature:

 Mobile Backup


 Two-Factor Authentication

You can go to the backup page in Mobile App "Ahsay Mobile" to start Mobile Backup.

This is a sample of the message displayed when using a third-party TOTP Authenticator App.

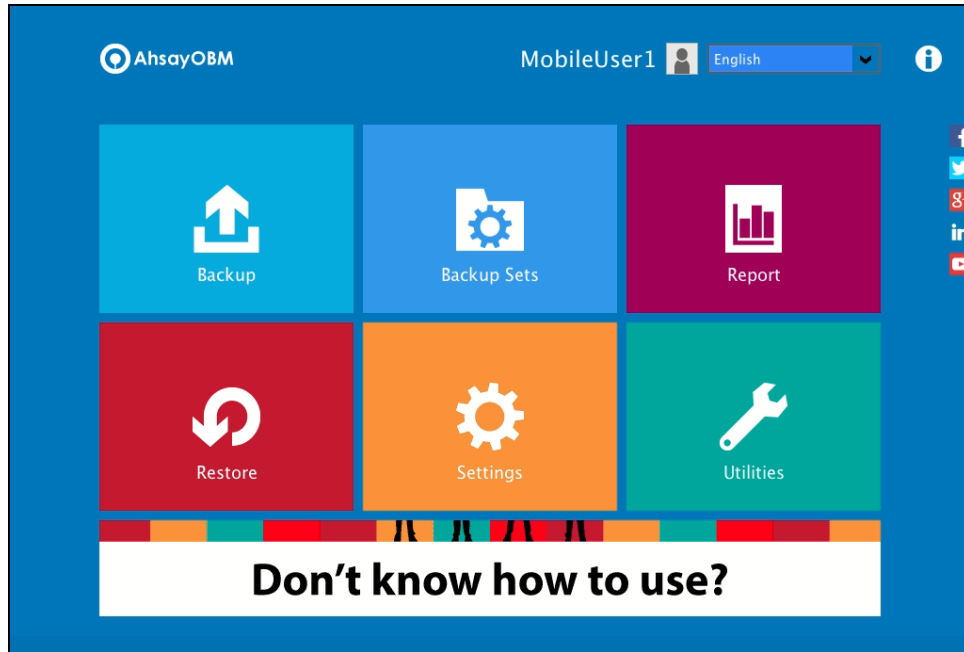
Mobile Setup

You have registered "MobileUser1" for the following feature:

 Two-Factor Authentication

Mobile Backup feature failed to be configured.
You can go to User Profile to configure Mobile Backup feature again.

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



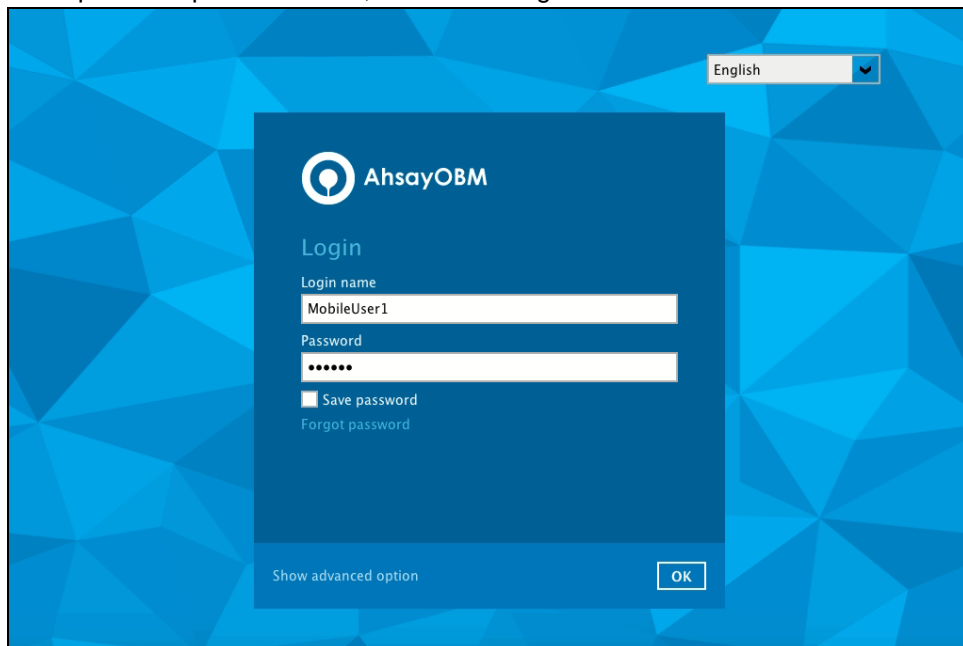
6.2.3 Subsequent login to AhsayOBM with no 2FA

For subsequent logins to AhsayOBM without two-factor authentication, please follow the steps below:

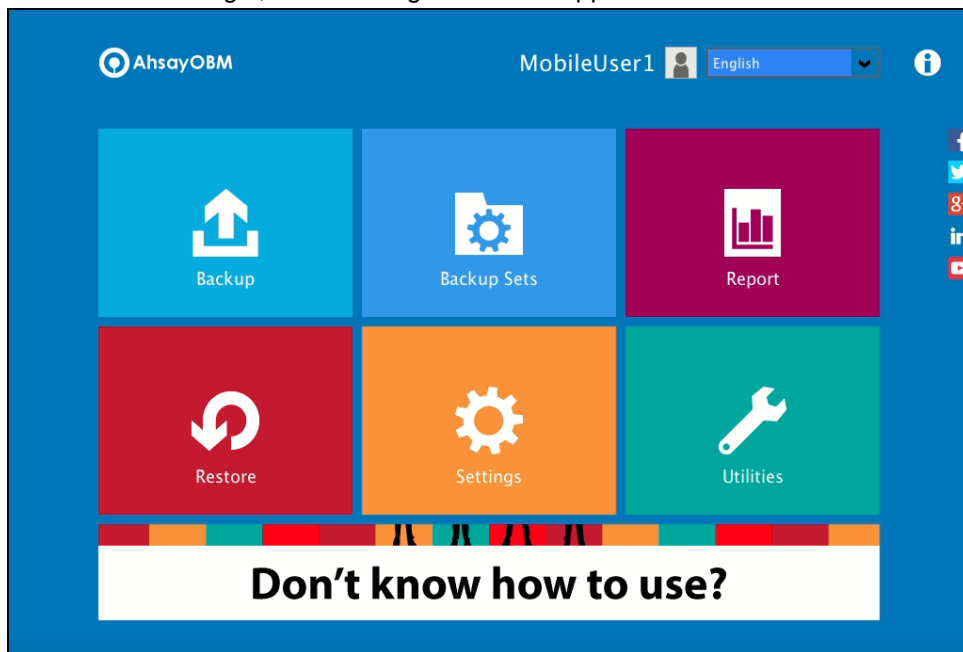
1. A shortcut icon of AhsayOBM will be available on your desktop after installation. Double-click the icon to launch the application.



2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



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



6.3 Login to AhsayOBM with 2FA using Android or iOS mobile device

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

▶ **Ahsay Mobile 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. Auth, Duo, Google)

To login to AhsayOBM with two-factor authentication, here are the three scenarios:

- ▶ [Initial login to AhsayOBM with 2FA and with no Mobile Add-on Module](#)
- ▶ [Initial login to AhsayOBM with 2FA and Mobile Add-on Module](#)
- ▶ [Subsequent login to AhsayOBM](#)

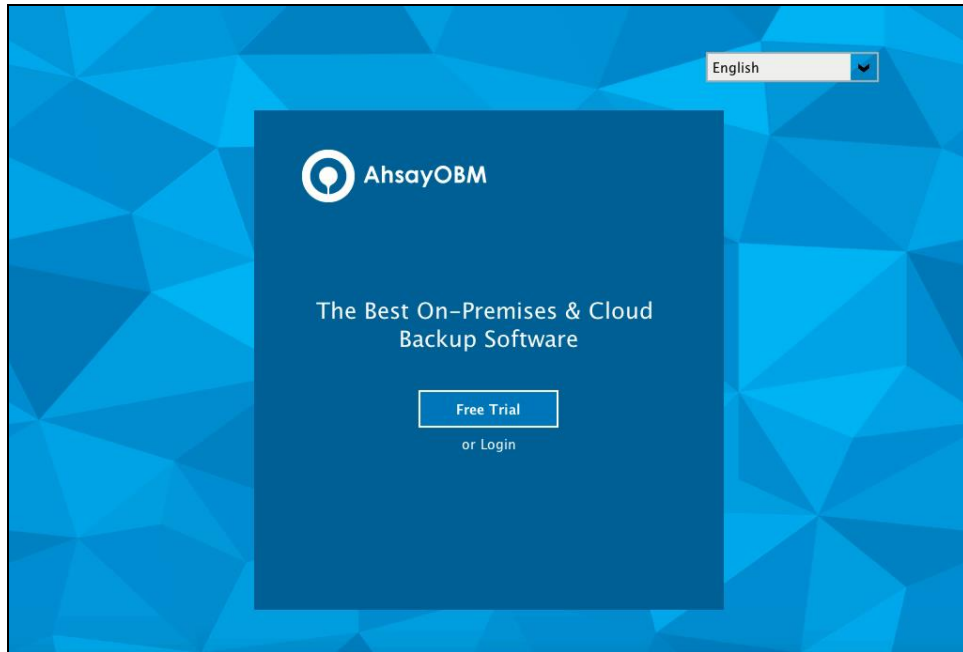
6.3.1 Initial login to AhsayOBM with 2FA and with no Mobile Add-on Module

When logging in to AhsayOBM for the first time with two-factor authentication and with Mobile Add-on Module not enabled, please follow the steps below:

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



2. The Free Trial Registration menu may be displayed when you login for the first time. If you want to create a free trial account please proceed to [Appendix E](#). Otherwise, click **Login** if you already have an AhsayOBM account.



3. Click **Show advanced option** to enter the backup server settings provided by your backup service provider. Then, click **OK** to save the changes.

Backup Server

http

Proxy (HTTP)

Use proxy to access the Internet

Off ☐

4. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.

AhsayOBM

Login

Login name

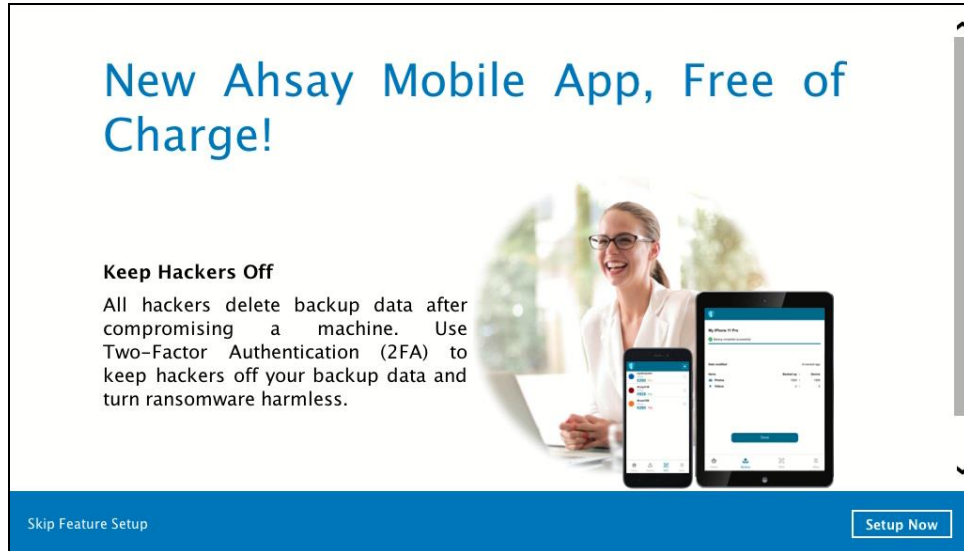
Password

☐ Save password

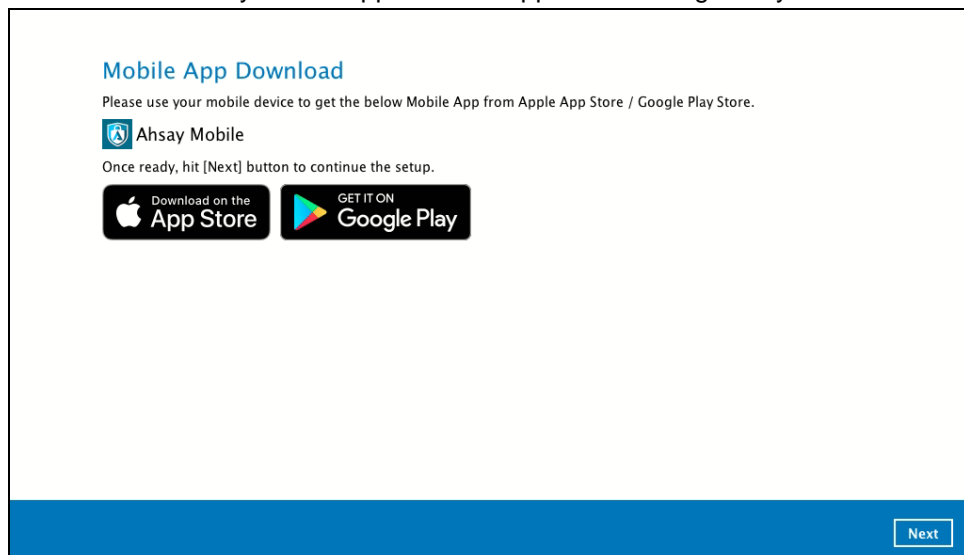
[Forgot password](#)

Show advanced option

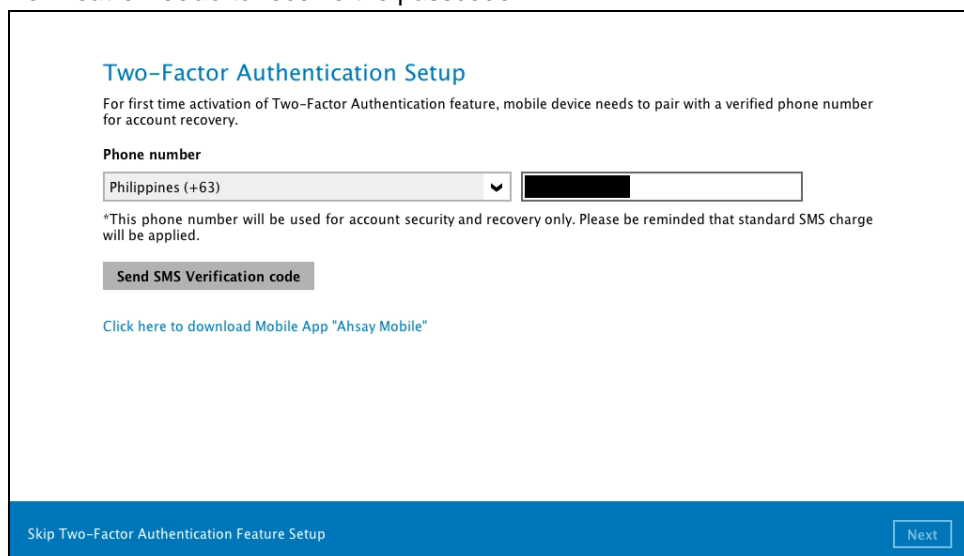
5. To set up your two-factor authentication click **Setup Now**.



6. Download the Ahsay Mobile app from the App Store / Google Play Store. Click **Next**.



7. Select your country code and enter your phone number. Click **Send SMS Verification code** to receive the passcode.



8. Enter the verification code sent to your mobile device and then click **Next**.

Two-Factor Authentication Setup

For first time activation of Two-Factor Authentication feature, mobile device needs to pair with a verified phone number for account recovery.

Phone number

Philippines (+63)

*This phone number will be used for account security and recovery only. Please be reminded that standard SMS charge will be applied.

Verification code

ANRJ -

706536

(00:04:37)

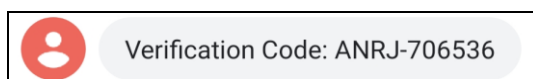
Resend SMS Verification code

[Click here to download Mobile App "Ahsay Mobile"](#)

Skip Two-Factor Authentication Feature Setup

Next

Example of the verification code sent to mobile device.



9. Ahsay Mobile supports two types of authentication method:

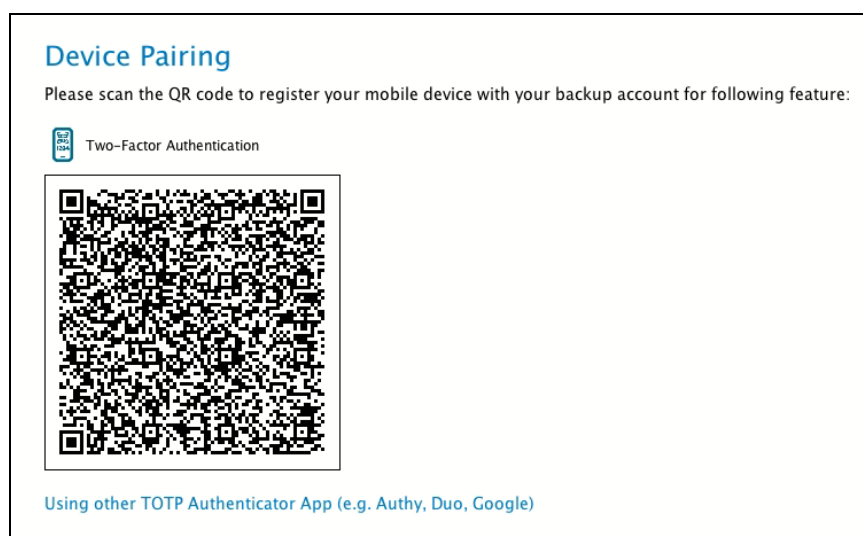
- ▶ Push Notification
- ▶ TOTP

Ahsay Mobile can be configured to support two 2FA modes:

- ▶ Push Notification and TOTP (default mode) or,
- ▶ TOTP only

Push Notification and TOTP (default mode)

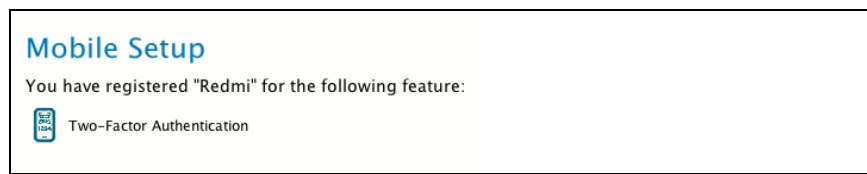
- i. To configure Push Notification and TOTP 2FA with Ahsay Mobile, simply scan the displayed QR code using the Ahsay Mobile app.



In this example, the Ahsay Mobile app is installed on a mobile device named “Redmi”.

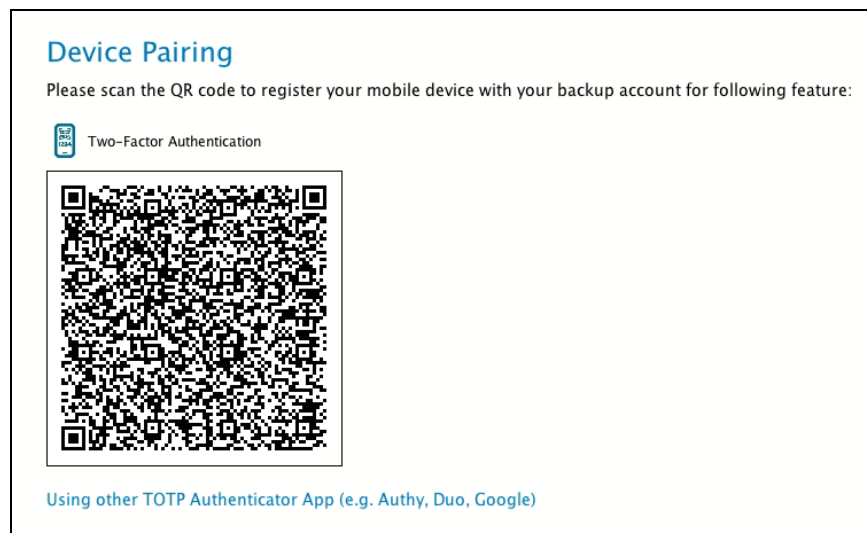


- ii. After successful scan of the QR code, you have now registered Ahsay Mobile for Push Notification and TOTP 2FA.



TOTP only


- i. To configure a TOTP only 2FA with Ahsay Mobile, click the “**Using other TOTP Authenticator App (e.g. Authy, Duo, Google)**” link.




- ii. After clicking the “Using other TOTP Authenticator App (e.g. Authy, Duo, Google)” link, the QR code for the TOTP Authenticator app will be displayed.

Device Pairing

Please scan the QR code or input Secret Key to register your mobile device with your backup account for following feature:

 Two-Factor Authentication



Secret Key: 6FHG JMI6 ONAJ Y3U4

Enter a display name for user profile.

Enter the one-time password generated by Authenticator App.

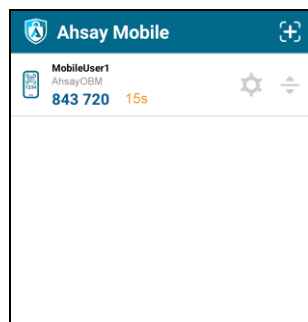
 (00:00:19)

[Using Ahsay Mobile](#)

- iii. Scan the QR code using the Ahsay Mobile app.




- iv. After successful scan of the QR code, a TOTP account corresponding to the login name of the AhsayOBM, i.e. “MobileUser1” is created on Ahsay Mobile.
- Example of the one-time password generated by Ahsay Mobile.




- v. Enter a display name for the user profile, then input the TOTP generated by Ahsay Mobile. After entering the necessary details, click **Next** to finish the registration process.

Device Pairing

Please scan the QR code or input Secret Key to register your mobile device with your backup account for following feature:

 Two-Factor Authentication



Secret Key: 6FHG JMI6 ONAJ Y3U4

Enter a display name for user profile.

Enter the one-time password generated by Authenticator App.


 (00:00:19)

[Using Ahsay Mobile](#)

- vi. Once the registration is successful, the following screen will be displayed. You have now registered Ahsay Mobile for TOTP only 2FA.

Mobile Setup

You have registered "MobileUser1" for the following feature:


 Two-Factor Authentication


Alternatively, you may also use a third-party TOTP Authenticator App (e.g. Authy, Duo, Google).

Either scan the QR code using the third-party authenticator app or enter the Secret Key in the third-party authenticator app. After doing so, the one-time password will be generated in the authenticator app. Enter a name and the one-time password generated in the authenticator app and click **Next**.

Device Pairing

Please scan the QR code or input Secret Key to register your mobile device with your backup account for following feature:

 Two-Factor Authentication



Secret Key: 6FHC BRJM 7P33 HRXW

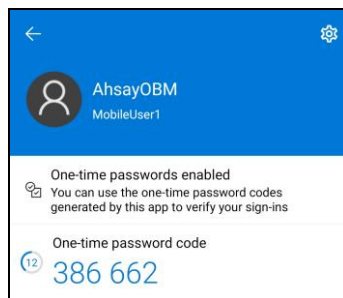
Enter a display name for user profile.

Enter the one-time password generated by Authenticator App.

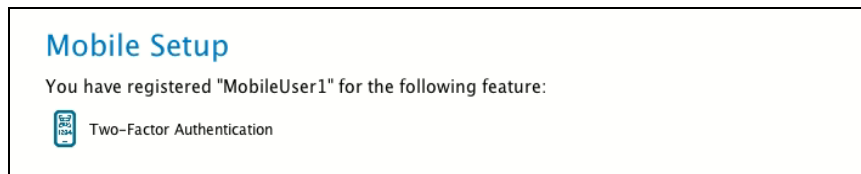
 (00:00:18)

[Using Ahsay Mobile](#)

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



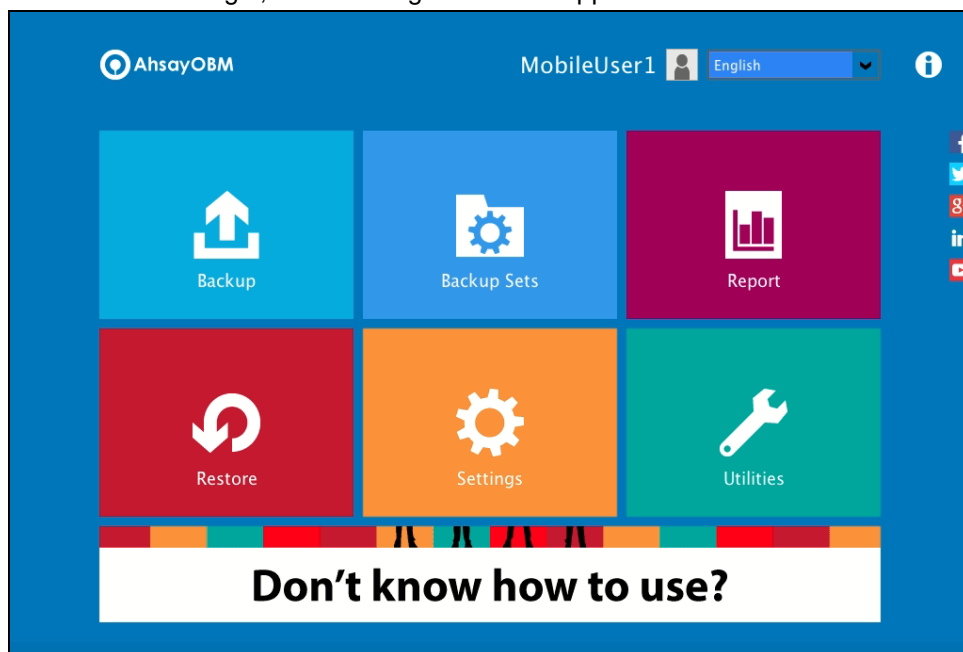
Once the registration is successful, the following screen will be displayed. You have now registered a third-party authenticator app for 2FA.



NOTE
In case device pairing takes a while, session timeout message will be displayed. Just click **OK** to resume with the device pairing.

Mobile Setup
Due to session timeout, Two-Factor Authentication feature failed to be configured.
You can go to User Profile to configure Two-Factor Authentication feature again.

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



NOTE
Please refer to the [Ahsay Mobile App User Guide for Android and iOS – Appendix A: Troubleshooting Login](#) if you are experiencing problems logging into AhsayOBM with Two-Factor Authentication using Ahsay Mobile app.

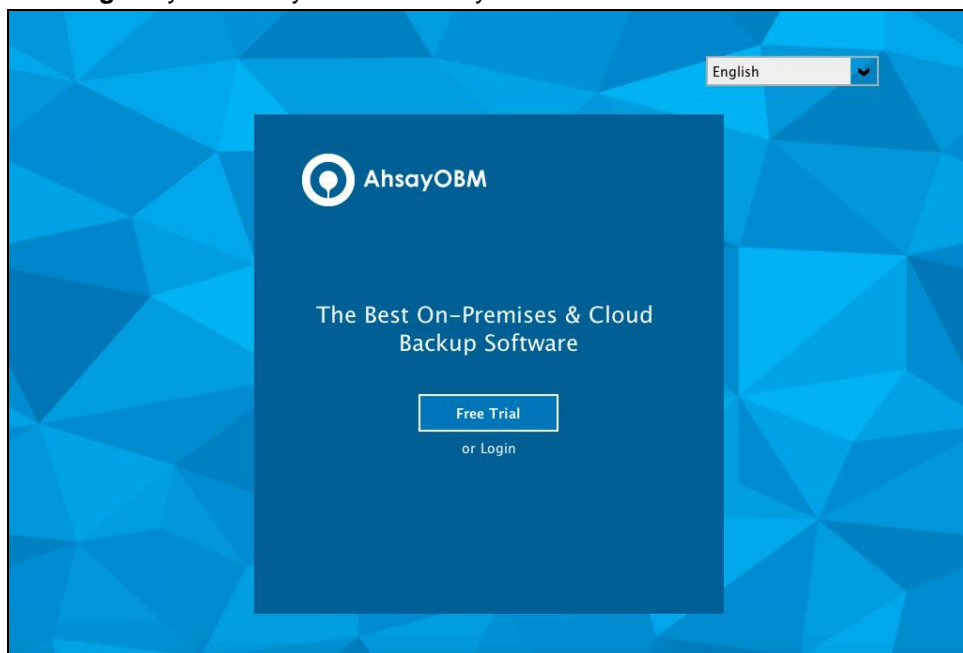
6.3.2 Initial login to AhsayOBM with 2FA and with Mobile Add-on Module

When logging in to AhsayOBM for the first time with two-factor authentication and with Mobile Add-on Module enabled, please follow the steps below:

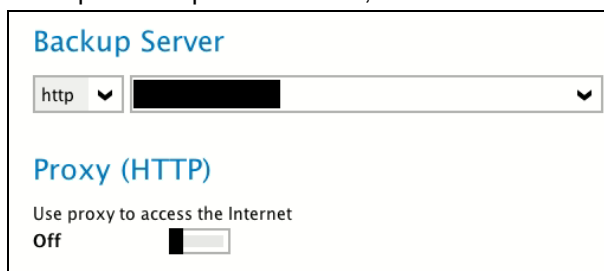
1. A shortcut icon of AhsayOBM will be available on your desktop after installation. Double-click the icon to launch the application.



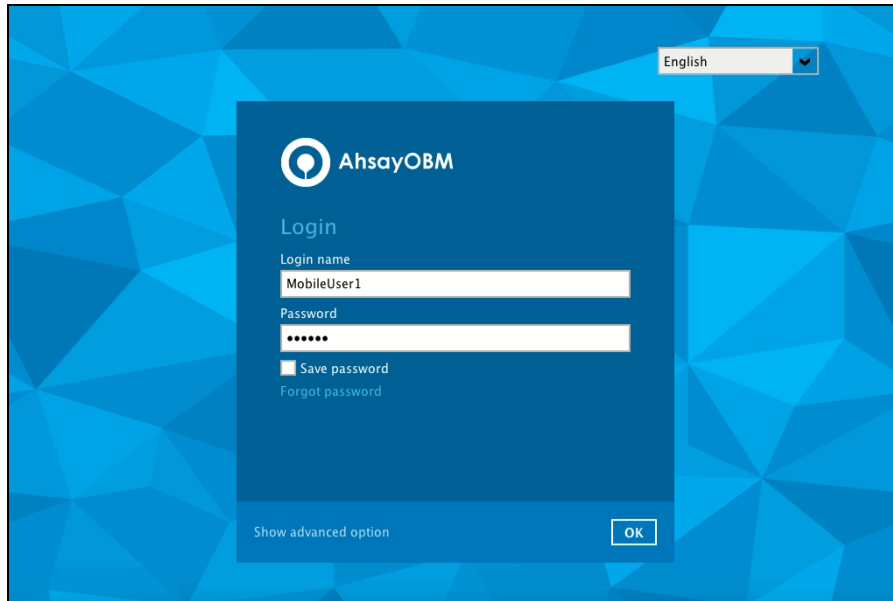
2. The Free Trial Registration menu may be displayed when you login for the first time. If you want to create a free trial account please proceed to [Appendix E](#). Otherwise, click **Login** if you already have an AhsayOBM account.



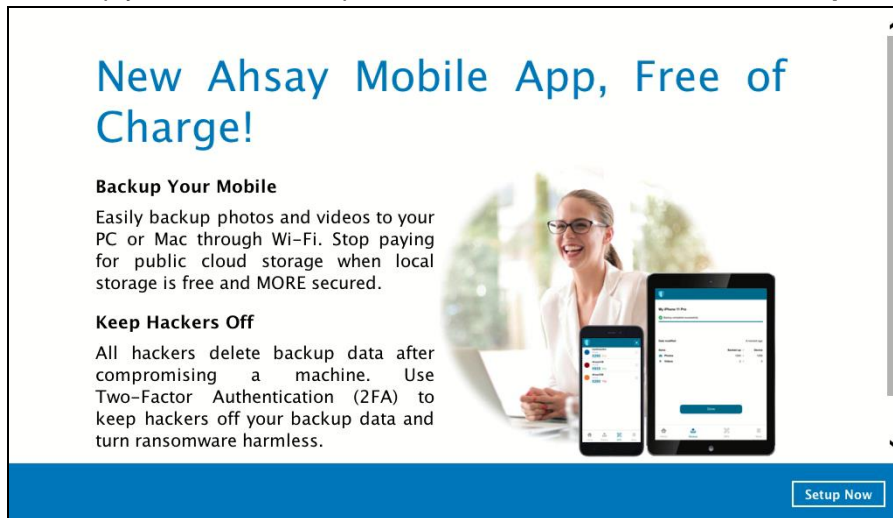
3. Click **Show advanced option** to enter the backup server settings provided by your backup service provider. Then, click **OK** to save the changes.

A dialog box titled 'Backup Server'. It contains a dropdown menu for the protocol, currently set to 'http', followed by a text input field for the server address. Below this, there is a section titled 'Proxy (HTTP)' with the text 'Use proxy to access the Internet' and a toggle switch currently set to 'Off'.

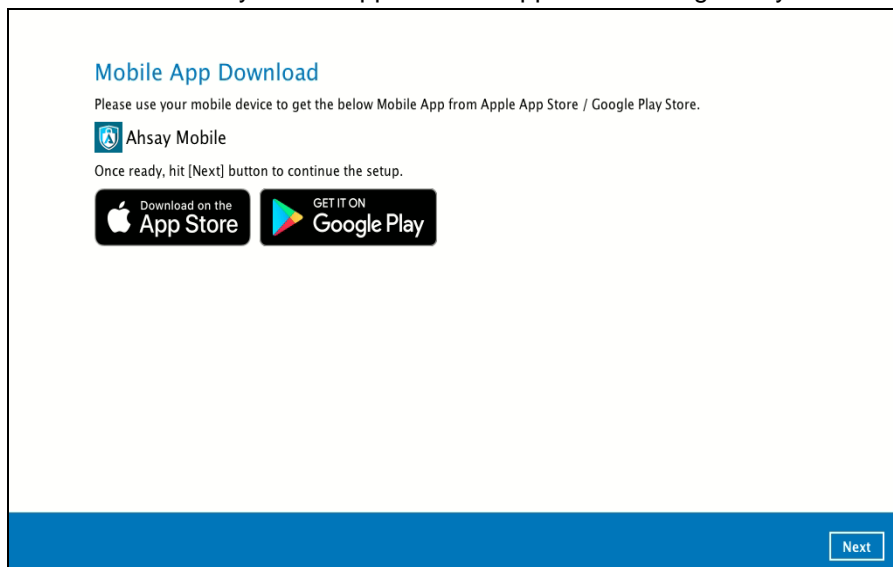
4. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.

The image shows the AhsayOBM login interface. It features a blue background with a geometric pattern. In the top right corner, there is a language dropdown menu set to 'English'. The central part of the screen is a dark blue box containing the AhsayOBM logo and the text 'Login'. Below this, there are two input fields: 'Login name' with the text 'MobileUser1' and 'Password' with masked characters '*****'. There is a checkbox for 'Save password' and a link for 'Forgot password'. At the bottom of the box, there is a 'Show advanced option' link and an 'OK' button.

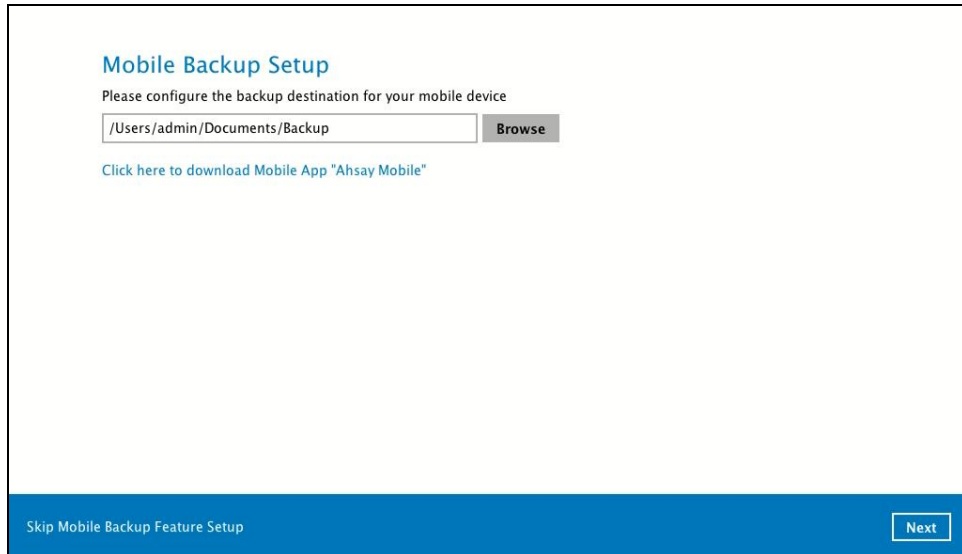
5. To set up your mobile backup and two-factor authentication click **Setup Now**.

The image is a promotional banner for the 'New Ahsay Mobile App, Free of Charge!'. It features a woman smiling next to a laptop and two smartphones displaying the app. The text on the left reads: 'Backup Your Mobile: Easily backup photos and videos to your PC or Mac through Wi-Fi. Stop paying for public cloud storage when local storage is free and MORE secured.' and 'Keep Hackers Off: All hackers delete backup data after compromising a machine. Use Two-Factor Authentication (2FA) to keep hackers off your backup data and turn ransomware harmless.' A 'Setup Now' button is located in the bottom right corner.

6. Download the Ahsay Mobile app from the App Store / Google Play Store. Click **Next**.

The image shows the 'Mobile App Download' screen. It has a blue header with the title 'Mobile App Download'. Below the title, it says 'Please use your mobile device to get the below Mobile App from Apple App Store / Google Play Store.' There is a small icon of a smartphone with the text 'Ahsay Mobile' next to it. Below this, it says 'Once ready, hit [Next] button to continue the setup.' There are two buttons: 'Download on the App Store' and 'GET IT ON Google Play'. A 'Next' button is located in the bottom right corner.

7. Click **Browse** to select the location where the backup of your device will be saved. Click **Next** to proceed.



Mobile Backup Setup

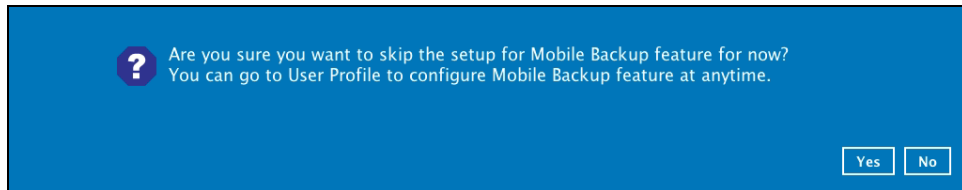
Please configure the backup destination for your mobile device

Browse

[Click here to download Mobile App "Ahsay Mobile"](#)

Skip Mobile Backup Feature Setup **Next**

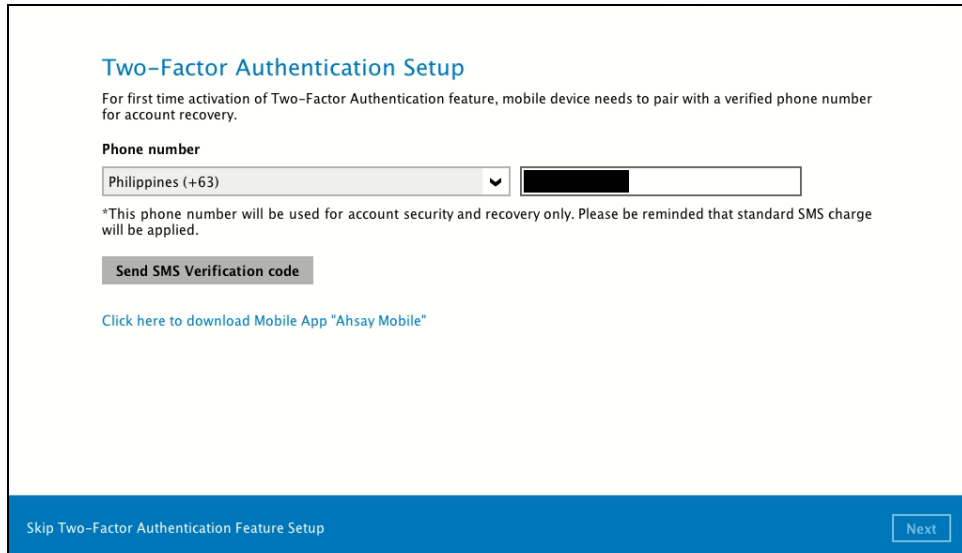
If you do not want to set up the mobile backup feature click **Skip Mobile Backup Feature Setup** link. Click **Yes** in the pop-up message that will be displayed. Otherwise click **No** to continue with the set-up of mobile backup feature.



? Are you sure you want to skip the setup for Mobile Backup feature for now?
You can go to User Profile to configure Mobile Backup feature at anytime.

Yes **No**

8. Select your country code and enter your phone number. Click **Send SMS Verification code** to receive the passcode.



Two-Factor Authentication Setup

For first time activation of Two-Factor Authentication feature, mobile device needs to pair with a verified phone number for account recovery.

Phone number

*This phone number will be used for account security and recovery only. Please be reminded that standard SMS charge will be applied.

Send SMS Verification code

[Click here to download Mobile App "Ahsay Mobile"](#)

Skip Two-Factor Authentication Feature Setup **Next**

9. Enter the verification code sent to your mobile device and then click **Next**.

Two-Factor Authentication Setup

For first time activation of Two-Factor Authentication feature, mobile device needs to pair with a verified phone number for account recovery.

Phone number

Philippines (+63)

*This phone number will be used for account security and recovery only. Please be reminded that standard SMS charge will be applied.

Verification code

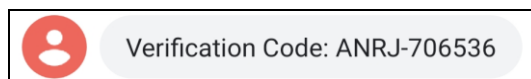
ANRJ - (00:04:37)

Resend SMS Verification code

[Click here to download Mobile App "Ahsay Mobile"](#)

Skip Two-Factor Authentication Feature SetupNext


Example of the verification code sent to mobile device.





10. To register Ahsay Mobile for 2FA (Push Notification and TOTP) and Mobile Backup, simply scan the displayed QR code using the Ahsay Mobile app.

Device Pairing

Please scan the QR code to register your mobile device with your backup account for following feature:

 Mobile Backup

 Two-Factor Authentication



Please make sure below 2 ports are not blocked by any Firewall settings before pairing your mobile device for backup

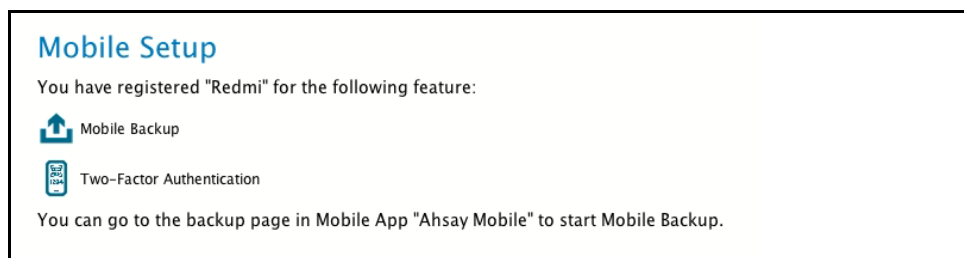
TCP Port: 54000
UDP Port: 54200

[Using other TOTP Authenticator App \(e.g. Authy, Duo, Google\)](#)

In this example, the Ahsay Mobile app is installed on a mobile device named “Redmi”.

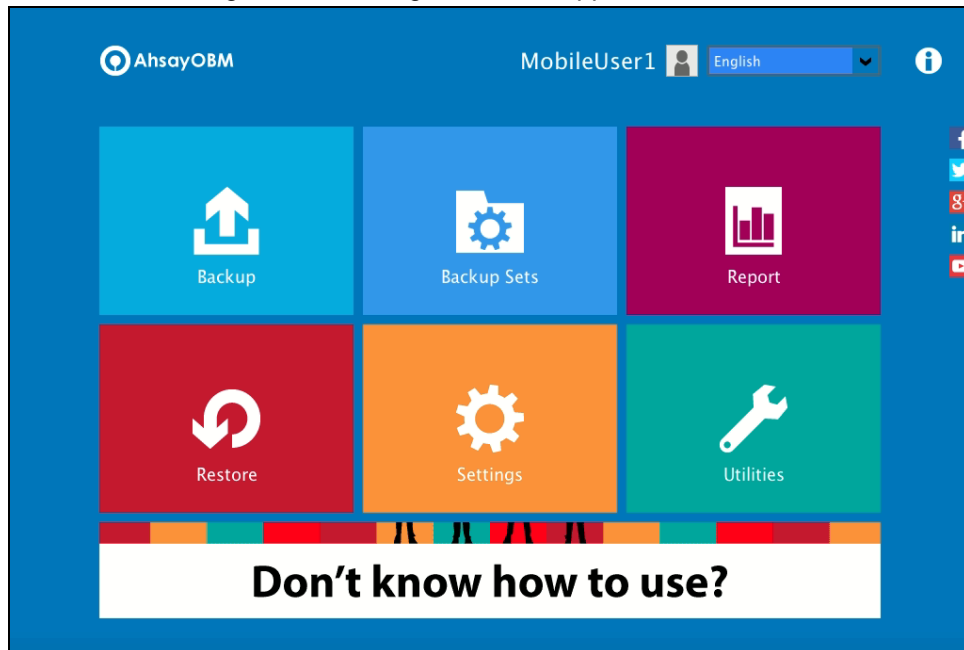


After successful scan of the QR code, you have now registered Ahsay Mobile for 2FA (Push Notification and TOTP) and Mobile Backup.



To configure a TOTP only 2FA with Ahsay Mobile, please refer to [TOTP only 2FA](#).

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



NOTE

Please refer to the [Ahsay Mobile App User Guide for Android and iOS – Appendix A: Troubleshooting Login](#) if you are experiencing problems logging into AhsayOBM with Two-Factor Authentication using Ahsay Mobile app.

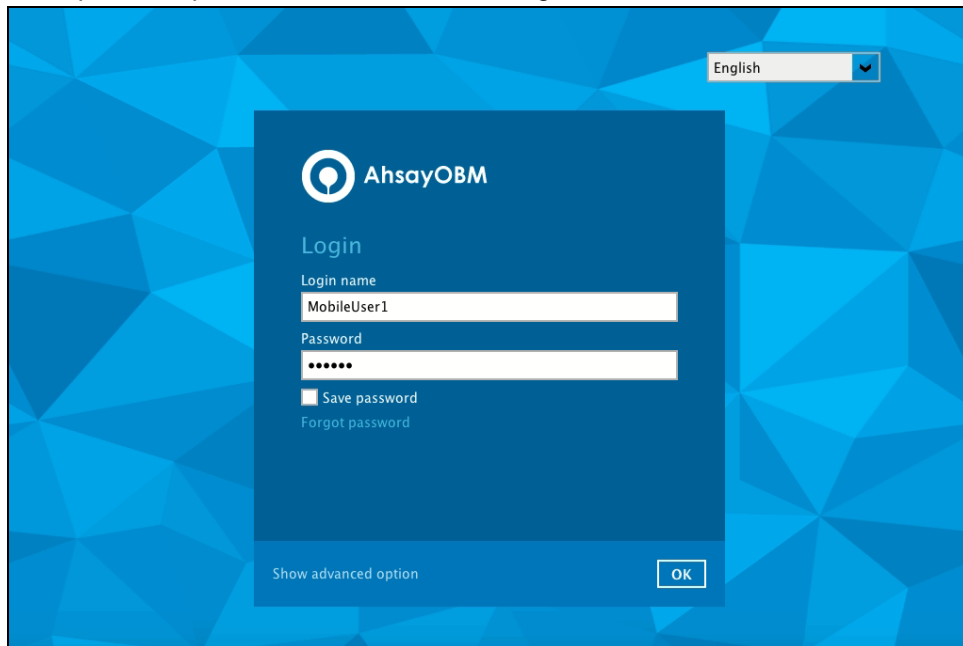
6.3.3 Subsequent login to AhsayOBM with 2FA

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

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



2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



3. Select the authentication method to continue with the login.

There are two authentication method to choose from it is possible to use both methods on the same AhsayOBM user account:

- [Ahsay Mobile app](#)
 - 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 App](#)
(e.g. Authy, Duo, Google)
-

If **Ahsay Mobile app** will be used as authenticator, there are two 2FA modes that can be selected:

🔵 **Push Notification and TOTP (default mode)**

Example of the 2FA alert screen on AhsayOBM after login with correct username and password.

Two-Factor Authentication

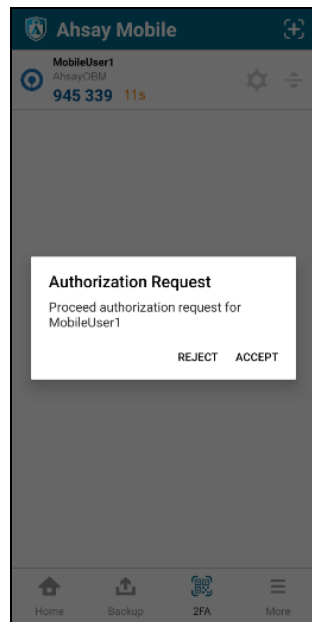
Please approve the notification request in Authenticator App on "Redmi".

🕒 Waiting for response (00:04:47)

[Authenticate with one-time password](#)

Push notification is the default 2FA mode. Accept the login request on Ahsay Mobile to complete the login.

Example of the login request sent to the Ahsay Mobile app.



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 Ahsay Mobile to complete the login.

Two-Factor Authentication

Please input the one-time password generated in Authenticator App from "Redmi Note 8".

(00:00:30)

• TOTP only

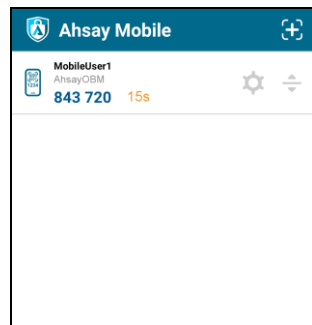
Example of the 2FA alert screen on AhsayOBM after login with correct username and password.

Two-Factor Authentication

Please input the one-time password generated in Authenticator App from "Redmi Note 8".

(00:00:30)

Example of the one-time password generated from Ahsay Mobile to complete the login.



If a third-party **TOTP Authenticator App** will be used instead, follow the steps below to login.

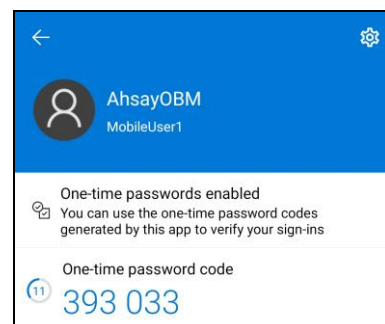
- Enter the one-time password that is generated by the authenticator app and click **Next**.

Two-Factor Authentication

Please input the one-time password generated in Authenticator App from "MobileUser1".

(00:00:24)

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



In the following example, both Ahsay Mobile and a third-party TOTP Authenticator App has been setup for 2FA, select your preferred 2FA method from the options available to complete the login.

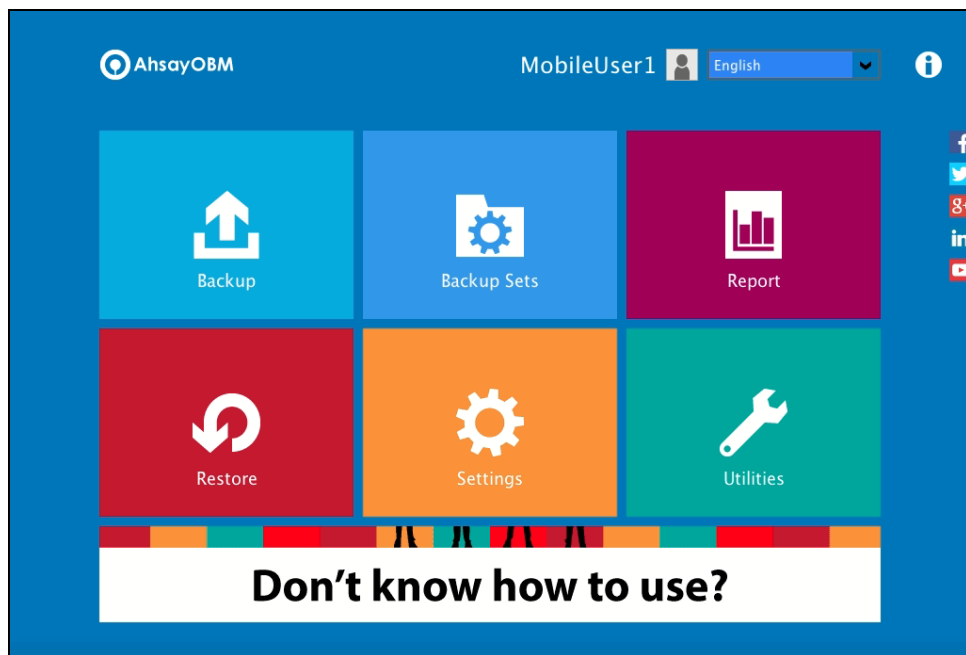
Two-Factor Authentication

Please select one Two-Factor Authentication method to continue.

☒ Approve request in Authenticator App from "Redmi"

☐ Input one-time password generated in Authenticator App from "MobileUser1"

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



NOTE

Please refer to the [Ahsay Mobile App User Guide for Android and iOS – Appendix A: Troubleshooting Login](#) if you are experiencing problems logging into AhsayOBM with Two-Factor Authentication using Ahsay Mobile app.

6.4 Login to AhsayOBM with 2FA using Twilio

For AhsayOBM user accounts using Twilio, please follow the steps below:

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



2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.

A screenshot of the AhsayOBM login dialog box. The dialog has a blue background with a white AhsayOBM logo and the text 'AhsayOBM'. Below the logo, it says 'Login'. There are two input fields: 'Login name' with the text 'MobileUser1' and 'Password' with masked characters '*****'. Below the password field, there is a checkbox labeled 'Save password' and a link 'Forgot password'. At the bottom left, there is a link 'Show advanced option', and at the bottom right, there is an 'OK' button. The background of the window is a blue geometric pattern.

3. Select your phone number to receive the passcode.

A screenshot of the Two-Factor Authentication dialog box. The title is 'Two-Factor Authentication'. Below the title, it says 'Please select phone number to receive passcode via SMS message to continue login.' There is a list of phone numbers with a phone icon next to the first one: 'Philippines (+63) - *****8106'. At the bottom right, there are 'Cancel' and 'Help' buttons.

4. Enter the passcode and click **Verify** to login.

Two-Factor Authentication

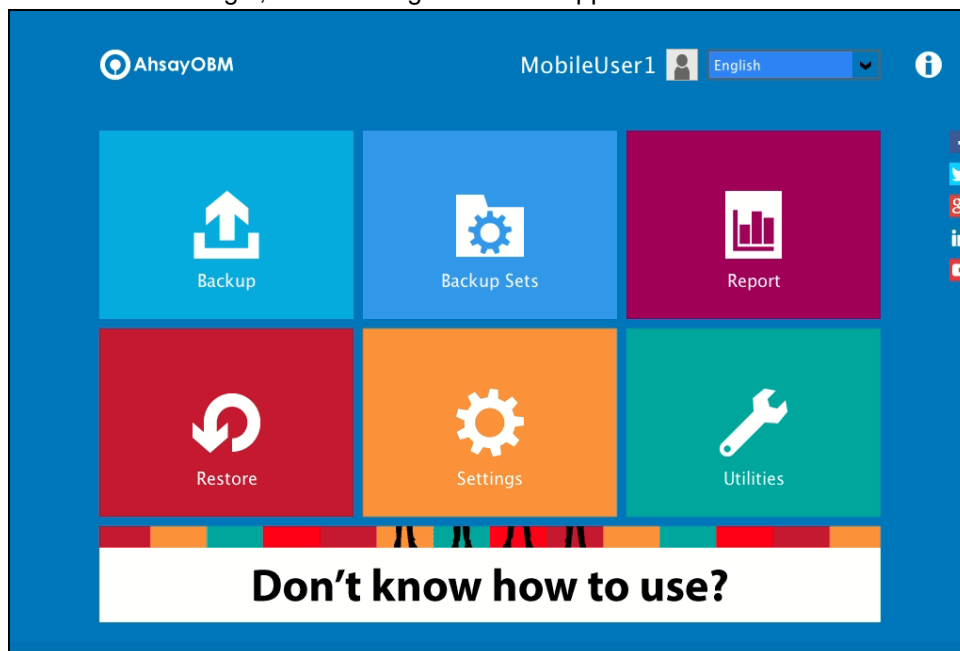
SMS message with a passcode was already sent to the phone number Philippines (+63) - *****8106
Please enter the passcode to continue login.

AMIE - (00:04:48)

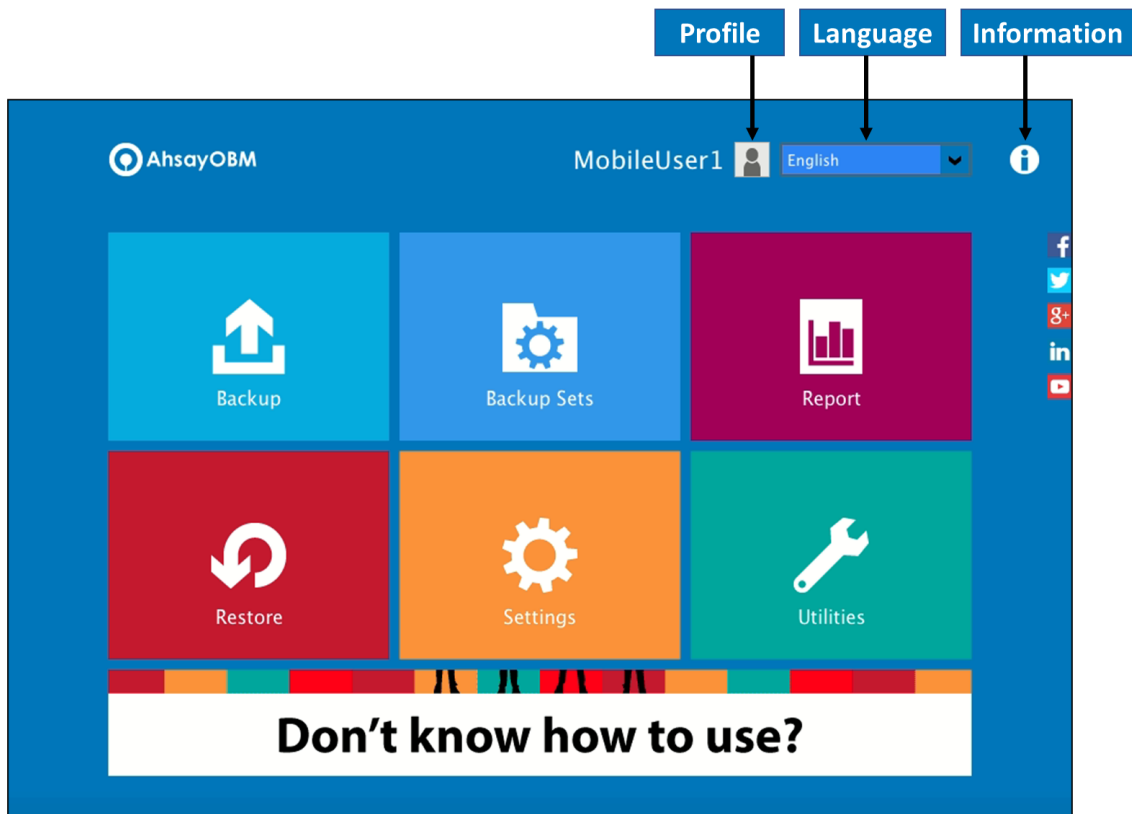
[Resend passcode](#)

[Verify](#) [Cancel](#) [Help](#)

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



7 AhsayOBM Overview

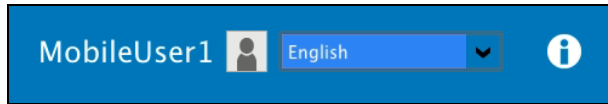


AhsayOBM main interface has nine (9) icons that can be accessed by the user, namely:

- Profile
- Language
- Information
- Backup
- Backup Sets
- Report
- Restore
- Settings
- Utilities

7.1 Profile

The Profile icon shows the settings that can be modified by the user. The features that will be shown will depend if the user accounts was using Twilio Two-Factor Authentication in prior to upgrading to v8.5.0.0 or above and continues to use Twilio.



There are eight (8) available features:

- ◉ [General](#)
- ◉ [Contacts](#)
- ◉ [Time Zone](#)
- ◉ [Encryption Recovery](#)
- ◉ [Password](#) (Only shown for backup accounts created prior to AhsayOBM v8.5.0.0 and using Twilio for two-factor authentication.)
- ◉ [Authentication](#)
- ◉ [Mobile Backup](#) (Only available if the mobile add-on module is enabled on the user profile. Please contact your backup service provider for details.)
- ◉ [Security Settings](#) (Only shown for backup accounts created prior to AhsayOBM v8.5.0.0 and using Twilio for two-factor authentication.)

7.1.1 General

The General tab displays the user information.

Profile

General

Contacts

Time Zone

Encryption Recovery

Authentication

Mobile Backup

User Information

Login name

MobileUser1

Display name

Save

Cancel

Help

Control	Description
Login name	Name of the backup account.
Display name	Display name of the backup account upon logging in to the AhsayCBS User Web Console.

This will be the General tab for old backup account using Twilio for two-factor authentication.

Profile

- General
- Contacts
- Time Zone
- Encryption Recovery
- Password
- Mobile Backup
- Security Settings

User Information

Login name MobileUser1
Display name

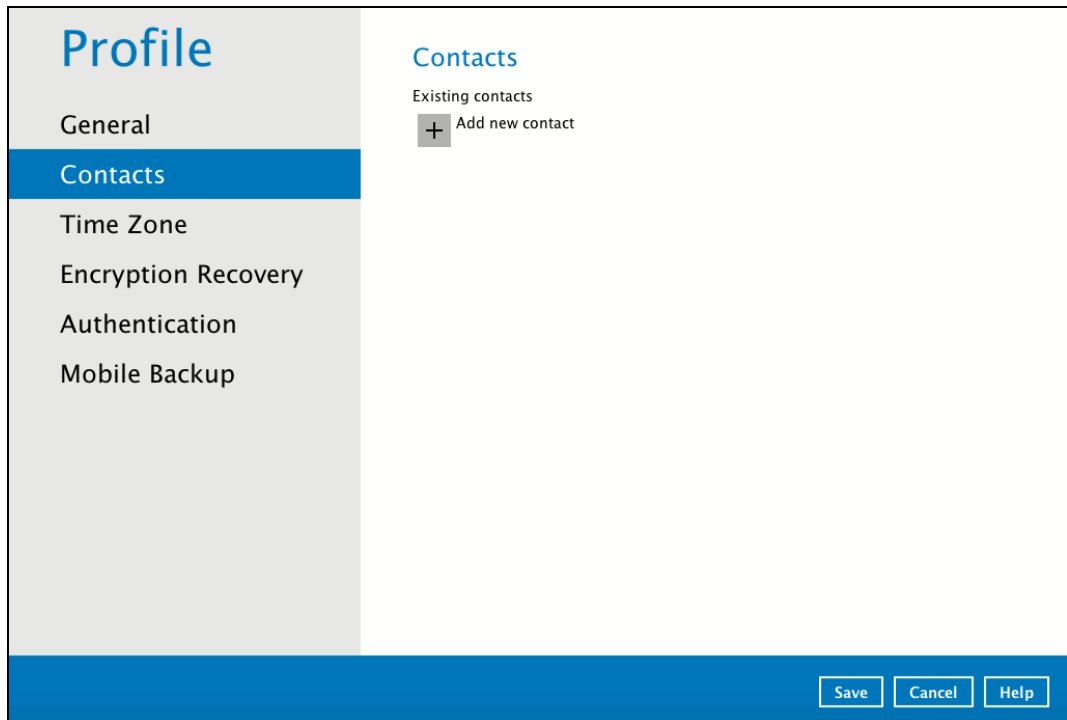
Last Successful Login

Time: 12/14/2020 19:57 (PHT)
IP address: 175.176.32.185
Phone number (MFA): 63-09205548106
Browser / App: OBM

Control	Description
Login name	Name of the backup account.
Display name	Display name of the backup account upon logging in to the AhsayCBS User Web Console.
Time	The date and time the user last logged in.
IP address	The IP address used to login.
Phone number (MFA)	The phone number where sms authentication will be sent when 2FA is enabled.
Browser / App	The browser or app used to login in to AhsayCBS User Web Console or AhsayOBM.

7.1.2 Contacts

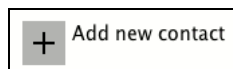
This refers to the contact information of the user. You can also add multiple contacts or modify existing contact information. Having this filled in will help in sending backup and daily reports and even recovered backup set encryption key in case it was forgotten or lost.



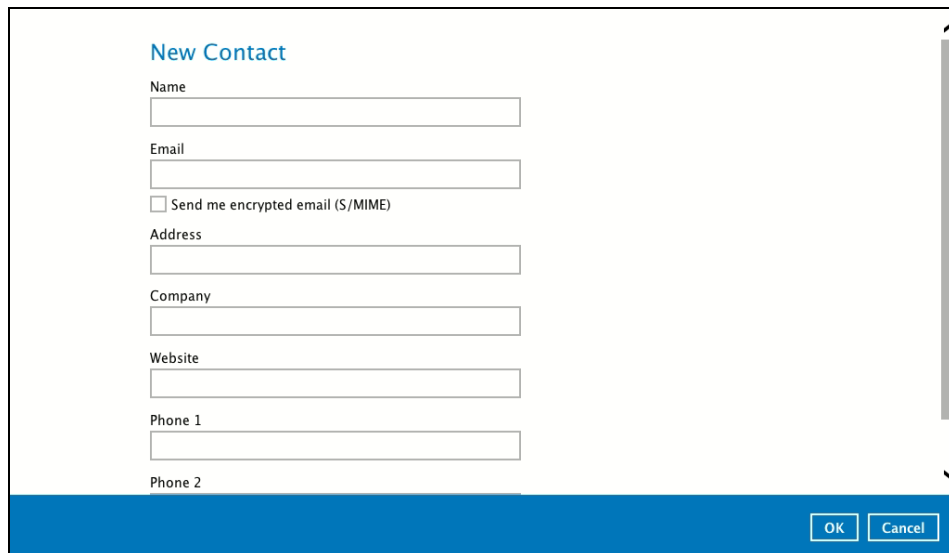
The screenshot shows a user interface with a left sidebar and a main content area. The sidebar is titled 'Profile' and contains a list of settings: 'General', 'Contacts' (highlighted in blue), 'Time Zone', 'Encryption Recovery', 'Authentication', and 'Mobile Backup'. The main content area is titled 'Contacts' and shows 'Existing contacts' with a '+ Add new contact' button. At the bottom right of the main content area, there are three buttons: 'Save', 'Cancel', and 'Help'.

To add a new contact, follow the instructions below:

1. Click the [+] plus sign to add a new contact.



2. Complete the following fields then click OK to return to the main screen.
 - Name
 - Email
 - Address
 - Company
 - Website
 - Phone 1
 - Phone 2



A screenshot of a 'New Contact' form. The form is titled 'New Contact' in blue. It contains several input fields: 'Name', 'Email', 'Address', 'Company', 'Website', 'Phone 1', and 'Phone 2'. There is a checkbox labeled 'Send me encrypted email (S/MIME)'. At the bottom right, there are 'OK' and 'Cancel' buttons. The form is set against a white background with a blue footer bar.

New Contact

Name

Email

☐ Send me encrypted email (S/MIME)

Address

Company

Website

Phone 1

Phone 2

OK Cancel

3. Click Save to store the contact information.



A screenshot of a 'Profile' page. The left sidebar has a 'Profile' header and a list of menu items: 'General', 'Contacts' (highlighted in blue), 'Time Zone', 'Encryption Recovery', 'Authentication', and 'Mobile Backup'. The main content area is titled 'Contacts' and shows 'Existing contacts' with a list containing one entry: 'samplename' with email 'sample_email@mail.com'. There is an 'Add' button below the list. At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons. The page has a blue footer bar.

Profile

General

Contacts

Time Zone


Encryption Recovery

Authentication

Mobile Backup

Contacts

Existing contacts

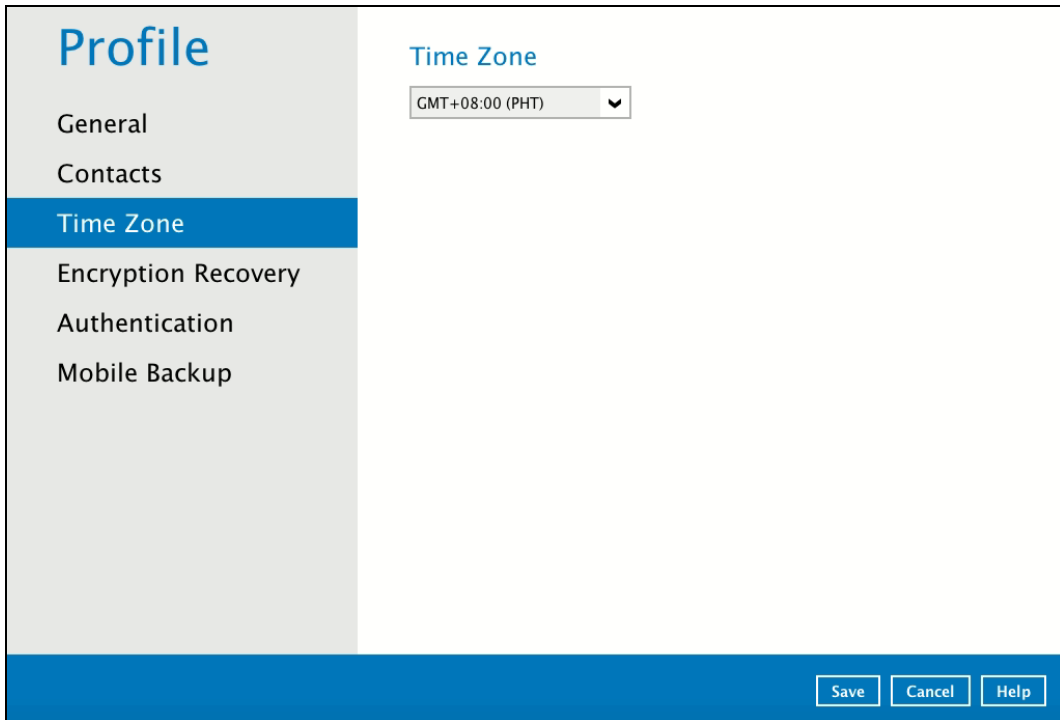
 **samplename**
sample_email@mail.com

Add

Save Cancel Help

7.1.3 Time Zone

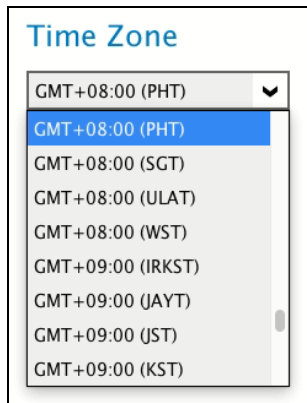
The time zone indicated.



The screenshot shows a web interface for a 'Profile' page. On the left is a sidebar with a blue header 'Profile' and a list of menu items: 'General', 'Contacts', 'Time Zone' (highlighted in blue), 'Encryption Recovery', 'Authentication', and 'Mobile Backup'. The main content area is titled 'Time Zone' and contains a dropdown menu currently set to 'GMT+08:00 (PHT)'. At the bottom right of the main area are three buttons: 'Save', 'Cancel', and 'Help'.

To modify the time zone, follow the instructions below:

1. Select from the dropdown list.



This image is a close-up of the 'Time Zone' dropdown menu. The menu is open, showing a list of time zone options. The first option, 'GMT+08:00 (PHT)', is highlighted in blue. Other visible options include 'GMT+08:00 (SGT)', 'GMT+08:00 (ULAT)', 'GMT+08:00 (WST)', 'GMT+09:00 (IRKST)', 'GMT+09:00 (JAYT)', 'GMT+09:00 (JST)', and 'GMT+09:00 (KST)'. A scroll bar is visible on the right side of the list.

2. Click Save to save the updated time zone.

7.1.4 Encryption Recovery

Backup set encryption key can be recovered by turning this feature on.

NOTE

This option may not be available. Please contact your backup service provider for more details.

Profile

- General
- Contacts
- Time Zone
- Encryption Recovery
- Authentication
- Mobile Backup

Encryption Recovery

With this option enabled, you can recover your backup set encryption keys by sending a request to us.

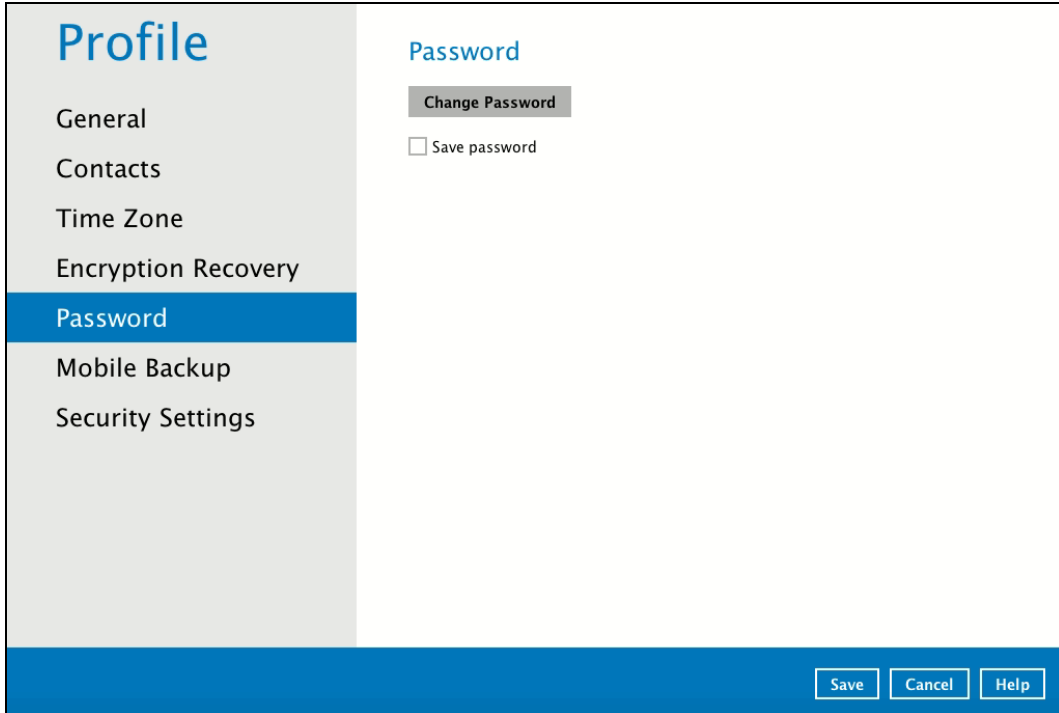
On ☒

[Save](#) [Cancel](#) [Help](#)

7.1.5 Password

The Password option is for backward compatibility with Twilio Two-Factor Authentication. It will only be visible if Twilio Two-Factor Authentication was enabled on the user account on pre-v8.5.0.0 AhsayOBM versions.

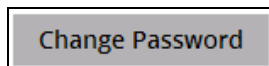
Login password can be modified anytime. Tick the [Save Password] box to bypass the password entry upon opening the AhsayOBM.



The screenshot shows the 'Profile' settings page. On the left is a sidebar with options: General, Contacts, Time Zone, Encryption Recovery, Password (highlighted in blue), Mobile Backup, and Security Settings. The main content area is titled 'Password' and contains a 'Change Password' button and an unchecked checkbox labeled 'Save password'. At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons.

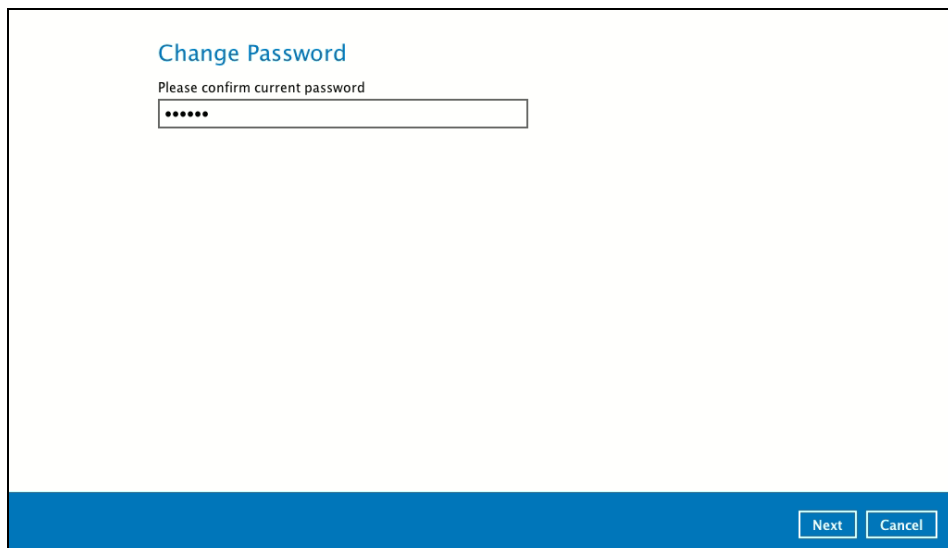
To modify the password, follow the instructions below:

1. Click Change Password



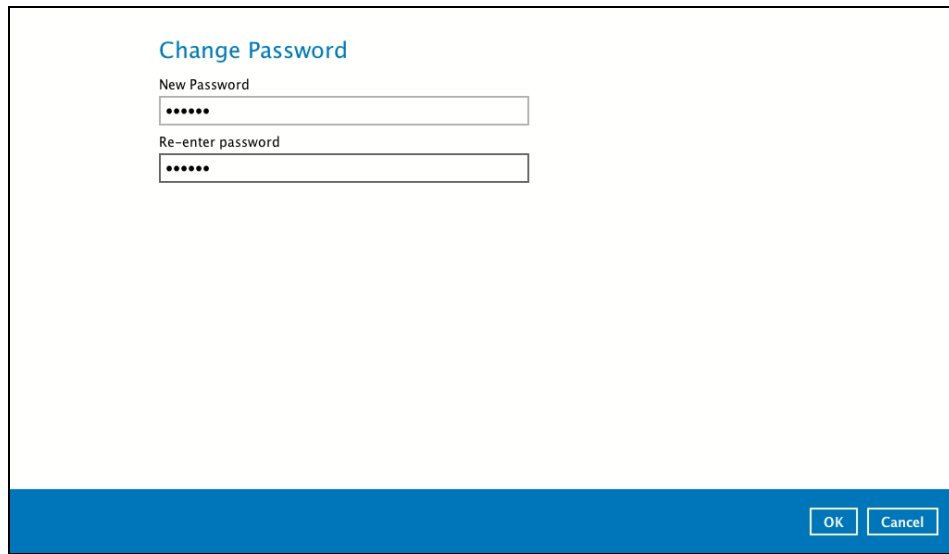
A close-up of the 'Change Password' button, which is a grey rectangular button with the text 'Change Password' in blue.

2. Enter the current password, then click Next.



The screenshot shows a 'Change Password' dialog box. It has the title 'Change Password' and the instruction 'Please confirm current password'. Below this is a password input field with six dots. At the bottom right, there are 'Next' and 'Cancel' buttons.

3. Enter the New Password and re-enter, then click OK button to return to the main screen.



A screenshot of a 'Change Password' dialog box. The title 'Change Password' is in blue text at the top left. Below it, there are two text input fields. The first field is labeled 'New Password' and contains six black dots. The second field is labeled 'Re-enter password' and also contains six black dots. At the bottom right of the dialog box, there are two buttons: 'OK' and 'Cancel'.

4. Click Save button to store the updated password.

7.1.6 Authentication

You can use the Authentication function to:

- Change the “[Password](#)”.
- Enable or disable the “[Two-Factor Authentication](#)”.
- Add one or more device(s) registered for Two-Factor Authentication (2FA).

NOTE

Please refer to the [Ahsay Mobile App User Guide for Android and iOS – Chapter 6.3.1](#) for the detailed step-by-step procedure.

- [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

For Two-Factor Authentication (2FA), you can register your mobile device on both Ahsay Mobile app and a third-party authenticator apps (e.g. Authy, Duo, Google Authenticator, Microsoft Authenticator, and LastPass Authenticator).

Profile

- General
- Contacts
- Time Zone
- Encryption Recovery
- Authentication**
- Mobile Backup

Password

Change Password

☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

Off ☐

Last Successful Login

No login record

Save

Cancel

Help

Password

Login password can be modified anytime. Tick the **Save Password** box to bypass the password entry upon opening the AhsayOBM.

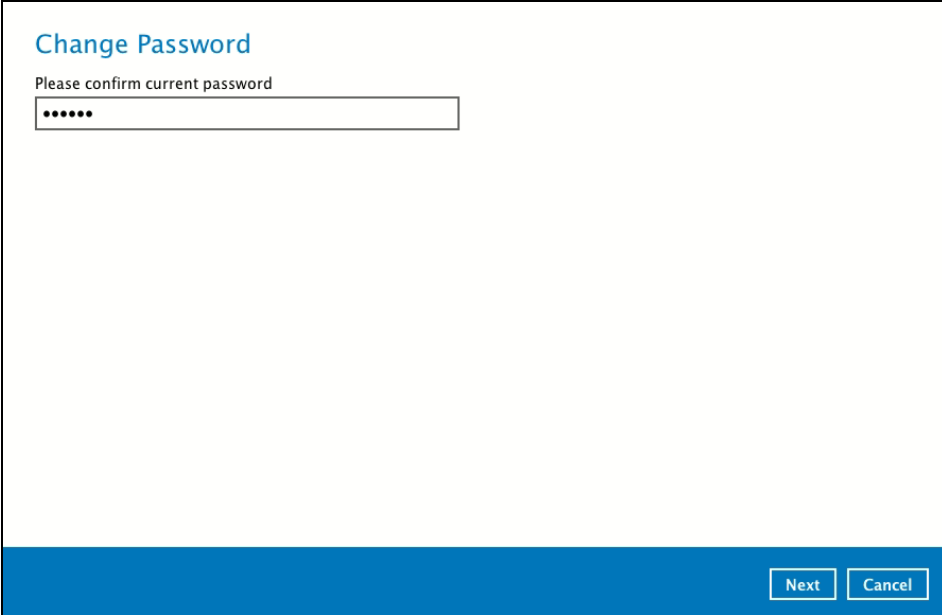
The screenshot shows the 'Profile' page with a sidebar on the left containing links: General, Contacts, Time Zone, Encryption Recovery, Authentication (highlighted in blue), and Mobile Backup. The main content area is titled 'Password' and includes a 'Change Password' button. Below this is a checkbox labeled 'Save password' which is checked. Further down is the 'Two-Factor Authentication' section, which states 'Require Authenticator App to sign in your account during startup' and has a toggle switch set to 'Off'. At the bottom of the main area is the 'Last Successful Login' section, which says 'No login record'. A blue footer bar at the very bottom contains 'Save', 'Cancel', and 'Help' buttons.

To change the password, follow the instructions below:

1. Click the **Change Password**.

This screenshot is identical to the one above, showing the 'Profile' page with the 'Password' section. The 'Change Password' button is highlighted with a grey background, indicating it is the next step in the process. The 'Save password' checkbox remains checked, and the 'Two-Factor Authentication' toggle is still 'Off'. The 'Last Successful Login' section continues to show 'No login record'. The blue footer bar with 'Save', 'Cancel', and 'Help' buttons is also present.

2. Enter the current password.



The dialog box is titled "Change Password" in blue text. Below the title, it says "Please confirm current password". There is a single text input field with six dots inside, representing the current password. At the bottom right, there are two buttons: "Next" and "Cancel".

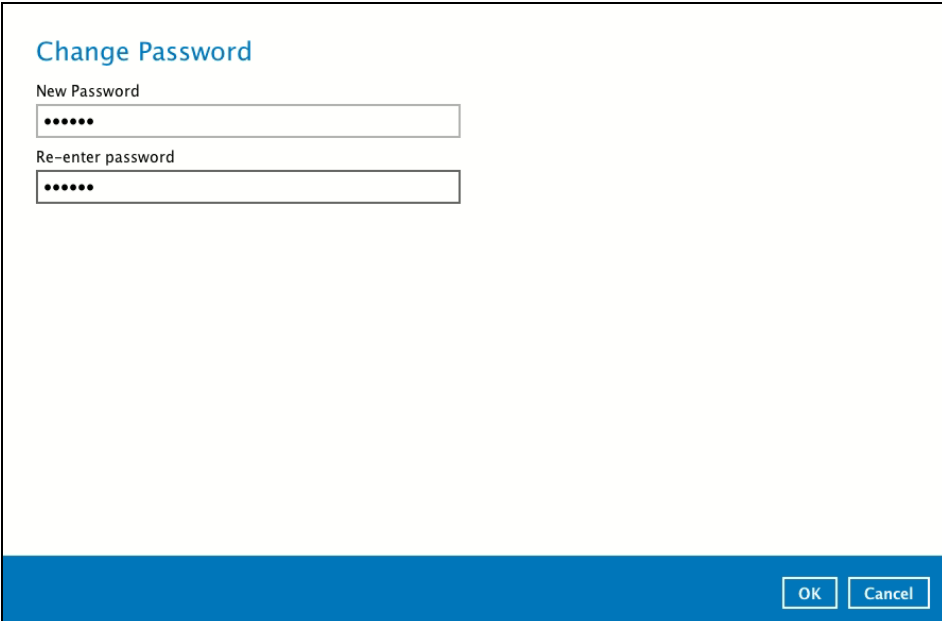
Change Password

Please confirm current password

.....

Next Cancel

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



The dialog box is titled "Change Password" in blue text. Below the title, it says "New Password". There is a text input field with six dots inside. Below that, it says "Re-enter password". There is another text input field with six dots inside. At the bottom right, there are two buttons: "OK" and "Cancel".

Change Password

New Password

.....

Re-enter password

.....

OK Cancel

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

Profile

- General
- Contacts
- Time Zone
- Encryption Recovery
- Authentication**
- Mobile Backup

Password

[Change Password](#)

☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

Off ☐

Last Successful Login

No login record

[Save](#) [Cancel](#) [Help](#)

Two-Factor Authentication

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

NOTE

The Ahsay Mobile app or a third-party authenticator apps is needed for 2FA.

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

The screenshot shows the 'Profile' settings screen. On the left is a sidebar menu with options: General, Contacts, Time Zone, Encryption Recovery, Authentication (highlighted in blue), and Mobile Backup. The main content area is titled 'Two-Factor Authentication' and includes the text 'Require Authenticator App to sign in your account during startup'. Below this, the toggle switch is in the 'Off' position. Other visible options include 'Change Password', 'Save password' (unchecked), and 'Last Successful Login' (No login record). At the bottom right are 'Save', 'Cancel', and 'Help' buttons.

2. Swipe lever to the right to turn it on.

For the detailed step-by-step procedure on how to add a mobile device, please refer to [Ahsay Mobile App User Guide for Android and iOS – Chapter 6.3.1](#)

This screenshot shows the same 'Two-Factor Authentication' settings screen, but the toggle switch is now in the 'On' position. An 'Add' button has appeared below the 'Registered Mobile Device(s)' label. The 'Save password' checkbox is now checked. All other elements, including the sidebar menu and bottom buttons, remain the same as in the previous screenshot.

To remove a mobile device, follow the instructions below:

1. Click the **[X]** button on the left side of the registered mobile device.

Profile

- General
- Contacts
- Time Zone
- Encryption Recovery
- Authentication**
- Mobile Backup

Password

[Change Password](#)

☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

On ☒

Registered Mobile Device(s)

- 1234 MobileUser1 **X**
- Redmi **X**

[Add](#)

Last Successful Login

Time: 12/14/2020 00:19 (PHT)
IP address: 175.176.32.99
Browser / App: OBM
Mobile Device: Redmi

[Save](#) [Cancel](#) [Help](#)

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

Profile

- General
- Contacts
- Time Zone

Confirmation Dialog:

Are you sure you want to delete the registered Mobile Device for Two-Factor Authentication feature?

[Yes](#) [No](#)

Last Successful Login

Time: 12/12/2020 22:35 (PHT)
IP address: 175.176.32.5
Browser / App: OBM
Mobile Device: MobileUser1

[Save](#) [Cancel](#) [Help](#)

3. Mobile device is successfully removed.

Profile

- General
- Contacts
- Time Zone
- Encryption Recovery
- Authentication**
- Mobile Backup

Password

Change Password


☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

On ☒

Registered Mobile Device(s)

 Redmi

X

Add

Last Successful Login

Time: 12/12/2020 22:35 (PHT)
IP address: 175.176.32.5
Browser / App: OBM
Mobile Device: MobileUser1

Save

Cancel

Help

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.

The screenshot shows the 'Profile' settings page. The left sidebar contains links: General, Contacts, Time Zone, Encryption Recovery, Authentication (highlighted), and Mobile Backup. The main content area has three sections: 'Password' with a 'Change Password' button and a 'Save password' checkbox; 'Two-Factor Authentication' with a toggle switch set to 'On', a list of registered devices ('MobileUser1' and 'Redmi'), and an 'Add' button; and 'Last Successful Login' showing details for a login on 12/14/2020. At the bottom right are 'Save', 'Cancel', and 'Help' buttons.

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

This screenshot shows the same 'Profile' settings page, but the 'Two-Factor Authentication' toggle switch is now set to 'Off'. The list of registered devices is empty, and the 'Last Successful Login' section indicates 'No login record'. The 'Save', 'Cancel', and 'Help' buttons remain at the bottom right.

Last Successful Login

Displays the Date, Time, IP address, and Browser / App the user last logged in and the registered Mobile Device.

- ▶ Time – the date and time the user last logged in.
- ▶ IP address – the IP address used to login.
- ▶ Browser / App – the browser or app used to login to AhsayCBS User Web Console or AhsayOBM.
- ▶ Mobile Device – the name of the device used for authentication when 2FA is enabled.

The screenshot shows the 'Profile' page with a sidebar menu containing: General, Contacts, Time Zone, Encryption Recovery, Authentication (selected), and Mobile Backup. The main content area is divided into three sections: 'Password' with a 'Change Password' button and a 'Save password' checkbox; 'Two-Factor Authentication' with a toggle set to 'On', a list of registered mobile devices (1234 MobileUser1 and Redmi), and an 'Add' button; and 'Last Successful Login' displaying the following information: Time: 12/14/2020 00:19 (PHT), IP address: 175.176.32.99, Browser / App: OBM, and Mobile Device: Redmi. At the bottom right are 'Save', 'Cancel', and 'Help' buttons.

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

This screenshot shows the same 'Profile' page as above, but with the 'Two-Factor Authentication' toggle set to 'Off'. The 'Last Successful Login' section now displays 'No login record'. The 'Save', 'Cancel', and 'Help' buttons remain at the bottom right.

7.1.7 Mobile Backup

You can use the Mobile backup function to:

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

NOTE

Please refer to the [Ahsay Mobile App User Guide for Android and iOS – Chapter 7](#) for the detailed step-by-step procedure.

- [Remove one or more device\(s\)](#) registered for Mobile Backup.
- Register your device multiple times on a different backup destination.

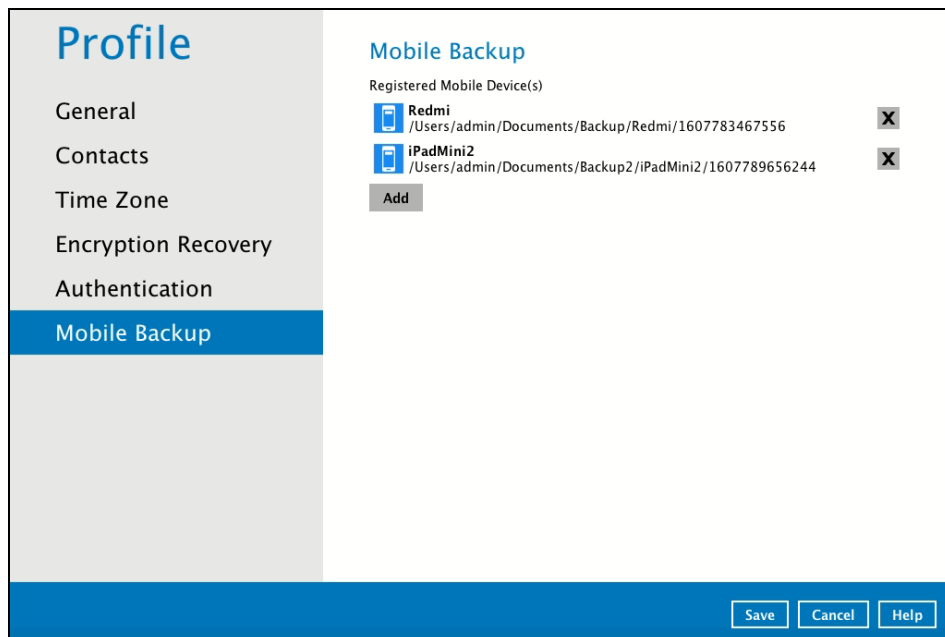
NOTE

For the restore of photos and videos to an alternate mobile device, the other mobile devices must be registered first for mobile backup on AhsayOBM.

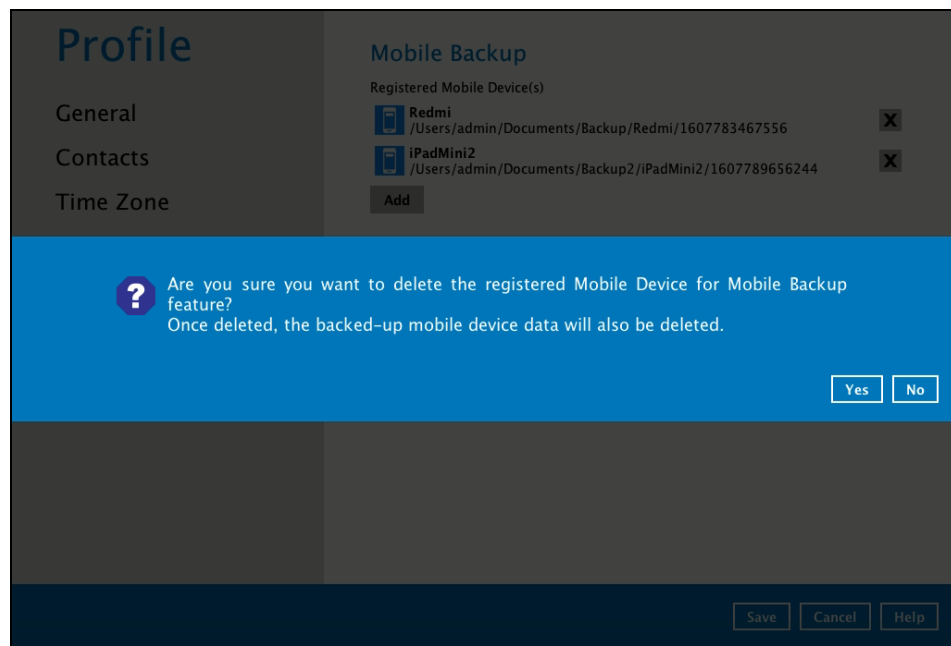
- Restore to a different mobile device on the same operating system.
- Restore to a different mobile device on another operating system, i.e., Android to iOS or iOS to Android.

To remove a mobile device, follow the instructions below:

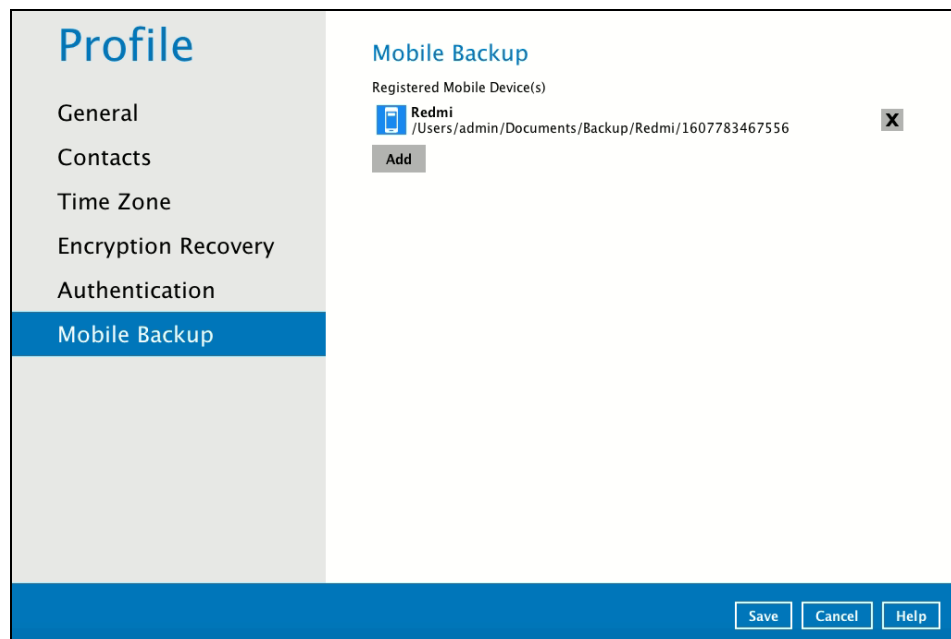
1. Click back **[X]** button on the left side of the registered mobile device.



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



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





7.1.8 Security Settings

The Security Settings option is for backward compatibility with Twilio Two-Factor Authentication. It will only be visible if Twilio Two-Factor Authentication was enabled on the user account on pre-v8.5.0.0 AhsayOBM versions.

Phone numbers that will be used for sending sms authentication will be listed here and will show the status if it is verified or not. You can also add phone numbers here that can be used for sending the sms authentication.

The screenshot shows a web interface for 'Profile' settings. On the left is a sidebar with a 'Profile' header and a list of settings: General, Contacts, Time Zone, Encryption Recovery, Password, Mobile Backup, and Security Settings (which is highlighted in blue). The main content area is titled 'Security Settings' and contains the text 'Phone numbers for SMS authentication'. Below this, there is a list of phone numbers. One number is shown: 'Philippines (+63) - 09205548106, Verified' with a blue phone icon and a red 'X' icon. Below the list is an 'Add' button. At the bottom right of the interface are three buttons: 'Save', 'Cancel', and 'Help'.

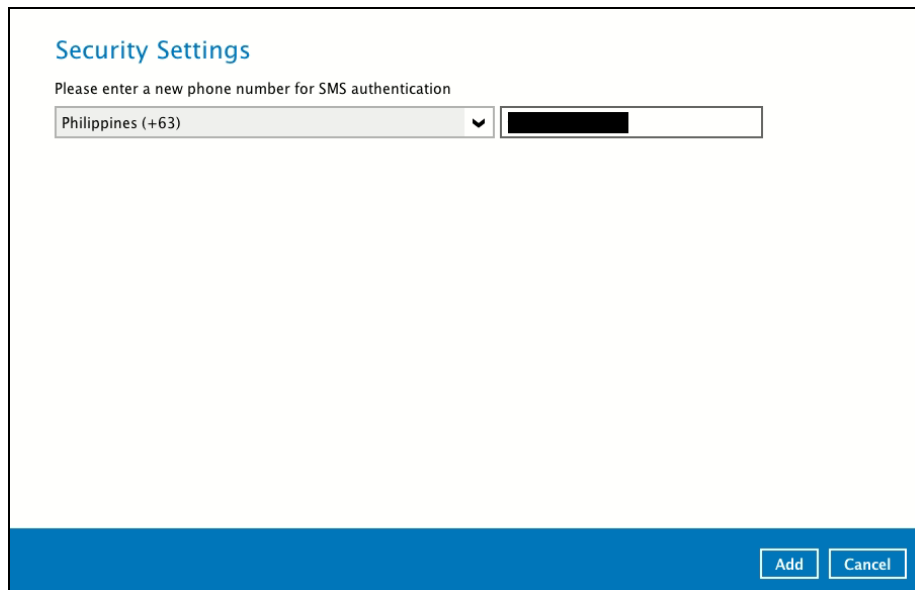
Phone numbers for SMS authentication
 Philippines (+63) - 09205548106, Verified 
Add

[Save](#) [Cancel](#) [Help](#)

1. Click Add.



2. Select the country and enter the phone number, click Add.

A screenshot of the "Security Settings" form. The title "Security Settings" is in blue. Below it, the text "Please enter a new phone number for SMS authentication" is in grey. There is a dropdown menu showing "Philippines (+63)" and a text input field for the phone number. At the bottom right, there are "Add" and "Cancel" buttons.

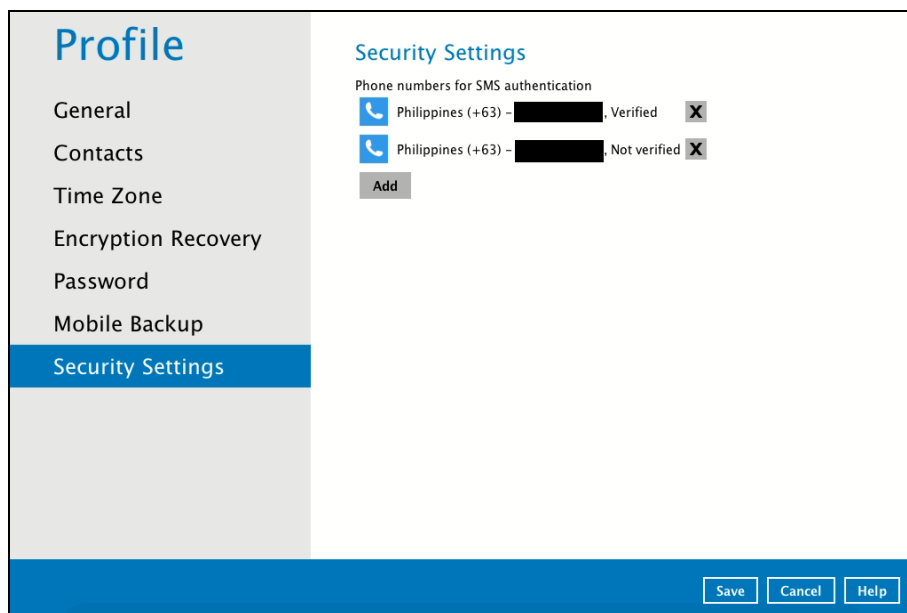
Security Settings

Please enter a new phone number for SMS authentication

Philippines (+63) [input field]

Add Cancel

3. Click Save to save the phone number.

A screenshot of the "Profile" page. On the left is a sidebar with a "Profile" header and a list of settings: General, Contacts, Time Zone, Encryption Recovery, Password, Mobile Backup, and Security Settings (which is highlighted in blue). The main content area is titled "Security Settings" and shows a list of "Phone numbers for SMS authentication". It contains two entries: "Philippines (+63) - [redacted] . Verified" and "Philippines (+63) - [redacted] . Not verified", each with a blue phone icon and a red 'X' icon. Below the list is an "Add" button. At the bottom right, there are "Save", "Cancel", and "Help" buttons.

Profile

General

Contacts

Time Zone

Encryption Recovery

Password

Mobile Backup

Security Settings

Security Settings

Phone numbers for SMS authentication

Philippines (+63) - [redacted] . Verified X

Philippines (+63) - [redacted] . Not verified X

Add

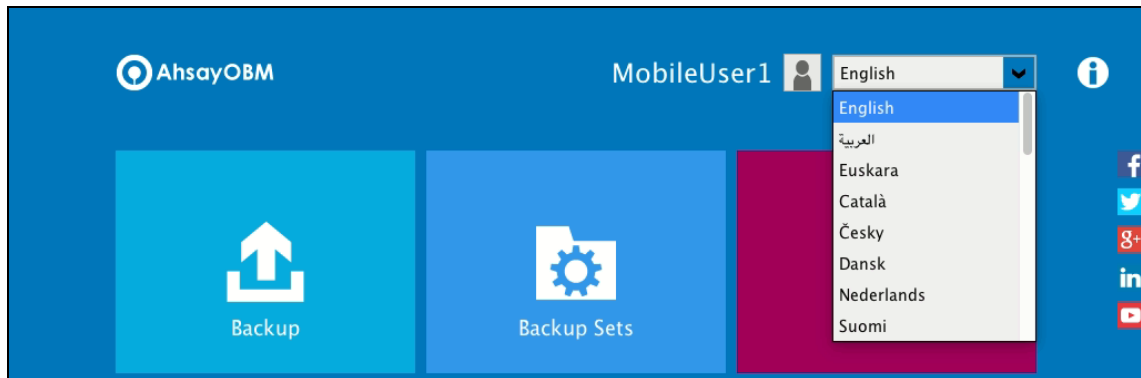
Save Cancel Help

7.2 Language

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

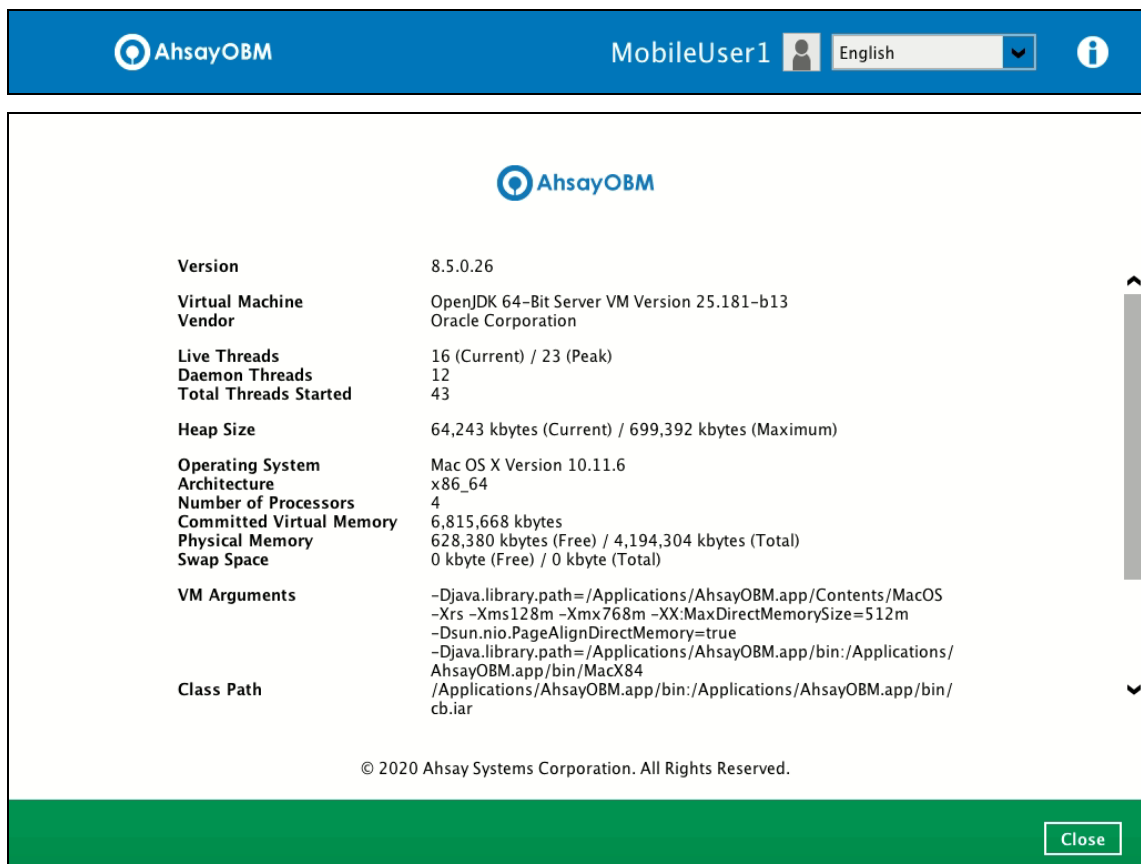


Once the language is set, it will reflect on the AhsayOBM interface right away.



7.3 Information

The **information** icon displays the product version and system information of the machine where the AhsayOBM is installed.



7.4 Backup

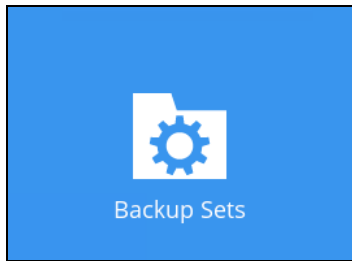
This feature is used to run your backup set(s).



To start backing up, follow the instructions on [Chapter 10 Run Backup Jobs](#).

7.5 Backup Sets

A **backup set** is a place for files and/or folders of your backed-up data. This feature allows user to select files individually or entirely in a selected folder to back up. It is also used to delete backup set(s).



To create or modify a backup set, follow the instructions on [Chapter 8 Create a Backup Set](#).

Backup Set Settings

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

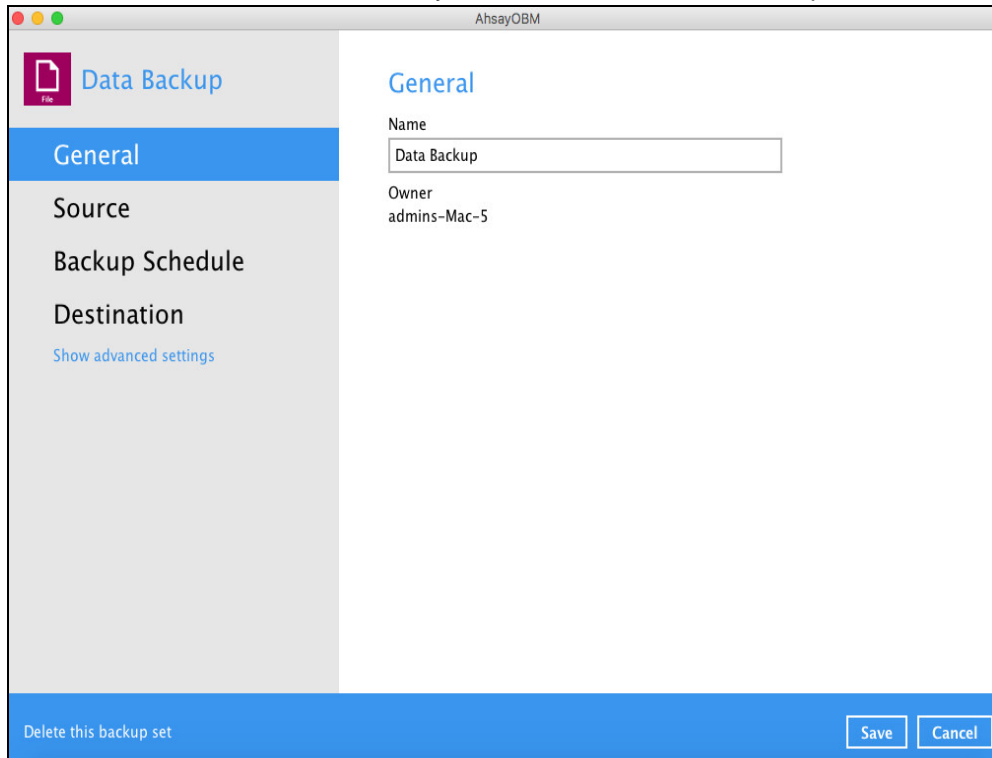
- [General](#)
- [Source](#)
- [Backup Schedule](#)
- [Destination](#)

(Advanced settings)

- [In-File Delta](#)
- [Retention Policy](#)
- [Command Line Tool](#)
- [Bandwidth Control](#)
- [Others](#)

General

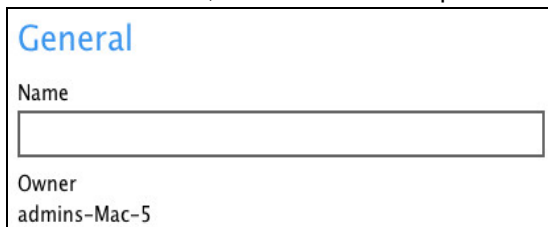
This feature allows the user to modify the current name of the backup set.



The screenshot shows a window titled "AhsayOBM" with a "Data Backup" icon and title. The left sidebar contains a "General" tab (selected), "Source", "Backup Schedule", "Destination", and a "Show advanced settings" link. The main area is titled "General" and contains a "Name" field with the value "Data Backup" and an "Owner" field with the value "admins-Mac-5". At the bottom, there is a blue bar with a "Delete this backup set" link on the left and "Save" and "Cancel" buttons on the right.

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

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



This is a close-up of the "General" settings form. It shows the "Name" field with a text input box and the "Owner" field with the value "admins-Mac-5".

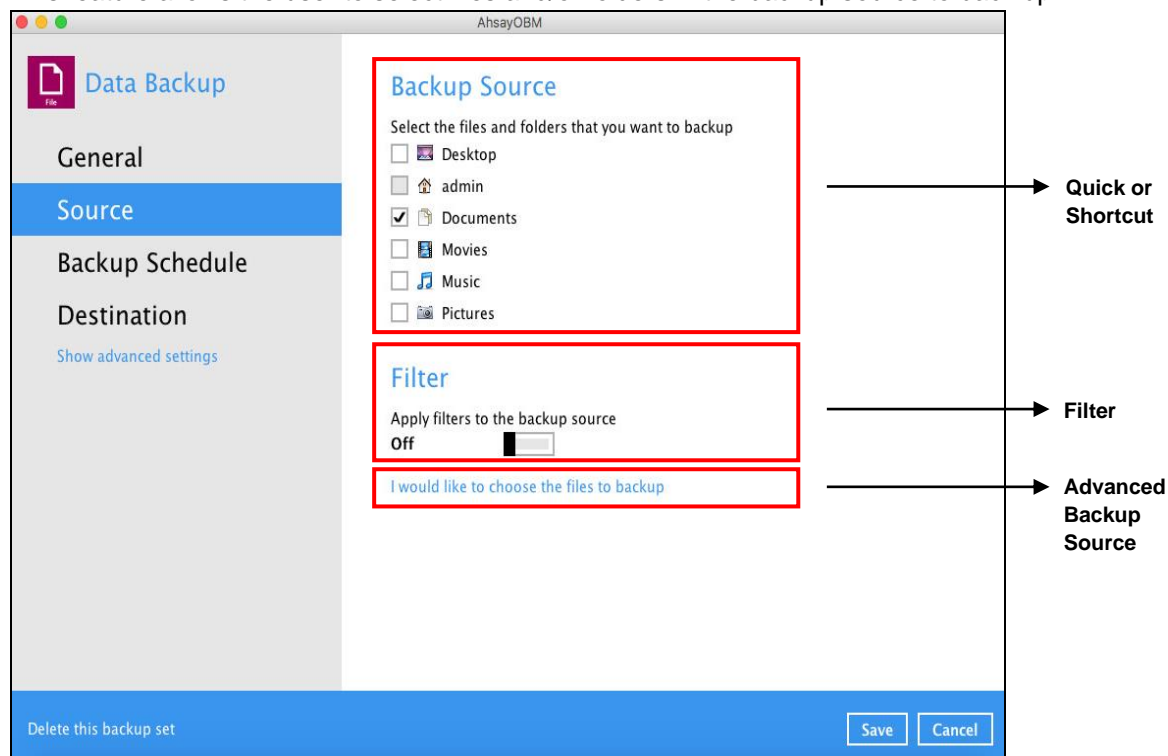
2. Click the [Save] button to save the updated backup set name.

NOTE

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

Source

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



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


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


Option no. 1: Quick or Shortcut


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


Backup Source


Select the files and folders that you want to backup


☐  Desktop

☐  admin





☒  Documents



☐  Movies

☐  Music

☐  Pictures

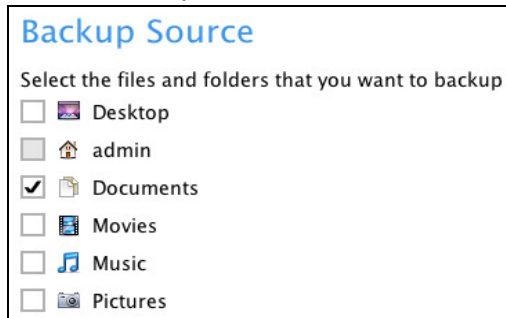
To know the locations of the folder(s) that will be backed up for each selected backup source, refer to the following table:

Backup Source		Description
Desktop		<p>If Desktop is selected, all files and/or folders in the following location will be backed up:</p> <p>%UserProfile%/admin/Desktop</p>
admin		<p>If admin is selected, all files and/or folders located in the following locations will be backed up:</p> <p>%UserProfile%/admin</p> <p>%UserProfile%/Library</p> <p>If the Follow Link is enabled, the following locations will also be included to the backup job:</p> <p>%UserProfile%/LocalStorage</p> <p>%UserProfile%/Applications</p> <p>%UserProfile%/admin/Downloads</p> <p>%UserProfile%/admin/Library</p> <p>%UserProfile%/admin/temp</p> <p>The Follow Link is configured as enabled by default.</p> <p>Note: If you select admin during the creation of backup set, the entire Backup Source in the Quick or Shortcut option will also be selected (e.g. Desktop, Documents, Movies, Music, Pictures), but you may choose to unselect any of each.</p>
Documents		<p>If Documents is selected, all files and/or folders located in the following location will be backed up:</p> <p>%UserProfile%/admin/Documents</p>
Movies		<p>If Movies is selected, all files and/or folders located in the following location will be backed up:</p> <p>%UserProfile%/admin/Movies</p>

Music		If Music is selected, all files and/or folders located in the following location will be backed up: <i>%UserProfile%/admin/Music</i>
Pictures		If Pictures is selected, all files and/or folders located in the following location will be backed up: <i>%UserProfile%/admin/Pictures</i>

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

1. Select a backup source.



Backup Source

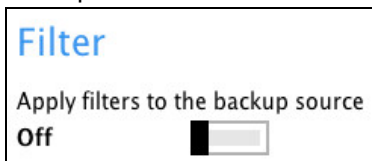
Select the files and folders that you want to backup

- ☐ Desktop
- ☐ admin
- ☒ Documents
- ☐ Movies
- ☐ Music
- ☐ Pictures

2. Click the [Save] button to save the selected backup source.

Option no. 2: Filter

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



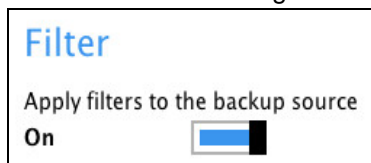
Filter

Apply filters to the backup source

Off ☐

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

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



Filter

Apply filters to the backup source

On ☒

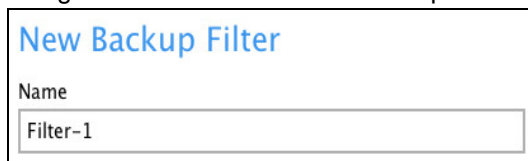
2. Click the [Add] button to create a filter.



Existing filters

Add new filter

3. Assign a desired name to the backup filter.



New Backup Filter

Name

Filter-1


4. Configure the following options.

For each of the matched files/folders under top directory

☒ Include them
☐ Exclude them



☐ Exclude all unmatched files/folders

Match file/folder names by

☒ Simple comparison 
☐ Regular expression (UNIX-style)

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

Existing patterns to match

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

Apply this filter to all files/folders in

☐ All hard disk drives
☒ This folder only


Apply to


☒ File ☒ Folder

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 by clicking the [Add] button.

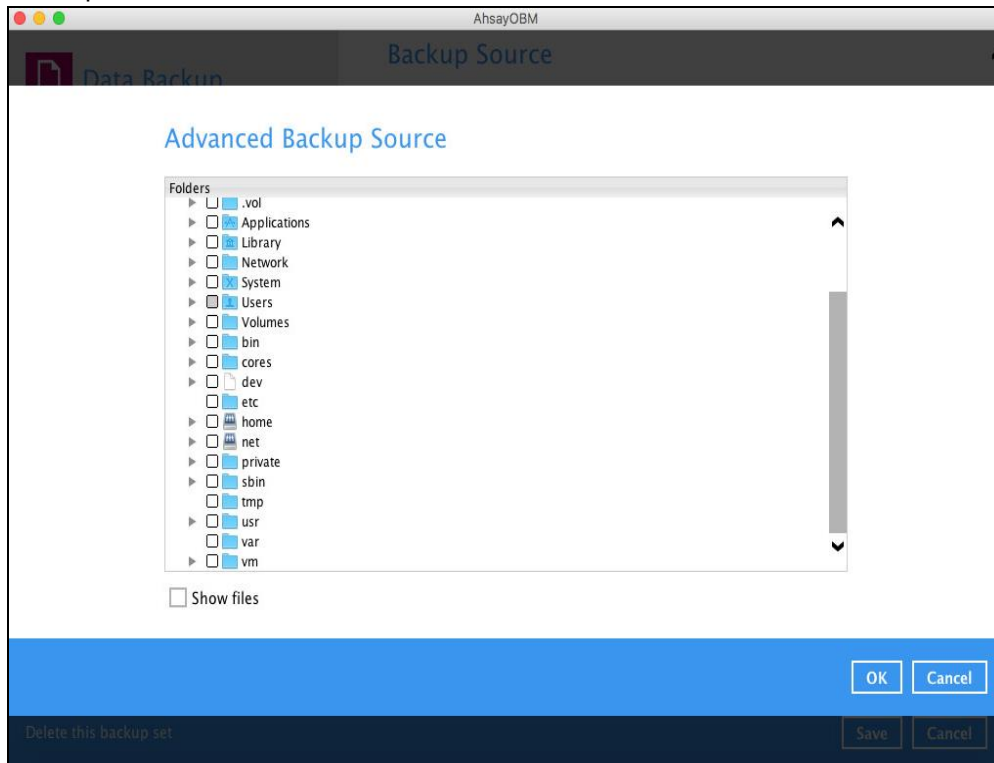
Existing filters

 **Filter-1**
/Users/admin/Desktop

 **Filter-2**
/Users/admin/Documents

Option no. 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.

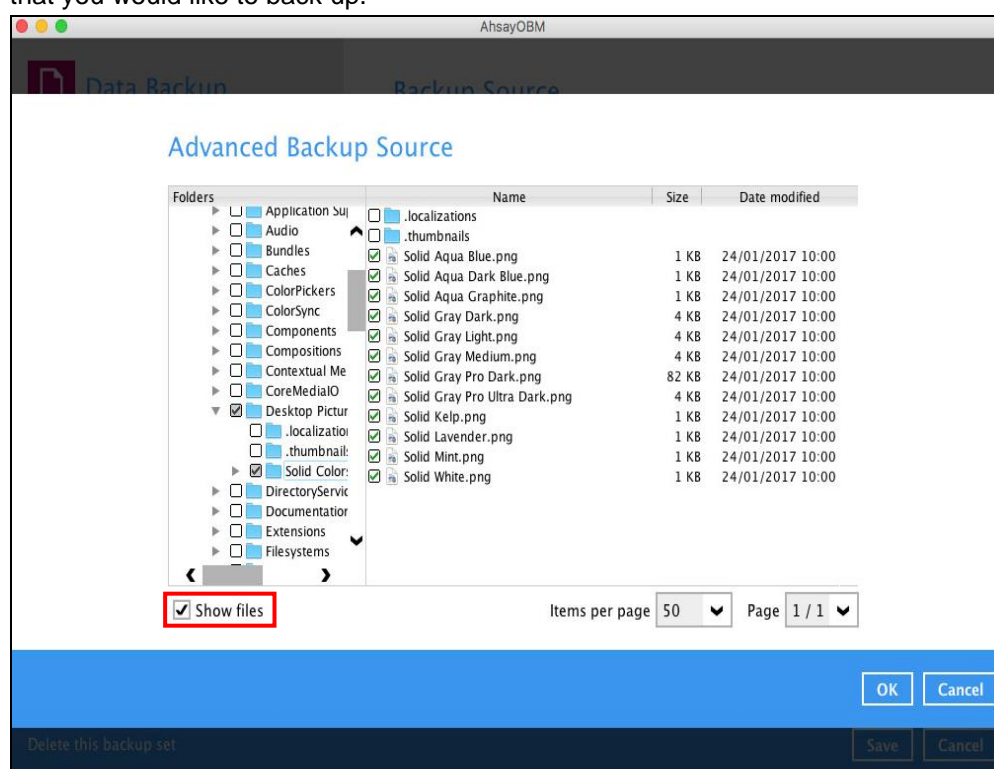


To select files and/or folders using the Advanced Backup Source, follow the steps below:

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

I would like to choose the files to backup

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



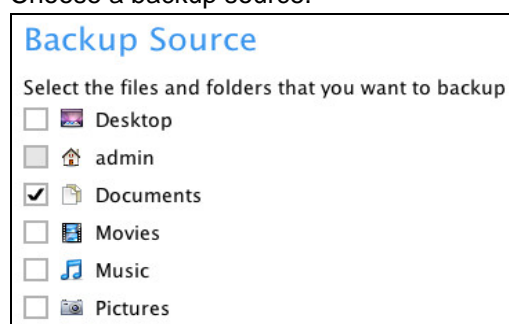
3. Click the [OK] button to save the selection, then click the [Save] button to store settings.

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

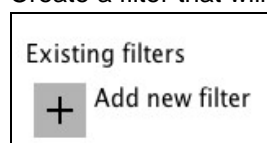
Scenario 1 (Quick or Shortcut + Filter)

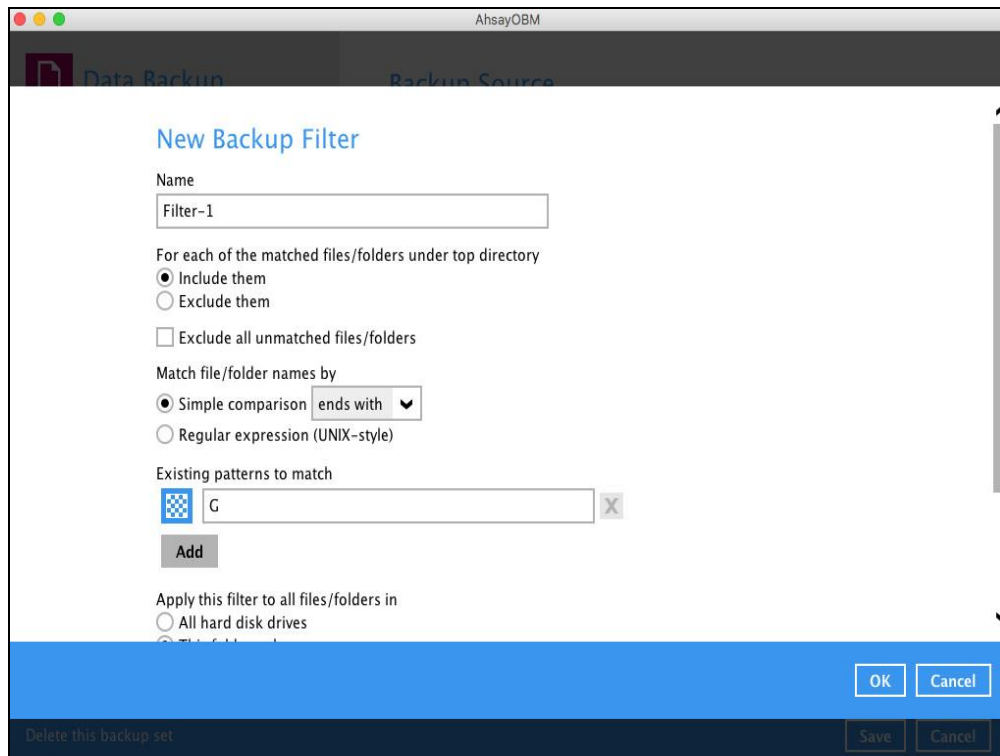
You can use the quick or shortcut option and apply filter to the selected backup source at the same time. To use this type of combination, follow the steps below:

1. Choose a backup source.



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



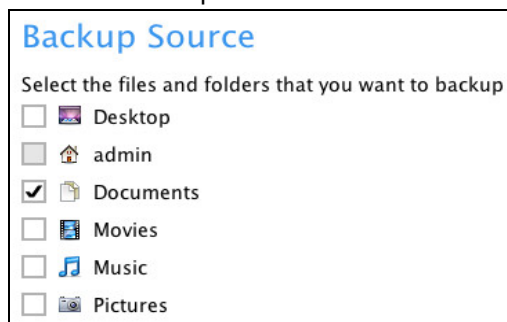


3. Click the [OK] button to save the created filter, then click the [Save] button to store settings.

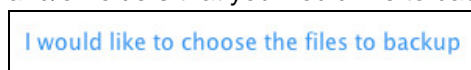
Scenario 2 (Quick or Shortcut + Advanced Backup Source)

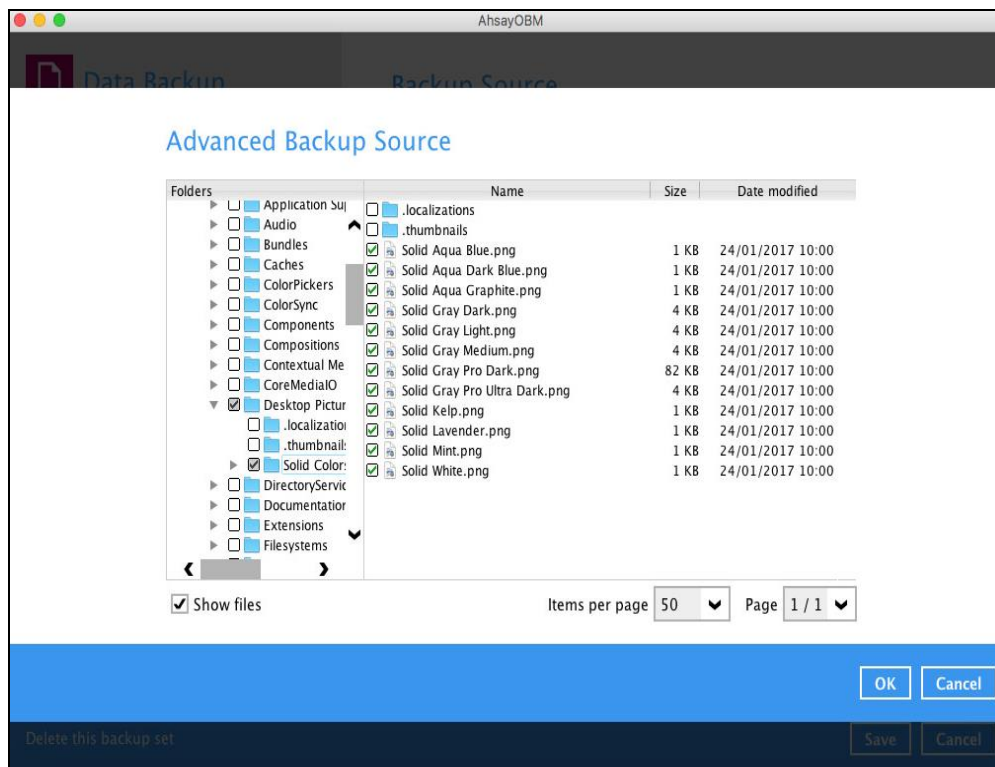
You can use the quick or shortcut option and select files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

1. Choose a backup source.



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



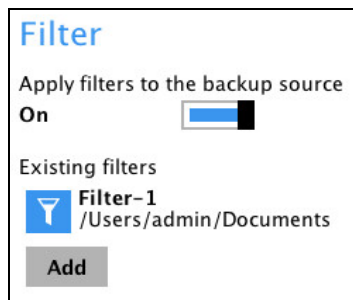


3. Click the [OK] button to save the selection, then click the [Save] button to save settings.

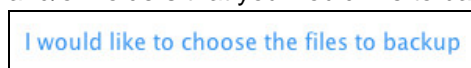
Scenario 3 (Filter + Advanced Backup Source)

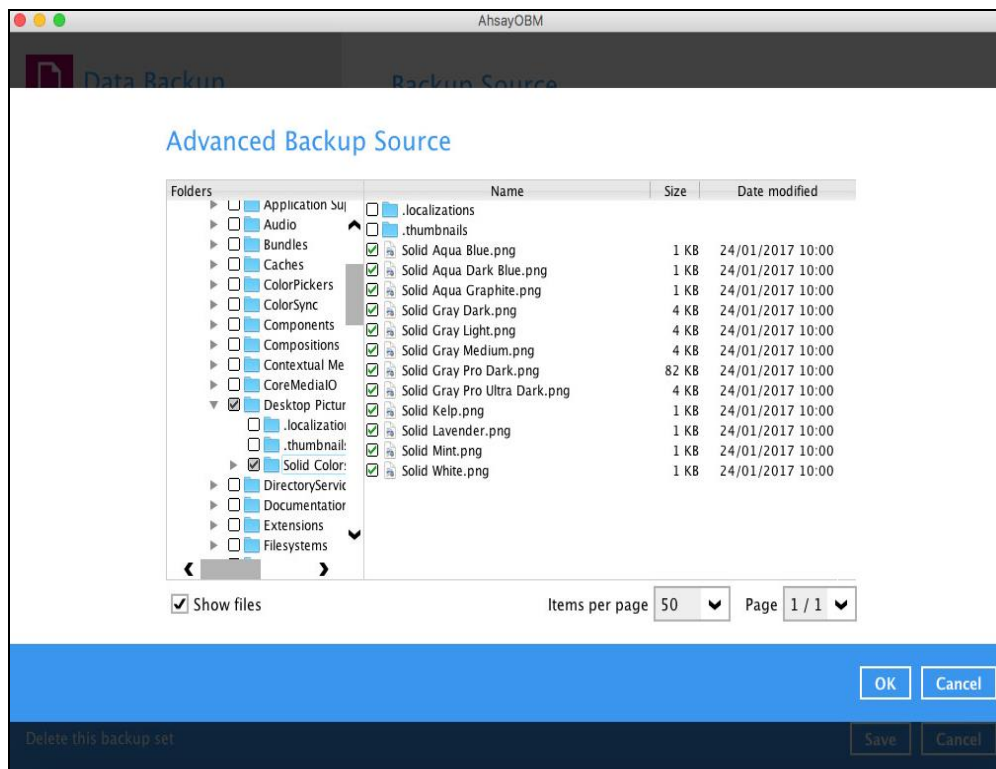
You can use the filter backup source and select files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

1. Create a filter.



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





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

Backup Schedule

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

The screenshot shows a configuration window for a backup set named "Sample Backup Set...". The left sidebar has tabs for "General", "Source", "Backup Schedule" (which is selected and highlighted in blue), and "Destination". Below the "Destination" tab is a link that says "Show advanced settings". The main area is titled "Schedule" and contains a toggle switch for "Run scheduled backup for this backup set" which is currently turned "On". Below this, under the heading "Existing schedules", there is a single entry: "Backup Schedule" with a calendar icon and the text "Daily (Everyday at 20:00)". An "Add" button is located below this entry. At the bottom of the window, there is a blue bar with the text "Delete this backup set" on the left and "Save" and "Cancel" buttons on the right.

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.

This is a close-up of the "Schedule" section from the previous screenshot. It shows the "Run scheduled backup for this backup set" toggle switch is turned "On". Below it, the "Existing schedules" section lists "Backup Schedule" with a calendar icon and "Daily (Everyday at 20:00)". An "Add" button is positioned below the schedule list.

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

This is a close-up of the "Existing schedules" section. It shows a single entry: "Backup Schedule" with a calendar icon and "Daily (Everyday at 20:00)". An "Add" button is located below the entry.

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 intervals in minutes/hours when the backup job will run.

New Backup Schedule

Name
Daily-1

Type
Daily

Start backup
at 00 : 00

Stop
until full backup completed

☒ Run Retention Policy after backup

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

New Backup Schedule

Name
Weekly-1

Type
Weekly

Backup on these days of the week
☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☒ Sat

Start backup
at 00 : 00

Stop
until full backup completed

☒ Run Retention Policy after backup

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

New Backup Schedule

Name
Monthly-1

Type
Monthly

Backup on the following day every month
☒ Day 1 ☐ First Sunday

Start backup at
00 : 00 on the selected days

Stop
until full backup completed

☒ Run Retention Policy after backup

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

New Backup Schedule

Name: Custom-1

Type: Custom

Backup on the following day once: 2020 December 31

Start backup at: 00:00

Stop: until full backup completed

☒ Run Retention Policy after backup

- **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.

Start backup

every 1 minute

Stop: until full backup completed

☒ Run Retention Policy after backup

Start backup

every 1 minute

Stop: until full backup completed

☒ Run Retention Policy after backup

Here is an example of backup set that has a periodic and normal backup schedule.

New Backup Schedule

Name: Weekly-1

Type: Weekly

Backup on these days of the week: ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

Start backup: every 4 hours

Stop: until full backup completed

☒ Run Retention Policy after backup

Figure 1.1

Figure 1.1 – Periodic scheduled every 4 hours Monday - Friday for business hours

New Backup Schedule

Name: Weekly-1

Type: Weekly

Backup on these days of the week: ☒ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☒ Sat

Start backup: at 21:00

Stop: until full backup completed

☒ Run Retention Policy after backup

Figure 1.2

Figure 1.2 – Normal schedule run at 21:00 or 9:00 PM daily on Saturday & Sunday for 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.

- **Run Retention Policy after backup** – if enabled, the AhsayOBM will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job.

4. Click the **[OK]** button to save the configured backup schedule settings.
5. Click the **[Save]** button to save settings.
6. Multiple backup schedules can be created.

Schedule

Run scheduled backup for this backup set

On ☐

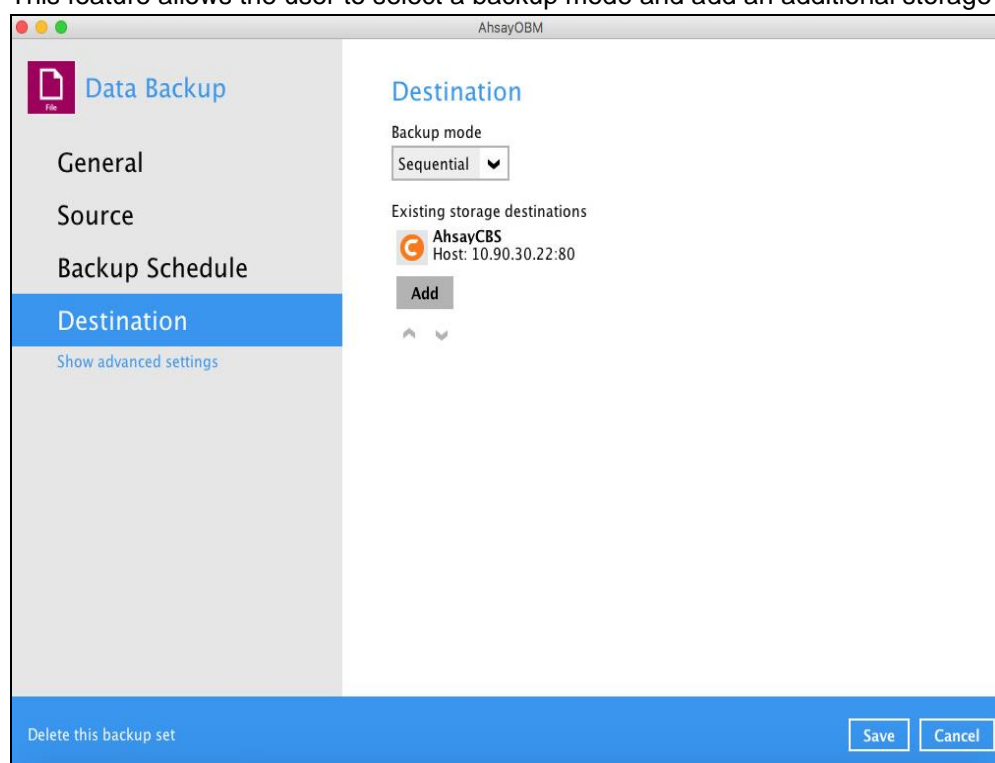
Existing schedules

- Daily-1**
Daily (Everyday at 19:00)
- Weekly-1**
Weekly - Saturday (Every week at 19:00)
- Monthly-1**
Monthly - The Last Day (Every month at 20:00)
- Custom-1**
Custom (31/03/2020 at 21:00)

Add

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:

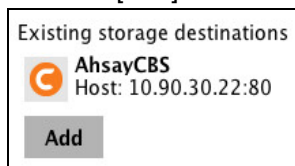
Backup mode	Description
Sequential	This is the configured backup mode by default. This backup mode will run a backup job to each backup destination one by one.
Concurrent	This backup mode will run a backup job to all backup destinations simultaneously.

Comparison between Sequential and Concurrent Backup mode

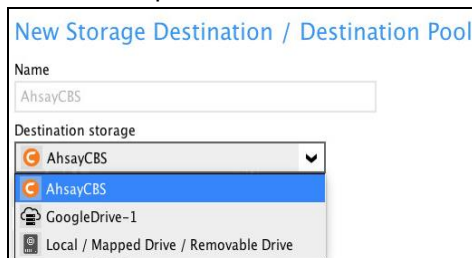
Backup mode	Pros	Cons
Sequential	<ul style="list-style-type: none">➤ Takes less resources in the local machine (e.g. memory, CPU, bandwidth, etc.) to complete a backup job.	<ul style="list-style-type: none">➤ Backup job is slower than in concurrent mode since the backup job will upload the backup data to the selected backup destinations one at a time.
Concurrent	<ul style="list-style-type: none">➤ Backup job is faster than in Sequential mode.➤ Maximum number of concurrent backup destinations can be configured.	<ul style="list-style-type: none">➤ Requires more resources in the local machine (e.g. memory, CPU, bandwidth, etc.) to complete a backup job.

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

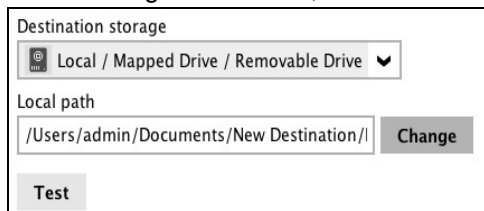
1. Click the [Add] button.



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

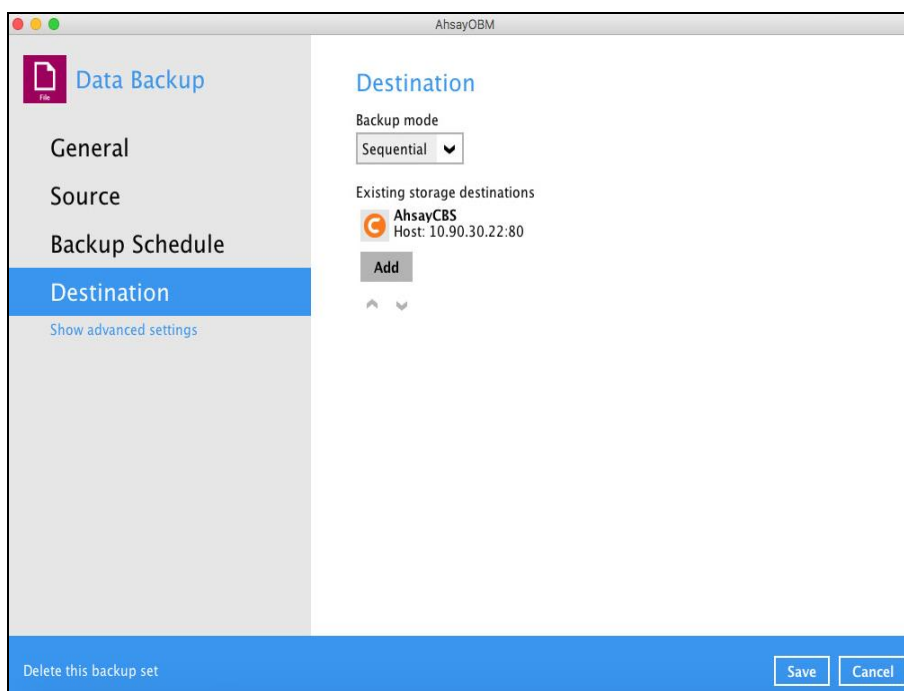


3. If the Local / Mapped Drive / Removable Drive is selected, click the [Change] button to select a new storage destination, then click the [Test] button to validate access to it.



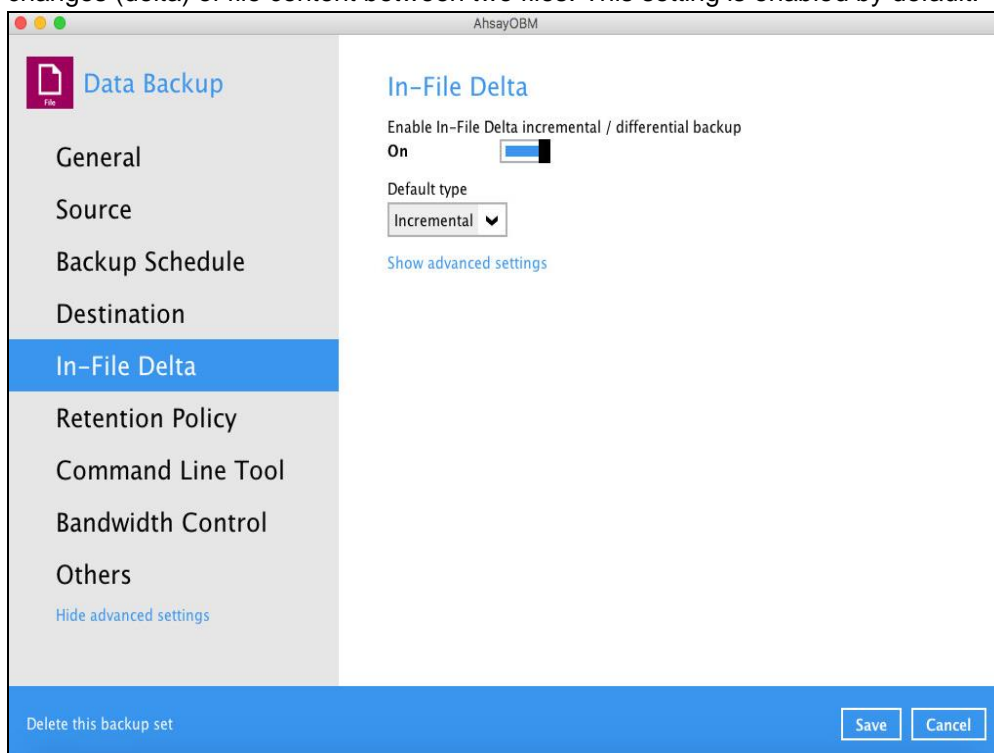
4. Click the [OK] button to save the added storage destination, then click the [Save] button to save the updated backup mode and the added storage destination.

Select **Show advanced settings** to modify the In-File Delta, Retention Policy, Command Line Tool, Bandwidth Control, and other configurable options.



In-File Delta

In-file delta technology is an advanced data block matching algorithm which is capable to pick up the changes (delta) of file content between two files. This setting is enabled by default.



There are two (2) default types of In-File Delta:

In-File Delta Type	Description
Differential	The delta is generated by comparing with the last uploaded full file only. Delta generated with this method will grow daily and uses more bandwidth.
Incremental	This is the configured In-file delta by default. The delta is generated by comparing with the last uploaded full of delta file. Delta generated with this method is smaller and uses the least bandwidth.

In-File Delta Type, Incremental and Differential Pros and Cons

Differential restore is faster than with incremental as it is only required to merge the full file with one differential delta file. To restore up to the required point-in-time. Backup process is slower than incremental delta backup as differential delta files are larger, it may take longer to generate. The larger file will also take longer to upload to the backup destination.

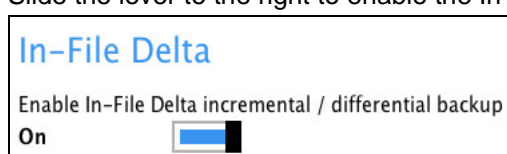
As differential delta files are larger than incremental delta files, more storage is required. Incremental backup process is faster as incremental delta files are smaller than differential delta files are quicker to generate. The small file will also take time to upload to the backup destination.

As incremental delta files are smaller than differential delta files less storage quota is required. Restore is slower than differential delta. As the full file and all the individual incremental delta files up to the required point-in-time. The merging of many incremental delta files with the full files takes much longer.

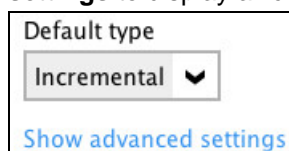
In-File Delta Type	Pros	Cons
Differential	<ul style="list-style-type: none">➤ Backup speed is faster than Full backup.➤ Restoration is faster than data backup with Incremental In-File Delta.➤ Less storage space is need than a Full backup.	<ul style="list-style-type: none">➤ Backup process is slower than Incremental In-File Delta backup.➤ Restoration is slower than data backup with Full backup.
Incremental	<ul style="list-style-type: none">➤ Backup process is fastest among all three (3) types; Full, Differential, and Incremental➤ Least storage space is required.	<ul style="list-style-type: none">➤ Restoration is slowest among all three (3) types; Full, Differential, and Incremental.➤ For restoration, the full file and all deltas that does not chain up to the required point-in-time may result to broken delta chain.

To configure the In-File Delta settings, follow the steps below:

1. Slide the lever to the right to enable the In-File Delta.



2. Click the drop-down button to choose an In-File Delta type, then select **Show advanced settings** to display all configurable options.



3. Click the drop-down button to specify the In-File Delta block size. This is configured as "Auto" by default.



- Click the drop-down button to select how much of the file size (MB) the In-File Delta logic will apply to. By default, the In-File Delta logic is configured to apply to files larger than 25 MB.

Only apply In-File Delta to files larger than

25 MB

- A full file will be uploaded when either of these conditions is met. This setting can also be configured.

Upload full file when either of these conditions is met

☒ Number of deltas is over 100

☒ Delta ratio (delta file size / full file size) is over 50

☒ Failed to generate delta file

- This allows the user to configure a different In-File Delta setting to override the default In-File Delta.

- Weekly variations** – for example, you set Sunday to perform a full backup, for the rest of the week, a backup based on the default In-File Delta will be run.

Weekly variations for overriding default type

<input checked="" type="checkbox"/> Sunday	Full	<input type="checkbox"/> Thursday	Full
<input type="checkbox"/> Monday	Full	<input type="checkbox"/> Friday	Full
<input type="checkbox"/> Tuesday	Full	<input type="checkbox"/> Saturday	Full
<input type="checkbox"/> Wednesday	Full		

- Yearly variations** – for example, you set a particular day in January to perform a full backup, for the rest of the year, a backup based on the default In-File Delta will be run.

Yearly variations for overriding default type and weekly variations

<input checked="" type="checkbox"/> January	Full	<input type="checkbox"/> July	Full
<input type="checkbox"/> February	Full	<input type="checkbox"/> August	Full
<input type="checkbox"/> March	Full	<input type="checkbox"/> September	Full
<input type="checkbox"/> April	Full	<input type="checkbox"/> October	Full
<input type="checkbox"/> May	Full	<input type="checkbox"/> November	Full
<input type="checkbox"/> June	Full	<input type="checkbox"/> December	Full

This allows the user to specify the day of the selected months in yearly variations the In-File Delta will be run.

Day of the selected months in yearly variations

☐ Day 1

☒ First Friday

[Hide advanced settings](#)

Retention Policy

When the AhsayOBM 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.

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

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

The default Retention Policy setting for a File Backup Set is 7 days, but the appropriate Retention Policy setting depends on individual, contractual, or regulatory requirements.

Data Backup

General

Source

Backup Schedule

Destination

In-File Delta

Retention Policy

Command Line Tool

Bandwidth Control

Others

[Hide advanced settings](#)

Retention Policy

How to retain the files in the backup set, which have been deleted in the backup source

☒ Simple

☐ Advanced

Keep the deleted files for

7 Day(s)

Delete this backup set

Save Cancel

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) 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 within 1 to 365 backup job(s)	Not applicable
Days	Can keep the deleted files within 1 to 365 day(s)	Can keep the deleted files within 1 to 365 day(s)
Type	Not applicable	<ul style="list-style-type: none"> ➤ 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 will be permanently removed from the backup set and cannot be restored.

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

1. In the [Retention Policy] tab, select **Simple**.

Retention Policy

How to retain the files in the backup set, which have been deleted in the backup source

☒ Simple
☐ Advanced

2. 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 seven (7) days by default.

Keep the deleted files for

▼

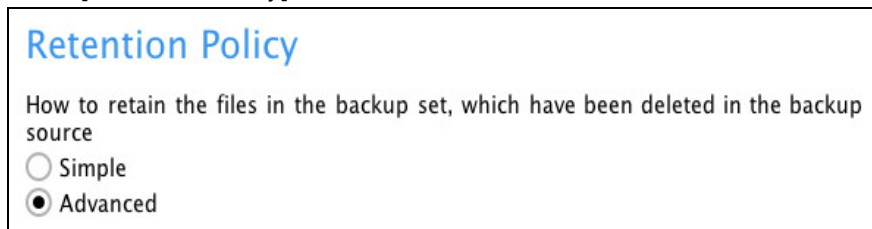
Day(s)

▼

3. Click the [Save] button to store the configured simple retention policy.

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

1. In the [Retention Policy] tab, select **Advanced**.



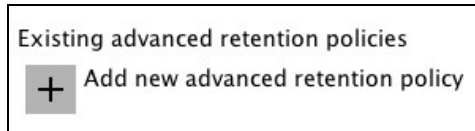
Retention Policy

How to retain the files in the backup set, which have been deleted in the backup source


☐ Simple

☒ Advanced

2. Click the [Add] button to create an advanced retention policy.



Existing advanced retention policies

 Add new advanced retention policy

3. Assign a desired name to the retention policy.

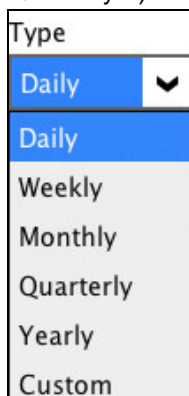


New Retention Policy

Name

Daily-1

4. Click the drop-down button to choose a retention type (e.g. Daily, Weekly, Monthly, Quarterly...).



Type

Daily

Daily

Weekly

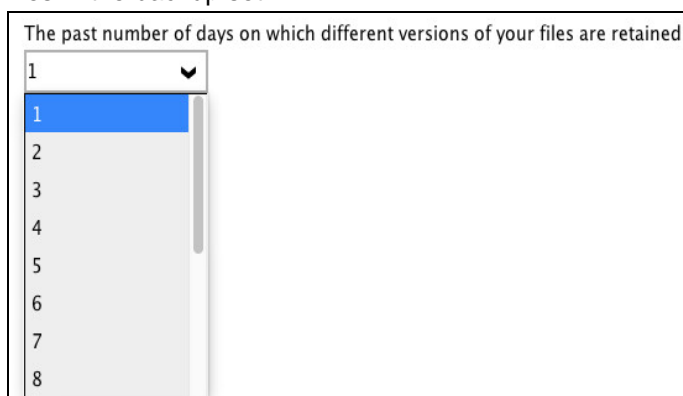
Monthly

Quarterly

Yearly

Custom

5. Click the drop-down button to specify the period on which the retention will keep the deleted files in the backup set.



The past number of days on which different versions of your files are retained

1

1

2

3

4

5

6

7

8

6. Click the [OK] button to store the configured advanced retention policy, then click the [Save] button to save settings.

There are different configuration settings for each retention type. For further details about how to configure an advanced retention policy for each type (Daily, Weekly, Monthly, Quarterly, Yearly), refer to the following examples:

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

Name

Daily-1

Type

Daily

The past number of days on which different versions of your files are retained

7

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

Name

Weekly-1

Type

Weekly

The days within a week on which different versions of your files are retained

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☒ Sat

The number of weeks to repeat the above selection

4

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

Name

Monthly-1

Type

Monthly

The day within a month on which different versions of your files are retained

☒ Day 1 ☐ First ☐ Sunday

The number of months to repeat the above selection

3

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

Name
Quarterly-1

Type
Quarterly

The day within a quarter on which different versions of your files are retained
☒ Day 1
☐ First Sunday

Months of quarter
January, April, July, October

The number of quarters to repeat the above selection
4

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

Name
Yearly-1

Type
Yearly

The day within a year on which different versions of your files are retained
☒ January
☒ Day 1
☐ First Sunday
☐ Sunday of Week 1

The number of years to repeat the above selection
7

NOTE

Multiple advanced retention policy can be created.

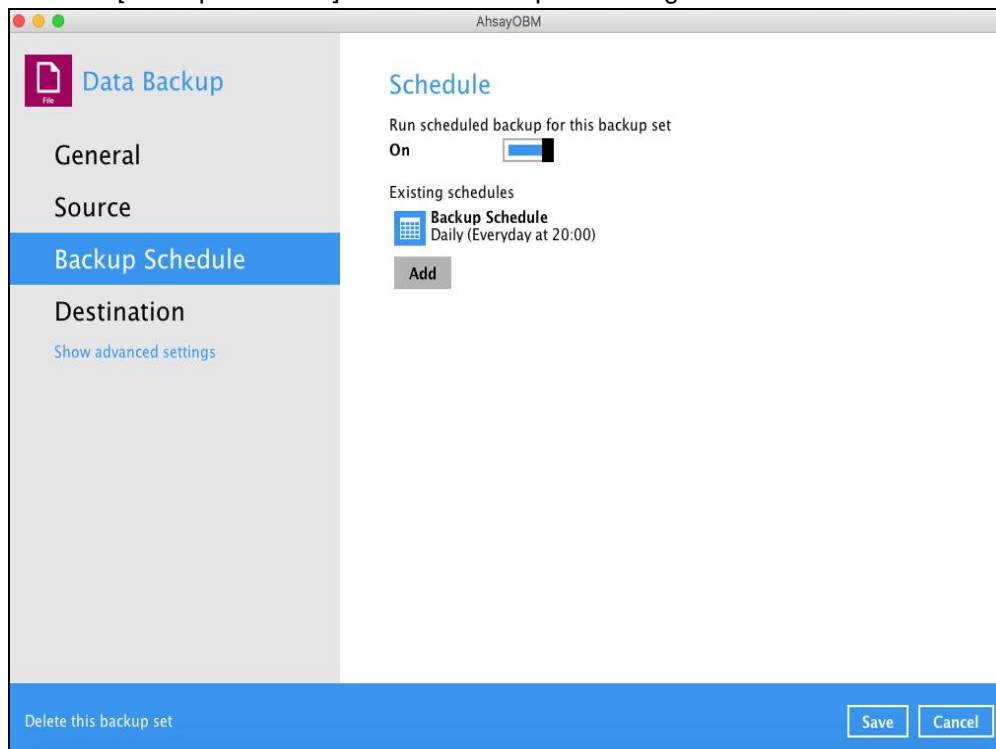
There are three (3) different ways to run the Retention Policy job:

- Backup Scheduler
- Manual Backup
- Space Freeing Up

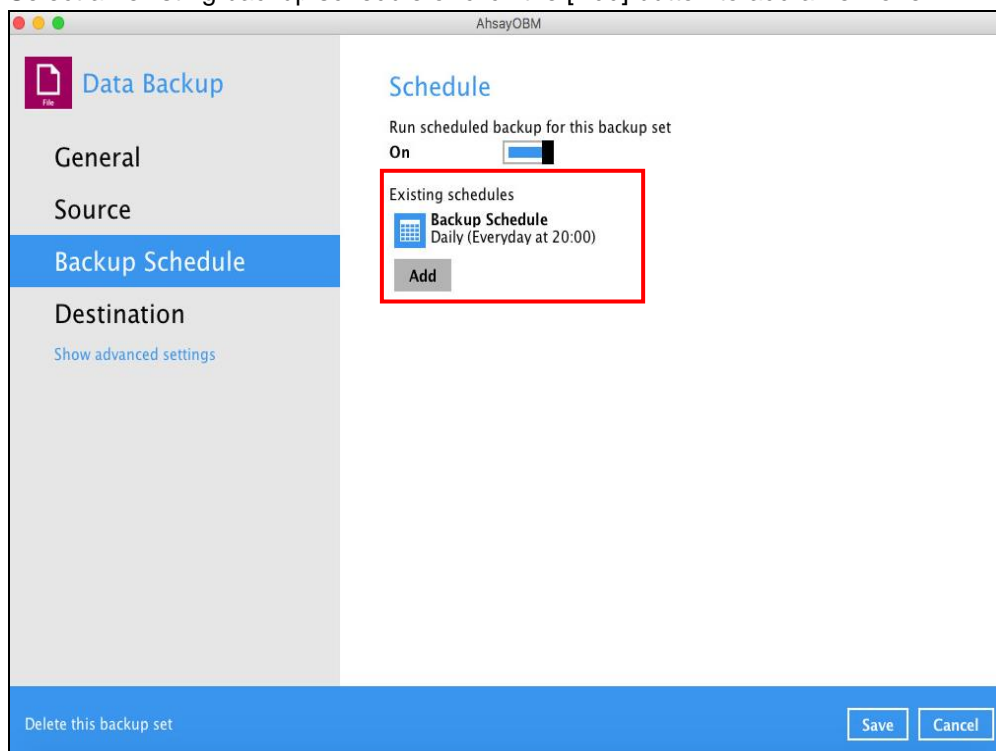
Backup Scheduler (Recommended)

To run a retention policy job after a scheduled backup job, follow the steps below:

1. Click the [Backup Schedule] tab in the backup set settings.



2. Select an existing backup schedule or click the [Add] button to add a new one.



3. In the Backup Schedule window, select 'Run Retention Policy after backup' to run a retention policy job after a scheduled backup job.

AhsayOBM

Backup Schedule

Name
Backup Schedule

Type
Daily

Start backup at
20 : 00

Stop
until full backup completed

☒ Run Retention Policy after backup

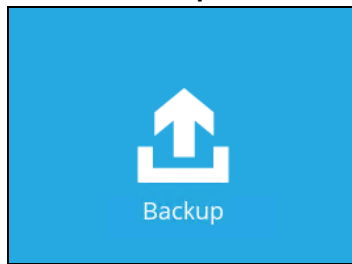
Delete this backup schedule OK Cancel

Delete this backup set Save Cancel

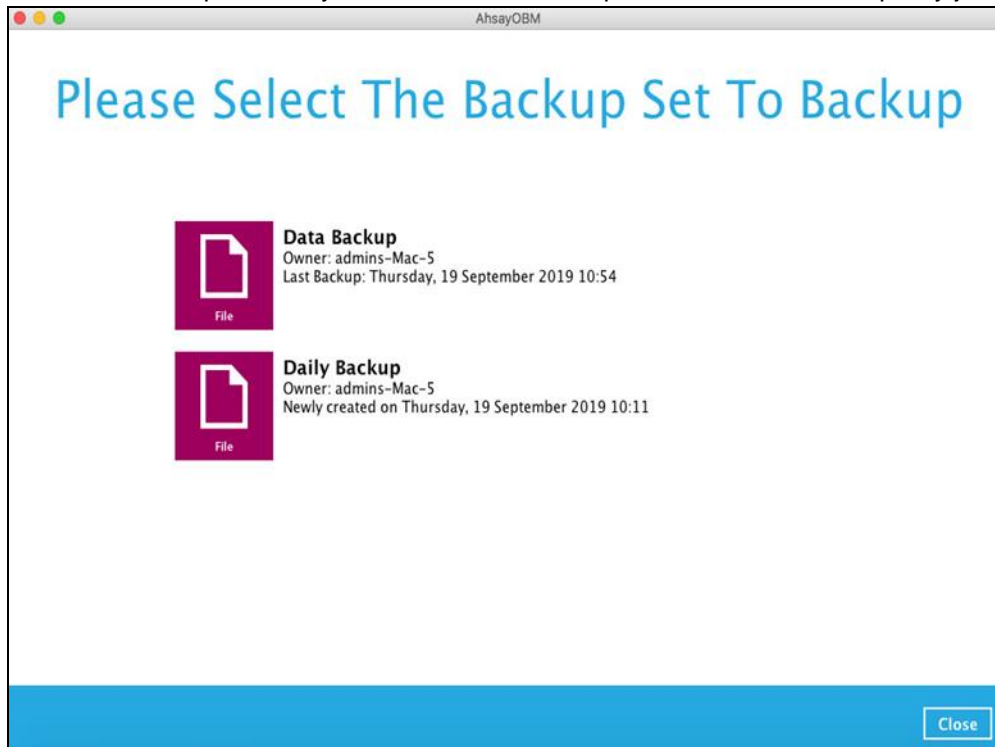
Manual Backup

To run a retention policy job after a manual backup, follow the steps below:

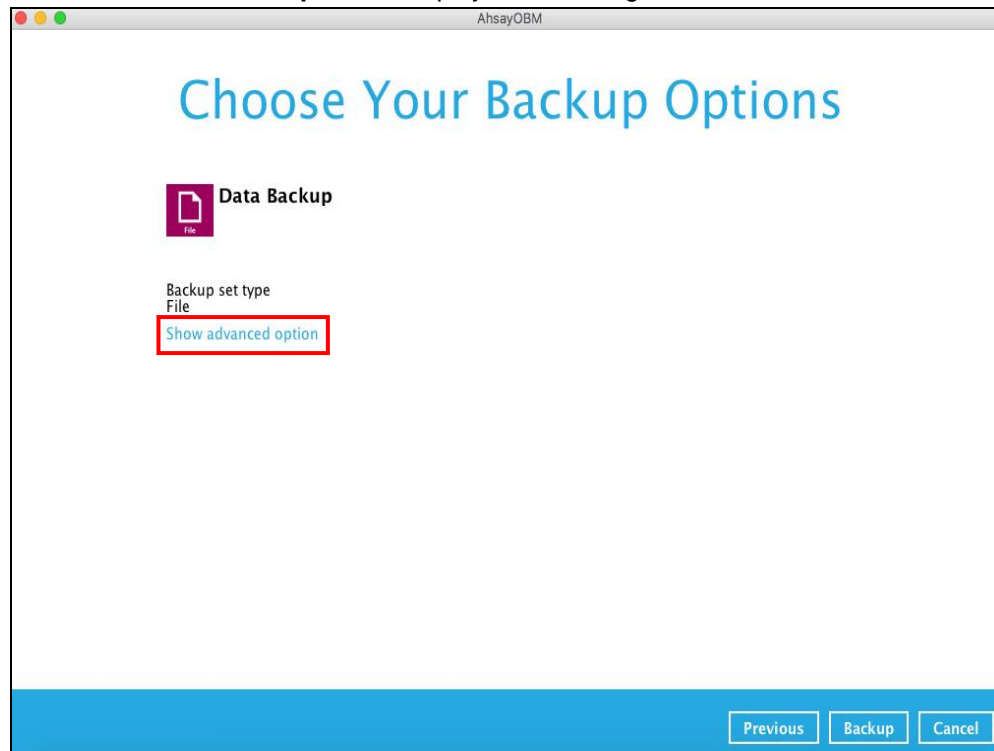
1. Click the **Backup** icon in the AhsayOBM main interface.



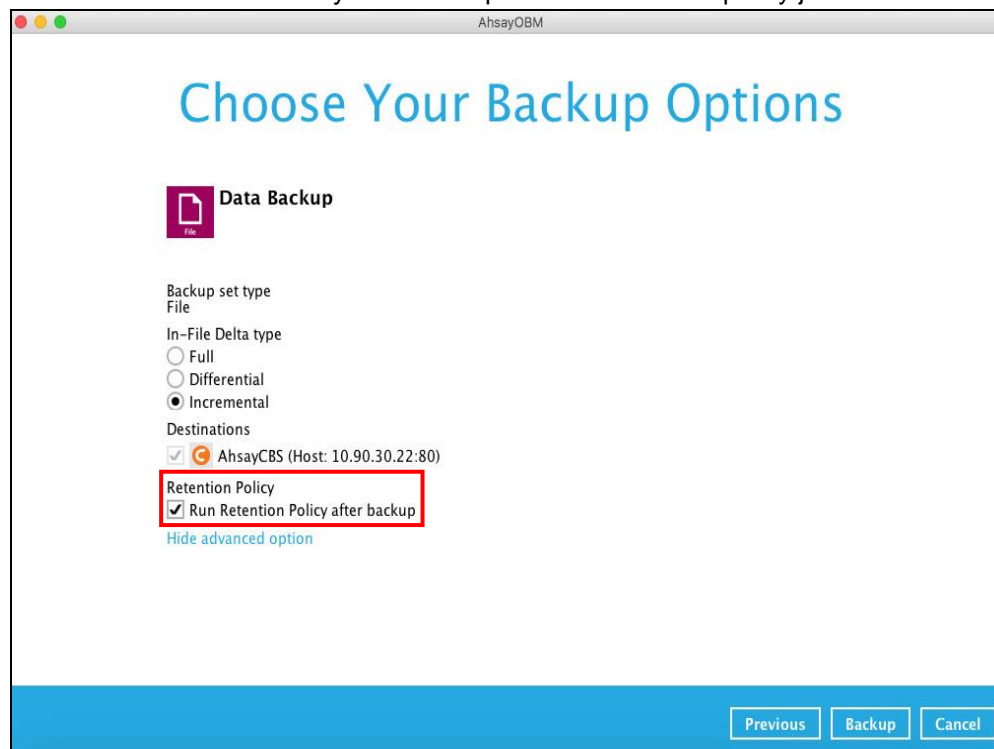
2. Select the backup set that you would like to back up and run the retention policy job on.



3. Click **Show advanced option** to display other settings.



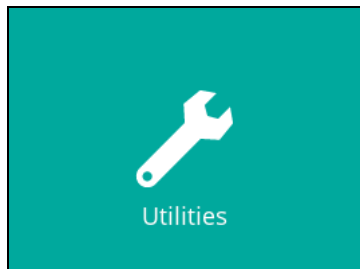
4. Select 'Run Retention Policy after backup' to run a retention policy job after a backup job.



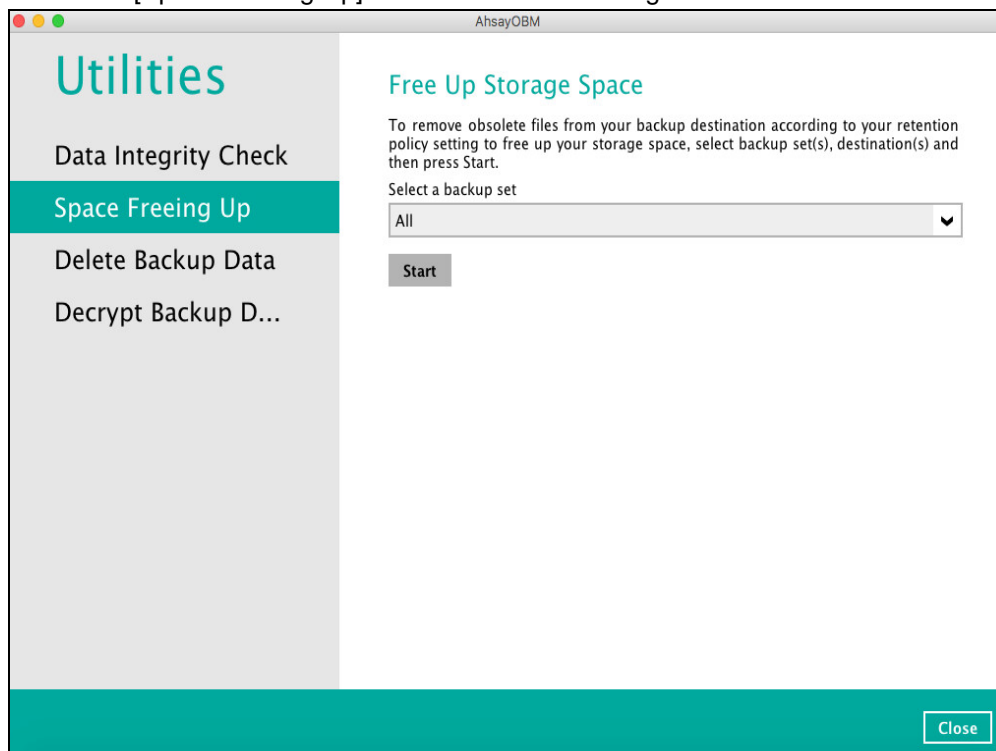
Space Freeing Up

To run a retention policy job manually via backup client interface, follow the steps below:

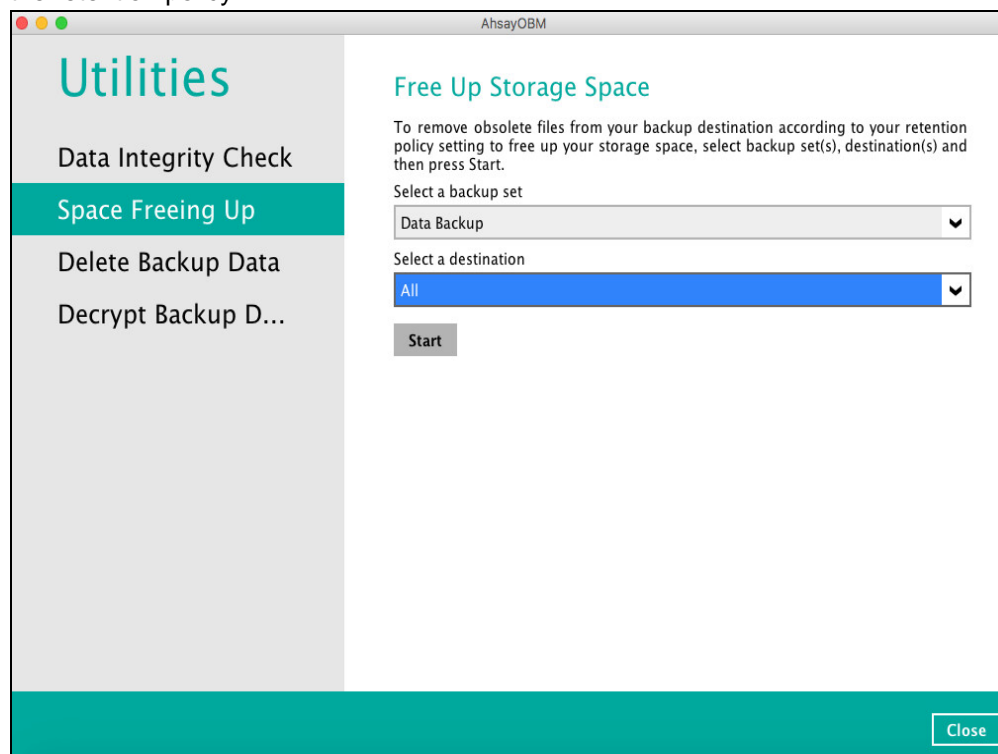
1. Click the **Utilities** icon in the AhsayOBM interface.



2. Select the [Space Freeing Up] tab in the Utilities settings.



3. Select the corresponding backup set and destination (e.g. AhsayCBS, local drive, cloud storage) where you want the retention policy job to run on, then click the [Start] button to run the retention policy.



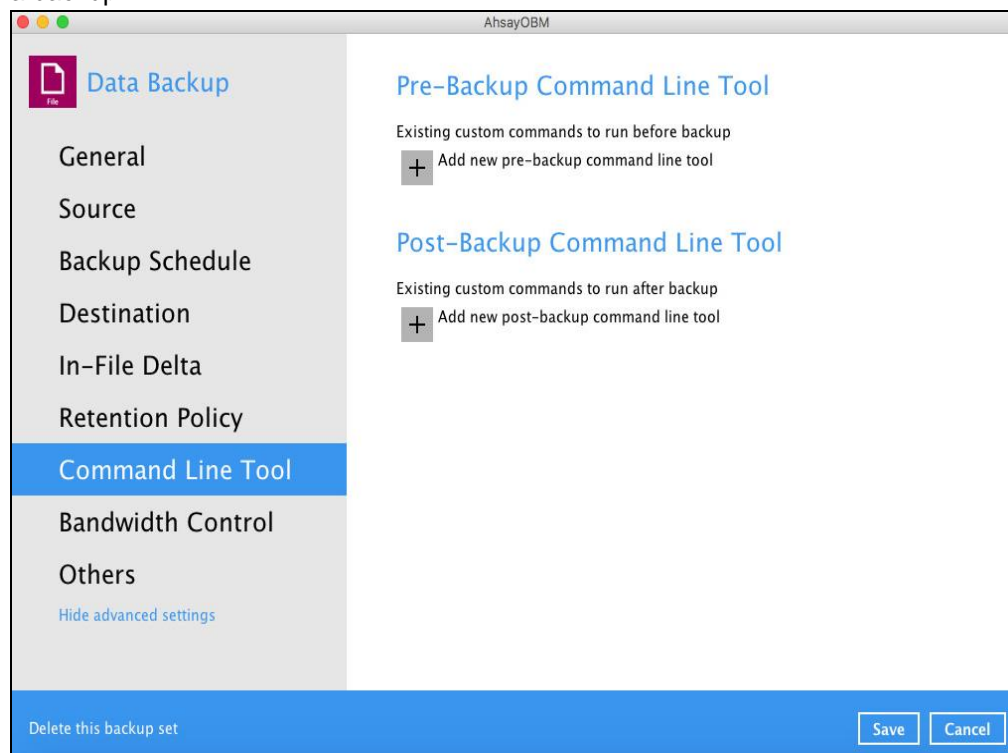
NOTE

For more details about Space Freeing Up, please refer to [Ch. 7.9.2 Space Freeing Up](#).

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 Ahsay) 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 6 AhsayOBM 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”, which can be viewed in the AhsayCBS User Web Console. Please refer to [AhsayCBS Backup Reports](#) for more details.

User Profile

Backup Set

Settings

Report

Statistics

Effective Policy





Backup

Restore

Backup Report for This User

View

Today

Backup Set	Destination	Start Time	End Time	Status
 Sample-2(1567584589206)	 AhsayCBS	04-Sep-2019 16:20	--	Backup not yet finished
 Daily Backup(1567576033951)	 AhsayCBS	04-Sep-2019 14:43	--	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 AhsayOBM has enough time to complete the backup process in order to send the backup job status to the AhsayCBS before the machine shuts down.

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

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.

Pre-Backup Command Line Tool

Existing custom commands to run before backup

 Add new pre-backup command line tool

2. Assign a desired name to the pre-backup command.

New Pre-Backup Command Line Tool

Name

Pre-Backup-1

3. Click the [Change] button to locate the working directory of the command.


Working Directory

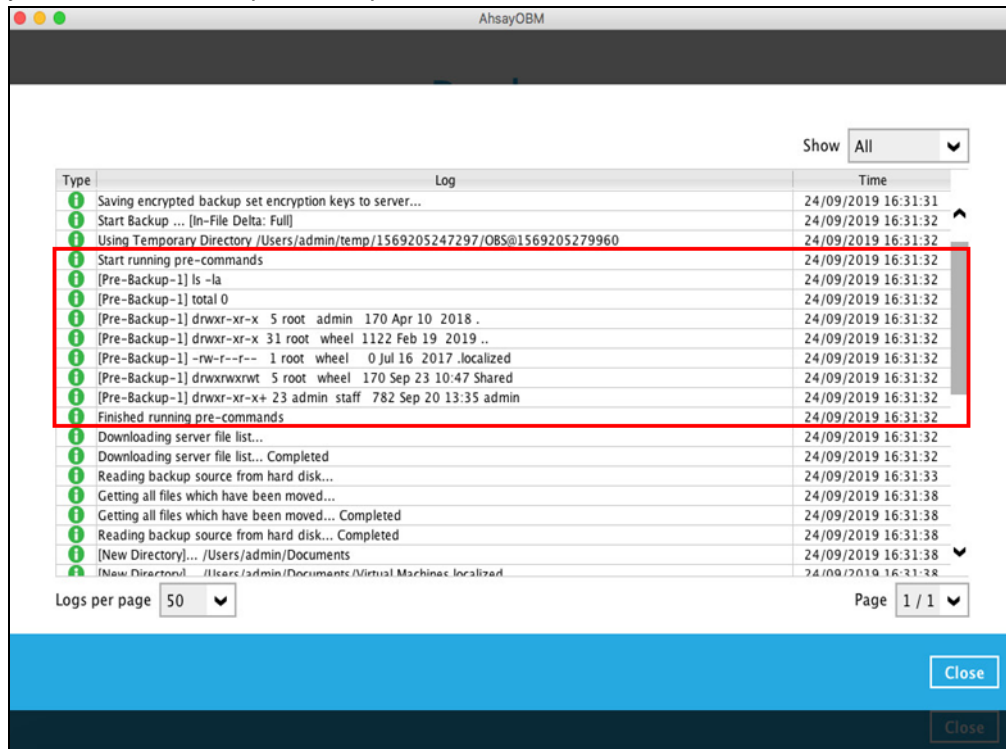
Change

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

Command
ls -la

- Click the [OK] button to save the created pre-backup command, then click the [Save] button to save settings.

- 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.



Type	Log	Time
i	Saving encrypted backup set encryption keys to server...	24/09/2019 16:31:31
i	Start Backup ... [In-File Delta: Full]	24/09/2019 16:31:32
i	Using Temporary Directory /Users/admin/temp/1569205247297/OBS@1569205279960	24/09/2019 16:31:32
i	Start running pre-commands	24/09/2019 16:31:32
i	[Pre-Backup-1] ls -la	24/09/2019 16:31:32
i	[Pre-Backup-1] total 0	24/09/2019 16:31:32
i	[Pre-Backup-1] drwxr-xr-x 5 root admin 170 Apr 10 2018 .	24/09/2019 16:31:32
i	[Pre-Backup-1] drwxr-xr-x 31 root wheel 1122 Feb 19 2019 ..	24/09/2019 16:31:32
i	[Pre-Backup-1] -rw-r--r-- 1 root wheel 0 Jul 16 2017 .localized	24/09/2019 16:31:32
i	[Pre-Backup-1] drwxrwxrwt 5 root wheel 170 Sep 23 10:47 Shared	24/09/2019 16:31:32
i	[Pre-Backup-1] drwxr-xr-x+ 23 admin staff 782 Sep 20 13:35 admin	24/09/2019 16:31:32
i	Finished running pre-commands	24/09/2019 16:31:32
i	Downloading server file list...	24/09/2019 16:31:32
i	Downloading server file list... Completed	24/09/2019 16:31:32
i	Reading backup source from hard disk...	24/09/2019 16:31:33
i	Getting all files which have been moved...	24/09/2019 16:31:38
i	Getting all files which have been moved... Completed	24/09/2019 16:31:38
i	Reading backup source from hard disk... Completed	24/09/2019 16:31:38
i	[New Directory]... /Users/admin/Documents	24/09/2019 16:31:38
i	[New Directory]... /Users/admin/Documents/Virtual Machines.localized	24/09/2019 16:31:38

Logs per page 50 Page 1 / 1

Close

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.



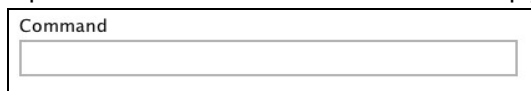
2. Assign a desired name to the pre-backup command.




3. Click the [Change] button to locate the working directory of the command.

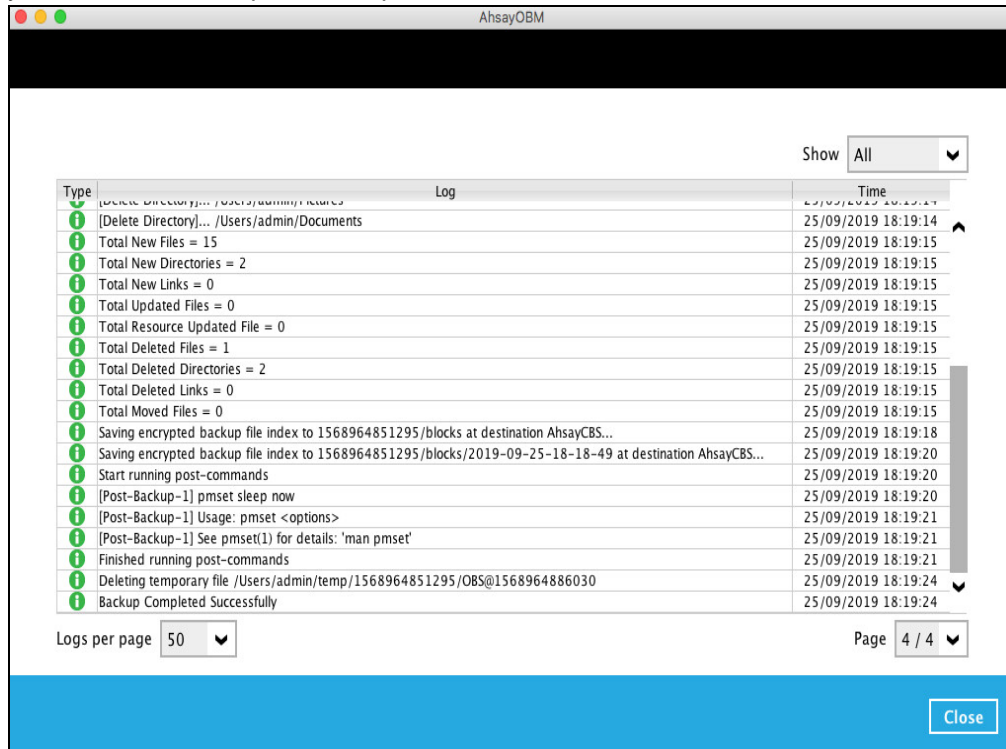


4. Input a command to be run before a backup job.



5. Click the [OK] button to save the created pre-backup command, then click the [Save] button to store settings.

6. 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.



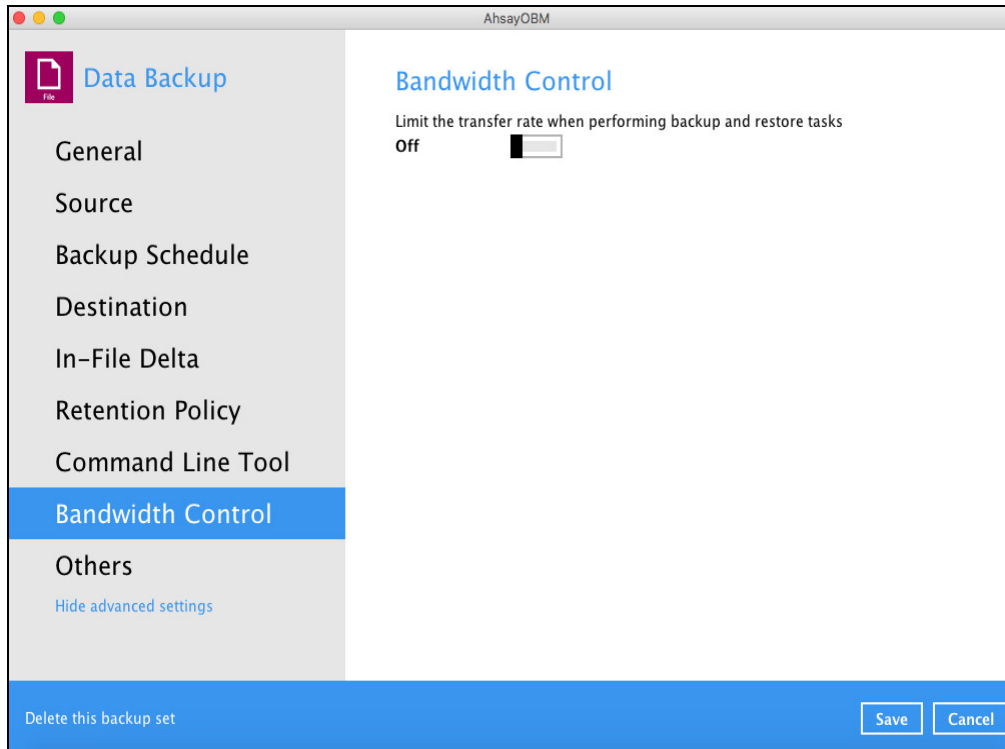
Type	Log	Time
i	[Delete Directory]... /Users/admin/Documents	25/09/2019 18:19:14
i	Total New Files = 15	25/09/2019 18:19:15
i	Total New Directories = 2	25/09/2019 18:19:15
i	Total New Links = 0	25/09/2019 18:19:15
i	Total Updated Files = 0	25/09/2019 18:19:15
i	Total Resource Updated File = 0	25/09/2019 18:19:15
i	Total Deleted Files = 1	25/09/2019 18:19:15
i	Total Deleted Directories = 2	25/09/2019 18:19:15
i	Total Deleted Links = 0	25/09/2019 18:19:15
i	Total Moved Files = 0	25/09/2019 18:19:15
i	Saving encrypted backup file index to 1568964851295/blocks at destination AhsayCBS...	25/09/2019 18:19:18
i	Saving encrypted backup file index to 1568964851295/blocks/2019-09-25-18-18-49 at destination AhsayCBS...	25/09/2019 18:19:20
i	Start running post-commands	25/09/2019 18:19:20
i	[Post-Backup-1] pmset sleep now	25/09/2019 18:19:20
i	[Post-Backup-1] Usage: pmset <options>	25/09/2019 18:19:21
i	[Post-Backup-1] See pmset(1) for details: 'man pmset'	25/09/2019 18:19:21
i	Finished running post-commands	25/09/2019 18:19:21
i	Deleting temporary file /Users/admin/temp/1568964851295/OBS@1568964886030	25/09/2019 18:19:24
i	Backup Completed Successfully	25/09/2019 18:19:24

Logs per page 50 Page 4 / 4

Close

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:

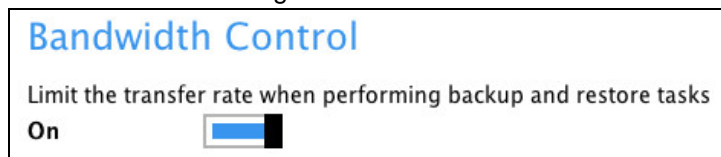
Bandwidth Control Type	Description
Independent	Each backup and restore has its assigned bandwidth.
Share	All backup and restore operations are sharing the same assigned bandwidth.

NOTE

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

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

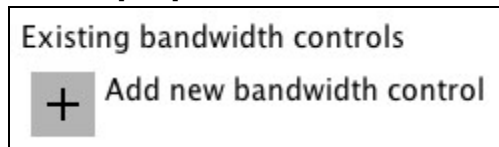
1. Slide the lever to the right to turn on the bandwidth control.



2. Select a bandwidth control mode.



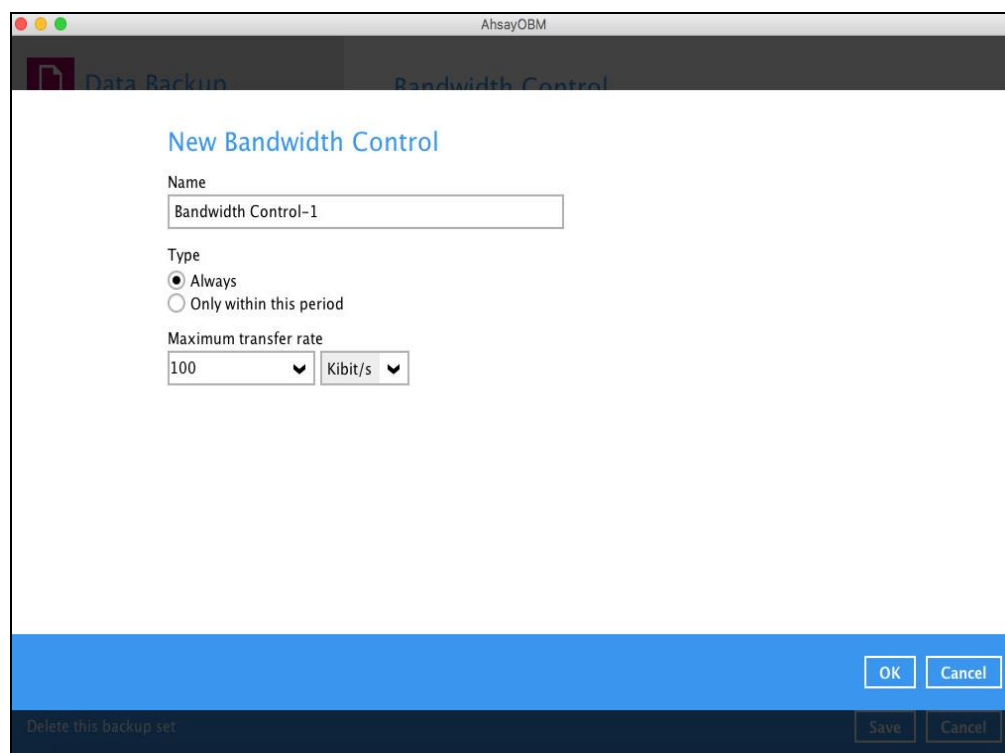
3. Click the [Add] button to create a modified bandwidth control.



4. Complete the following fields:

- 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.

A screenshot of the "New Bandwidth Control" dialog box in the AhsayOBM application. The dialog has a title bar with "AhsayOBM" and a dark header with "Data Backup" and "Bandwidth Control" tabs. The main content area is white and contains the following fields: "Name" with a text input field containing "Bandwidth Control-1"; "Type" with two radio buttons, "Always" (selected) and "Only within this period"; and "Maximum transfer rate" with a numeric input field containing "100" and a unit dropdown menu set to "Kibit/s". At the bottom, there is a blue bar with "OK" and "Cancel" buttons, and a dark bar with "Delete this backup set" and "Save" and "Cancel" buttons.

5. Click the [OK] button to save the created bandwidth control set, then click the [Save] button to store settings.

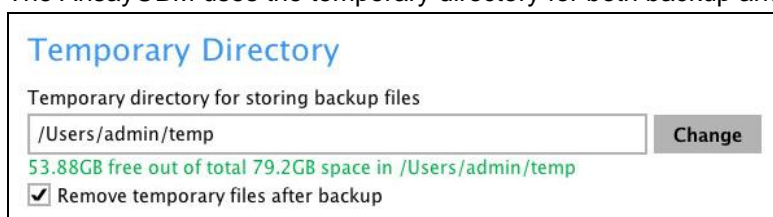
Others

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

- [Temporary Directory](#)
- [Follow Link](#)
- [OpenDirect](#) (Not supported on Mac platform)
- [Compressions](#)
- [Encryption](#)

Temporary Directory

The AhsayOBM 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.
- Incremental/Differential delta files generated during backups.

For a **restore job**, it is used to temporarily store:

- Full and Incremental/Differential delta files retrieved from the backup destination.

Merging of the Full and Incremental/Differential delta files as part of the restore process.

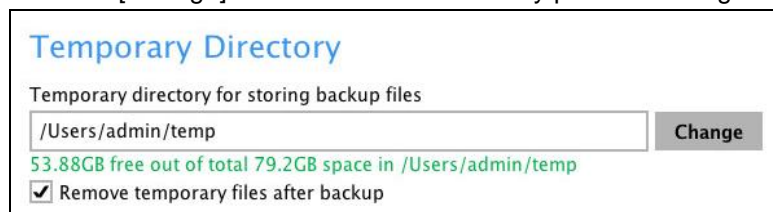
NOTES

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

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

To change the temporary directory, follow the steps below:

1. Click 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.

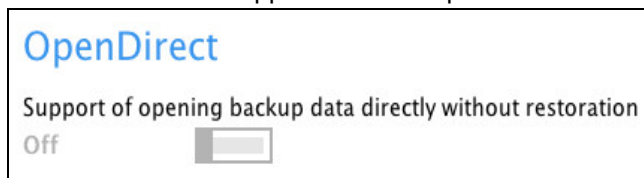


NOTE

Applicable for File Backup Sets only.

OpenDirect

This feature is not supported on Mac platform.



Compressions

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



There are four (4) different data compression types:

- No Compression
- Normal
- Fast (Compressed size larger than normal)
- Fast with optimization for local

NOTE

The Compression type can be changes 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.

Encryption

Encryption key	•••••
Unmask encryption key	
Algorithm	AES
Method	CBC
Key length	256 bits

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

1. In the backup set settings, select the [Others] tab. Scroll down to display the Encryption.

The screenshot shows the 'File Backup' settings window with the 'Others' tab selected. The left sidebar lists various settings categories, with 'Others' highlighted. The main content area shows settings for 'Follow Link', 'OpenDirect', 'Compressions', and 'Encryption'. The 'Encryption' section at the bottom displays the encryption key as masked (•••••), along with links for 'Copy to clipboard' and 'Unmask encryption key'. Other encryption settings shown are Algorithm: AES, Method: CBC, and Key length: 256 bits. At the bottom of the window are buttons for 'Delete this backup set', 'Save', and 'Cancel'.

2. Click 'Unmask encryption key' to display the encryption key of the backup set.

Encryption

Encryption key	•••••
Unmask encryption key	
Algorithm	AES
Method	CBC
Key length	256 bits

Encryption

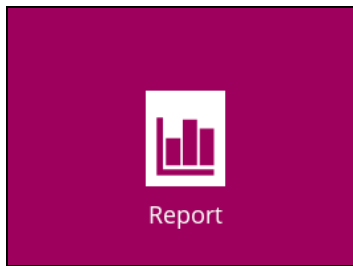
Encryption key	EqP4A5d/FJl3MzuL0xbQ9LoCbnu09H6GiNen8mjQmyA=
Mask encryption key	
Algorithm	AES
Method	CBC
Key length	256 bits

NOTE

The encryption setting can only be configured during the creation of backup set. For more details about encryption settings, please refer to step no. 13 in [Chapter 8 Create a Backup Set](#).

7.6 Report

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



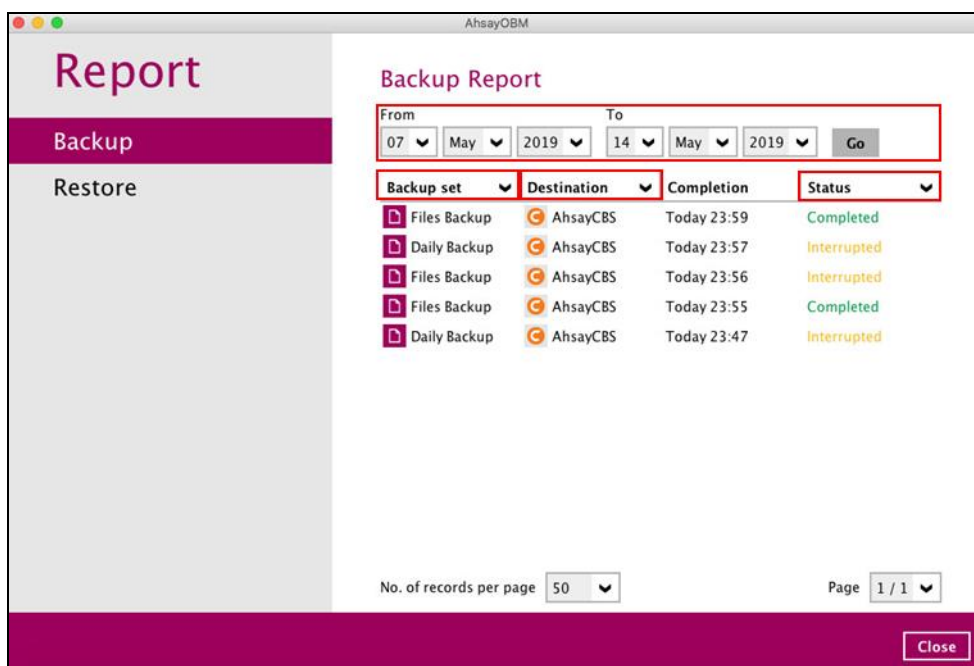
There are two (2) options available for this feature:

- **Backup**
- **Restore**

7.6.1 Backup

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

- **Date**
- **Backup set**
- **Destination**
- **Status**



Report

Backup

Restore

Backup Report

From: 07 May 2019 To: 14 May 2019 Go

Backup set	Destination	Completion	Status
Files Backup	AhsayCBS	Today 23:59	Completed
Daily Backup	AhsayCBS	Today 23:57	Interrupted
Files Backup	AhsayCBS	Today 23:56	Interrupted
Files Backup	AhsayCBS	Today 23:55	Completed
Daily Backup	AhsayCBS	Today 23:47	Interrupted

No. of records per page: 50 Page: 1 / 1

Close

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

Backup Report			
From		To	
08	May	2019	15 May 2019
		Go	
Backup set	Destination	Completion	Status
Files Backup	Local-1	Today 00:16	Completed
Files Backup	GoogleDrive-1	Today 00:16	Completed
Files Backup	AhsayCBS	Today 00:13	Completed
Files Backup	AhsayCBS	14/05/2019 23:59	Completed
Daily Backup	AhsayCBS	14/05/2019 23:57	Interrupted
Files Backup	AhsayCBS	14/05/2019 23:56	Interrupted
Files Backup	AhsayCBS	14/05/2019 23:55	Completed
Daily Backup	AhsayCBS	14/05/2019 23:47	Interrupted

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

Backup Report			
From		To	
08	May	2019	15 May 2019
		Go	
Backup set	Destination	Completion	Status
Backup set	AhsayCBS	Today 00:25	Completed
AhsayOBM Backup	Local-1	Today 00:16	Completed
Files Backup	GoogleDrive-1	Today 00:16	Completed
Daily Backup	AhsayCBS	Today 00:13	Completed
Files Backup	AhsayCBS	14/05/2019 23:59	Completed
Daily Backup	AhsayCBS	14/05/2019 23:57	Interrupted
Files Backup	AhsayCBS	14/05/2019 23:56	Interrupted
Files Backup	AhsayCBS	14/05/2019 23:55	Completed
Daily Backup	AhsayCBS	14/05/2019 23:47	Interrupted

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

Backup Report			
From		To	
08	May	2019	15 May 2019
		Go	
Backup set	Destination	Completion	Status
AhsayOBM Bac...	Destination	Today 00:25	Completed
Files Backup	AhsayCBS	Today 00:16	Completed
Files Backup	Local-1	Today 00:16	Completed
Files Backup	GoogleDrive-1	Today 00:13	Completed
Files Backup	AhsayCBS	14/05/2019 23:59	Completed
Daily Backup	AhsayCBS	14/05/2019 23:57	Interrupted
Files Backup	AhsayCBS	14/05/2019 23:56	Interrupted
Files Backup	AhsayCBS	14/05/2019 23:55	Completed
Daily Backup	AhsayCBS	14/05/2019 23:47	Interrupted

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

Backup Report

From 08 May 2019 To 15 May 2019 [Go](#)

Backup set	Destination	Completion	Status
Files Backup	Local-1	Today 01:11	Status
Files Backup	GoogleDrive-1	Today 01:10	Completed
Files Backup	AhsayCBS	Today 01:10	Interrupted
AhsayOBM Backup	AhsayCBS	Today 01:09	Interrupted with error(s)
AhsayOBM Backup	AhsayCBS	Today 00:25	Completed
Files Backup	Local-1	Today 00:16	Completed
Files Backup	GoogleDrive-1	Today 00:16	Completed
Files Backup	AhsayCBS	Today 00:13	Completed
Files Backup	AhsayCBS	14/05/2019 23:59	Completed
Daily Backup	AhsayCBS	14/05/2019 23:57	Interrupted
Files Backup	AhsayCBS	14/05/2019 23:56	Interrupted
Files Backup	AhsayCBS	14/05/2019 23:55	Completed

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

Backup Report

From 08 May 2019 To 15 May 2019 [Go](#)

Backup set	Destination	Completion	Completed
AhsayOBM Bac...	AhsayCBS	Today 00:25	Completed
Files Backup	Local-1	Today 00:16	Completed
Files Backup	GoogleDrive-1	Today 00:16	Completed
Files Backup	AhsayCBS	Today 00:13	Completed
Files Backup	AhsayCBS	14/05/2019 23:59	Completed
Files Backup	AhsayCBS	14/05/2019 23:55	Completed

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

Backup Report

From 08 May 2019 To 15 May 2019 [Go](#)

Backup set	Destination	Completion	Completed
AhsayOBM Backup	AhsayCBS	15/05/2019 00:24	Completed

Backup set AhsayOBM Backup

Destination AhsayCBS

Job 15/05/2019 00:24

Time Today 00:24 - 00:25 (PST)

Status ✓ Completed successfully

New files * 1 [16/0 (0%)]

Updated files * 0

Attributes Changed Files * 0

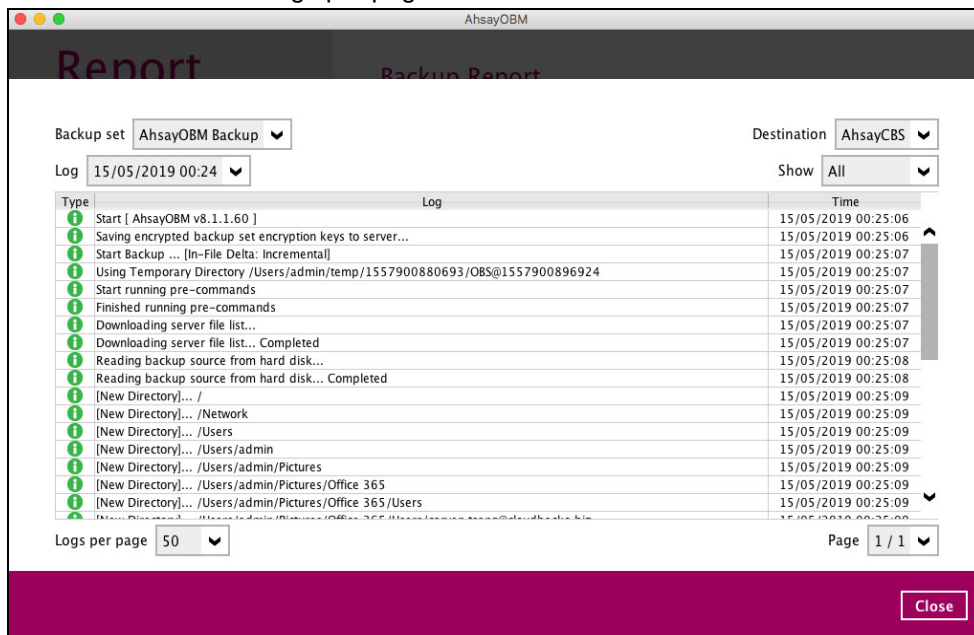
Moved files * 0

Deleted files * 0

* Unit = No of files [Total zipped size / Total unzipped size (compression ratio)]

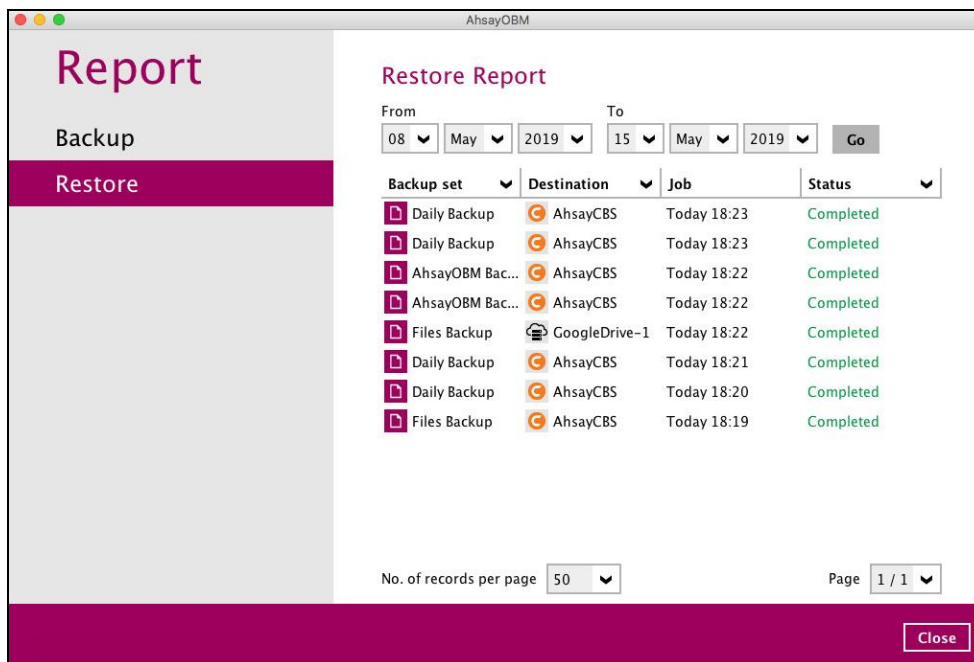
[View log](#)

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



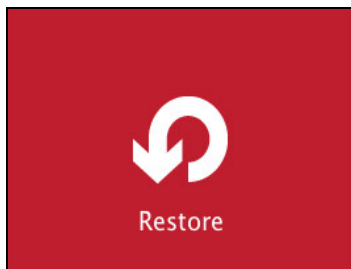
7.6.2 Restore

This feature is used for viewing restore report(s). You can also apply filter on **time**, **backup set**, **destination**, and **status** here.

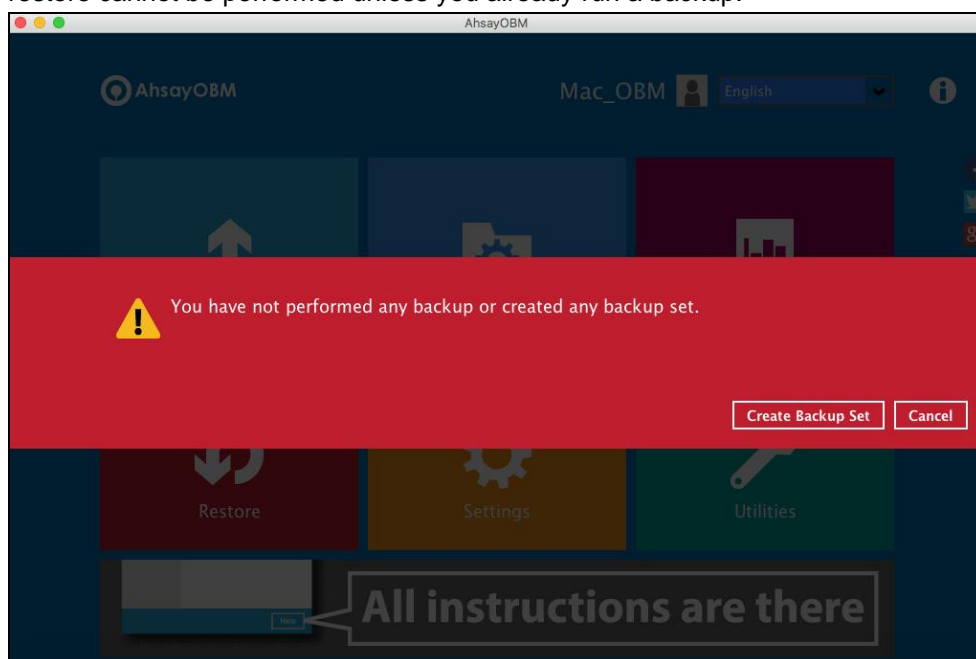


7.7 Restore

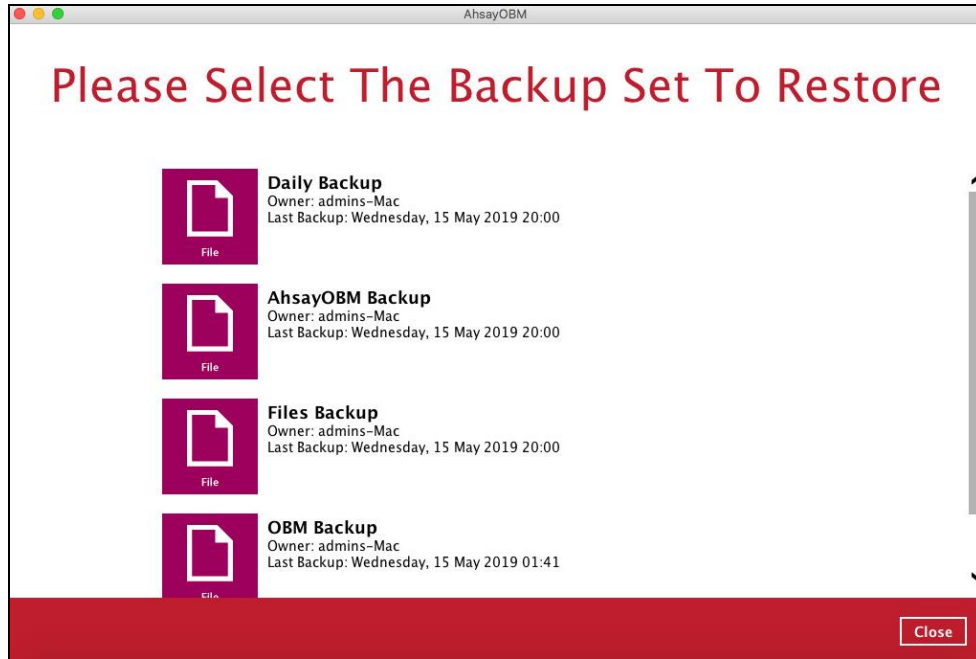
This feature is used to copy the backed-up file(s) from the backup set and restoring it to its original location or new location.



If using AhsayOBM 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.

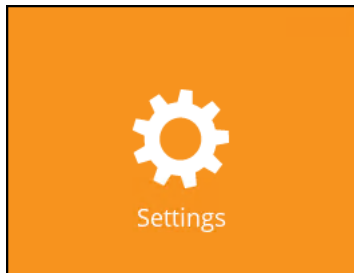


If a backup job has been performed, select a backup set you wish to restore.

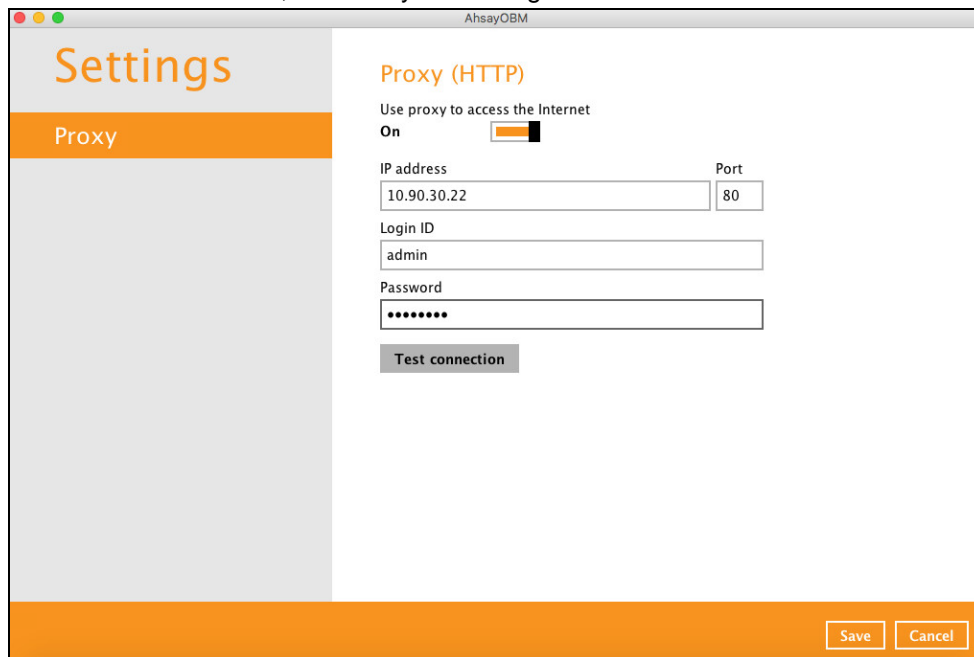


7.8 Settings

This feature allows user to enable the **Proxy Settings**.

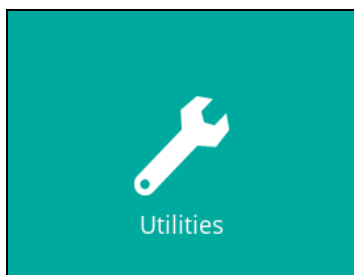


When this feature is on, the AhsayOBM will gain access to the internet.



7.9 Utilities

This feature allows user to perform quality check on the backed up data, free up storage from obsolete files, delete, and decrypt backed up data.



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

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

7.9.1 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).

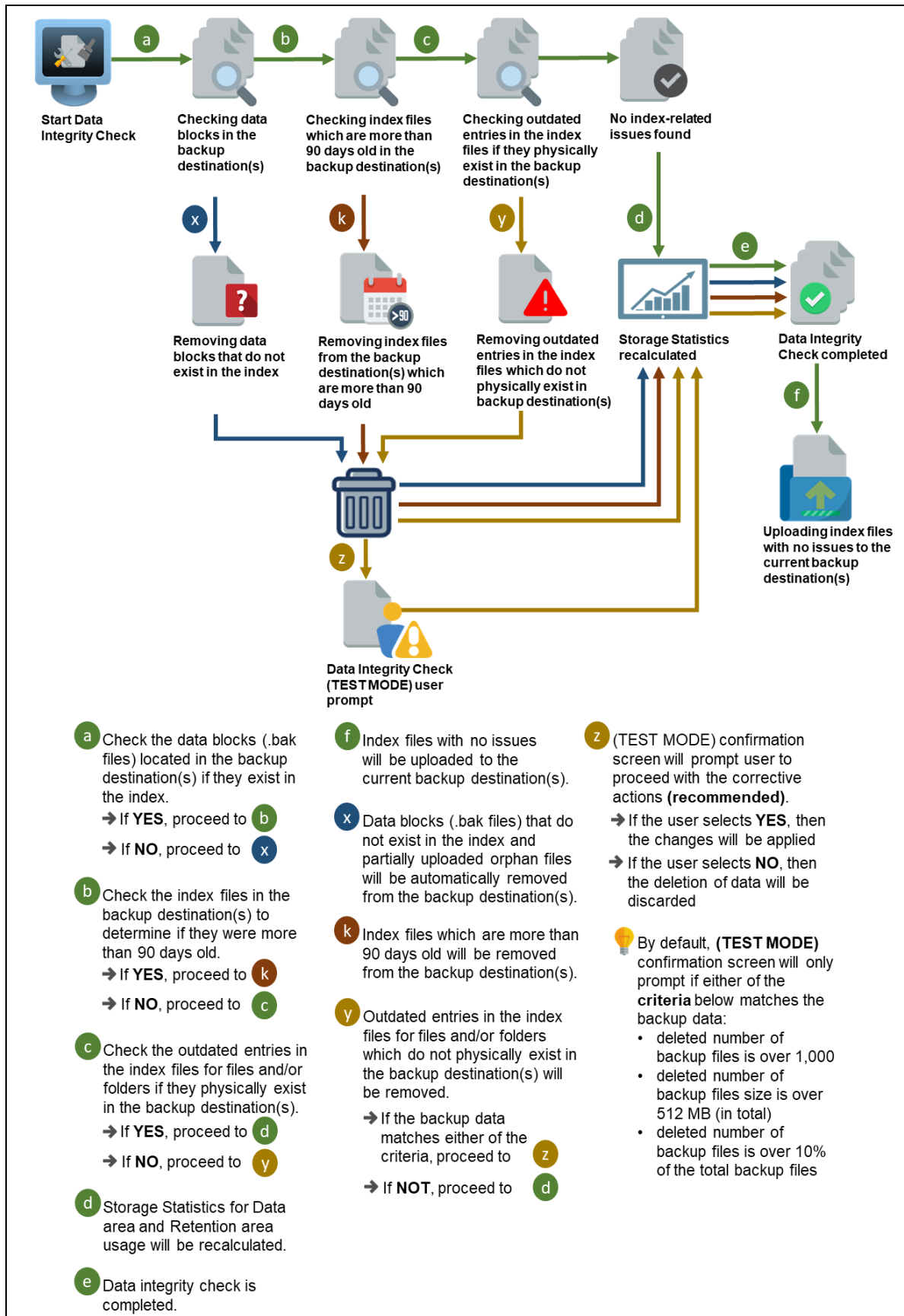
There are four (4) options in performing the Data Integrity Check:

Option 1 <input type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check <input type="checkbox"/> Rebuild index Start	For checking of index and data.
Option 2 <input checked="" type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check <input type="checkbox"/> Rebuild index Start	For checking of index and integrity of files against the checksum file generated at the time of the backup job.
Option 3 <input type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check <input checked="" type="checkbox"/> Rebuild index Start	For checking and rebuilding of index.
Option 4 <input checked="" type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check <input checked="" type="checkbox"/> Rebuild index Start	For checking of index, integrity of files against the checksum file generated at the time of the backup job, and rebuilding of index.

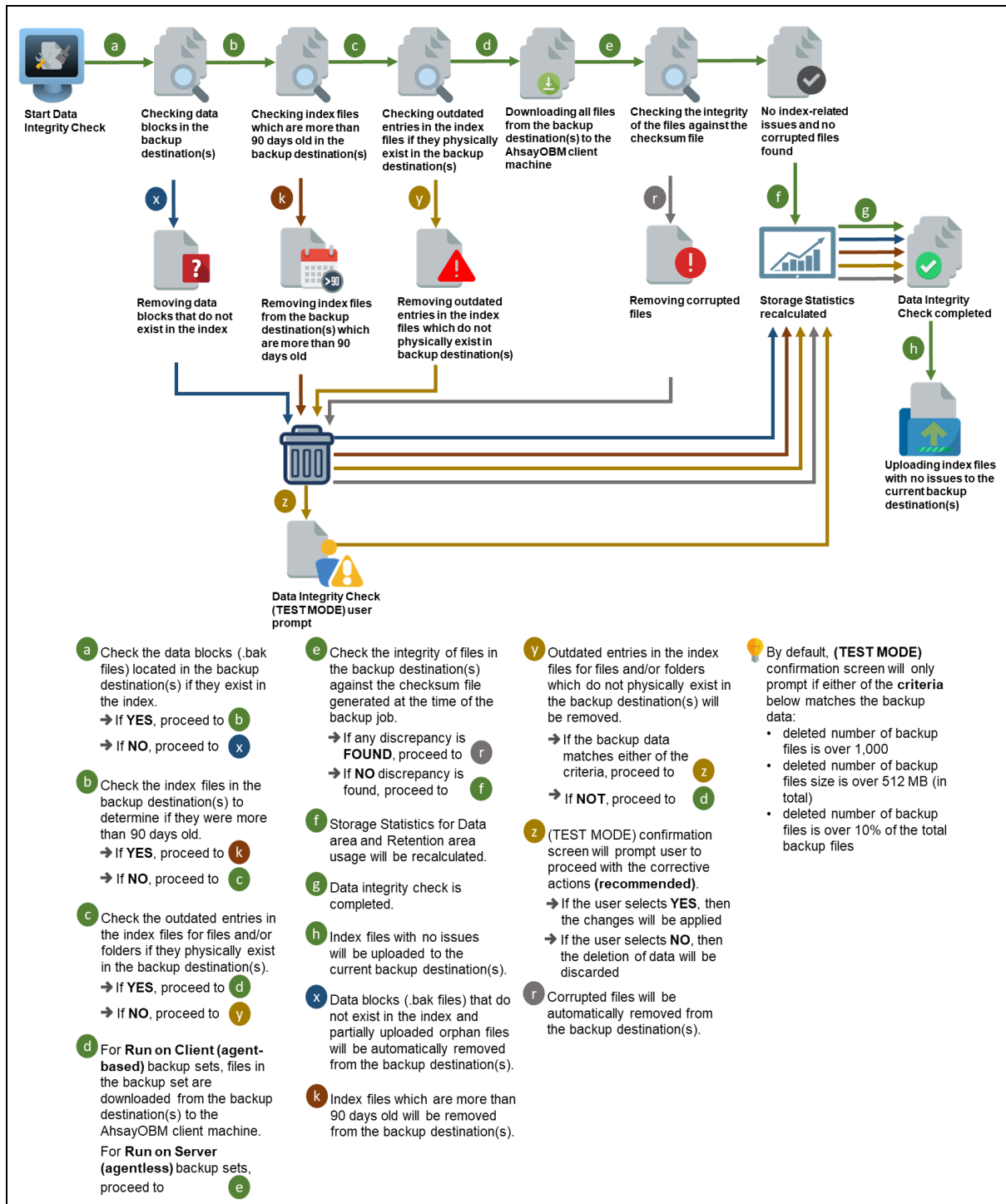
The following diagrams show the detailed process of the Data Integrity Check (DIC) in four (4) modes:

- **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

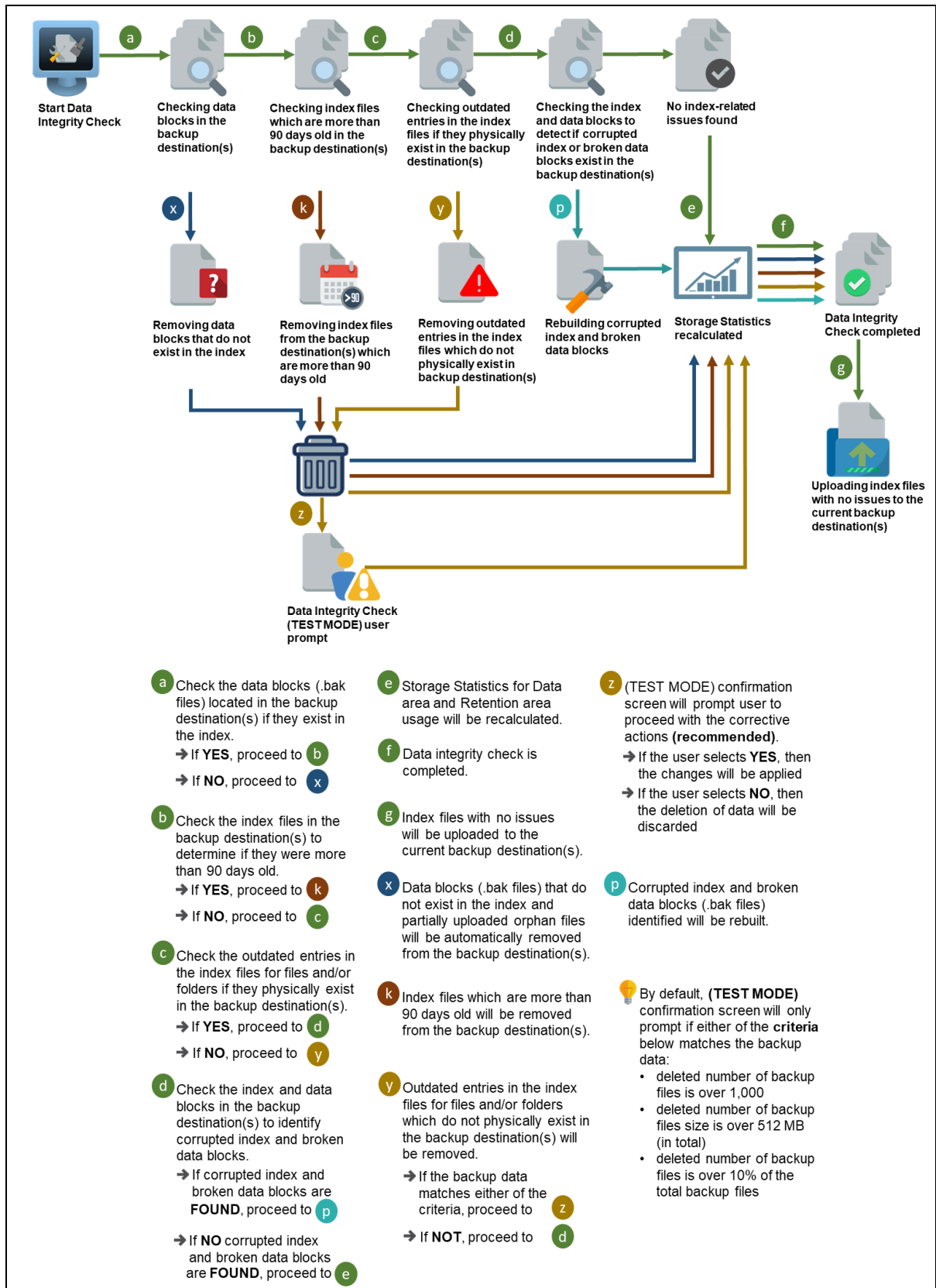
Option 1 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Rebuild index DISABLED (Default mode)



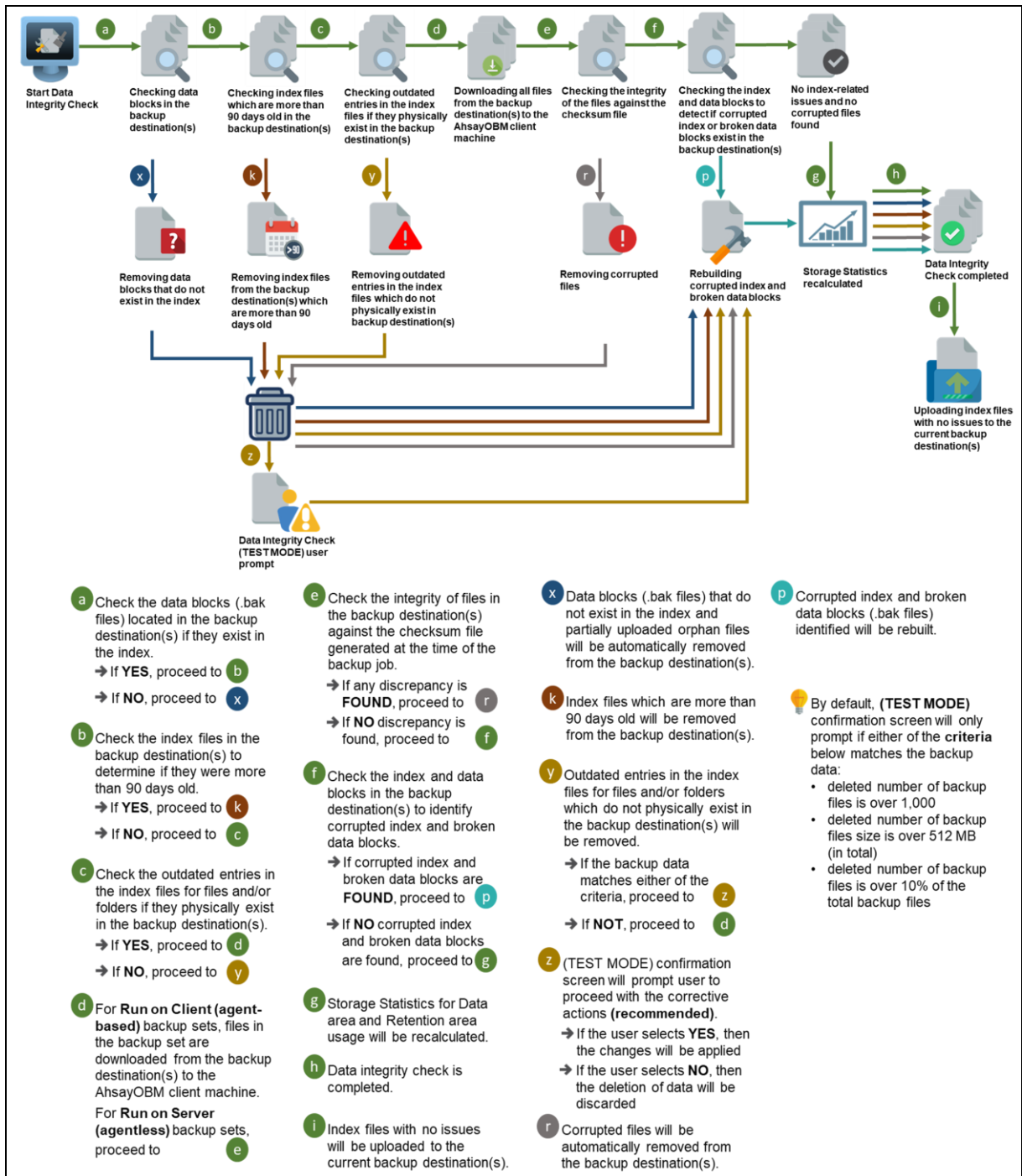
Option 2 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) **ENABLED** and Rebuild index **DISABLED**

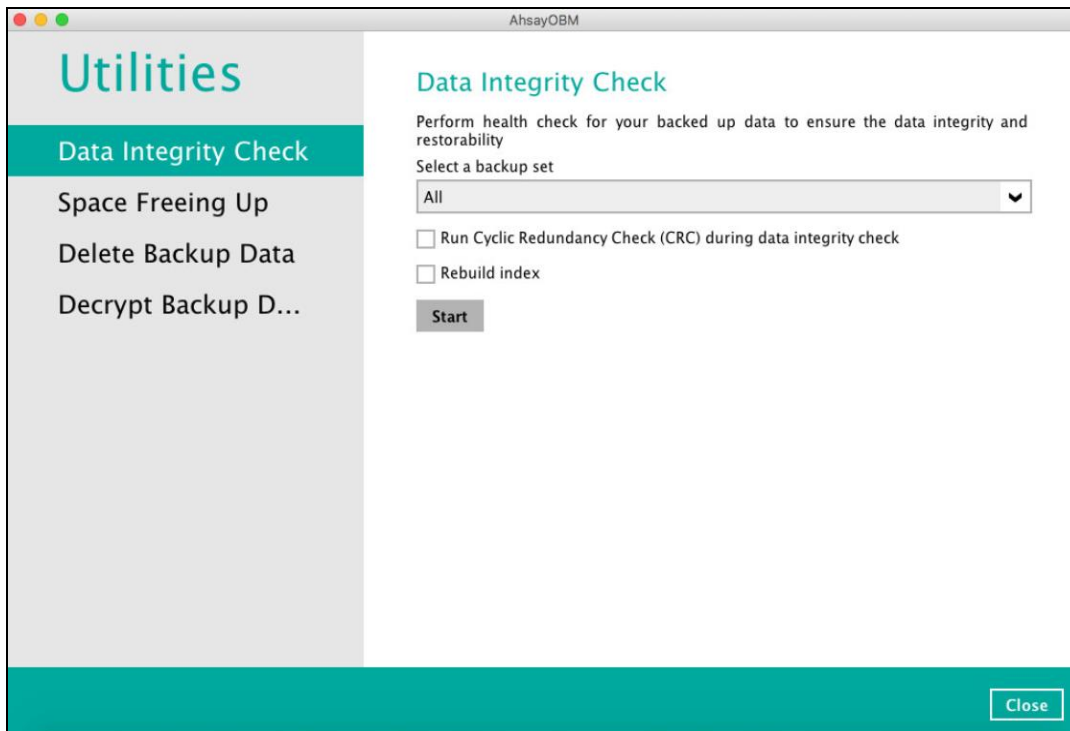


Option 3 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) **DISABLED** and Rebuild index **ENABLED**



Option 4 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Rebuild index **ENABLED**

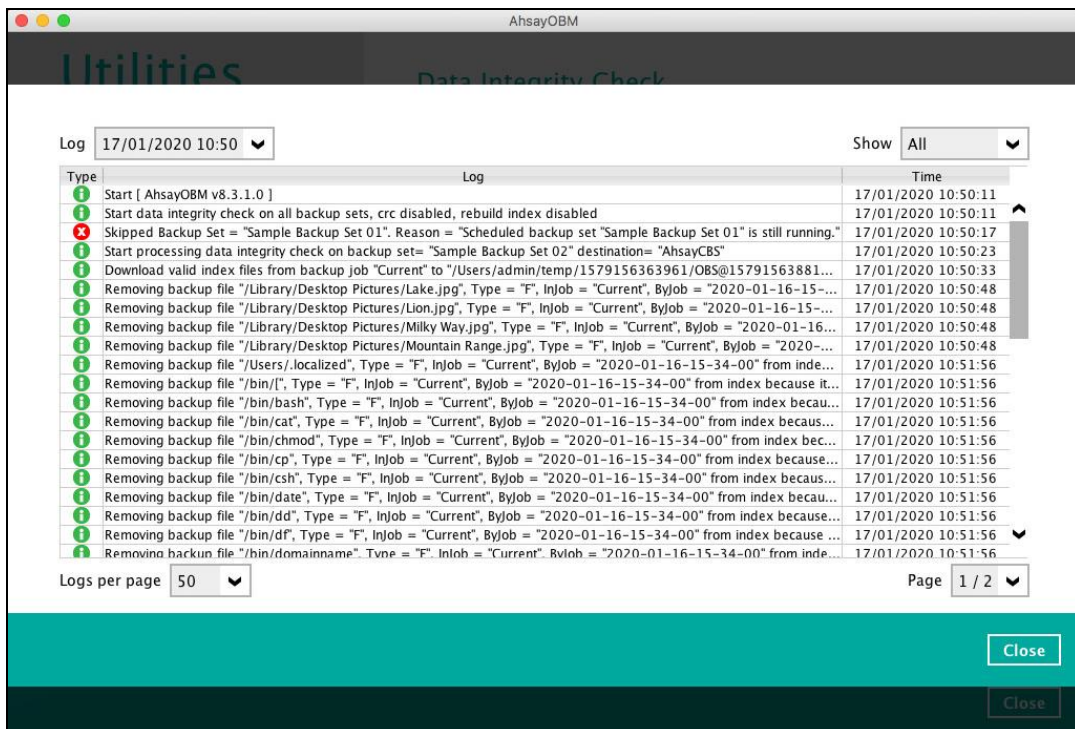
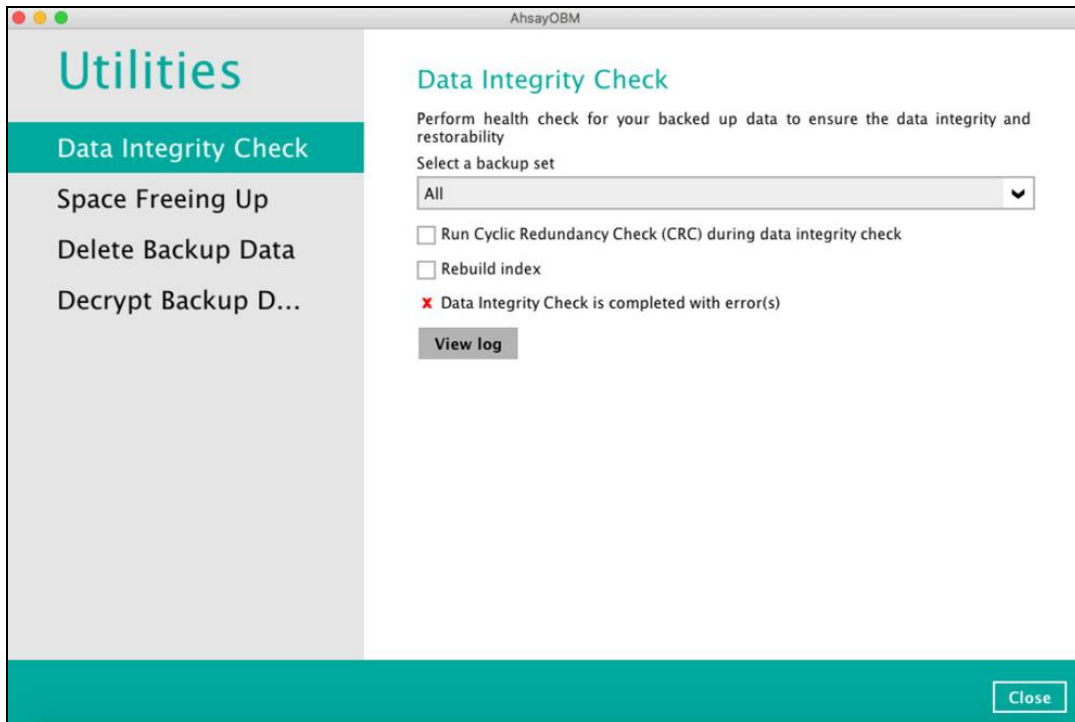


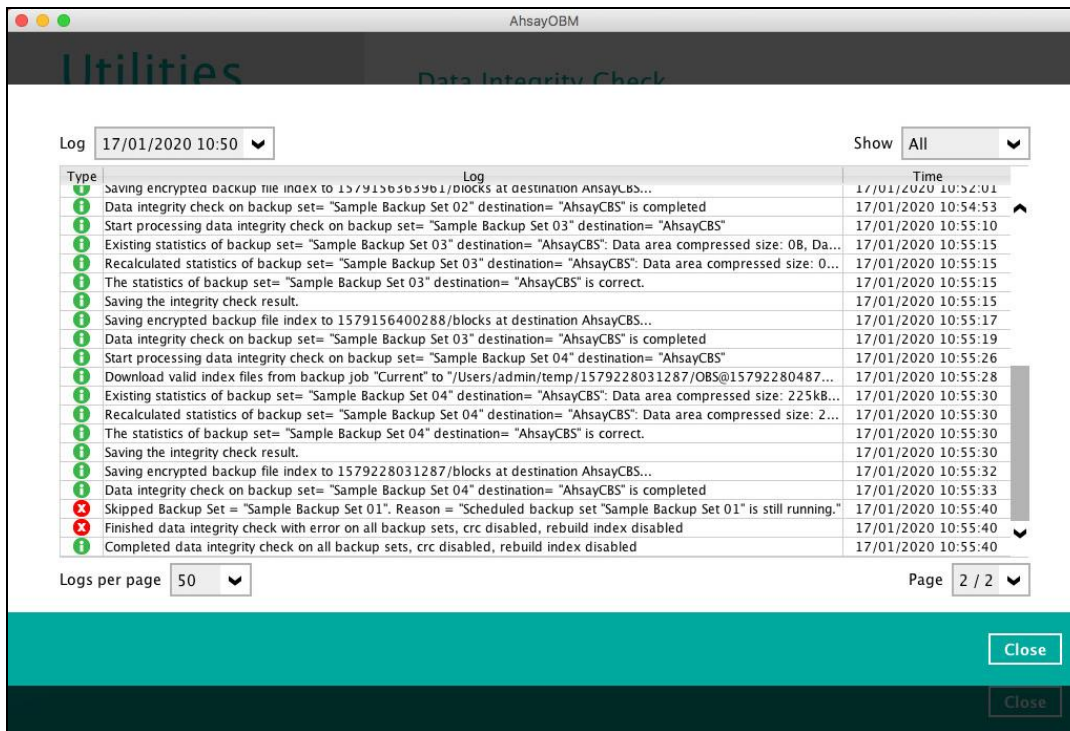


NOTES

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.

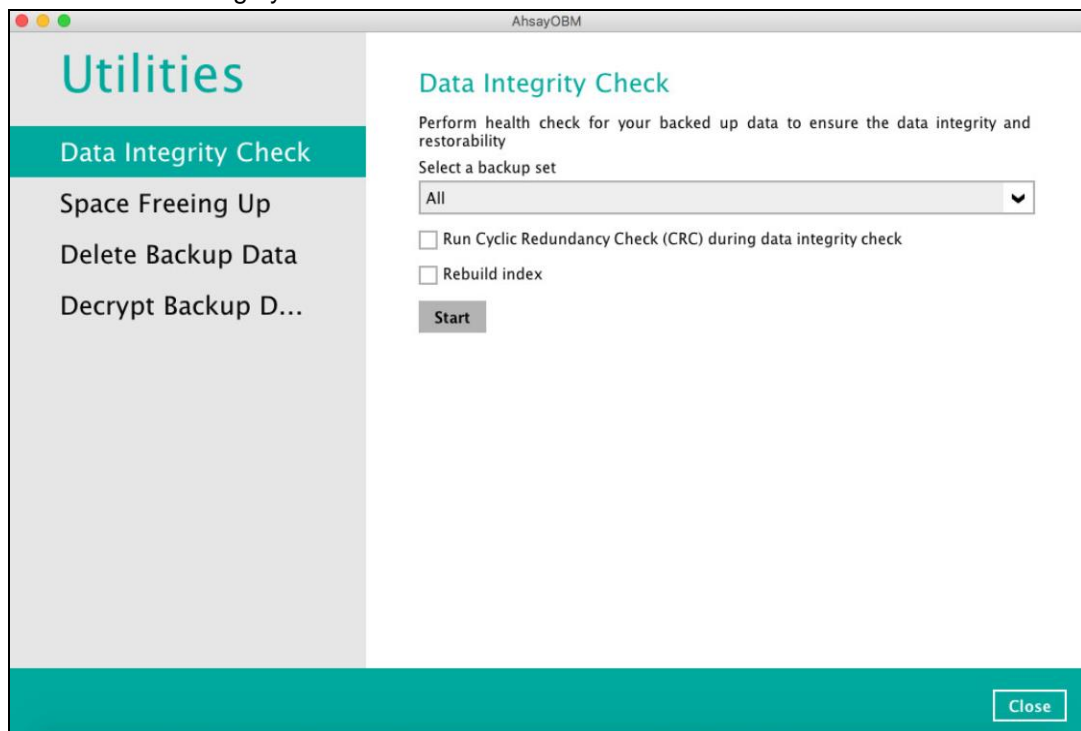
The following screenshot is an example of a Data Integrity Check completed with error(s). A Data Integrity Check is run on a backup set with an active backup job running which resulted the Data Integrity Check to stop with error(s). Clicking the **View log** button will display the details of the Data Integrity Check job error(s).



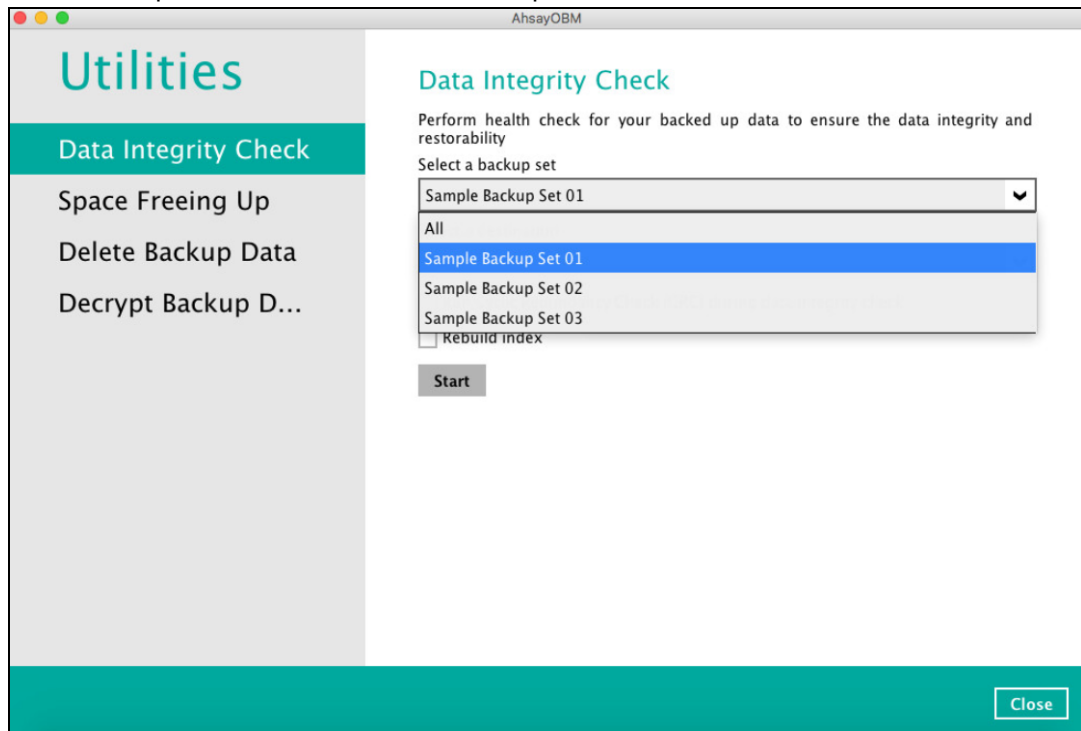


To perform a Data Integrity Check, follow the instructions below:

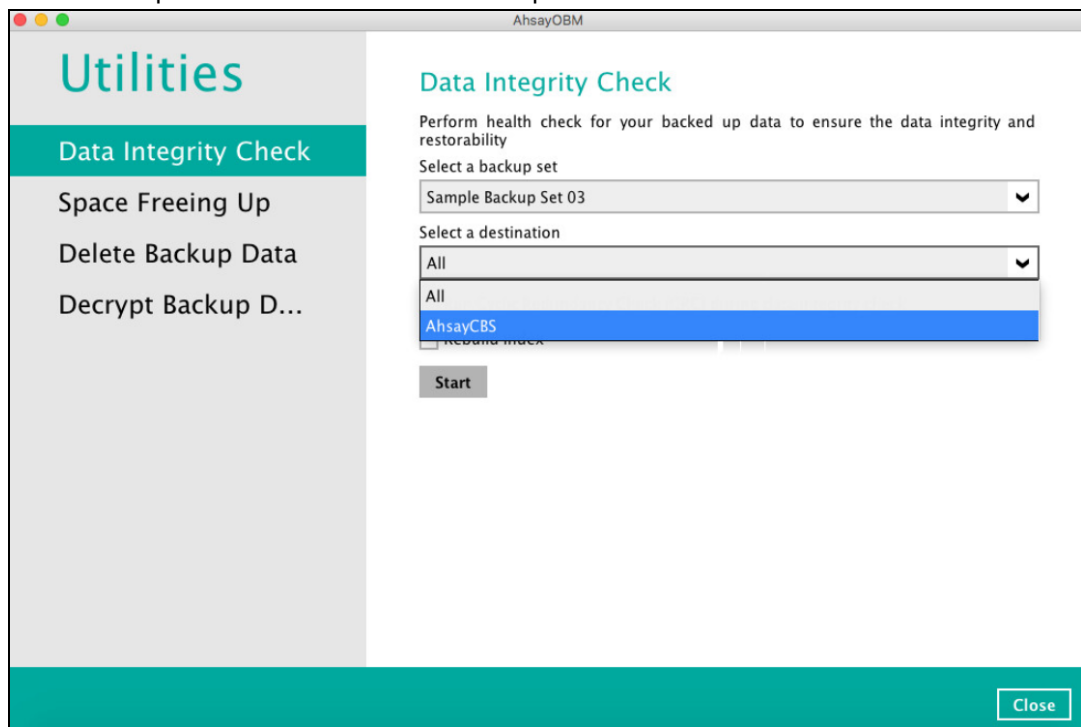
1. Go to the Data Integrity Check tab in the Utilities menu.



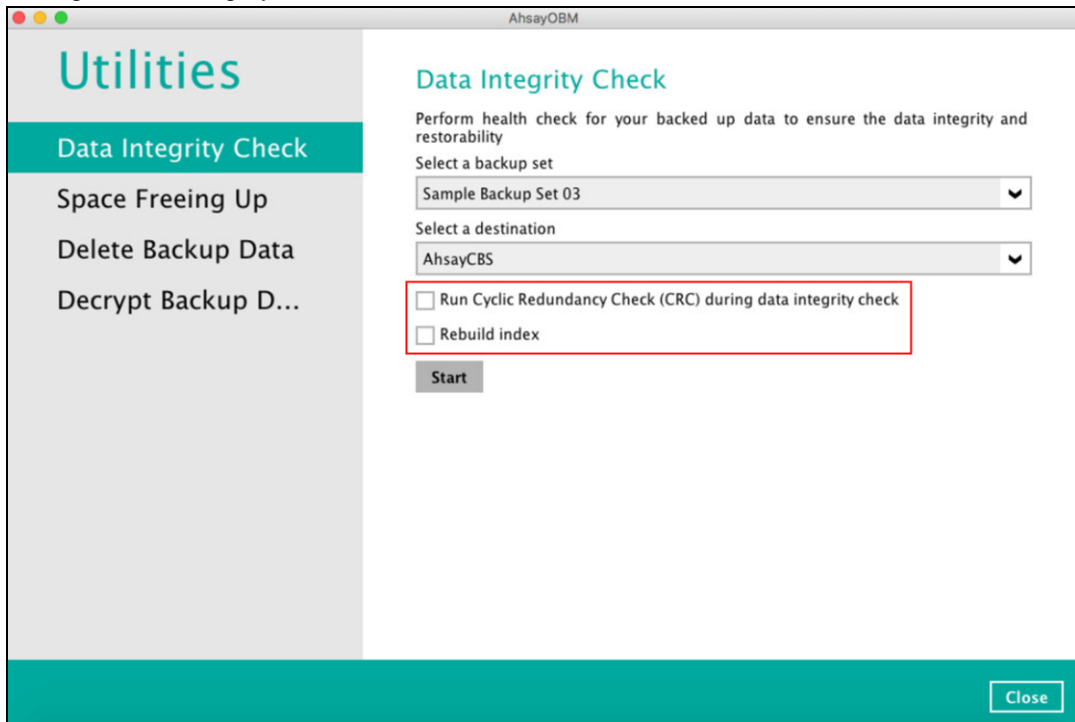
2. Click the drop-down button to select a backup set.



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



4. Unchecked Run Cyclic Redundancy Check (CRC) and Rebuild index options is the default setting of data integrity check.



Run Cyclic Redundancy Check (CRC)

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

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

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

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

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

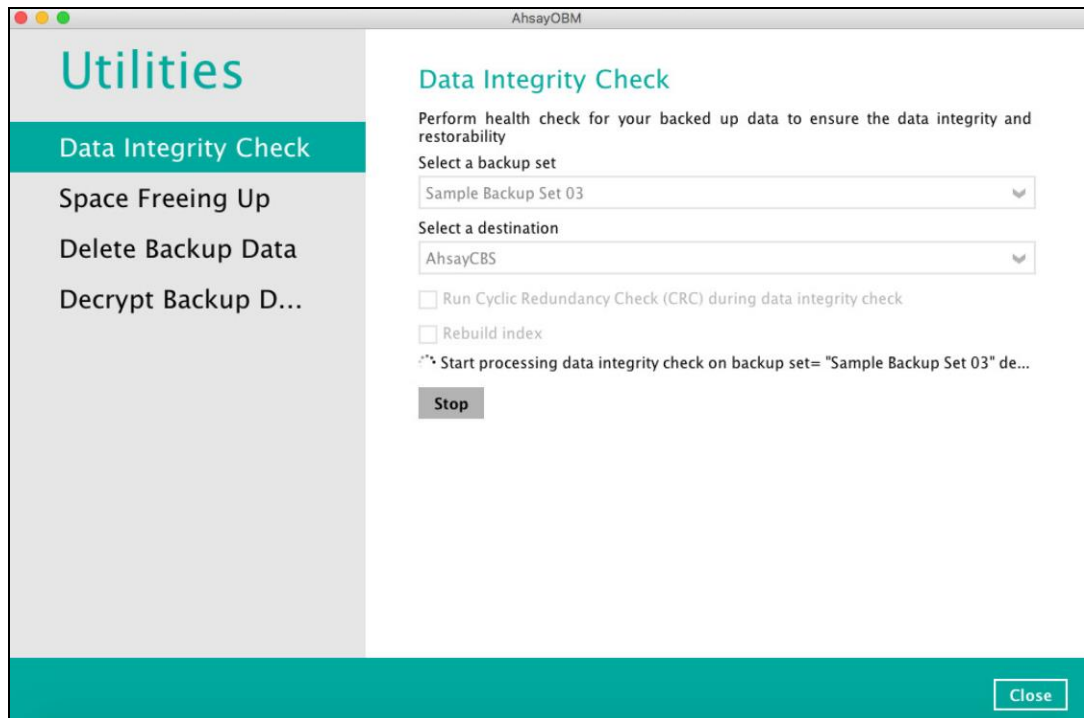
NOTE

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.

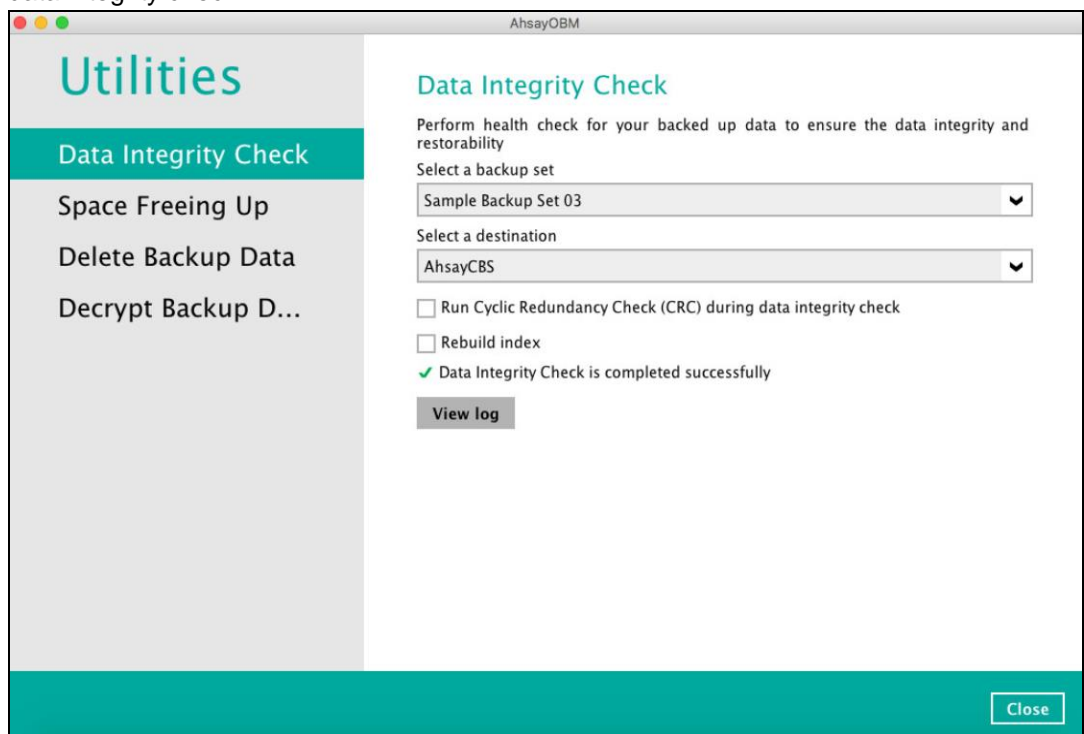
Rebuild index

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

5. Click the [Start] button to begin the Data Integrity Check.
6. Data Integrity Check will start running on the selected backup set(s) and backup destination(s).




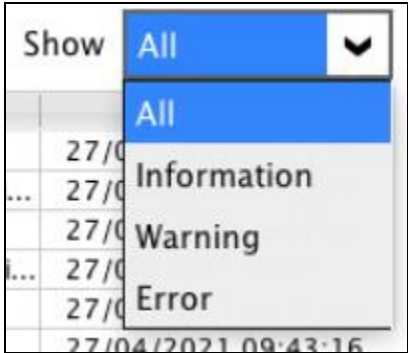
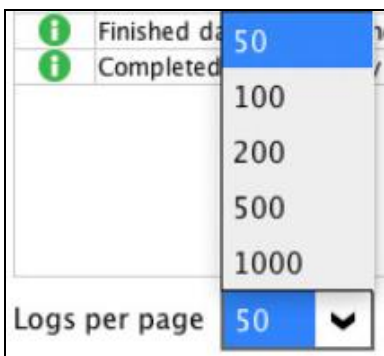
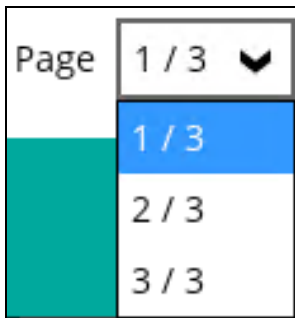
7. Once the DIC is completed, click the **View log** button to check the detailed process of the data integrity check.



8. The detailed log of data integrity check process will be displayed.

The following options can be used for further viewing of the detailed DIC log:

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

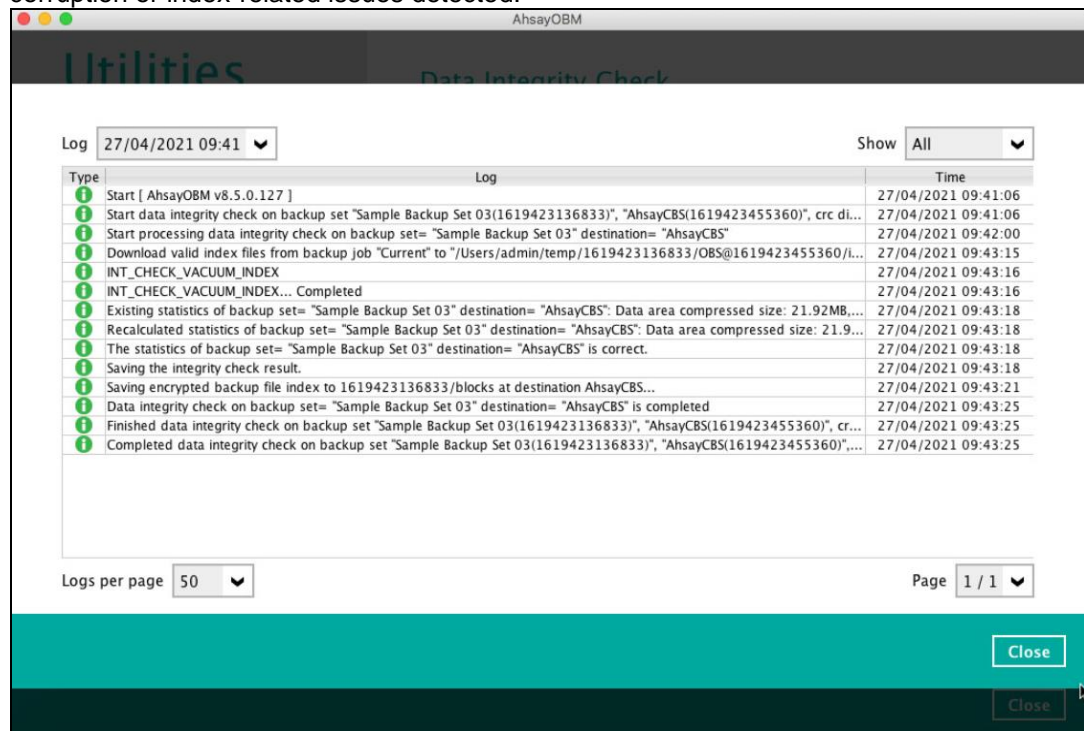
Control	Screenshot	Description
Log filter		This option is used to display the logs of the previous data integrity check jobs.
Show filter		<p>This option is used to sort the data integrity check log by its status (i.e., All, Information, Warning, and Error).</p> <p>With this filter, it will be easier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

Data Integrity Check Result

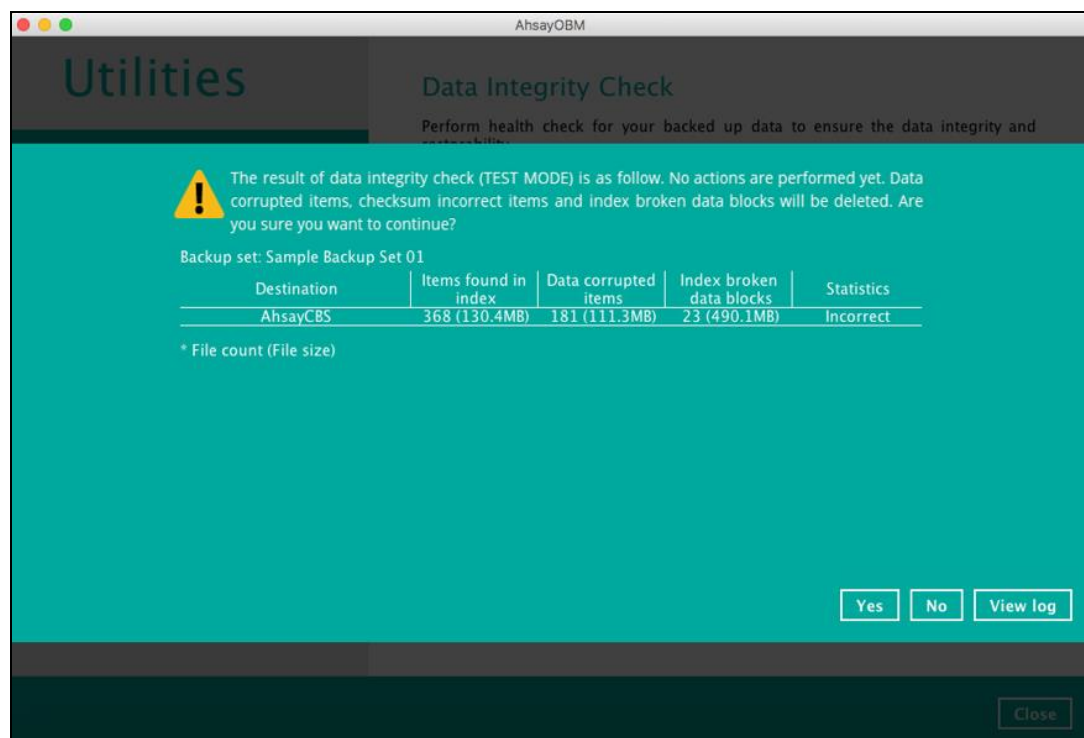
There are two possible outcomes after the completion of a data integrity check:

- Data Integrity Check is completed successfully with no data corruption or index-related 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 or index-related 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)




Test Mode confirmation

The (TEST MODE) confirmation screen will ONLY appear if either of the **criteria** below matches the backup data during the data integrity check process:

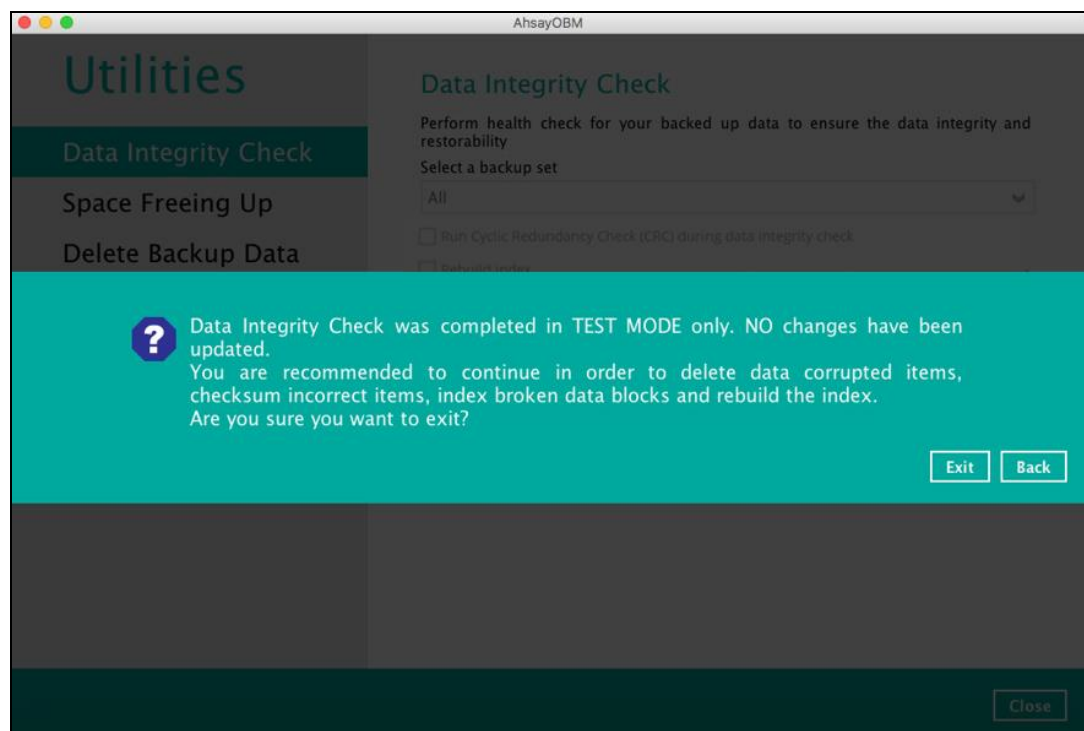
- deleted number of backup files is over 1,000
- deleted number of backup file size is over 512 MB (in total)
- deleted number of backup files is over 10% of the total backup files

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

There are three (3) options on the (TEST MODE) confirmation screen:

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

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



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

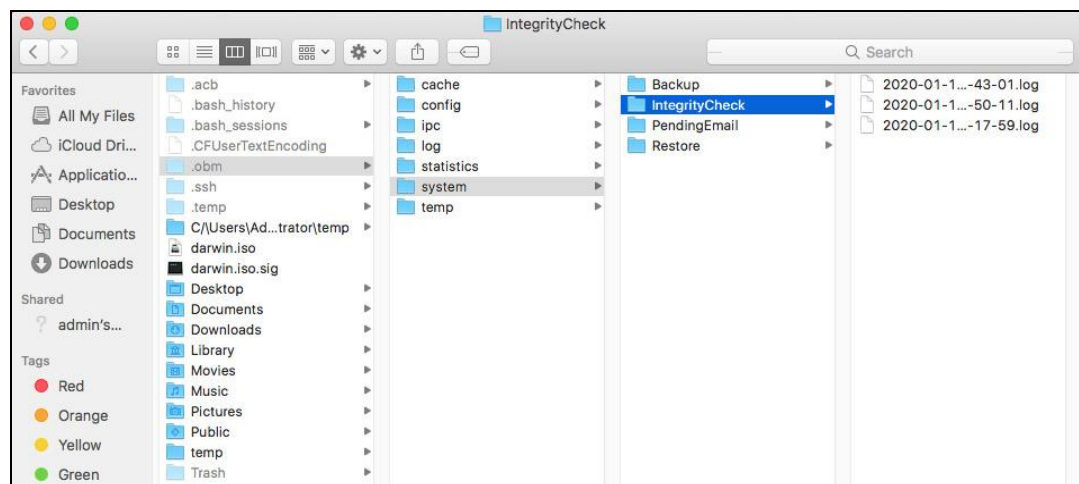
If the **Back** button is clicked, it will go back to the (TEST MODE) confirmation screen.

NOTES

1. It is strongly recommended to apply corrective actions when the (TEST MODE) confirmation screen pops up (clicking the **Yes** button). This is to ensure that the remaining corrupted file(s) will be removed from the backup destination(s), therefore 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 do not have related index entries, then these physical data blocks will be **automatically** removed from the backup destination(s) without the (TEST MODE) prompt.

Aside from viewing the Data Integrity Check logs directly on AhsayOBM client, they can also be viewed on the file system of the AhsayOBM client machine. For AhsayOBM on macOS, the DIC logs are located in the following directory:

%UserProfile%\lobm\system\IntegrityCheck

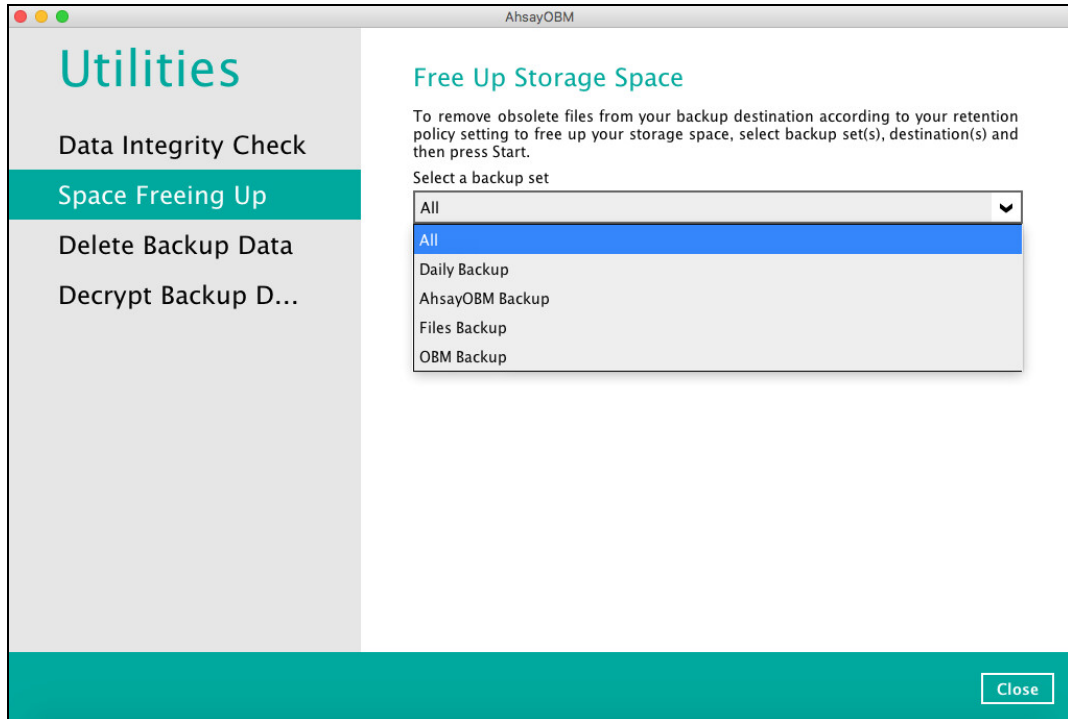


7.9.2 Space Freeing Up

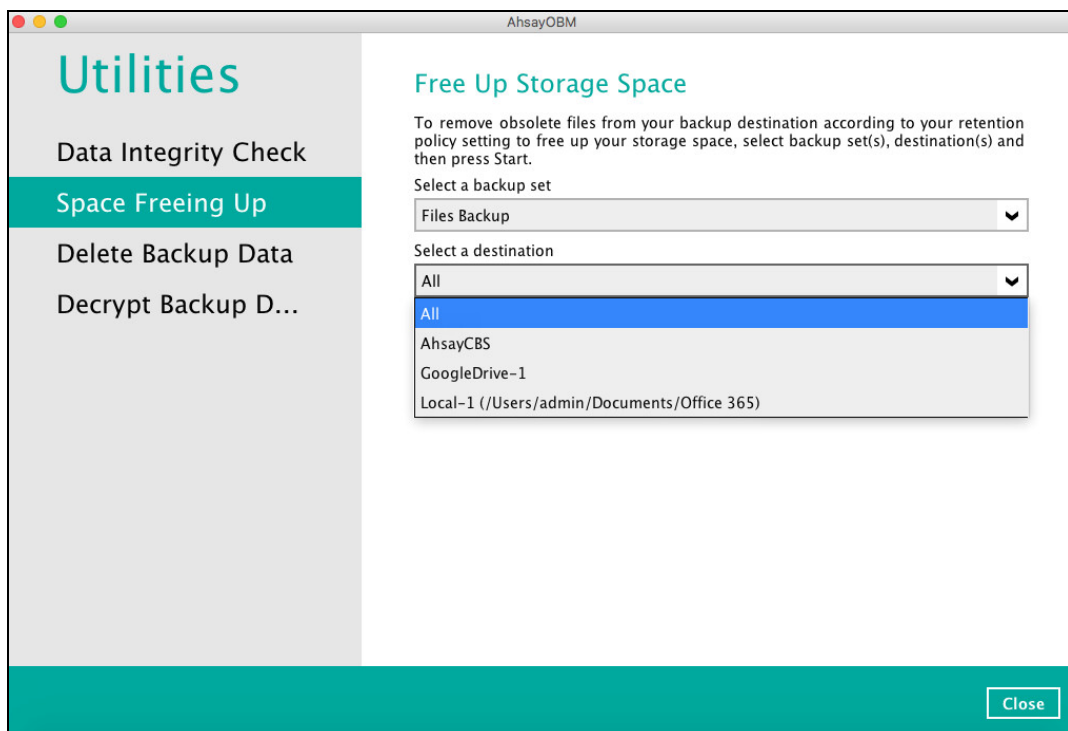
This feature is used to remove obsolete file(s) from your backup set and destination (manually start retention policy). After the Space Freeing Up job is completed, the storage statistics of the backup set(s) are updated.

To perform Space Freeing Up, follow the instructions below:

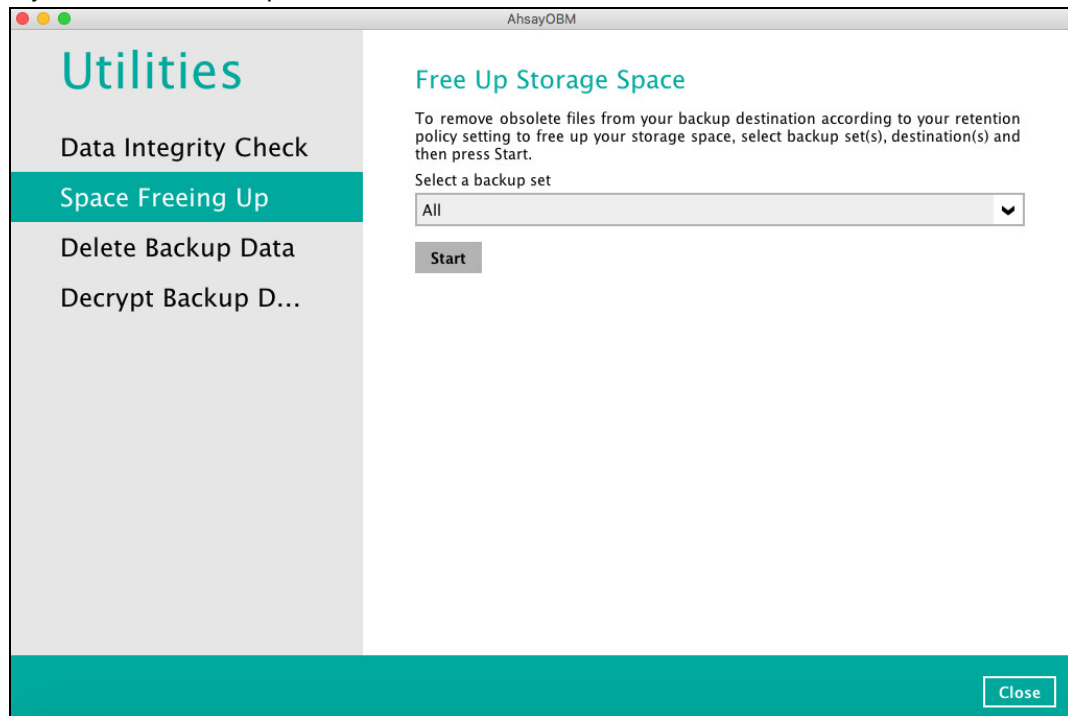
1. Select a backup set from the drop-down list.



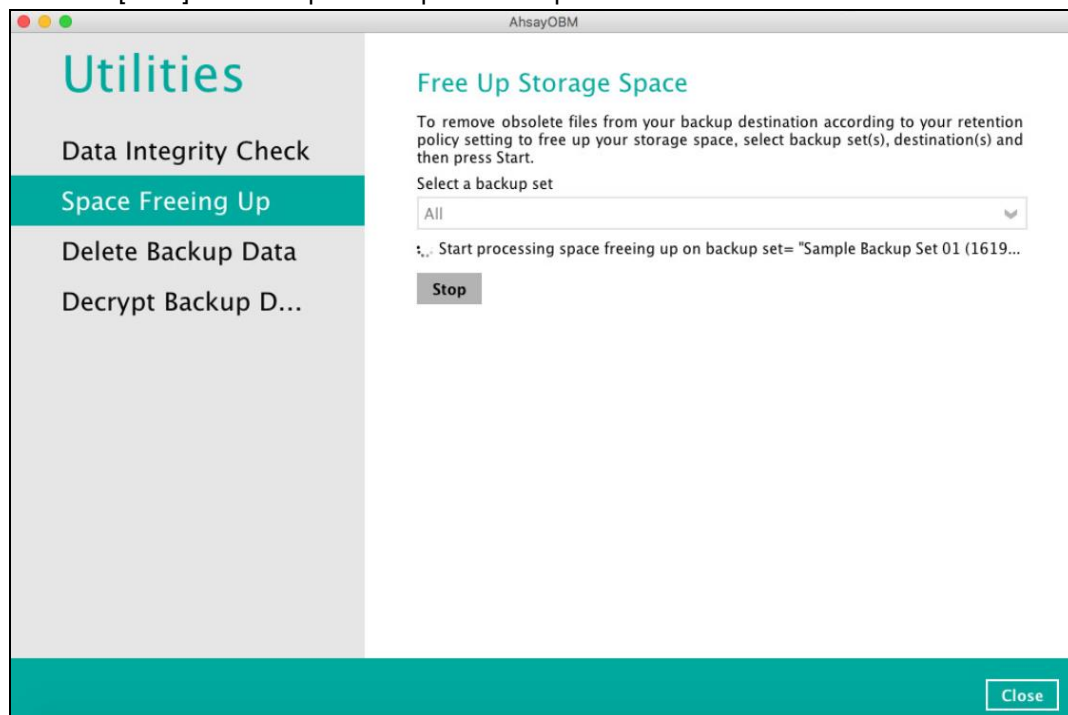
If you select a specific backup set, then you will also have to select a specific destination or all destinations.



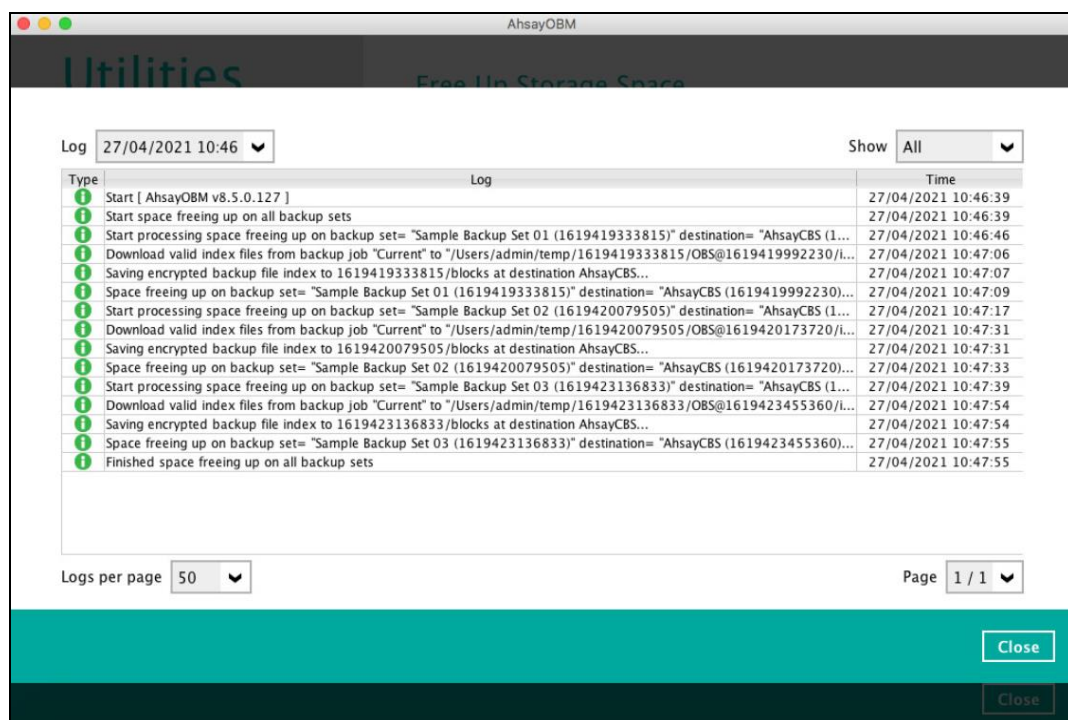
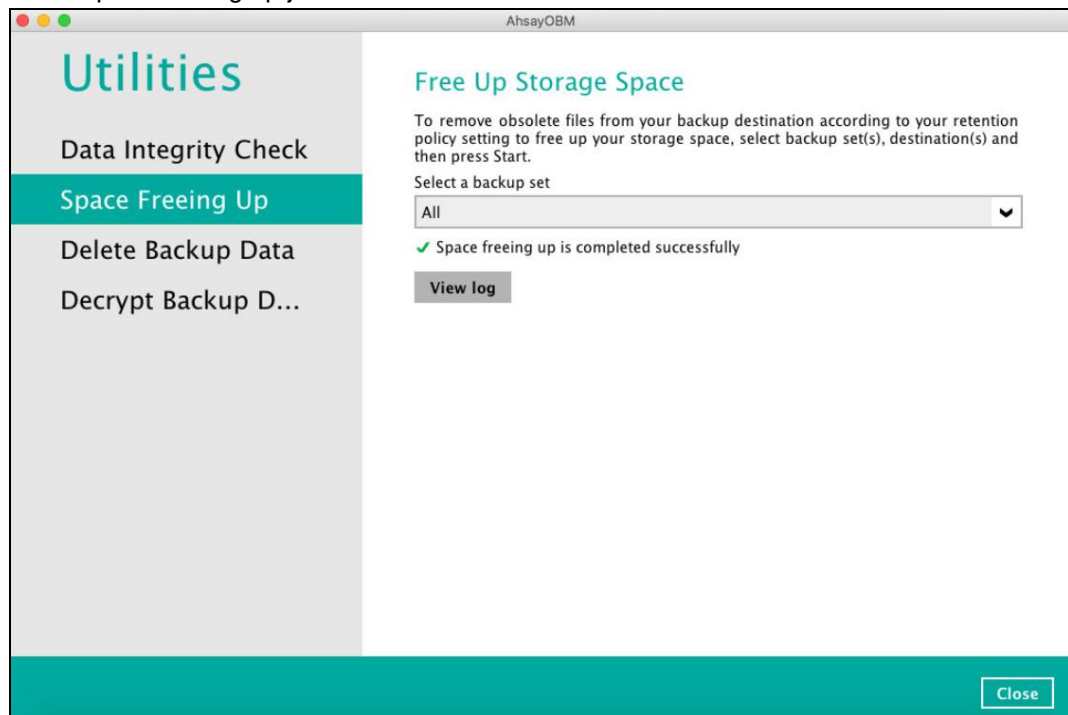
If you select All backup sets, then there is no need to select a destination.



2. Click the [Start] button to perform space free up.



- The status will be shown once completed. Click the [View log] button to see the detailed report of the space freeing up job.

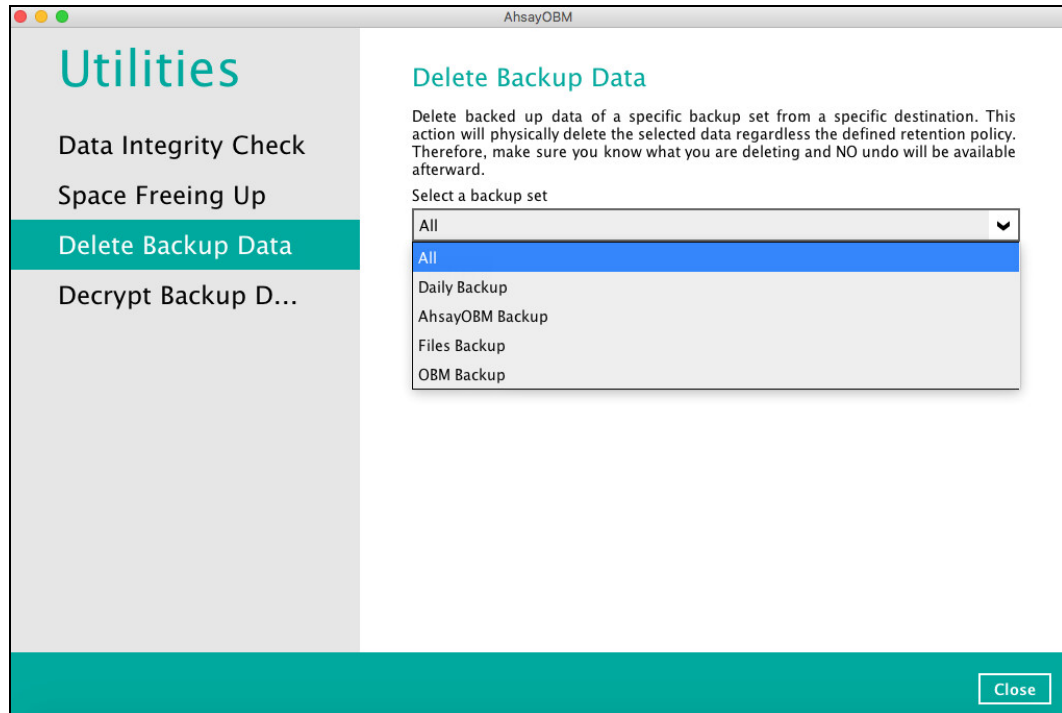


7.9.3 Delete Backup Data

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.

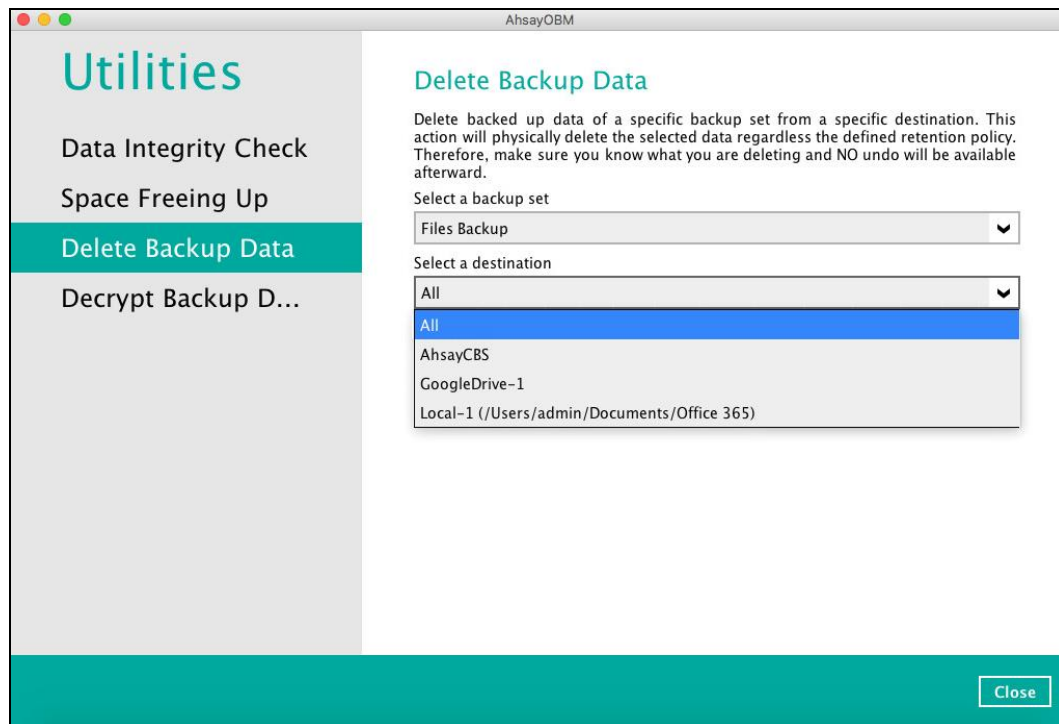
To perform deletion of backup data, follow the instructions below:

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

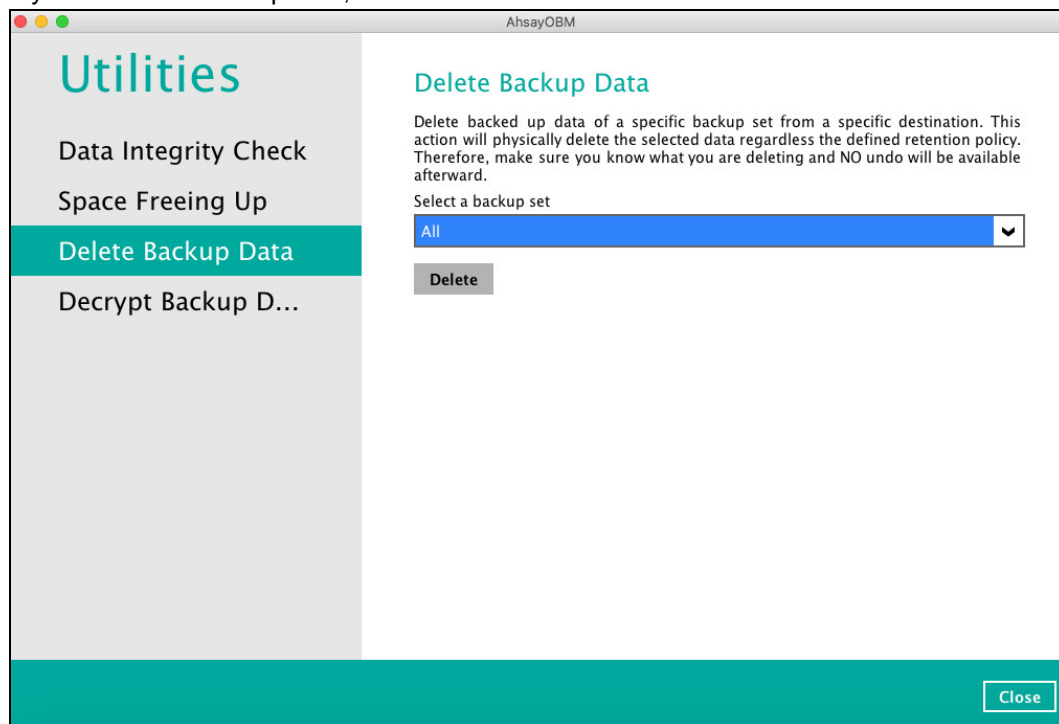


NOTE: This will only delete the backed up files in a backup set(s) and destination(s), but the backup set and destination will remain.

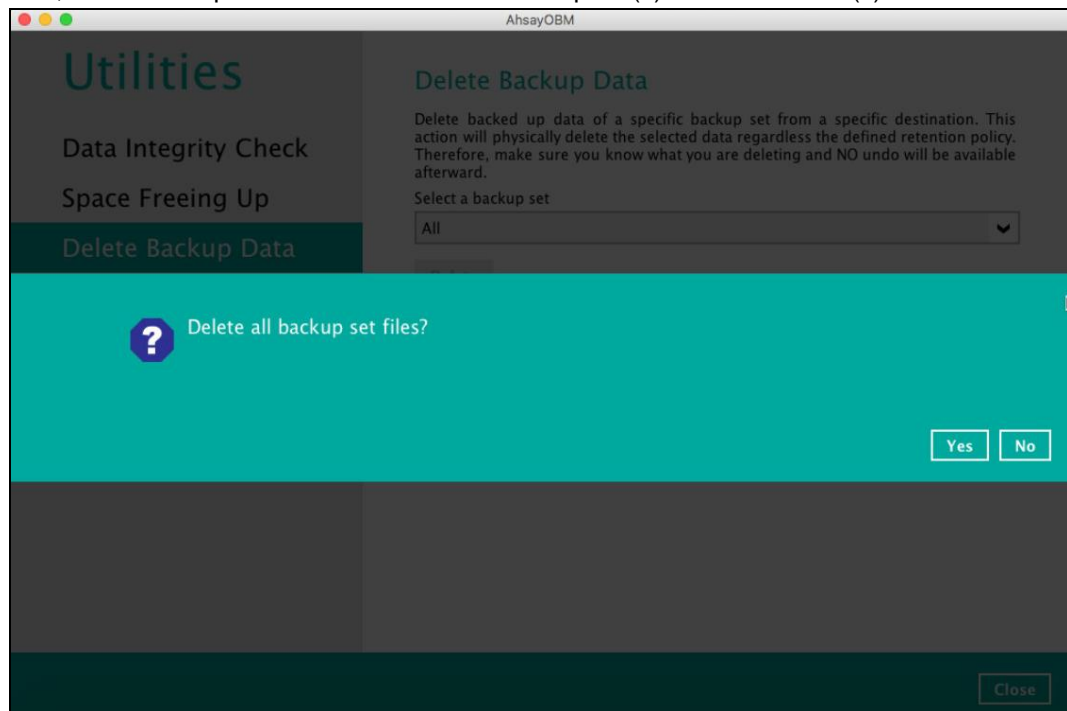
If you select a specific backup set, then you will also have to select a specific destination or all destinations.



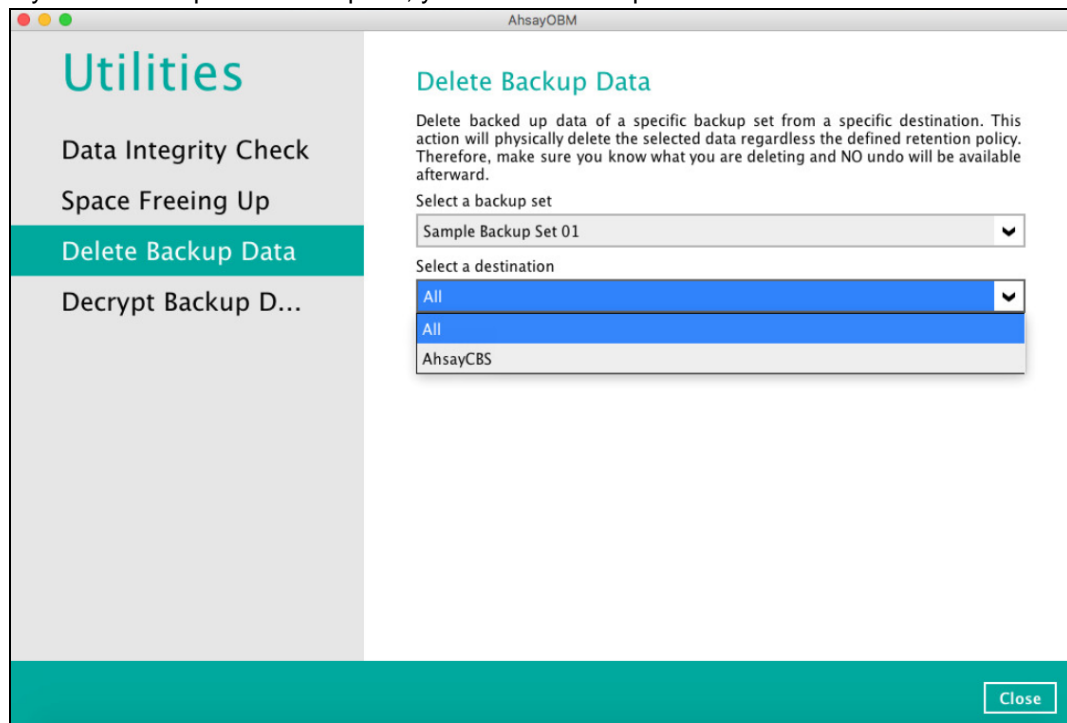
If you select **All** backup sets, then there is no need to select a destination.



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

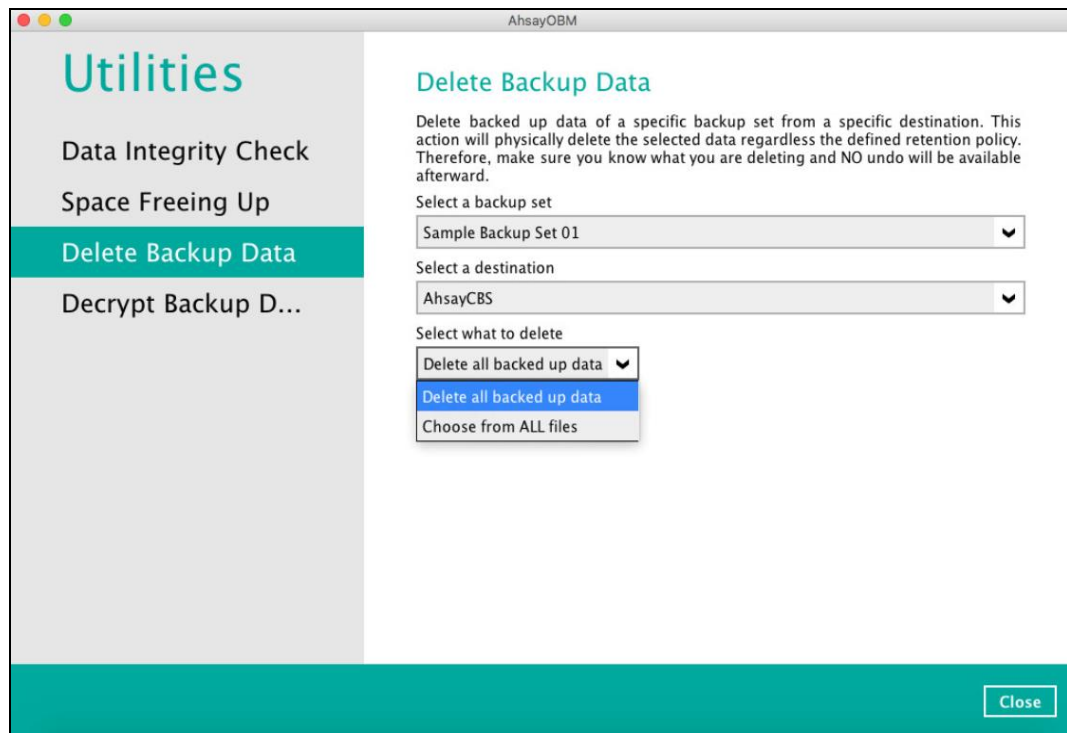


If you select a specific backup set, you will have an option to choose a destination.



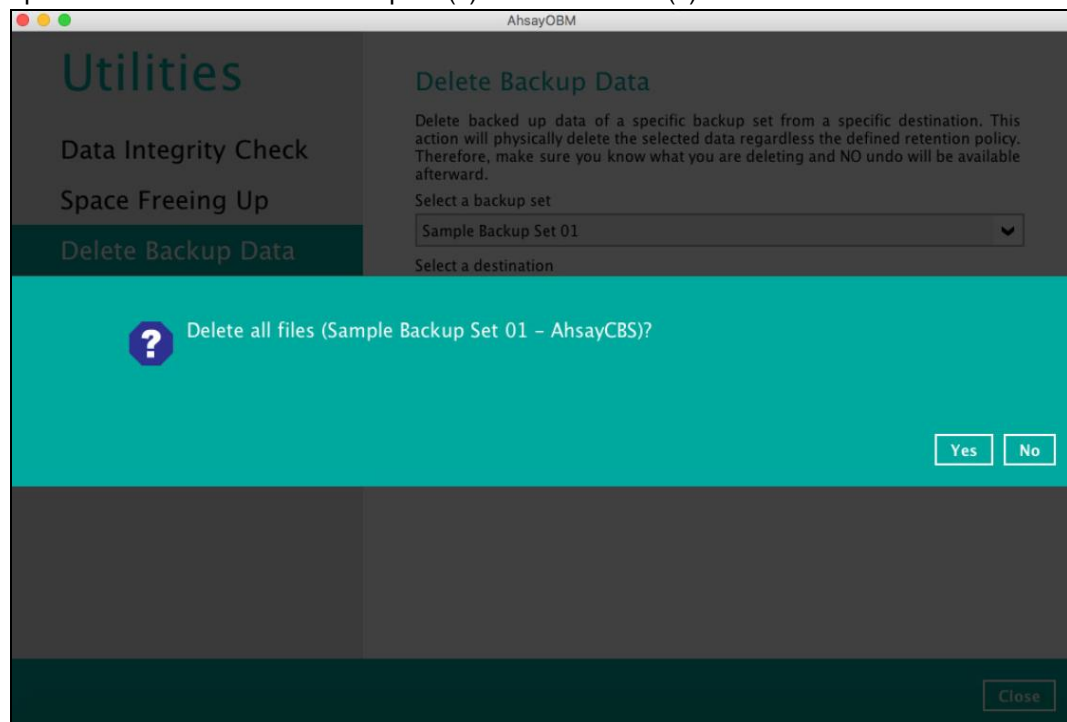
If you select a specific destination, there are two (2) available options for the type of files you wish to delete.

- Delete all backed up data
- Choose from ALL files



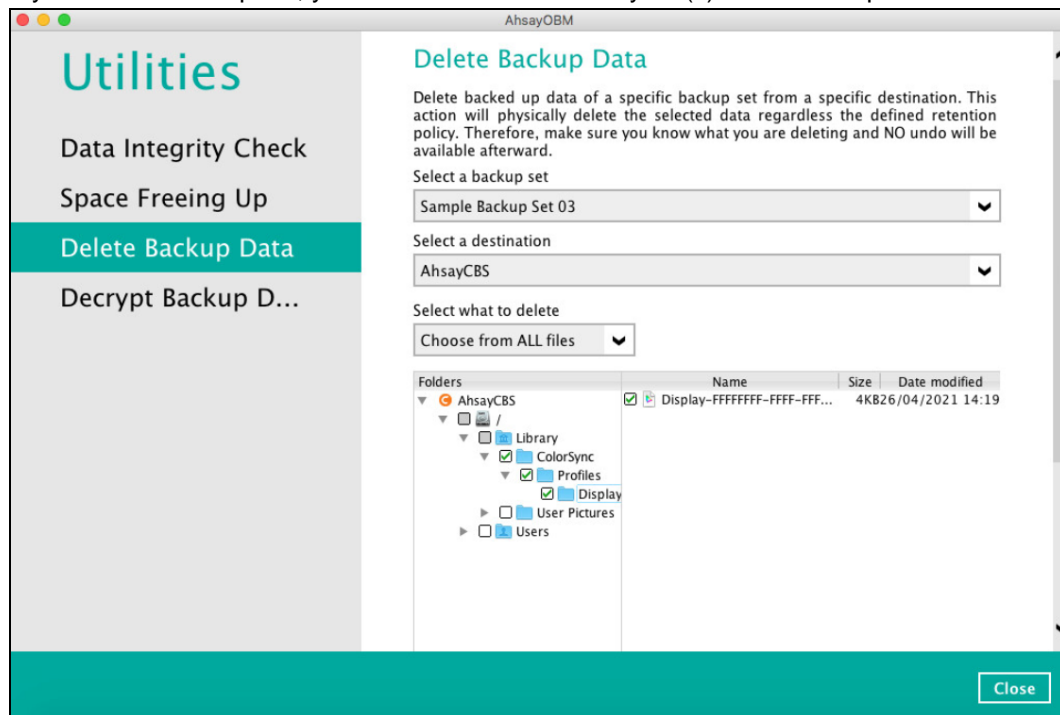
Delete all backed up data

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

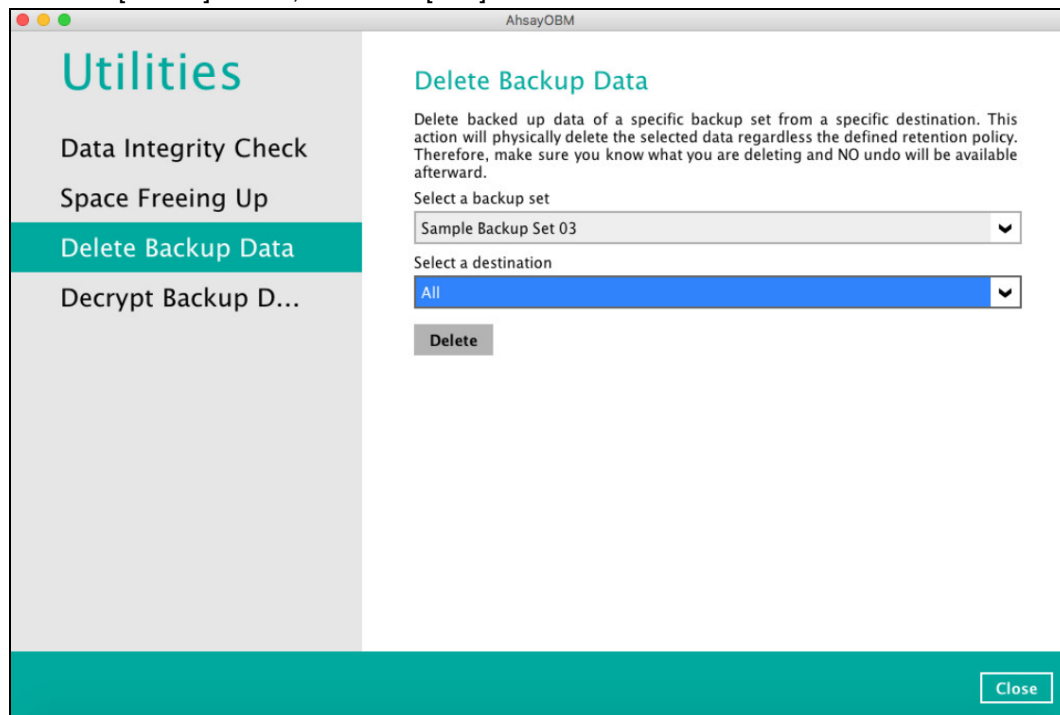


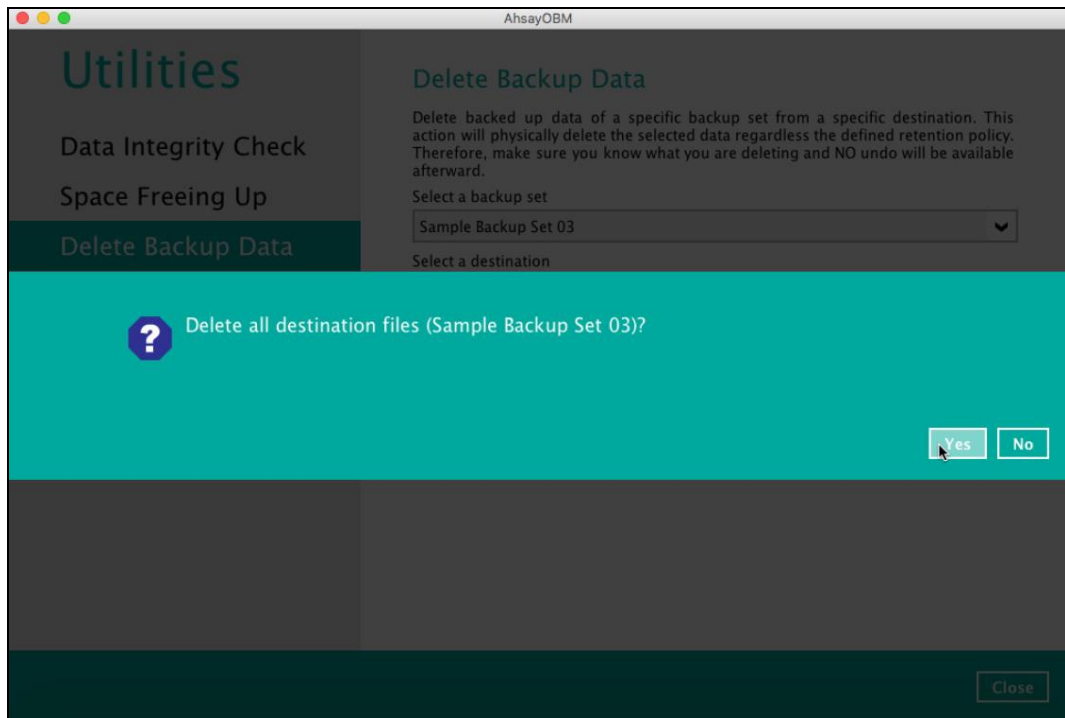
Choose from ALL files

If you choose this option, you can select to delete any file(s) in the backup set.

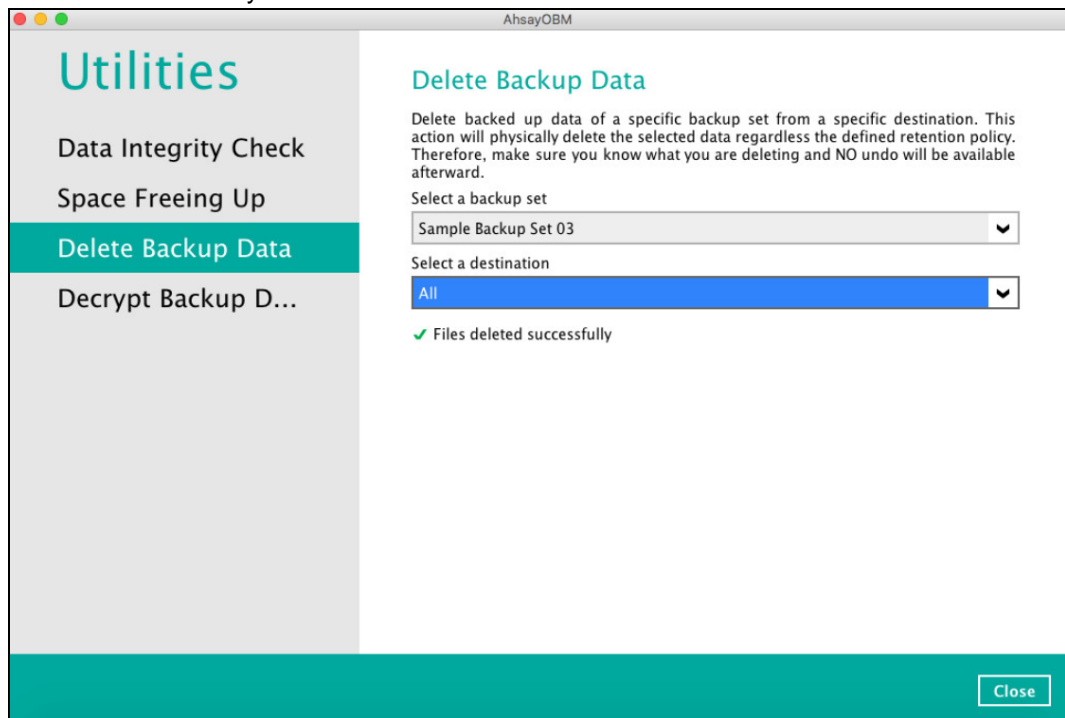


3. Click the [Delete] button, then click [Yes] to start the deletion of files.



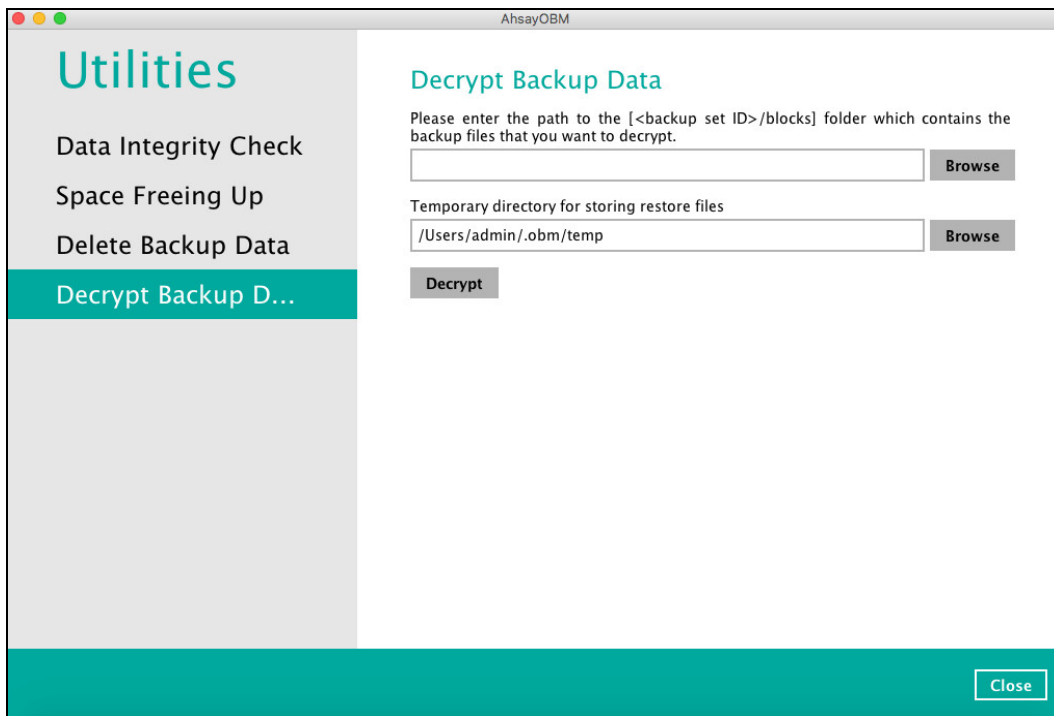


4. Files are successfully deleted.



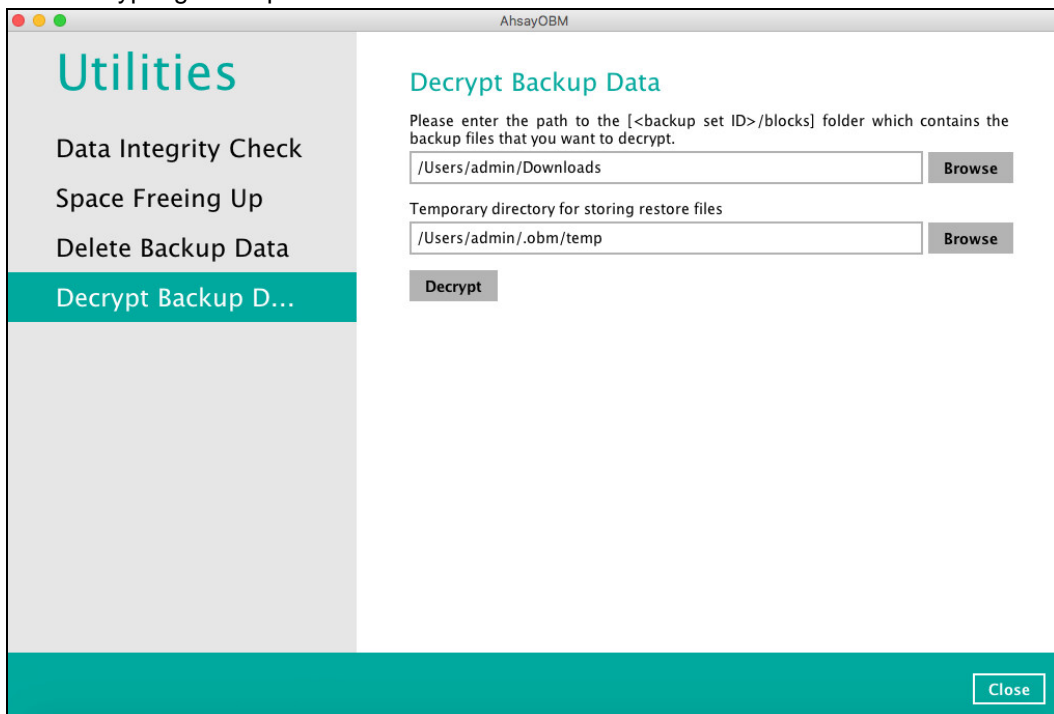
7.9.4 Decrypt Backup Data

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



The screenshot shows the AhsayOBM Utilities window. On the left is a sidebar with the title "Utilities" and four menu items: "Data Integrity Check", "Space Freeing Up", "Delete Backup Data", and "Decrypt Backup D...". The "Decrypt Backup D..." item is highlighted in teal. The main area of the window is titled "Decrypt Backup Data" and contains the following text: "Please enter the path to the [<backup set ID>/blocks] folder which contains the backup files that you want to decrypt." Below this text is a text input field and a "Browse" button. Further down, it says "Temporary directory for storing restore files" followed by another text input field containing the path "/Users/admin/.obm/temp" and a "Browse" button. At the bottom of the main area is a "Decrypt" button. A teal bar at the very bottom of the window contains a "Close" button.

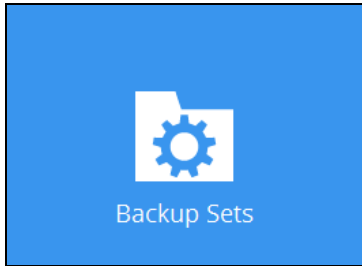
Enter the path of the folder which contains the backup files you want to decrypt. Click **decrypt** to start decrypting backup data.



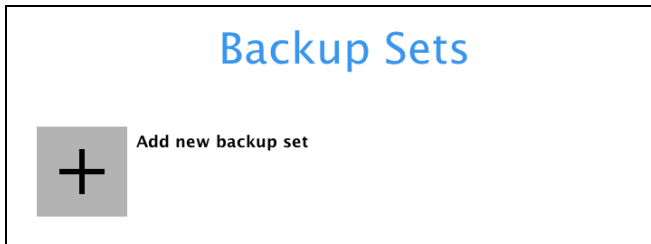
This screenshot is identical to the one above, but the text input fields are now populated. The first input field, for the backup files folder, contains the path "/Users/admin/Downloads". The second input field, for the temporary directory, still contains the path "/Users/admin/.obm/temp". All other elements, including the sidebar, buttons, and window title, remain the same.

8 Create a Backup Set

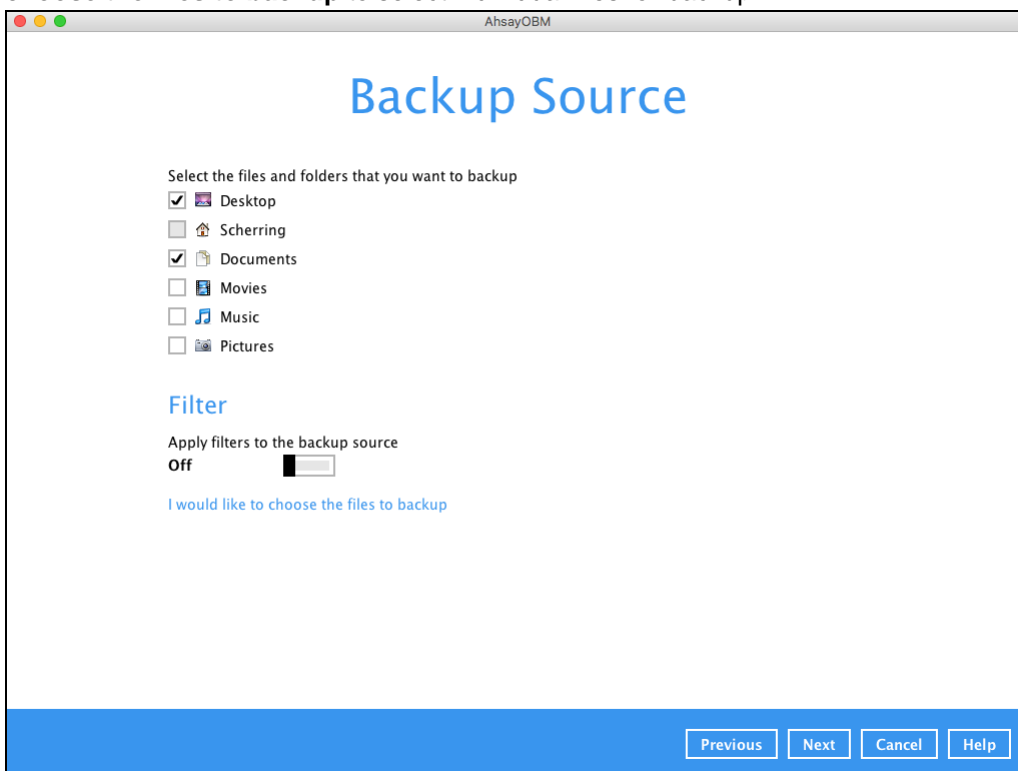
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.



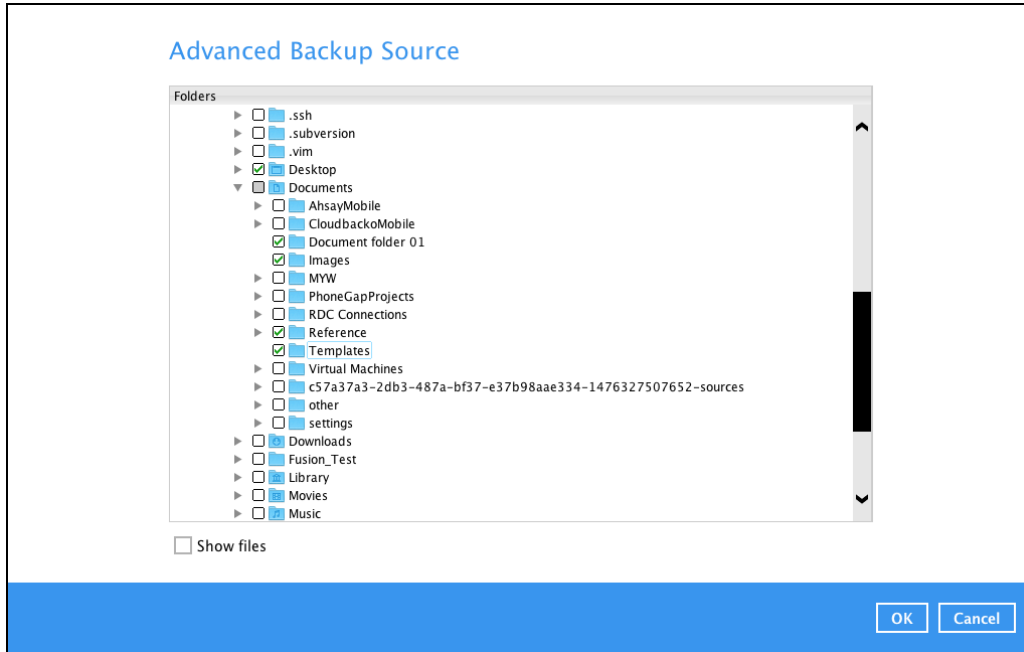
2. Create a new backup set by clicking **+** next to **Add new backup set**.



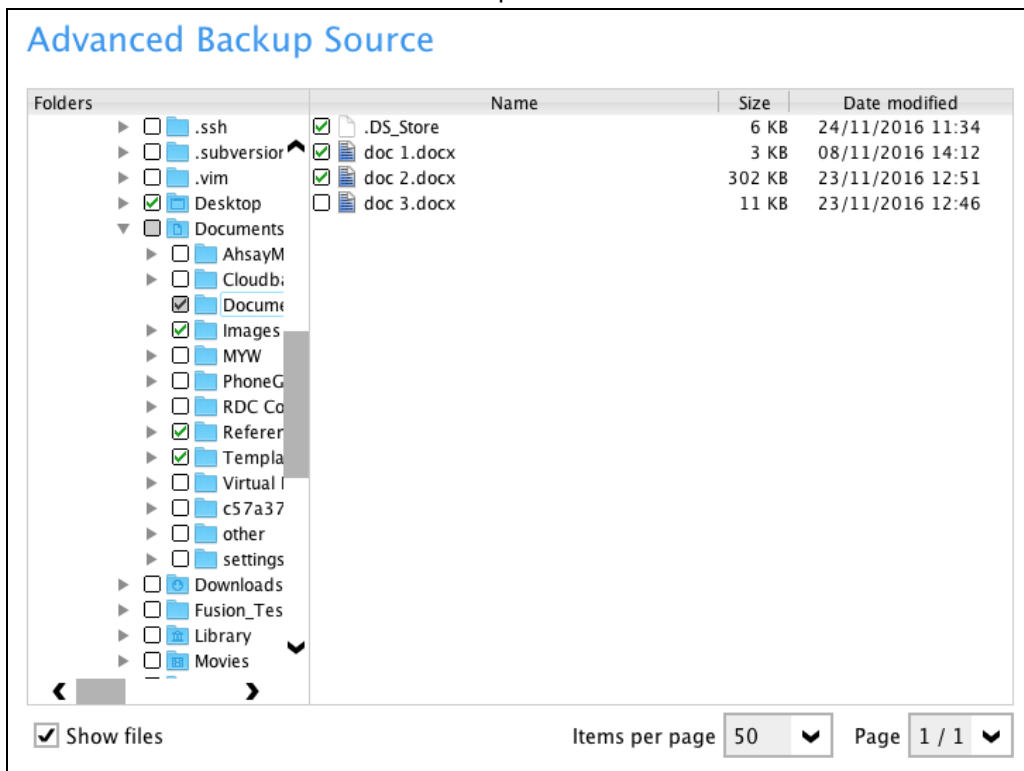
3. When the Create Backup Set window appears, name your new backup set, and select the **Backup set type**. Then, click **Next** to proceed.
4. In the Backup Source window, select the source files and folders for backup. Click **I would like to choose the files to backup** to select individual files for backup.




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

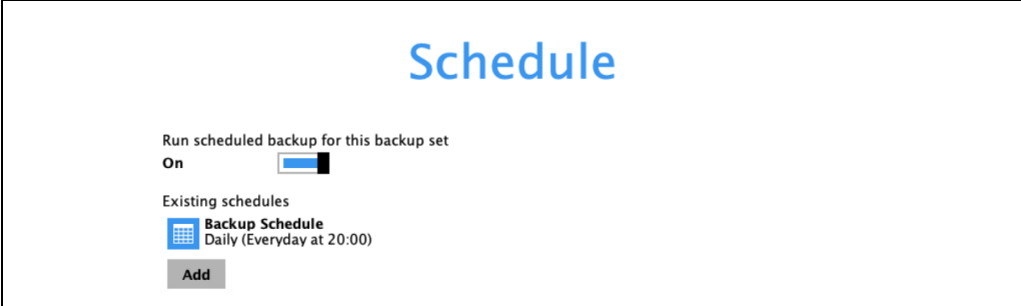


- Alternatively, if you want to back up only specific files instead of all files in your selected folder(s), select the **Show files** checkbox at the bottom of the screen. A list of files will appear on the right-hand side. Select the checkbox(es) next to the file(s) to back up. Then, click **OK** to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

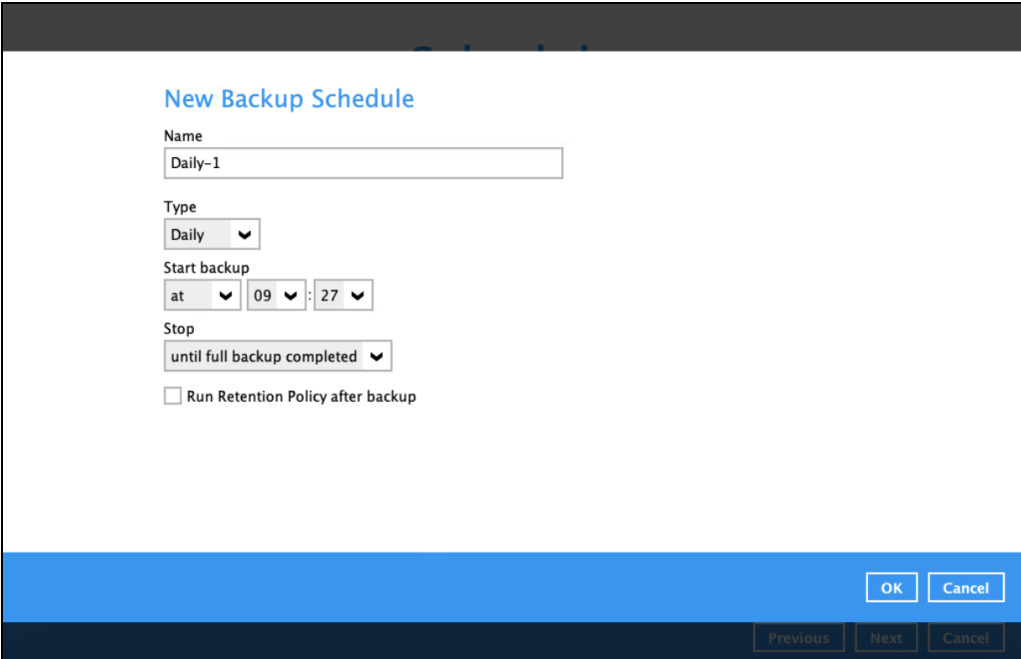


- In the Backup Source window, click **Next** to proceed.
- In the Schedule window, you can configure a backup schedule to automatically run a backup job at your specified time interval. In the Schedule window, the Run scheduled backup for this backup set is **On** by default.

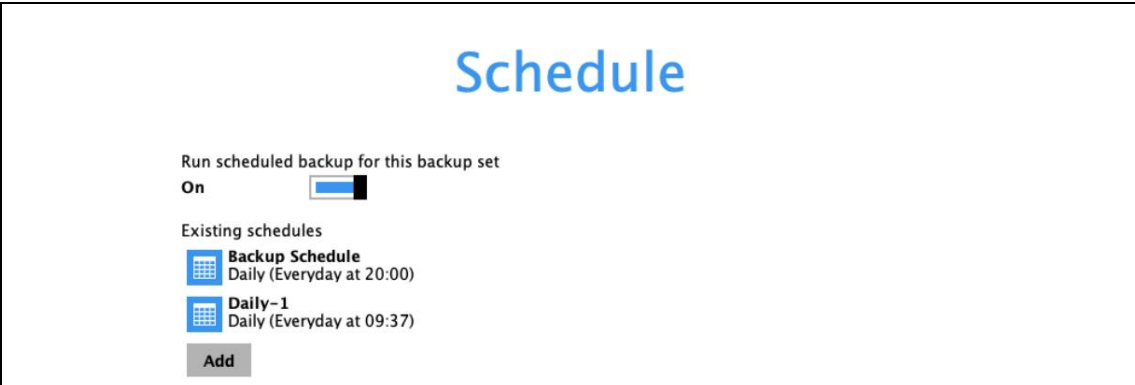
- ④ If you want to add a schedule now, click  next to **Add New schedule**.



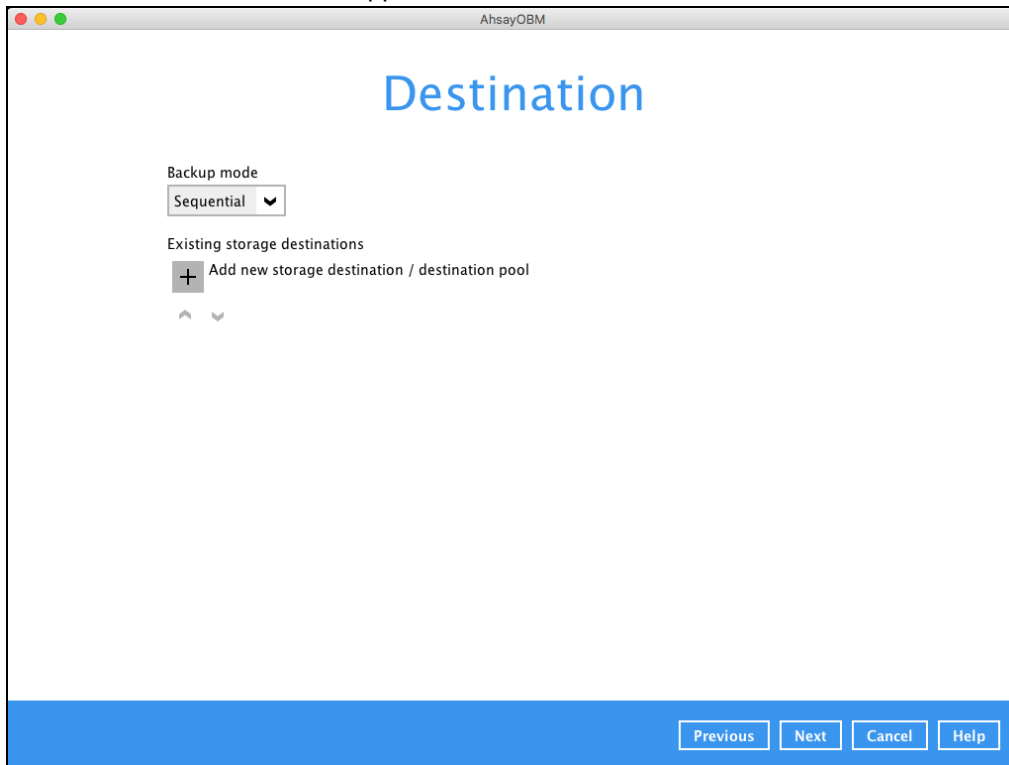
When the New Backup Schedule window appears, specify your backup schedule. Then, click **OK** to save your changes and close the New Backup Schedule window.



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




10. The **Destination** window will appear.

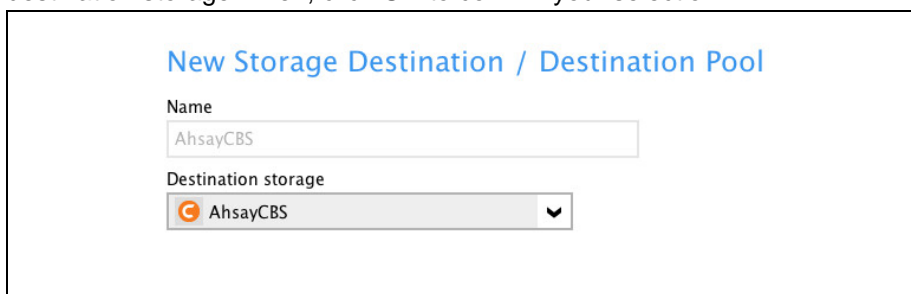


Select the appropriate option from the **Backup mode** dropdown menu.


- ☒ **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**.

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



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

The screenshot shows the 'Destination' window. At the top, the word 'Destination' is displayed in a large blue font. Below it, the 'Backup mode' is set to 'Sequential' in a dropdown menu. Under 'Existing storage destinations', there is a list item for 'CBS' with a host address of '10.3.1.8:443'. Below this list is a grey 'Add' button. At the bottom left, there are two small upward and downward arrow icons.

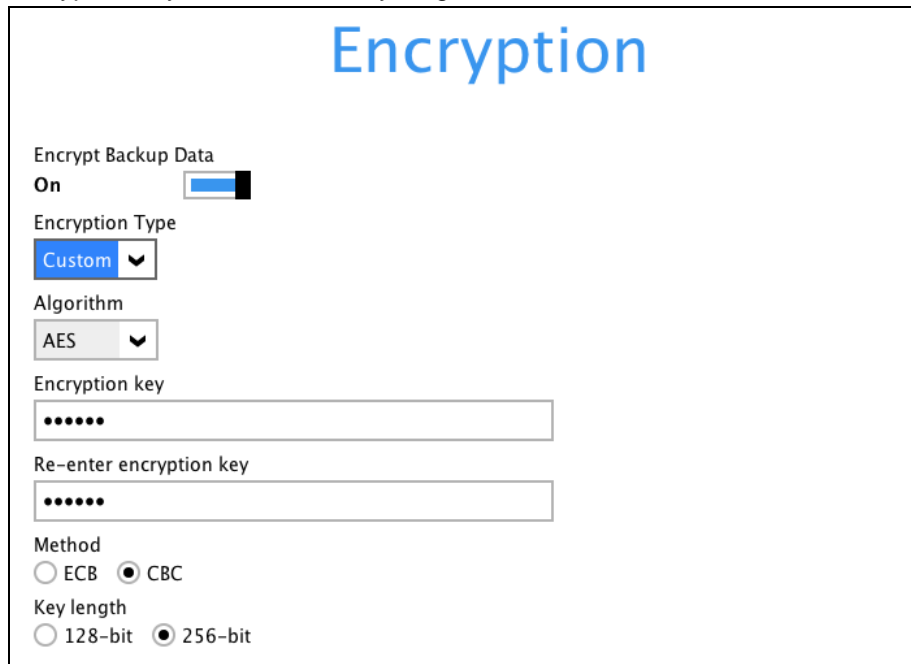
13. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.

The screenshot shows the 'Encryption' window. At the top, the word 'Encryption' is displayed in a large blue font. Below it, the 'Encrypt Backup Data' option is turned 'On', indicated by a blue slider. Under 'Encryption Type', a dropdown menu is open, showing three options: 'Default' (which is highlighted in blue), 'User password', and 'Custom'.

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

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.

- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method, and key length.



Note: For best practice on managing your encryption key, refer to the following Wiki article.

https://wiki.ahsay.com/doku.php?id=public:5034_best_practices_for_managing_encryption_key

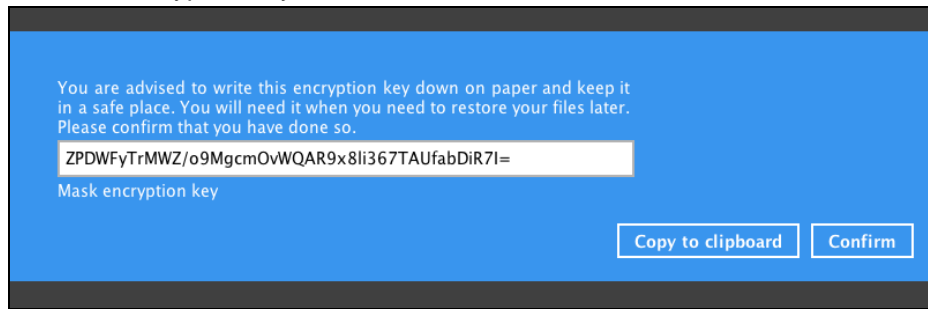
Click **Next** when you are done setting.

14. 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.



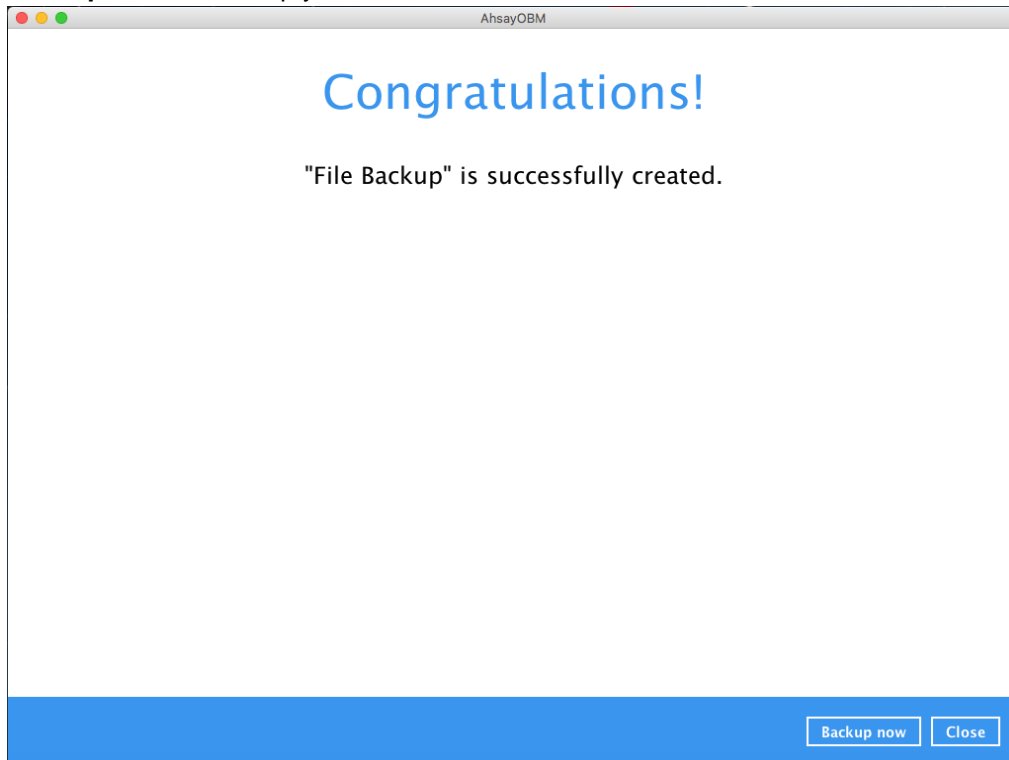
The pop-up window has the following three options to choose from:

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



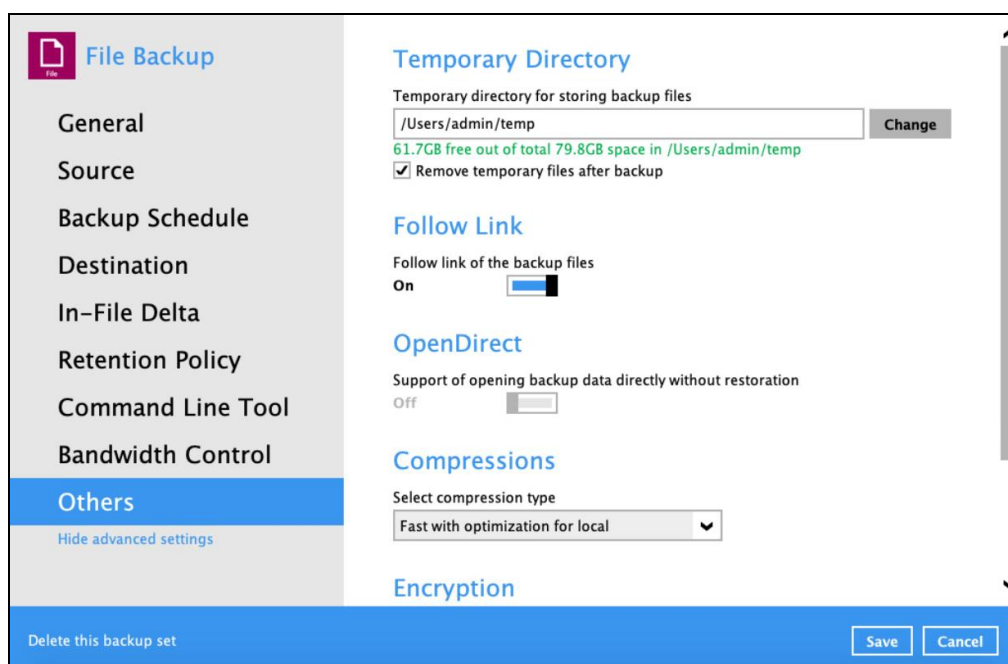
- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

15. 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.



16. It is highly recommended to change the Temporary Directory. Select another location with sufficient free disk space other than /Users/admin//temp.

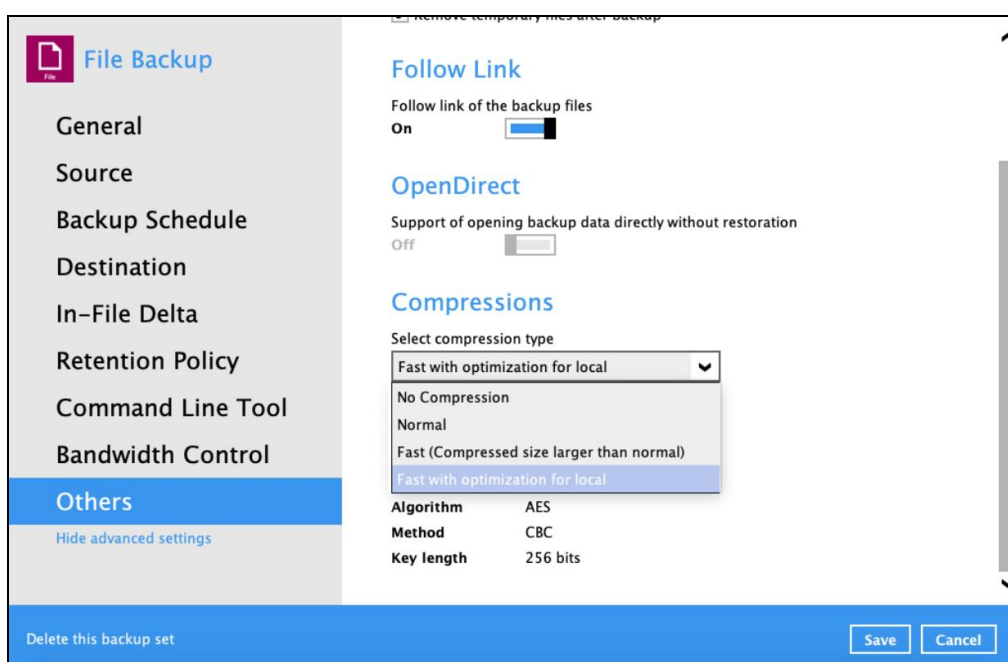
Go to **Others > Temporary Directory**. Click **Change** to browse for another location.



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

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

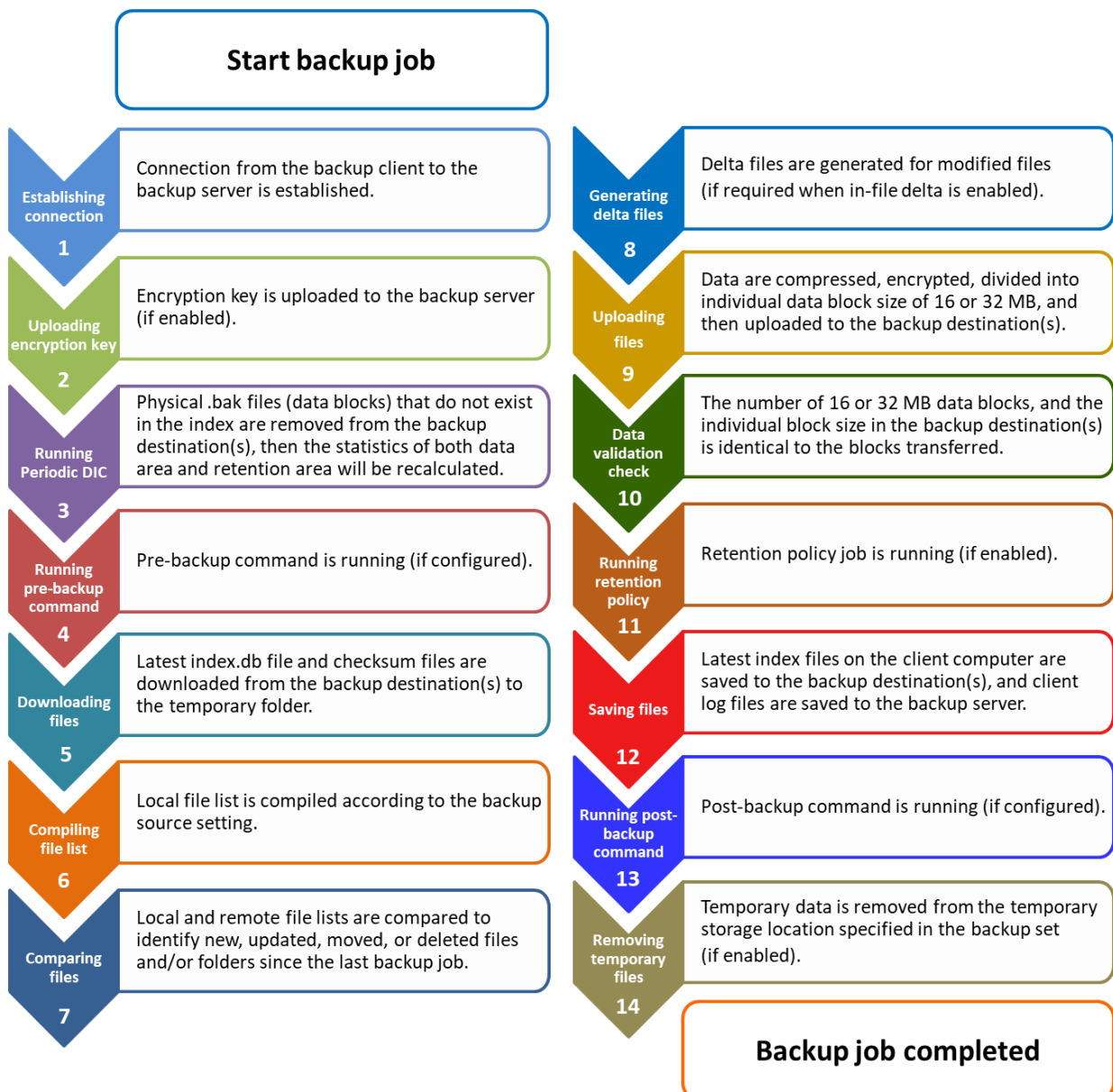
- No Compression
- Normal
- Fast (Compressed size larger than normal)
- Fast with optimization for local



9 Overview on Backup Process

The following steps are performed during a backup job. For an overview of the detailed process for Steps 3, 5, 10, and 12, please refer to the following chapters.

- [Periodic Data Integrity Check \(PDIC\) Process \(Step 3\)](#)
- Backup Set Index Handling Process
 - [Start Backup Job \(Step 5\)](#)
 - [Completed Backup Job \(Step 12\)](#)
- [Data Validation Check Process \(Step 10\)](#)



9.1 Periodic Data Integrity Check Process

For AhsayOBM v8.3.6.0 (or above), the PDIC will run on the first backup job that falls on the corresponding day of the week from **Monday to Friday**.

To minimize the impact of the potential load of large number of PDIC jobs running at the same time on the AhsayCBS server, 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:

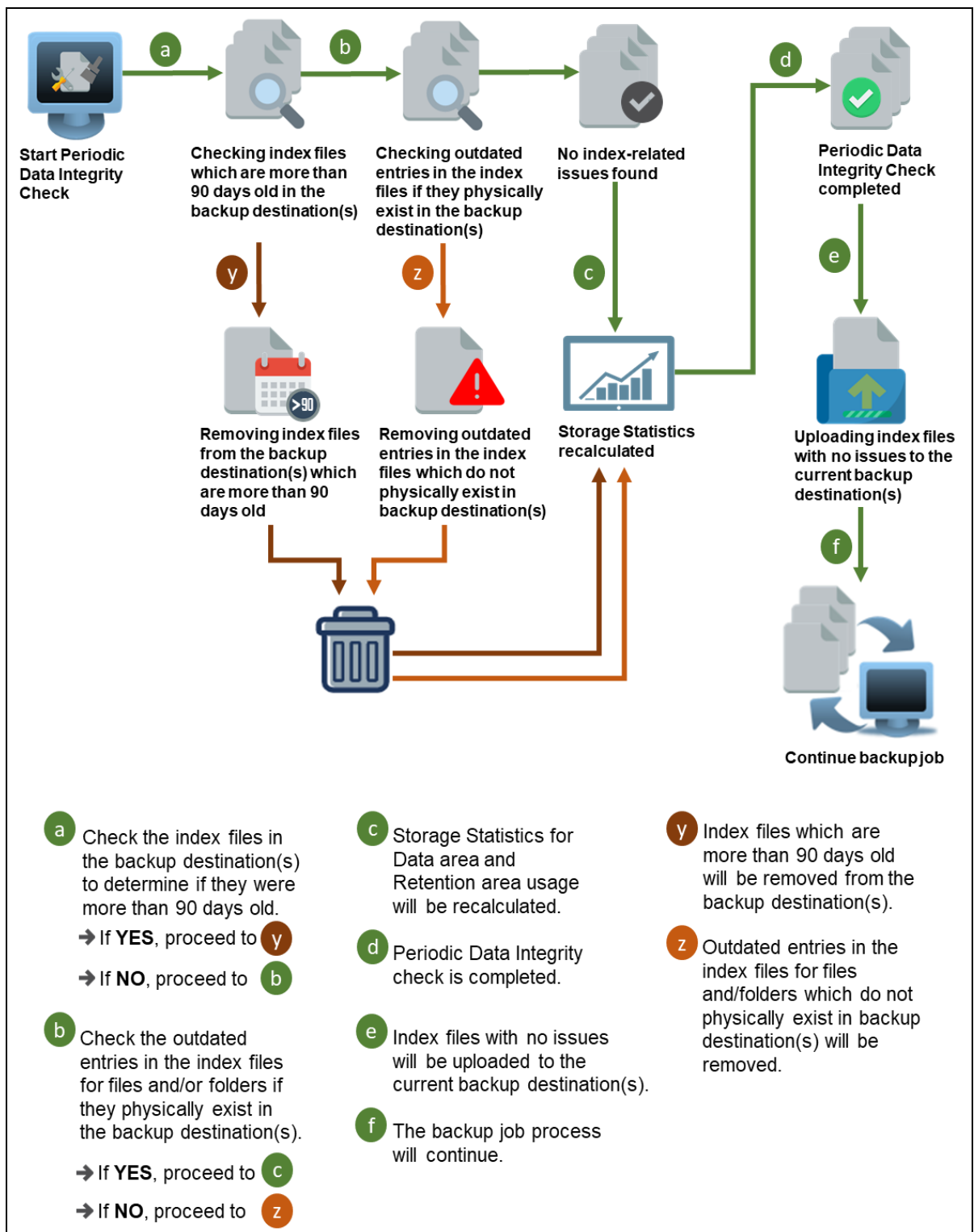
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTES

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:

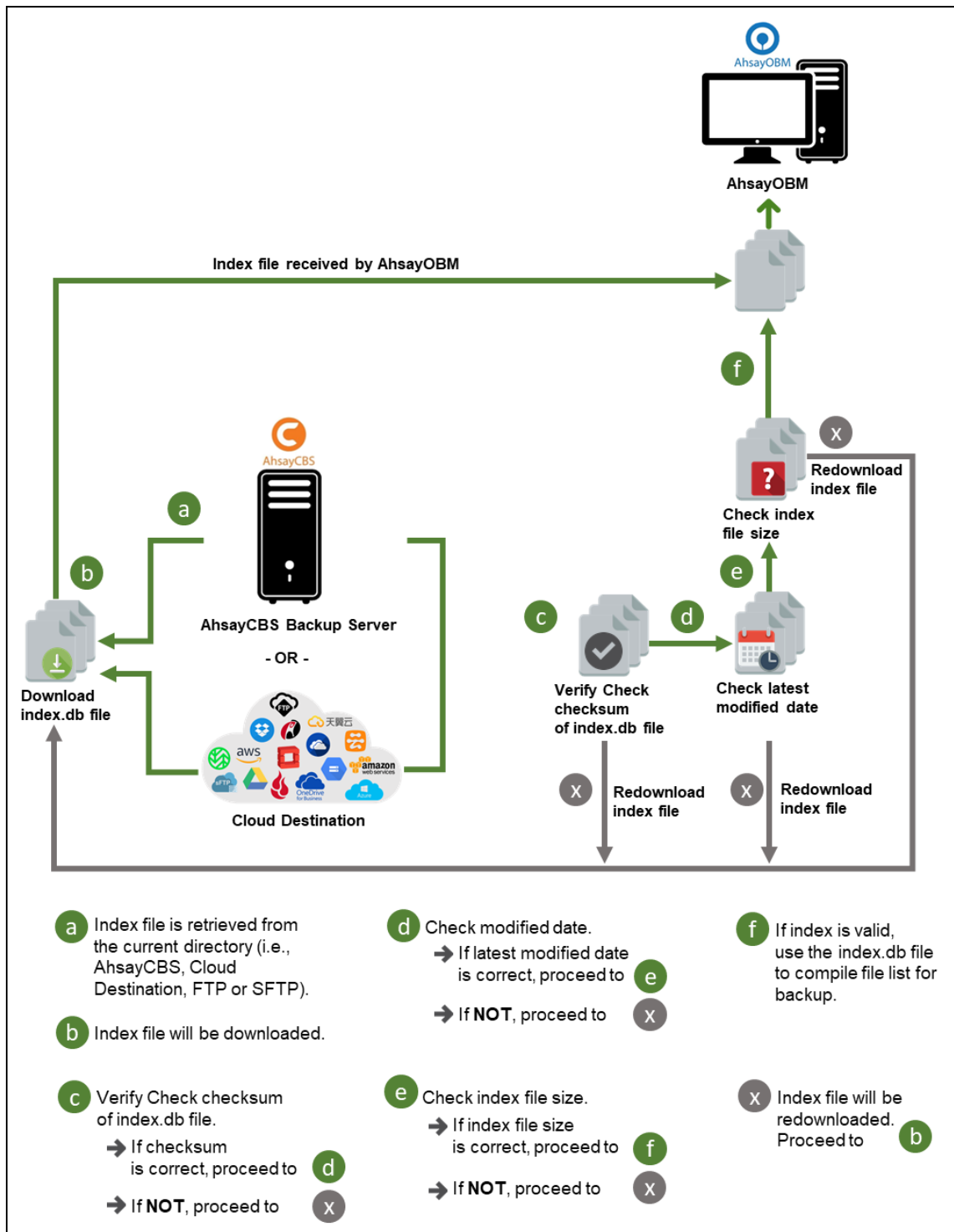
1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it detects that the previous PDIC job was run more than 7 days ago.
3. 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.
4. 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.
5. The PDIC job will not run on a backup set that contains any data which still in v6 format. It will only run if all v6 data format on a backup set has undergone data migration to v8 block format.



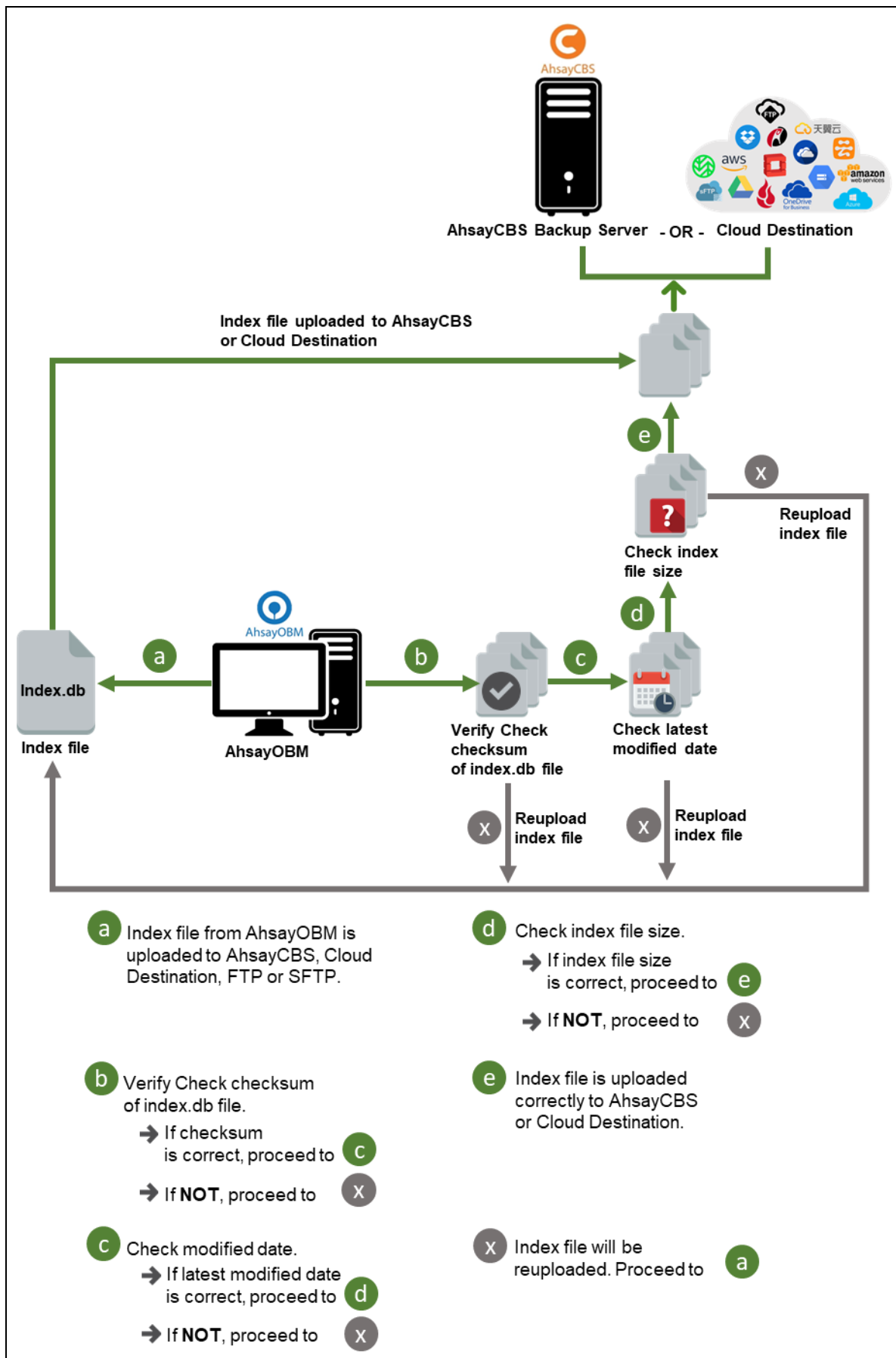
9.2 Backup Set Index Handling Process

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

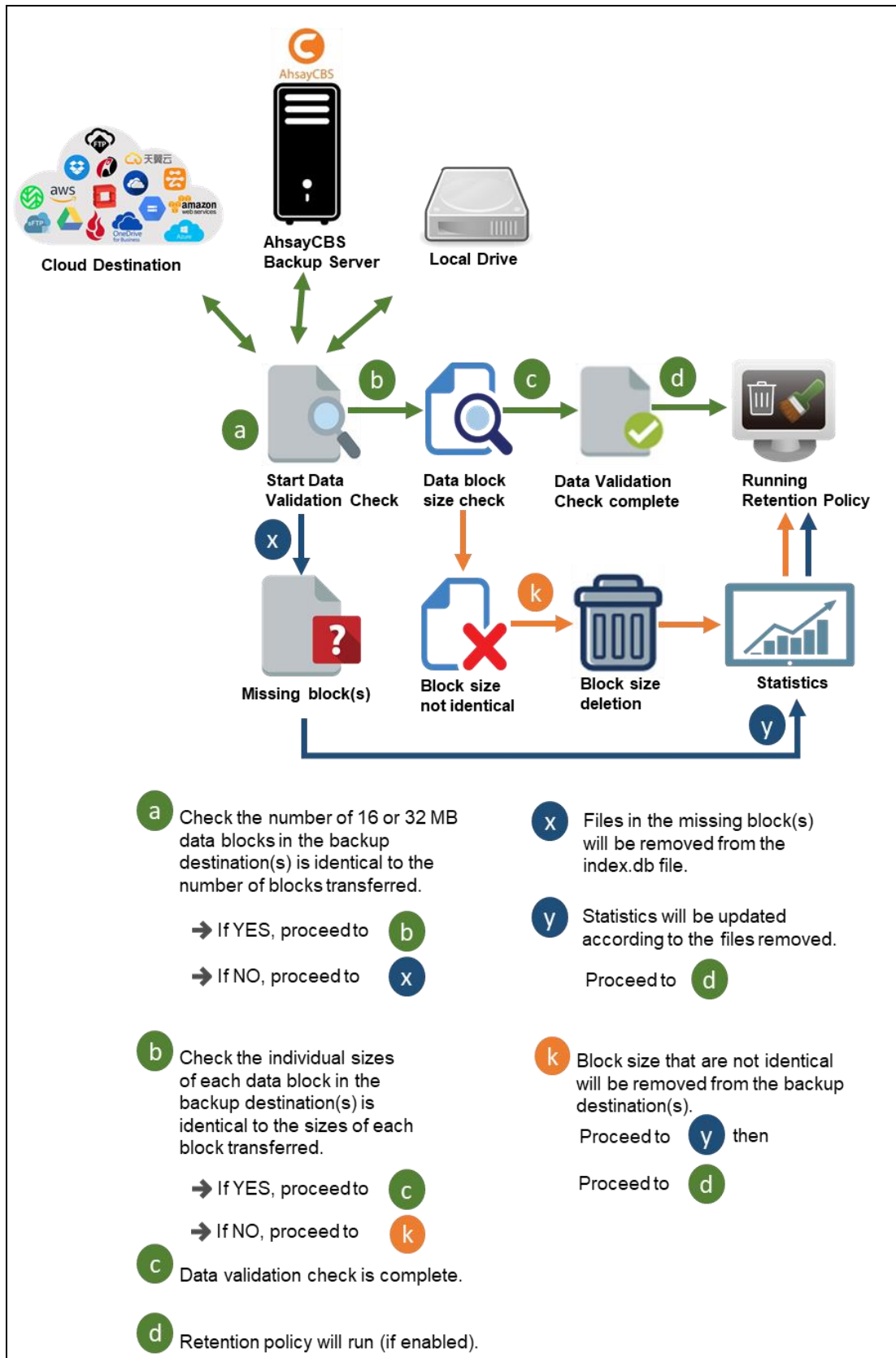


9.2.2 Completed Backup Job



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 Run Backup Jobs

10.1 Login to AhsayOBM

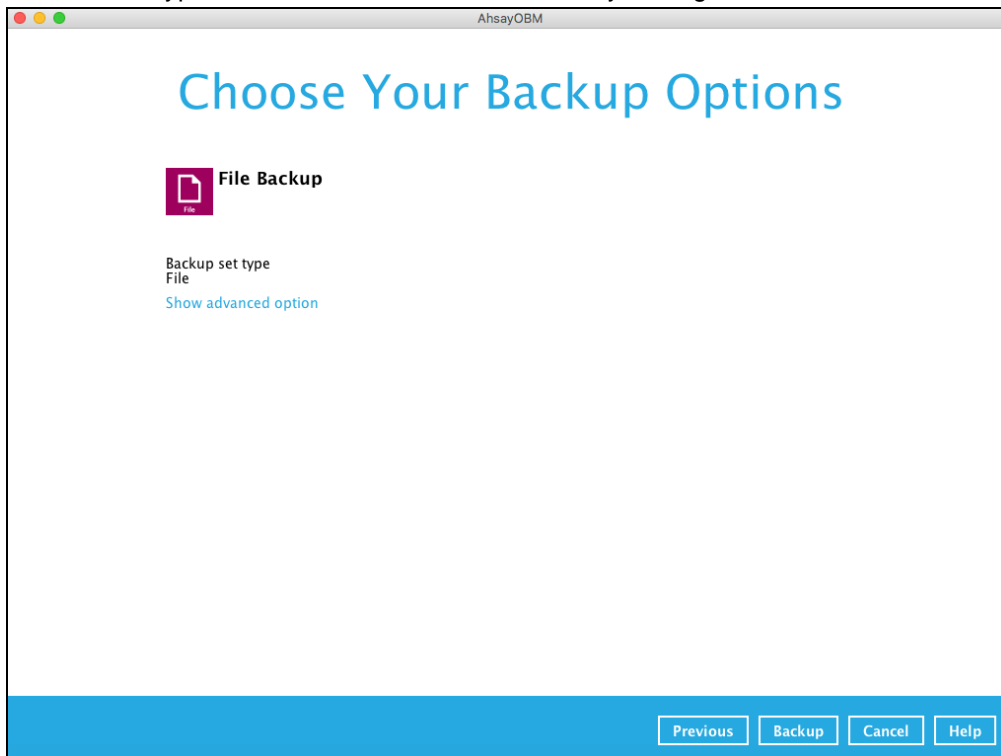
Login to the AhsayOBM application according to the instructions in [Chapter 6 Login to AhsayOBM](#).

10.2 Start a Manual Backup


1. Click **Backup** on the main interface of AhsayOBM.



2. Select the backup set that you would like to start a backup job for. In case you want to modify the In-File Delta type, Destinations and Retention Policy settings, click **Show advanced option**.






- When advanced options are shown, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** in the Retention Policy section at the bottom. This will help you save hard disk quota in the long run. In the In-File Delta type section, the following three options are available:

Backup set type
File
In-File Delta type
☒ Full
☐ Differential
☐ Incremental
Destinations
☒  CBS (Host: 10.3.1.8:443)
Retention Policy
☒ Run Retention Policy after backup
[Hide advanced option](#)

- Full** – A full backup captures all the data that you want to protect. When you run a backup job for the first time, AhsayOBM will run a full backup regardless of the in-file delta setting.
- Differential** – A differential backup captures only the changes made as compared with the last uploaded full file only (i.e. changes since the last full backup, not since the last differential backup).
- Incremental** – An incremental backup captures only the changes made as compared with the last uploaded full or delta file (i.e. changes since the last incremental backup).

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

 CBS (Host: 10.3.1.8:443)

Downloading server file list... Completed


Estimated time left 0 sec



Backed up 0 (0 file, 0 directory, 0 link)

Elapsed time 2 sec

Transfer rate 0bit/s

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

 CBS (Host: 10.3.1.8:443)


Total Moved Files = 0

Estimated time left 0 sec

Backed up 2.94M (99 files, 33 directories, 0 link)

Elapsed time 16 sec

Transfer rate 686.95kbit/s

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.

Show All

Type	Log	Time
	Start [Mac OS X 10.11.1 (Scherrings-Mac-mini), AhsayACB v7.9.0.0]	24/11/2016 15:12:17
	Saving encrypted backup set encryption keys to server...	24/11/2016 15:12:23
	Start Backup ... [In-File Delta: Full]	24/11/2016 15:12:23
	Using Temporary Directory /Users/Scherring/temp/1479952176042/OBS@1479970446499	24/11/2016 15:12:23
	Downloading server file list...	24/11/2016 15:12:23
	Downloading server file list... Completed	24/11/2016 15:12:27
	Reading backup source from hard disk...	24/11/2016 15:12:30
	Reading backup source from hard disk... Completed	24/11/2016 15:12:30
	[New Directory]... /	24/11/2016 15:12:30
	[New Directory]... /Users	24/11/2016 15:12:30
	[New Directory]... /Users/Scherring	24/11/2016 15:12:30
	[New Directory]... /Users/Scherring/Desktop	24/11/2016 15:12:30
	[New Directory]... /Users/Scherring/Documents	24/11/2016 15:12:30
	[New Directory]... /Users/Scherring/Documents/Document folder 01	24/11/2016 15:12:31
	[New Directory]... /Users/Scherring/Documents/Templates	24/11/2016 15:12:31
	[New Directory]... /Users/Scherring/Documents/Reference	24/11/2016 15:12:31
	[New Directory]... /Users/Scherring/Documents/Images	24/11/2016 15:12:31
	[New Directory]... /Users/Scherring/Desktop/=====	24/11/2016 15:12:31
	[New Directory]... /Users/Scherring/Desktop/=====Scherring	24/11/2016 15:12:31
	[New Directory]... /Users/Scherring/Desktop/=====Scherring/Desktop	24/11/2016 15:12:31
	[New Directory]... /Users/Scherring/Desktop/=====Scherring/Desktop/Sample_Test_Data	24/11/2016 15:12:31
	[New Directory]... /Users/Scherring/Desktop/=====Scherring/Desktop/Sample_Test_Data/Internationalization	24/11/2016 15:12:31
	[New Directory]... /Users/Scherring/Desktop/=====Scherring/Desktop/Sample_Test_Data/Internationalization/Intè...	24/11/2016 15:12:31
	[New Directory]... /Users/Scherrina/Desktop/CBK Mobile App Certs	24/11/2016 15:12:31

Logs per page 50

Page 1 / 4

Close

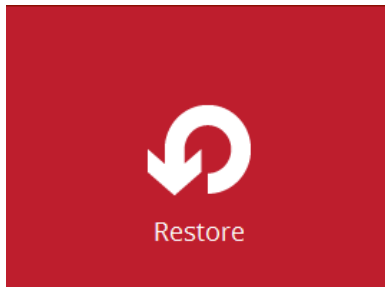
11 Restore Data

11.1 Login to AhsayOBM

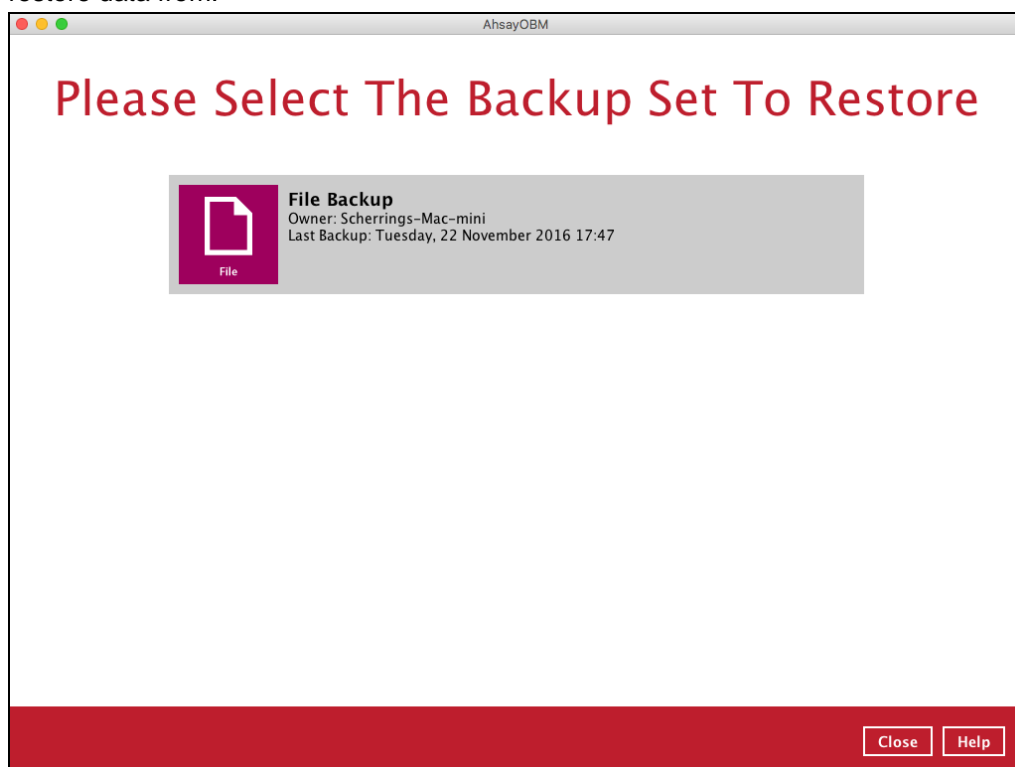
Login to the AhsayOBM application according to the instructions in [Login to AhsayOBM](#).

11.2 Restore Data

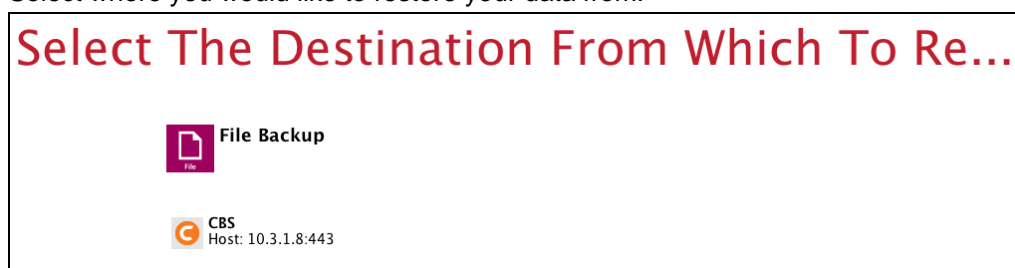
1. Click the **Restore** icon on the main interface of AhsayOBM.



2. All the available backup sets for restore will be listed. Select the backup set that you would like to restore data from.



3. Select where you would like to restore your data from.



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.

Select what to restore

Choose from files as of job ▼ 24/11/2016 ▼ Latest ▼

Choose from files as of job

Choose from ALL files

Name

Select what to restore

Choose from files as of job ▼ 24/11/2016 ▼ Latest ▼

Show filter

24/11/2016

23/11/2016

22/11/2016

Folders

▼ CBS

▼ /

Select what to restore

Choose from files as of job ▼ 24/11/2016 ▼ Latest ▼

Show filter

Latest

10:52

10:49

09:43

Folders

▼ CBS

▼ /

► Users

Name

- ⦿ **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.

Select Your Files To Be Restored

Select what to restore

Choose from ALL files ▼

Show filter

Folders	Name	Size	Date modified
▼ CBS	<input type="checkbox"/> File 1.rtf	449 b...	25/11/2016 09:47
▼ /	<input type="checkbox"/> File 1.rtf	439 b...	25/11/2016 09:45
▼ Users	<input type="checkbox"/> File 1.rtf	430 b...	25/11/2016 09:42
▼ Scherring	<input type="checkbox"/> File 1.rtf	426 b...	25/11/2016 09:34
► Desktop			
► Documents			
► Files 01			
► MYW			

The following is an example showing all the available backup versions of the file **1.rtf**. The latest version is shown in solid black color and all the previous versions are shown in grey color. You can identify the file version from the **Date modified**

column.

	Name	Size	Date modified
<input type="checkbox"/>	File 1.rtf	449 b...	25/11/2016 09:47
<input type="checkbox"/>	File 1.rtf	439 b...	25/11/2016 09:45
<input type="checkbox"/>	File 1.rtf	430 b...	25/11/2016 09:42
<input type="checkbox"/>	File 1.rtf	426 b...	25/11/2016 09:34

When the restore is done, you will see all the selected backup versions in the restore destination. The latest backup version has the file name as the original file, while the previous versions have the time stamps added to their file names for easy identification.

<< Common ▶ KMT ▶ Steven ▶ Others ▶ File Snapshot			
	Name		Date modified
<input type="checkbox"/>	File snapshot testing		11/7/2016 6:54 PM
<input type="checkbox"/>	File snapshot testing_2016-11-07-18-39-11		11/7/2016 6:39 PM
<input type="checkbox"/>	File snapshot testing_2016-11-07-18-51-55		11/7/2016 6:51 PM
<input type="checkbox"/>	File snapshot testing_2016-11-07-18-53-26		11/7/2016 6:52 PM

- Click the **Show files** checkbox to select individual files for restoration. Click **Next** to proceed when you are done with the selections.
- Select to restore the files to their **Original location**, or to an **Alternate location**. Then, click **Next** to proceed.
 - Original location** – the backed-up data will be restored to the computer running the AhsayOBM under the same directory path as on the machine storing the backup source. For example, if the backup source files are stored under **Users/[User's Name]/Downloads** folder, the data will be restored to **Users/[User's Name]/Downloads** as well on the computer running the AhsayOBM.

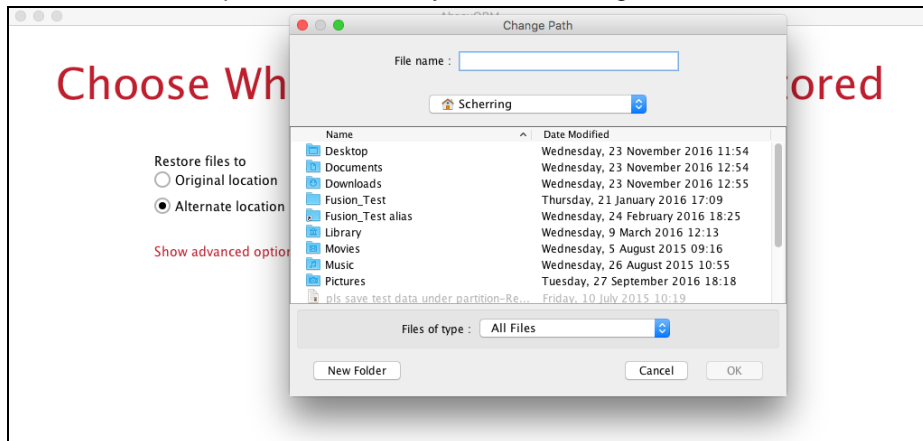
Choose Where The Files To Be Restored

Restore files to

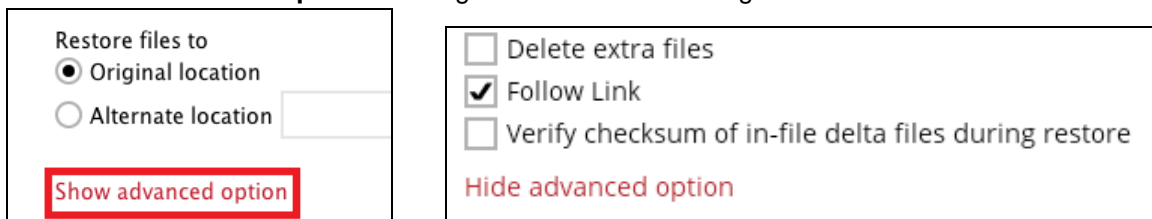
☒ Original location
 ☐ Alternate location

[Show advanced option](#)

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



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

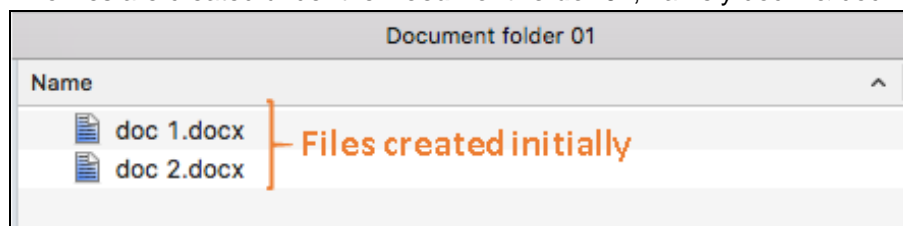


- ⦿ **Delete extra files**

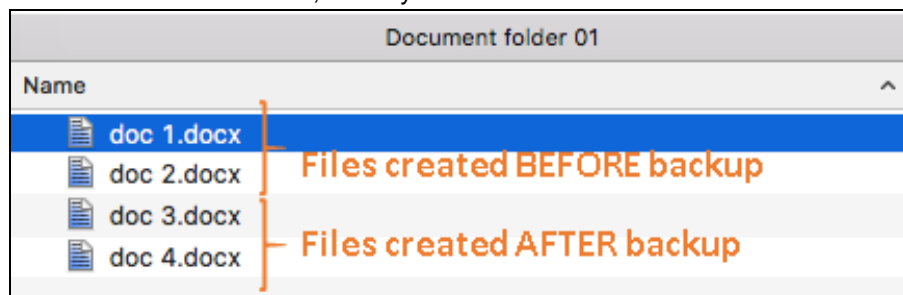
By enabling this option, the restore process will attempt to synchronize the selected restore source with the restore destination, making sure the data in the restore destination is exactly the same as the restore source. Any data created after backup will be treated as “extra files” and will be deleted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

Example:

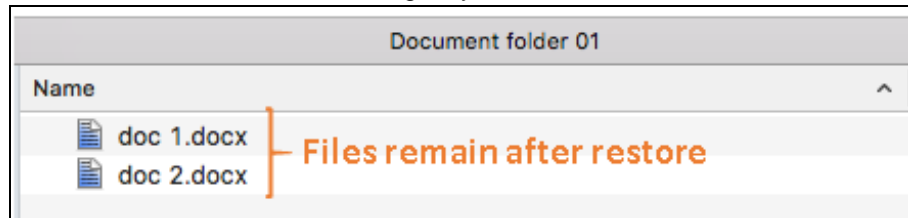
- Two files are created under the **Document folder 01**, namely doc 1 & doc 2.



- A backup is performed for folder **Document folder 01**.
- Two new files are created, namely doc 3 & doc 4.



- iv) A restore is performed for the **Document folder 01**, with **Delete extra files** option enabled.
- v) Since doc 3 & doc 4 have never been backed up, therefore they will be deleted from **Document folder 01**, leaving only the two files that have been backed up.



WARNING

Please exercise extra caution when enabling this feature. Consider what data in the restore source has not been backed up and what impact it would cause if those data is deleted.

Prior to the data restore and synchronization, a warning message shows as the one shown below. Only clicking **Yes** will the “extra file” be deleted. You can click **Apply to all** to confirm deleting all the “extra files” at a time.

Follow Link (Enabled by default)

When this option is enabled, not only the symbolic link or junction point will be restored, the directories and files that the symbolic link or junction point links to will also be restored.

The table below summarizes the behaviors when a restore is performed with different settings.

Follow Link	Restore to	Behavior
Enabled	Original location	Symbolic link or junction point is restored to the original backup location. Target directories or files are also restored to the original backup location.
	Alternate location	Symbolic link or junction point is restored to the location specified. Target directories or files are also restored to the alternate location specified.
Disabled	Original location	Symbolic link or junction point is restored to the original backup location. Target directories or files are NOT restored to the original backup location.
	Alternate location	Symbolic link or junction point is restored to the location specified. Target directories or files are NOT restored to the alternate location specified.

④ **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 file were correct.

8. Click **Next** to proceed when you are done with the settings.
9. Select the temporary directory for storing temporary files, such as delta files, when they are being merged.

By default, the temporary files are stored under the temp directory of the user profile directory. In case the same directory path does not exist in the computer you are running AhsayOBM, you have to click **Browse** to define a new location for storing the temporary files. Otherwise, you will not be able to perform a restore.

Temporary Directory

Temporary directory for storing restore files

Browse

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

C

CBS (Host: 10.3.1.8:443)🔍 ✕

Restoring... \\LAUREL\Departments\Customer Services\Common\KMT\Steven\Graphic\...

Estimated time left 0 sec (1.76M)

Restored 1.52M (23 files)

Elapsed time 2 sec

Transfer rate 27.51Mbit/s

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

C

CBS (Host: 10.3.1.8:443)🔍


✓ Restore Completed Successfully












Estimated time left 0 sec

Restored 8.86k (1 file)

Elapsed time 4 sec

Transfer rate 8.86kbit/s

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.

Type	Log	Time
	Start [Mac OS X 10.11.1 (Scherrings-Mac-mini), AhsayOBM v7.9.0.0]	24/11/2016 10:22:46
	Initializing decrypt action...	24/11/2016 10:22:46
	Initializing decrypt action... Completed	24/11/2016 10:22:46
	Downloading... "/Users/Scherring/Documents/Document folder 01/doc 1.docx" (Total 11k bytes)	24/11/2016 10:22:47
	"/Users/Scherring/Documents/Images/pic 1.jpg" contains the same file resource. Skip restore file resource.	24/11/2016 10:22:47
	"/Users/Scherring/Documents/Images/pic 2.jpg" contains the same file resource. Skip restore file resource.	24/11/2016 10:22:47
	"/Users/Scherring/Documents/Images/pic 4.jpg" contains the same file resource. Skip restore file resource.	24/11/2016 10:22:47
	"/Users/Scherring/Documents/Images/pic 3.jpg" contains the same file resource. Skip restore file resource.	24/11/2016 10:22:47
	"/Users/Scherring/Documents/Images" contains the same file resource. Skip restore file resource.	24/11/2016 10:22:47
	"/Users/Scherring/Documents/Document folder 01/doc 1.docx" contains the same file resource. Skip restore file resource.	24/11/2016 10:22:48
	Restore Completed Successfully	24/11/2016 10:22:49

Logs per page 50 Page 1 / 1

12. In the Restore window, click **Cancel** to close the Restore window.
13. To exit AhsayOBM, 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 AhsayOBM again, you will then have to launch it again.

11.3 Restore Filter

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

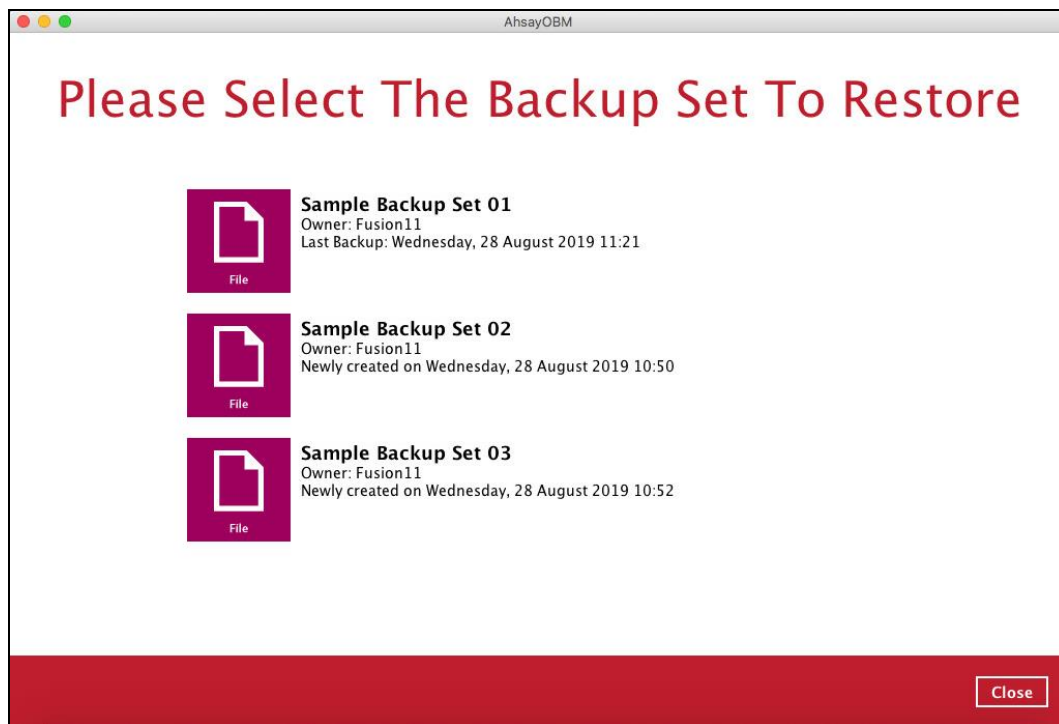
To make it more flexible, the search feature offers filtering. You can add additional pattern upon searching. Pattern includes the following criteria:

- ▶ **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 AhsayOBM, refer to [Appendix B: Example Scenarios for Restore Filter](#).

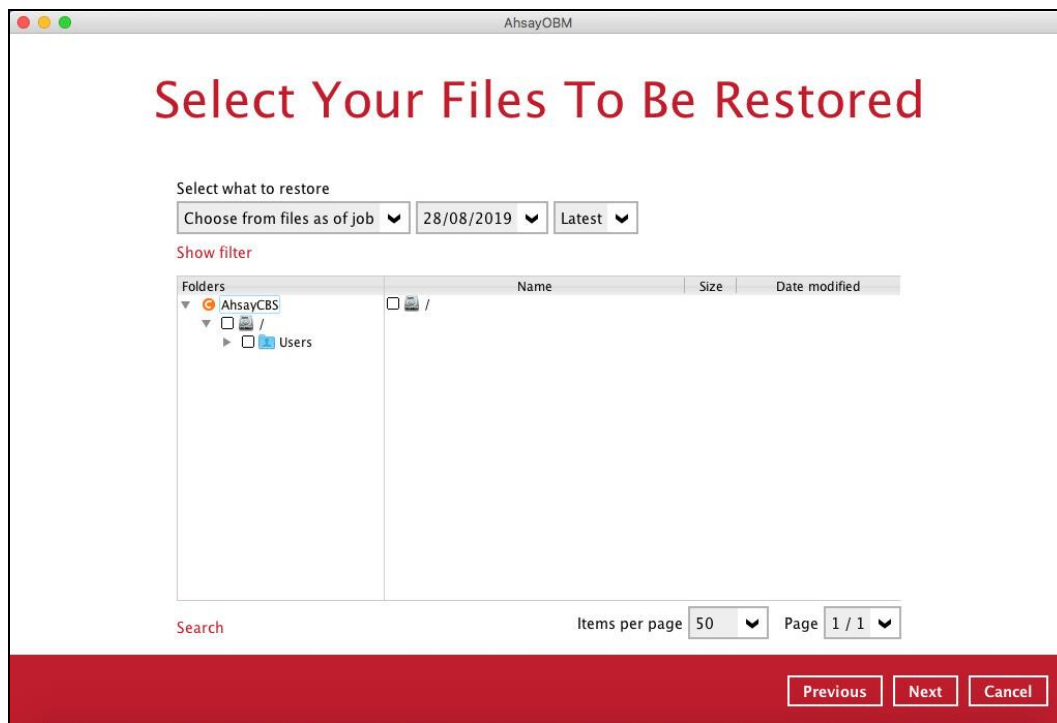
1. Login to AhsayOBM according to the instructions in [Login to AhsayOBM](#).
2. Click the [Restore] icon on the main interface of AhsayOBM.
3. Select the backup set the you would like to restore.



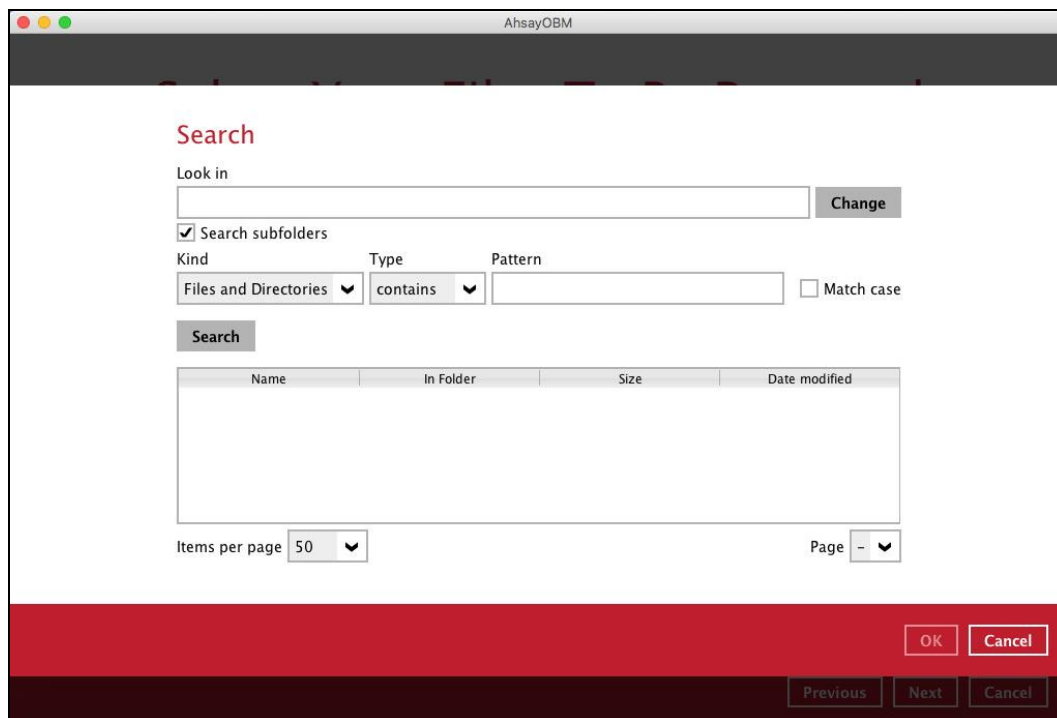
4. Select the backup destination that you would like to restore backed-up items to.

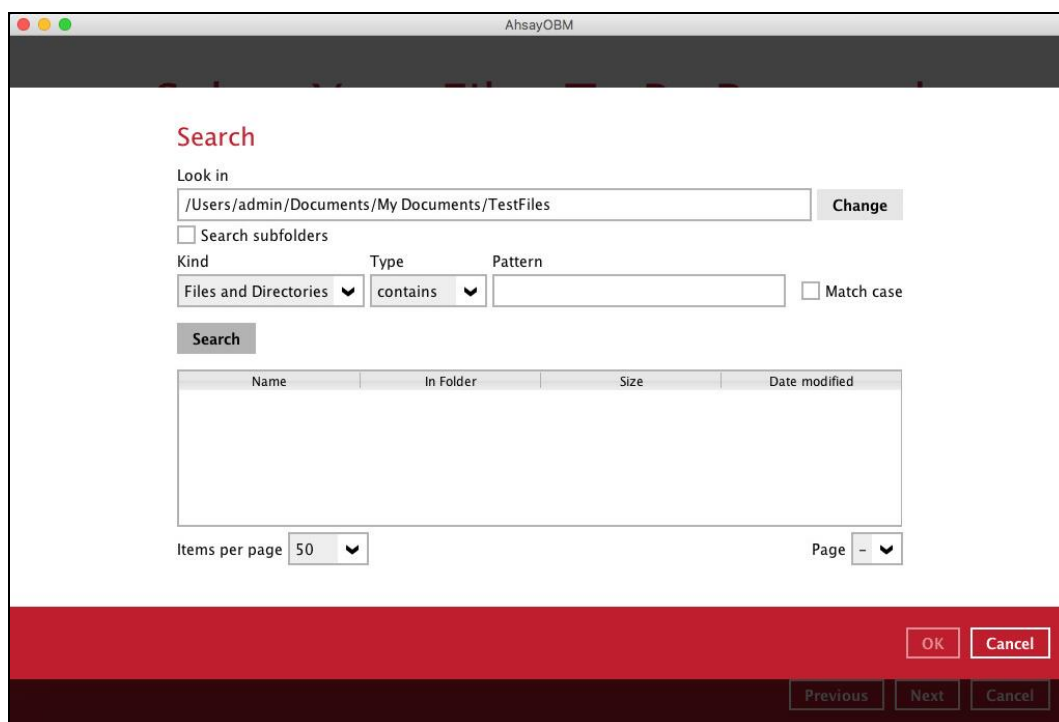
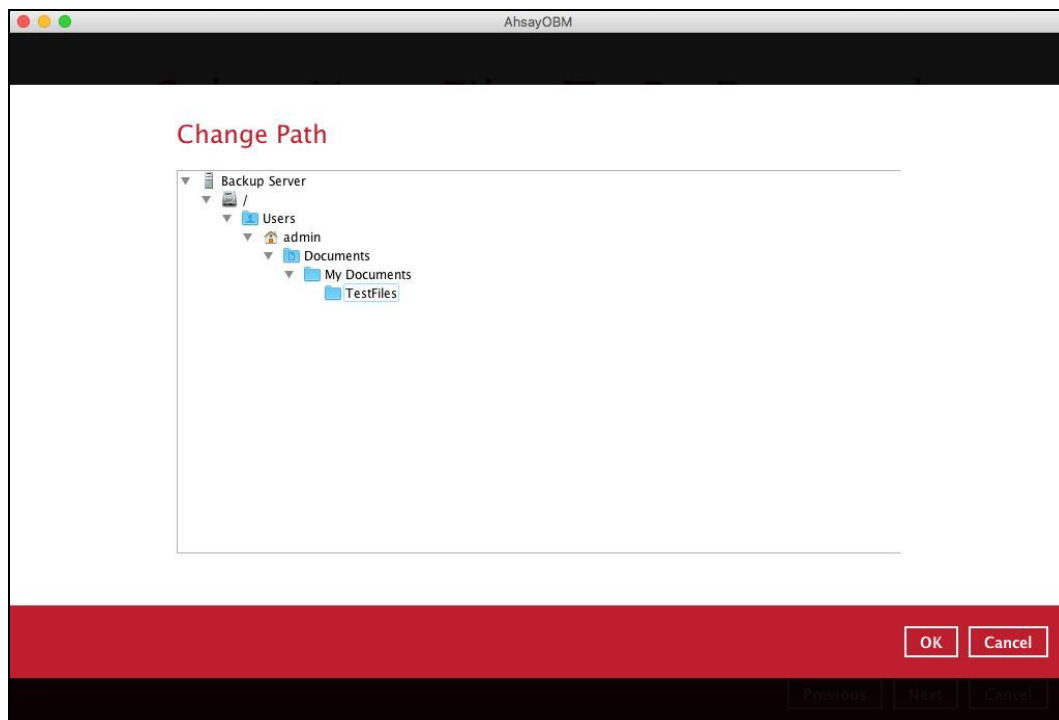


5. Click the [Search] located on the lower left side of the screen.



6. Click the [Change] button to change the path of the restore items from other location.





7. Tick the [Search subfolders] to include available subfolders upon searching.

☐ Search subfolders

☒ Search subfolders

8. Select from the following Kind of files you want to search.

- Files and Directories
- Files only
- Directories

9. Select from the following Type of filtering you want to search.

- Contains
- Exact
- Starts With
- Ends With

10. Enter a pattern you want and tick the [Match case] box if you want to accurately search for a specific file.

Pattern
 ☐ Match case

Pattern
 ☒ Match case

11. Click the [Search] button and the result will be displayed.

12. 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.

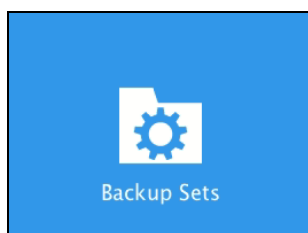
12 Mobile Backup and Restore to AhsayCBS and Predefined Destination

To do a mobile backup and restore to AhsayCBS and Predefined Destination, follow the steps:

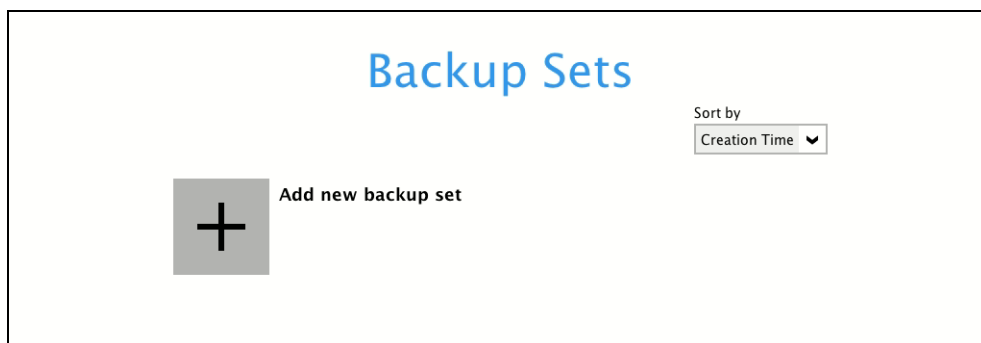
- ▶ Backup photos and videos from Ahsay Mobile app to AhsayOBM local destination. For more detailed information, check [Ahsay Mobile App User Guide for Android and iOS – Chapter 10](#).
- ▶ [Create a File Backup Set](#) on AhsayOBM and follow these setup:
 - Backup source should be photos and videos backed up in AhsayOBM local destination. Example: **/Users/admin/Documents/Backup/Redmi**
 - Backup destination should be to AhsayCBS and Predefined Destination. Examples of predefined destinations: Google Drive, OneDrive, Wasabi, etc.
- ▶ [Run a Backup Job](#) on AhsayOBM.
- ▶ [Restore Data](#) on AhsayOBM. This can be from Original or Alternate location.

12.1 Create a File Backup Set

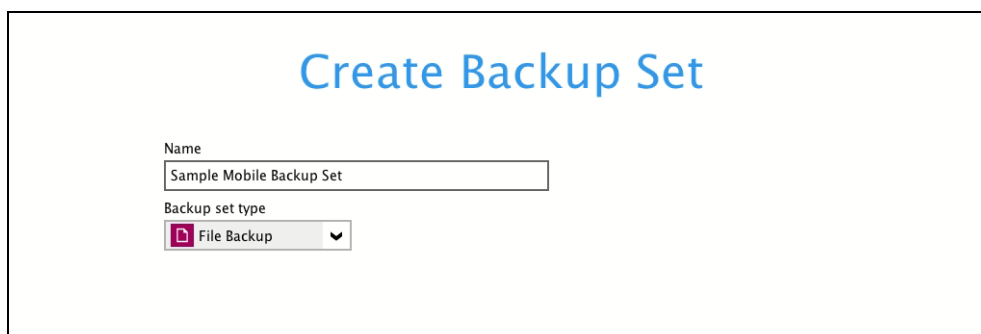
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.



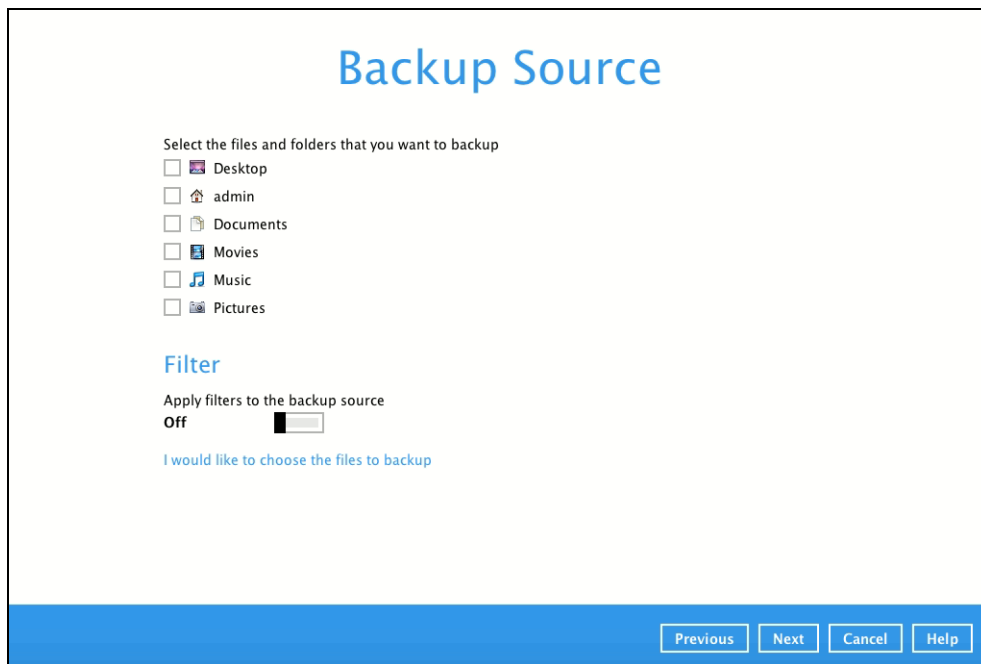
2. Create a new backup set by clicking  next to **Add new backup set**.



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.

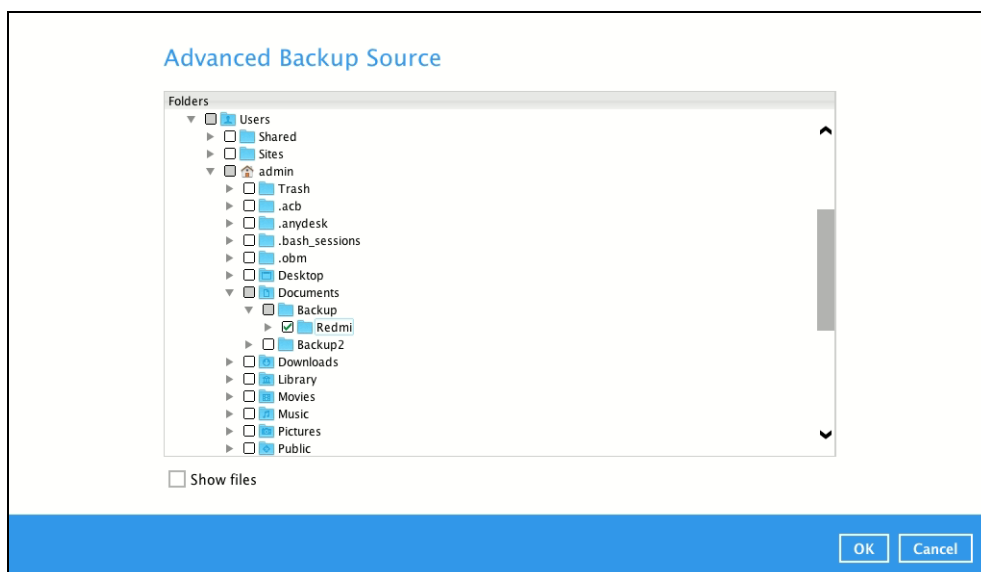


4. In the Backup Source window, select the mobile backup source for backup. Click **I would like to choose the files to backup**.

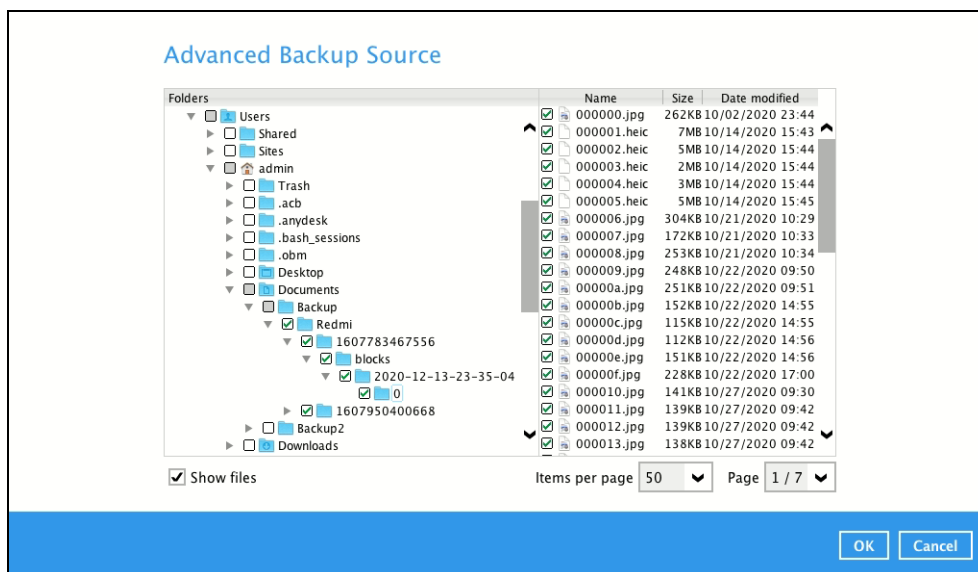


In the **Advanced Backup Source** window, select the mobile backup source.

In this example, Redmi folder is selected. The mobile backup source is in **/Users/admin/Documents/Backup**.

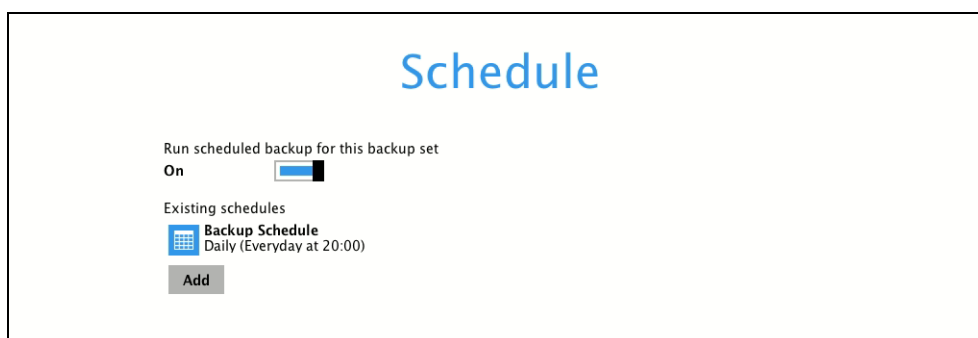


Alternatively, if you want to back up only specific files instead of all files in your selected folder(s), select the **Show files** checkbox at the bottom of the screen. A list of files will appear on the right-hand side. Select the checkbox(es) next to the file(s) to back up. Then, click **OK** to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

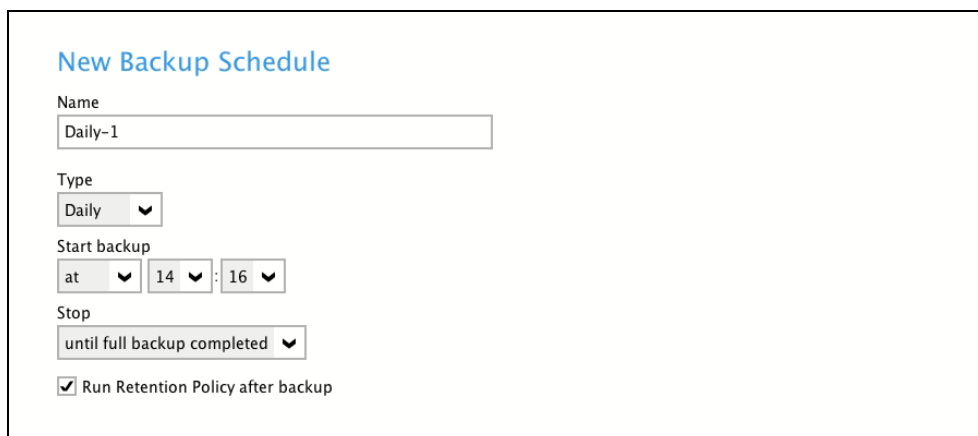


In the Backup Source window, click Next to proceed.

5. In the Schedule window, the Run scheduled backup for this backup set is **On** by default. You can configure a backup schedule to automatically run a backup job at your specified time interval. Click Add to add a new schedule.



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.



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

Schedule

Run scheduled backup for this backup set
On

Existing schedules

- Backup Schedule**
Daily (Everyday at 20:00)
- Daily-1**
Daily (Everyday at 14:16)

Add

Previous **Next** **Cancel** **Help**

6. 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**.

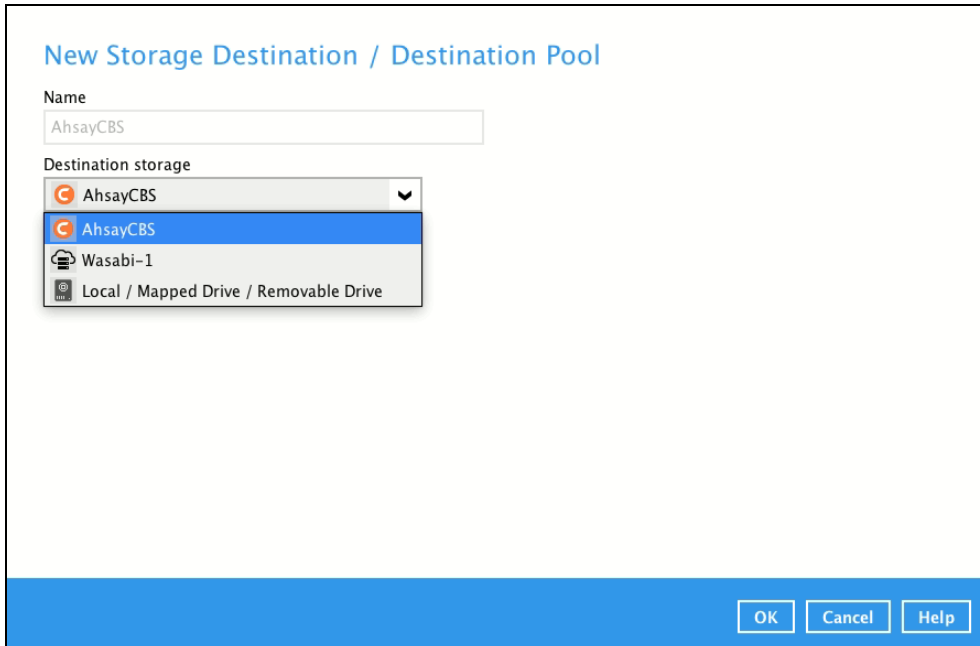
Destination

Backup mode
Sequential

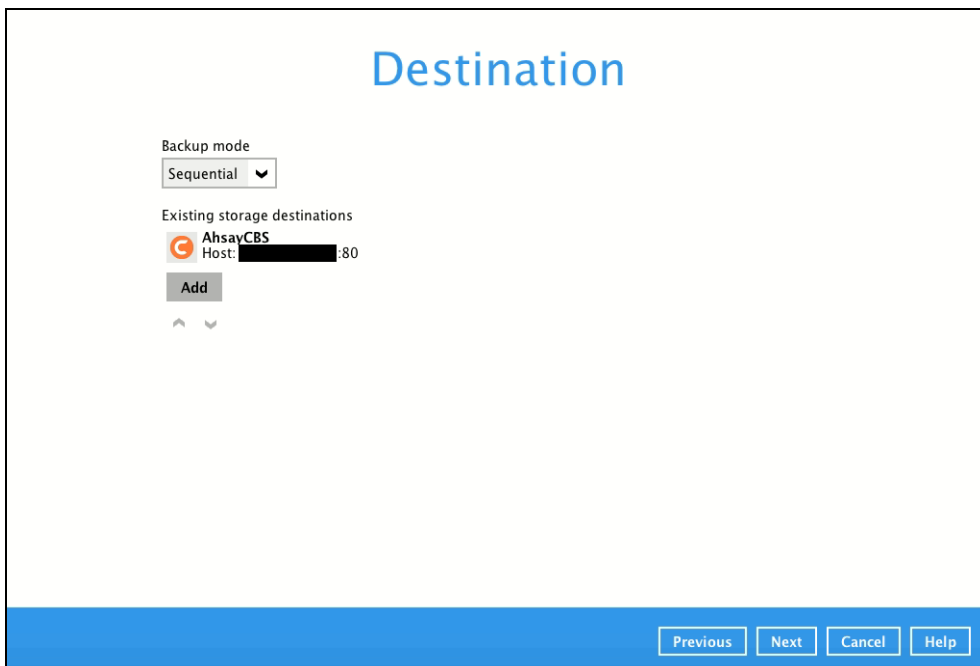
Existing storage destinations
+ Add new storage destination / destination pool

Previous **Next** **Cancel** **Help**

In the New Storage Destination/Destination Pool window, select AhsayCBS or a Predefined destination. Then, click **OK** to confirm your selection.



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



7. The **OpenDirect Restore** feature should be disabled. Click **Next** to proceed.

OpenDirect

OpenDirect
Off ☐

Support of opening backup data directly without restoration.

When OpenDirect is enabled, to optimize restore performance both compression and encryption will be disabled for this backup set.

Once OpenDirect is enabled and the setting is saved, it cannot be disabled without re-creating the backup set.

Previous Next Cancel Help

8. 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

Encryption

Encrypt Backup Data
On ☐

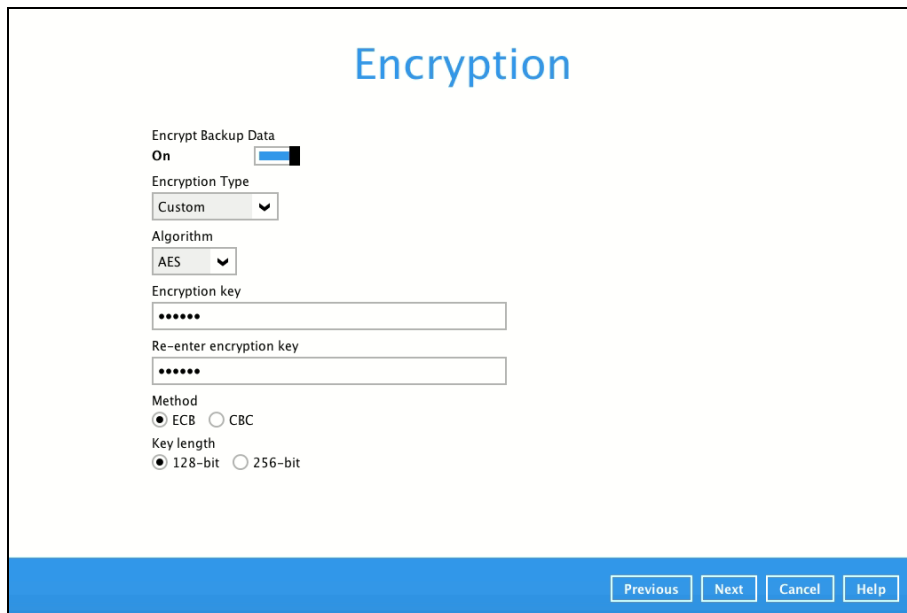
Encryption Type
Default ▼

Default
User password
Custom

Previous Next Cancel Help

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

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method, and key length.



Encryption

Encrypt Backup Data
On ☒

Encryption Type
 Custom ▼

Algorithm
 AES ▼

Encryption key

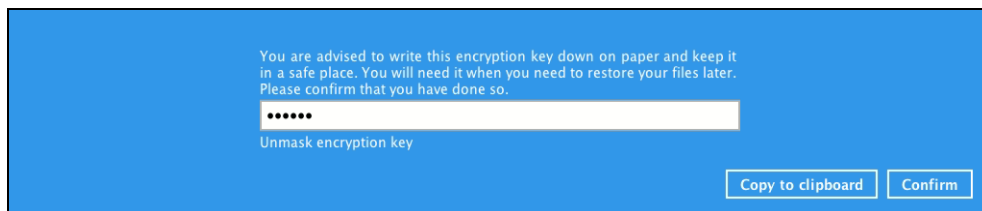
Re-enter encryption key

Method
☒ ECB ☐ CBC

Key length
☒ 128-bit ☐ 256-bit

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

9. 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.



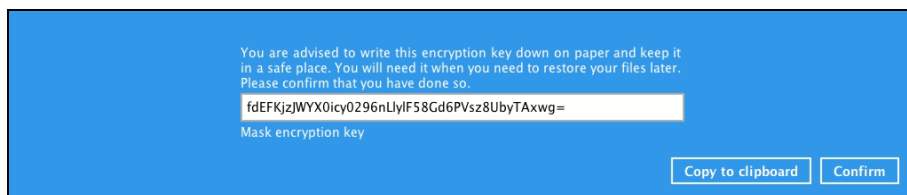
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

.....

Unmask encryption key

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.



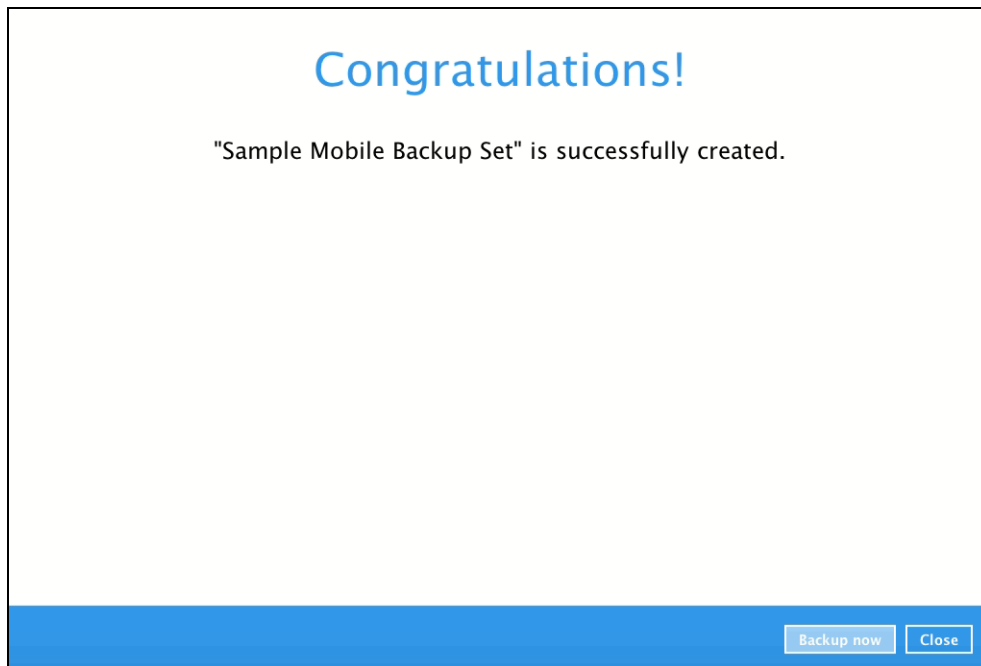
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

fdEFKjzJWYX0icy0296nLlylF58Gd6PVsz8UbyTAxwg=

Mask encryption key

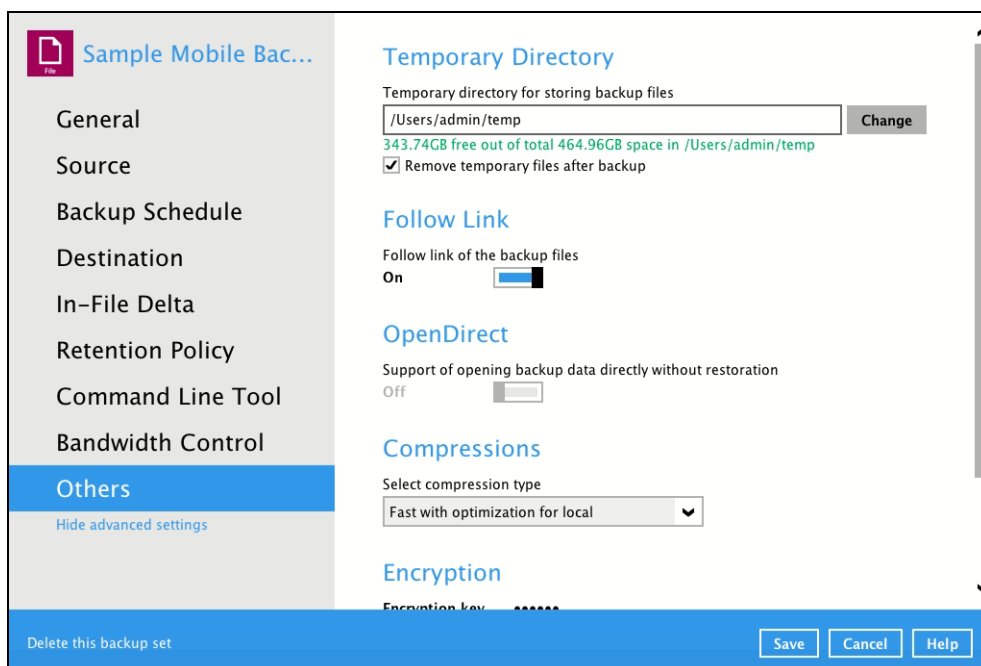
- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

10. 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.



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

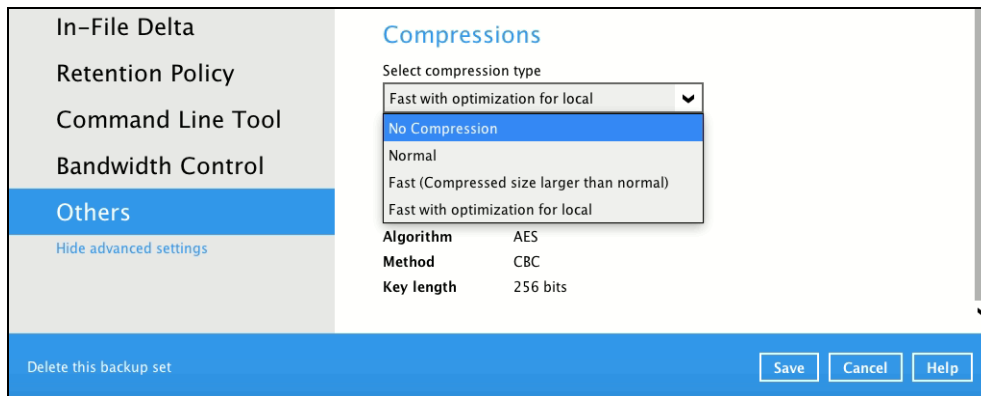
Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



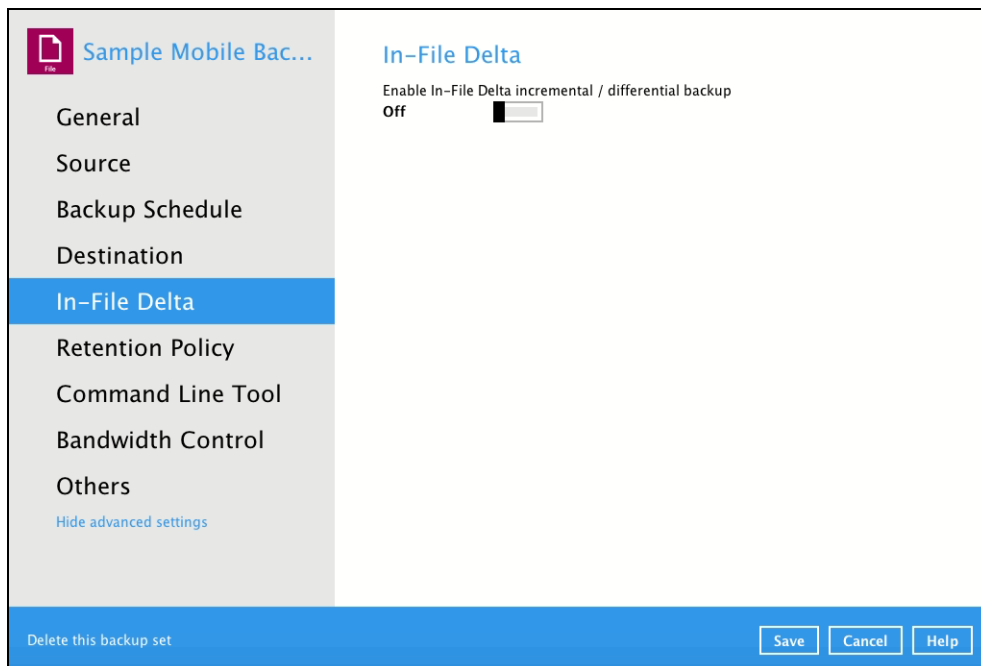
12. Optional: Select your preferred **Compression** type. By default, the compression is set Optimal for Local (Low CPU Usage) Go to **Others > Compressions**.

Select from the following list:

- No Compression
- Normal
- Fast
- Optimal for Local (Low CPU Usage)

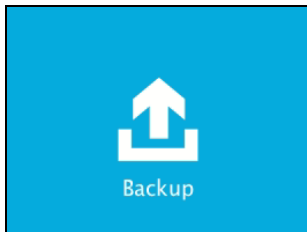


13. Optional: It is recommended to disable the **In-File Delta** as the files are relatively small, photos and videos are also not updated.

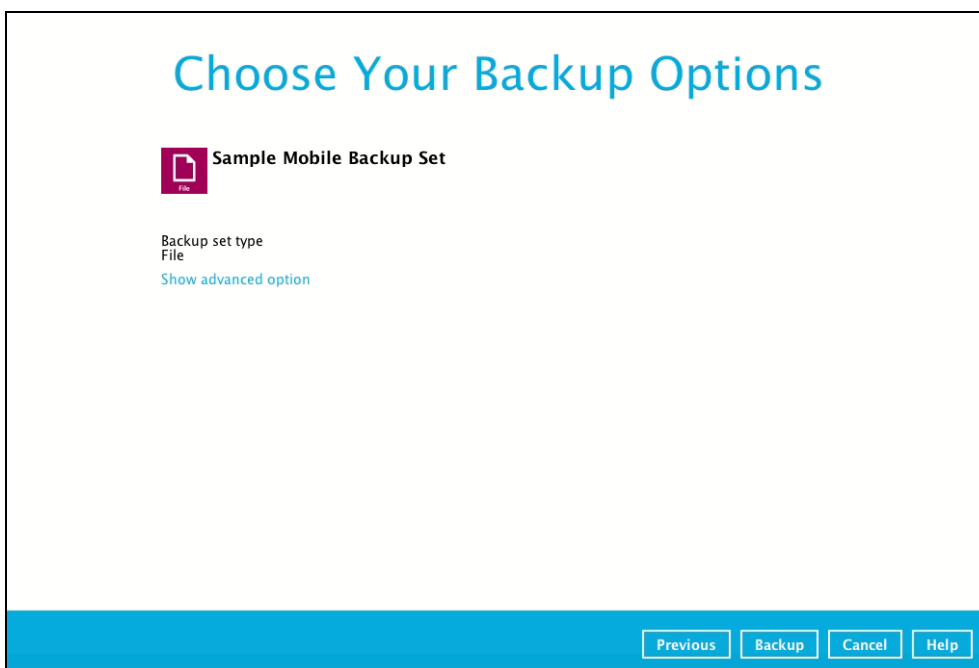
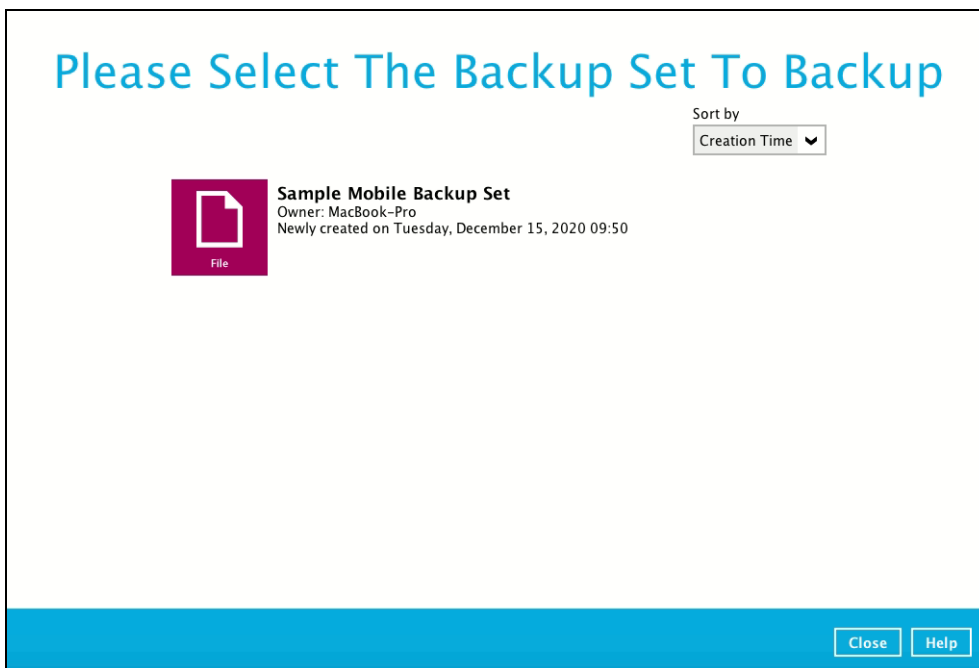


12.2 Run a Backup Job

1. Click **Backup** on the main interface of AhsayOBM.

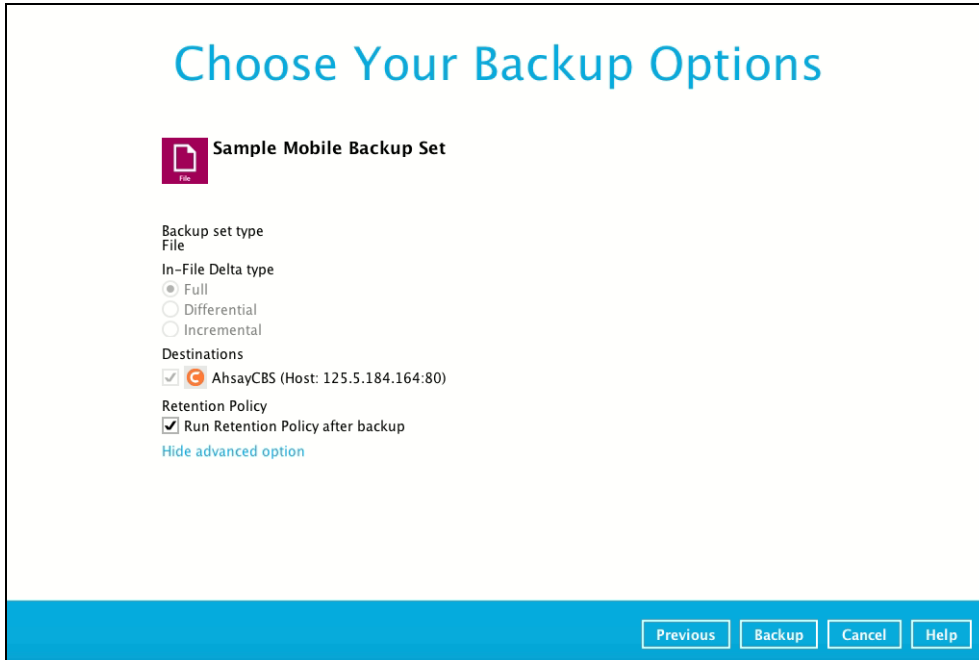


2. Select the backup set that you would like to start a backup job for. In case you want to modify the In-File Delta type, Destinations and Retention Policy settings, click **Show advanced option**.



- When advanced options are shown, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** in the Retention Policy section at the bottom.

This will help you save hard disk quota in the long run. In the In-File Delta type section, it is recommended to run in **Full** as a full backup captures all the data that you want to protect. When you run a backup job for the first time, AhsayOBM will run a full backup regardless of the in-file delta setting.

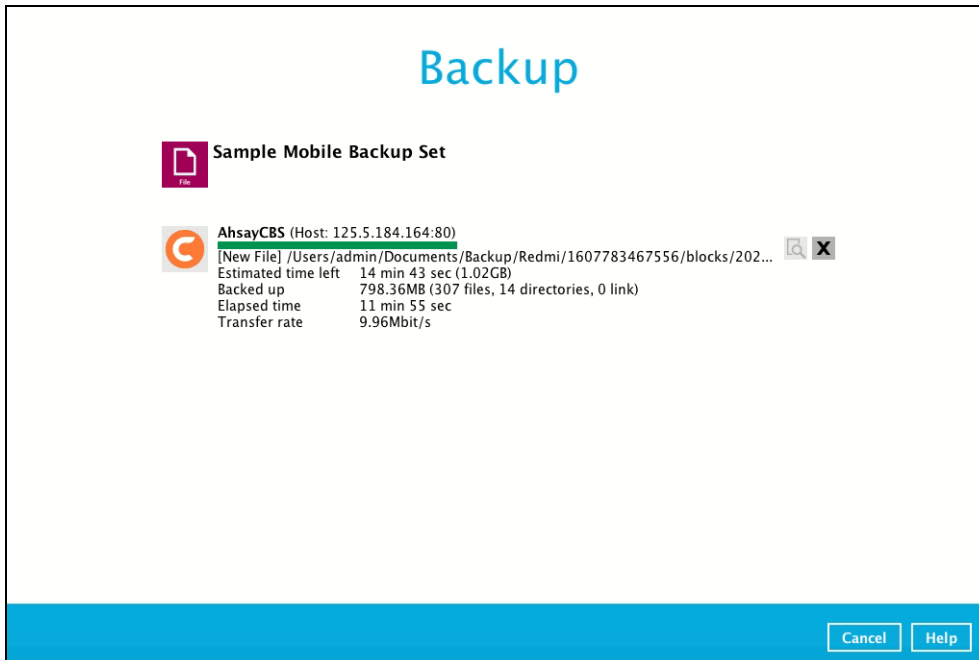


The screenshot shows a dialog box titled "Choose Your Backup Options". It contains the following settings:

- Sample Mobile Backup Set** (indicated by a file icon)
- Backup set type:** File
- In-File Delta type:** ☒ Full, ☐ Differential, ☐ Incremental
- Destinations:** ☒ AhsayCBS (Host: 125.5.184.164:80)
- Retention Policy:** ☒ Run Retention Policy after backup
- A link: [Hide advanced option](#)

At the bottom right, there are four buttons: Previous, Backup, Cancel, and Help.

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



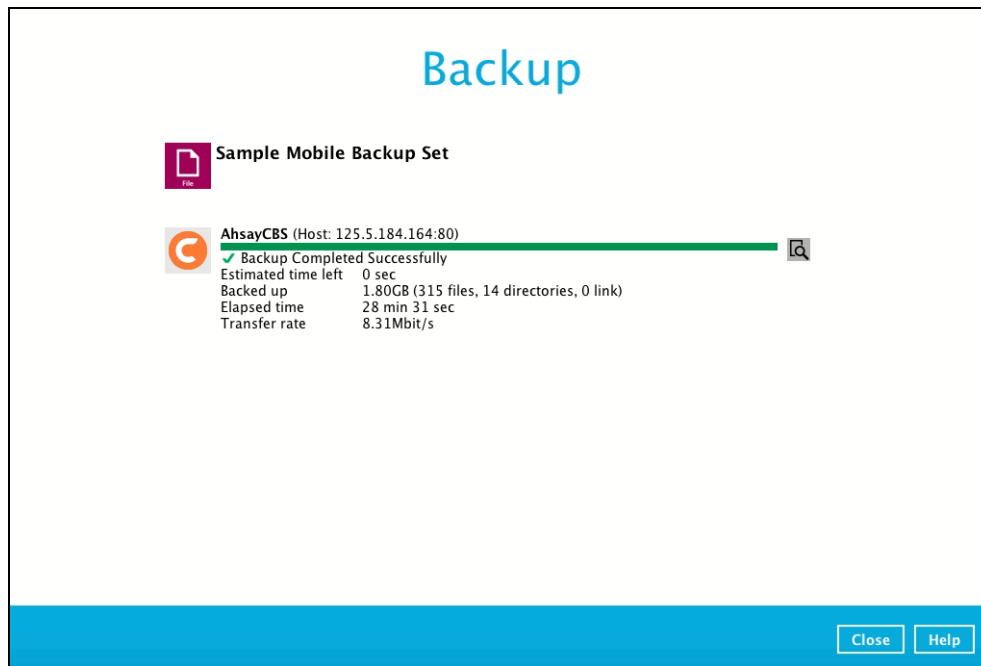
The screenshot shows a dialog box titled "Backup". It displays the progress of the backup job for the "Sample Mobile Backup Set" to the destination "AhsayCBS (Host: 125.5.184.164:80)".


Backup details:

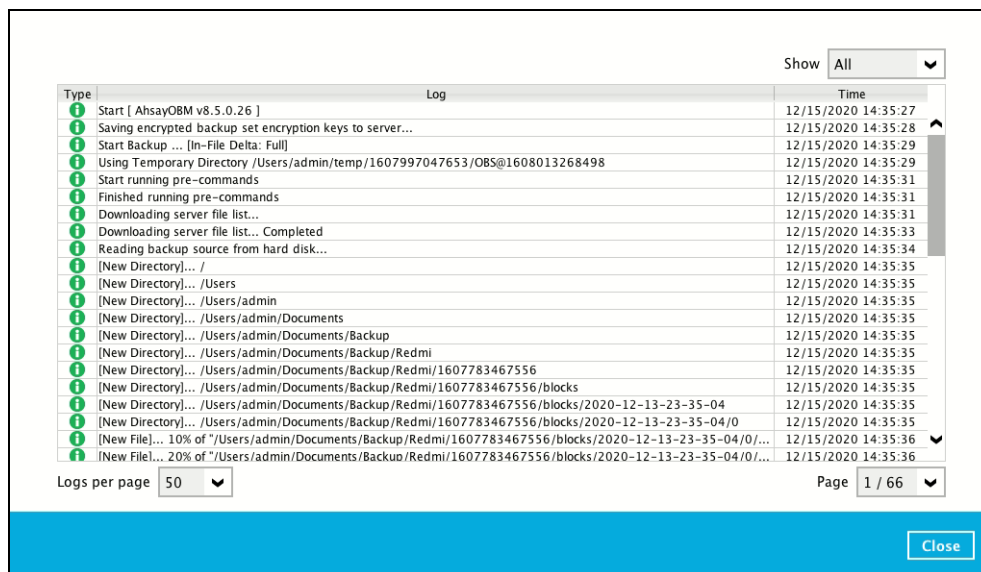
- Path: [New File] /Users/admin/Documents/Backup/Redmi/1607783467556/blocks/202...
- Estimated time left: 14 min 43 sec (1.02GB)
- Backed up: 798.36MB (307 files, 14 directories, 0 link)
- Elapsed time: 11 min 55 sec
- Transfer rate: 9.96Mbit/s

At the bottom right, there are two buttons: Cancel and Help.

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



- 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.



12.3 Restore Data

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

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

Using this option, you can perform seamless restore to your mobile device as the location is the same with the mobile backup destination.

- Alternate location, data will be restored on an alternate location which can be setup anywhere in the AhsayOBM 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 Ahsay Mobile app to restore the photos and videos back to your mobile device.
- Option 2: Copy the restored data from the alternate location to your Android or iOS mobile device.

Examples:

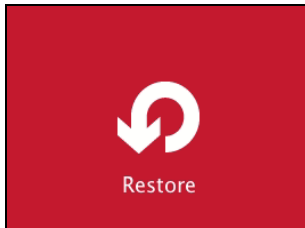
- For an Android device, you need to plug your cable and transfer the restored data from the alternate location to your mobile device storage.
- For an iOS device, you need to transfer the restored data from the alternate location to iCloud.

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

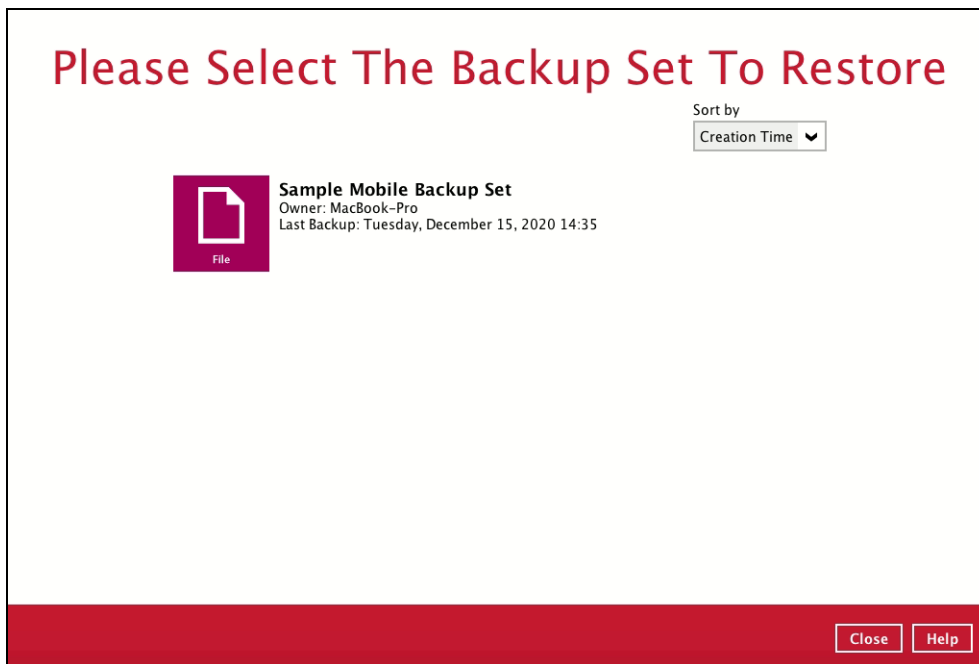
In case the original machine is no longer available, AhsayOBM will be able to restore the photos and videos from AhsayCBS or Predefined Destination to the mobile backup destination folder. However, as the mobile devices were not originally paired with the new installation or machine, the mobile devices will not be able to restore the photos and videos from the AhsayOBM.

12.3.1 Original Location

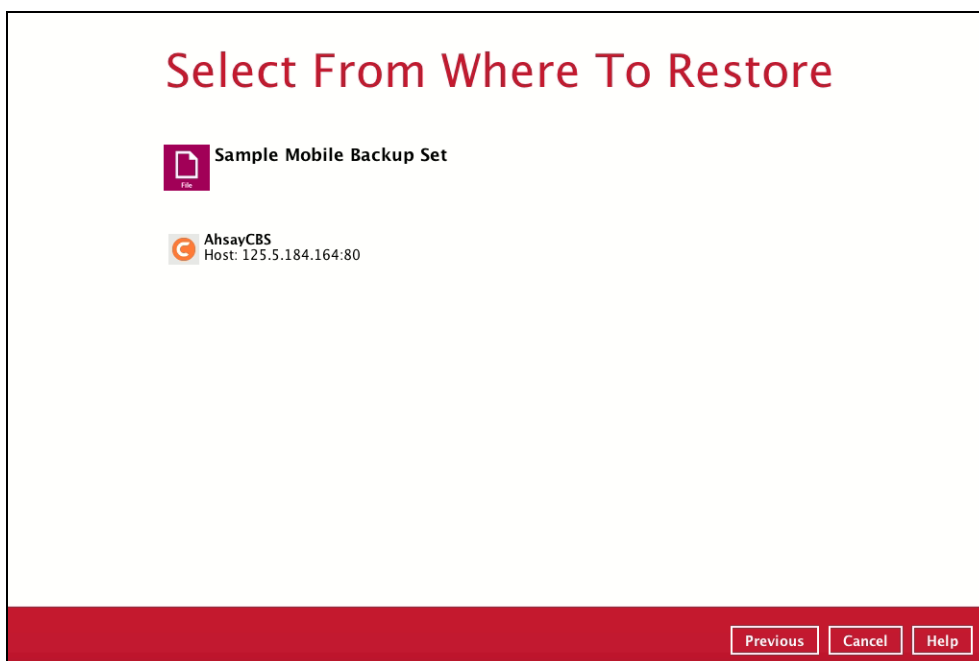
1. Click the **Restore** icon on the main interface of AhsayOBM.



2. All the available backup sets for restore will be listed. Select the backup set that you would like to restore data from.



3. Select where you would like to restore your data from.



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:

Select Your Files To Be Restored

Select what to restore

Choose from files as of job 12/15/2020 Latest

Show filter

Folders

- AhsayCBS
 - /
 - Users

Name Size Date modified

Search

Items per page 50 Page 1 / 1

Previous Next Cancel Help

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

Select what to restore

Choose from files as of job 12/15/2020 Latest

Choose from files as of job

Choose from ALL files

Name

Folders

- AhsayCBS
 - /
 - Users

Select what to restore

Choose from files as of job 12/15/2020 Latest

Show filter

12/15/2020

Name

Folders

- AhsayCBS
 - /
 - Users

Select what to restore

Choose from files as of job 12/15/2020 Latest

Show filter

Latest

14:35

Name

Folders

- AhsayCBS
 - /
 - Users

- **Choose from ALL files** – This option allows you to restore all files for this backup set.

Select what to restore

Choose from ALL files ▼

Show filter

Folders	Name	Size	Date modified
▼ AhsayCBS	000000.jpg	262KB	10/02/2020 23:44
▼ /	000001.heic	7MB	10/14/2020 15:43
▼ Users	000002.heic	5MB	10/14/2020 15:44
▼ admin	000003.heic	2MB	10/14/2020 15:44
▼ Documents	000004.heic	3MB	10/14/2020 15:44
▼ Backup	000005.heic	5MB	10/14/2020 15:45
▼ Redmi	000006.jpg	304KB	10/21/2020 10:29
▼ 1607783467556	000007.jpg	172KB	10/21/2020 10:33
▼ blocks	000008.jpg	253KB	10/21/2020 10:34
▼ 2020-12-13-23-3	000009.jpg	248KB	10/22/2020 09:50
▼ 0	00000a.jpg	251KB	10/22/2020 09:51
▼ 1607950400668	00000b.jpg	152KB	10/22/2020 14:55
	00000c.jpg	115KB	10/22/2020 14:55
	00000d.jpg	112KB	10/22/2020 14:56
	00000e.jpg	151KB	10/22/2020 14:56
	00000f.jpg	228KB	10/22/2020 17:00
	000010.jpg	141KB	10/27/2020 09:30
	000011.jpg	139KB	10/27/2020 09:42

Search

Items per page 50 Page 1 / 7

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

5. Select to restore the files to **Original location**. Then, click **Next** to proceed.

The backed-up data will be restored to the computer running the AhsayOBM under the same directory path as on the machine storing the backup source.

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

Choose Where The Files To Be Restored

Restore files to

☒ Original location

☐ Alternate location

Show advanced option

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

Restore files to
☒ Original location
☐ Alternate location
[Show advanced option](#)

Choose Where The Files To Be Restored

Restore files to
☒ Original location
☐ Alternate location

☒ Follow Link
☐ Verify checksum of in-file delta files during restore
[Hide advanced option](#)

• **Follow Link (Enabled by default)**

When this option is enabled, not only the symbolic link or junction point will be restored, the directories and files that the symbolic link or junction point links to will also be restored.

The table below summarizes the behaviors when a restore is performed with different settings.

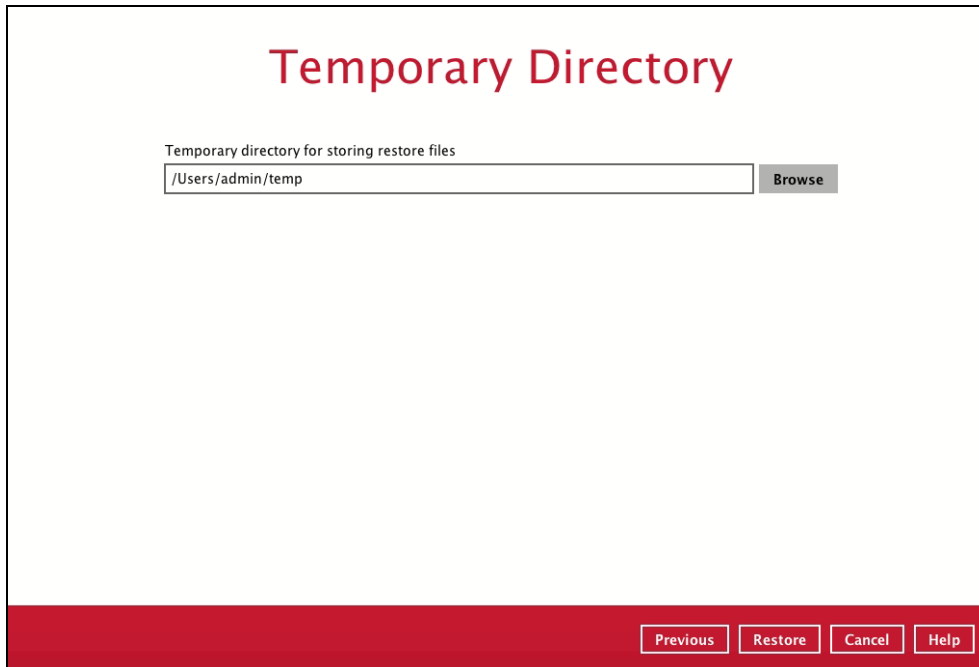
Follow Link	Restore to	Behavior
Enabled	Original location	Symbolic link or junction point is restored to the original backup location. Target directories or files are also restored to the original backup location.
	Alternate location	Symbolic link or junction point is restored to the location specified. Target directories or files are also restored to the alternate location specified.
Disabled	Original location	Symbolic link or junction point is restored to the original backup location. Target directories or files are NOT restored to the original backup location.
	Alternate location	Symbolic link or junction point is restored to the location specified. Target directories or files are NOT restored to the alternate location specified.

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

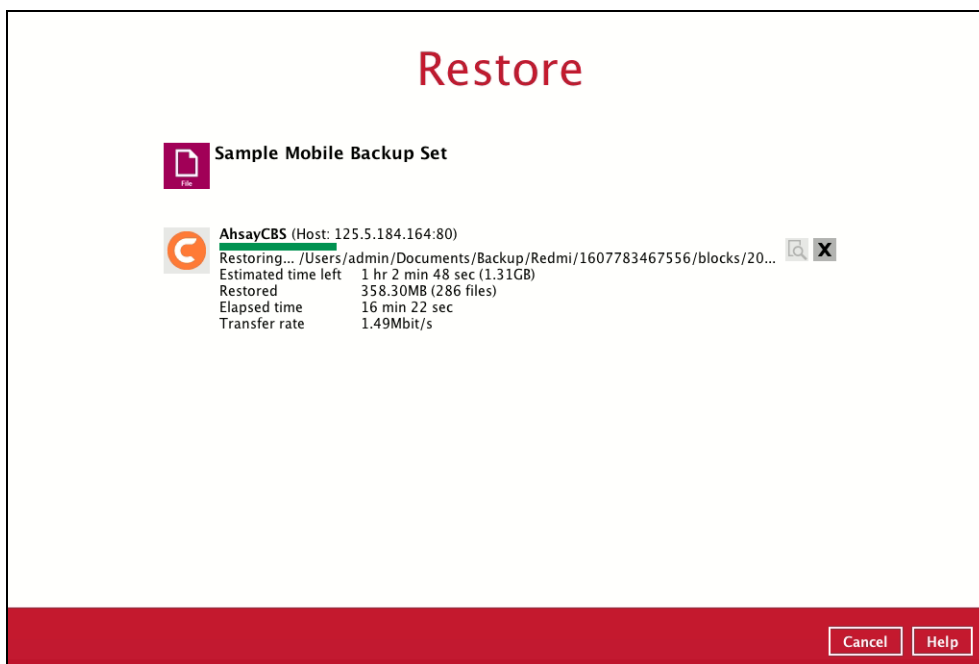
Verify checksum of in-file delta files during restore is disabled by default. You can enable the feature by ticking the checkbox so that the checksum of in-file delta files will be verified. As the feature will make the restore process time longer, it is recommended to enable the feature only if you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




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

7. Select the temporary directory for storing temporary files, such as delta files, when they are being merged. By default, the temporary files are stored under the temp directory of the user profile directory. In case the same directory path does not exist in the computer you are running AhsayOBM, you have to click **Browse** to define a new location for storing the temporary files. Otherwise, you will not be able to perform a restore.



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



- # Restore
- **Sample Mobile Backup Set**
- **AhsayCBS (Host: 125.5.184.164:80)**
- ✓ Restore Completed Successfully

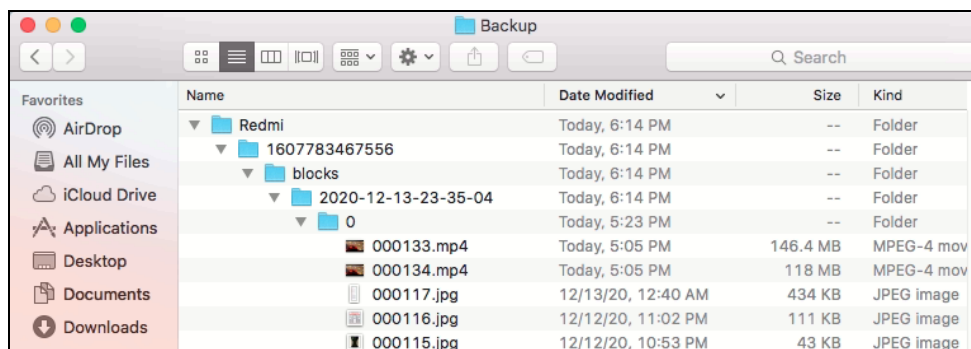
Estimated time left	0 sec
Restored	1.66GB (315 files)
Elapsed time	47 min 38 sec
Transfer rate	4.97Mbit/s
- Close

Help

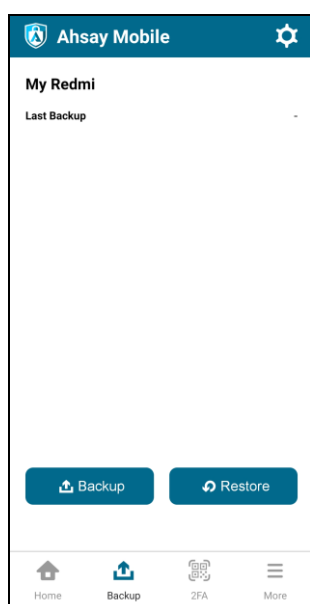
- | | | Show | All | |
|------|---|------------|----------|--|
| Type | Log | Time | | |
| | Start [AhsayOBM v8.5.0.26] | 12/15/2020 | 20:05:00 | |
| | Initializing decrypt action... | 12/15/2020 | 20:05:01 | |
| | Initializing decrypt action... Completed | 12/15/2020 | 20:05:01 | |
| | Creating new directory... "/Users/admin/Documents/Backup/Redmi" | 12/15/2020 | 20:05:01 | |
| | Creating new directory... "/Users/admin/Documents/Backup/Redmi/1607783467556" | 12/15/2020 | 20:05:01 | |
| | Creating new directory... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks" | 12/15/2020 | 20:05:01 | |
| | Creating new directory... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04" | 12/15/2020 | 20:05:01 | |
| | Creating new directory... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04..." | 12/15/2020 | 20:05:01 | |
| | Downloading... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04/0/000..." | 12/15/2020 | 20:05:01 | |
| | Downloading... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04/0/000..." | 12/15/2020 | 20:05:01 | |
| | Downloading... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04/0/000..." | 12/15/2020 | 20:05:01 | |
| | Restoring File Resource: /Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04... | 12/15/2020 | 20:06:03 | |
| | Downloading... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04/0/000..." | 12/15/2020 | 20:06:03 | |
| | Restoring File Resource: /Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04... | 12/15/2020 | 20:06:03 | |
| | Downloading... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04/0/000..." | 12/15/2020 | 20:06:03 | |
| | Restoring File Resource: /Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04... | 12/15/2020 | 20:06:03 | |
| | Restoring File Resource: /Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04... | 12/15/2020 | 20:06:03 | |
| | Downloading... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04/0/000..." | 12/15/2020 | 20:06:03 | |
| | Downloading... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04/0/000..." | 12/15/2020 | 20:06:03 | |
| | Restoring File Resource: /Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04... | 12/15/2020 | 20:06:03 | |
| | Downloading... "/Users/admin/Documents/Backup/Redmi/1607783467556/blocks/2020-12-13-23-35-04/0/000..." | 12/15/2020 | 20:06:03 | |

11. You can restore the restored data from the original location to your mobile device by using the Ahsay Mobile app.

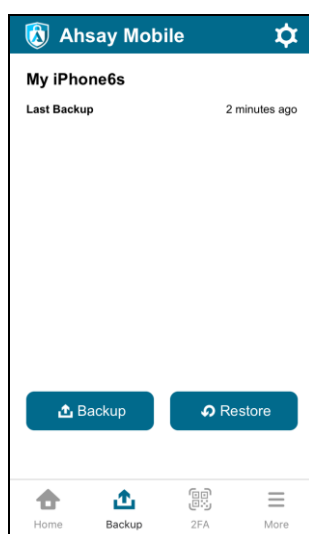
Original location: **/Users/admin/Documents/Backup/Redmi**



Android device

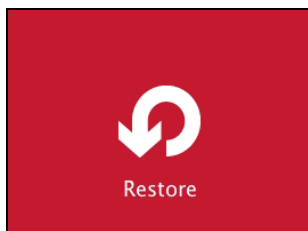


iOS device

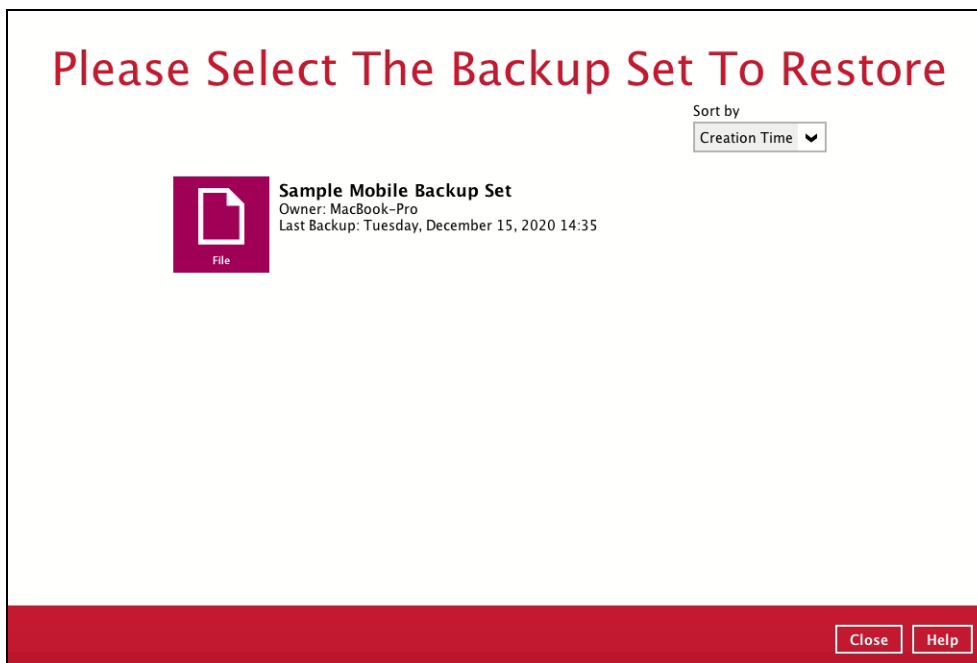


12.3.2 Alternate Location

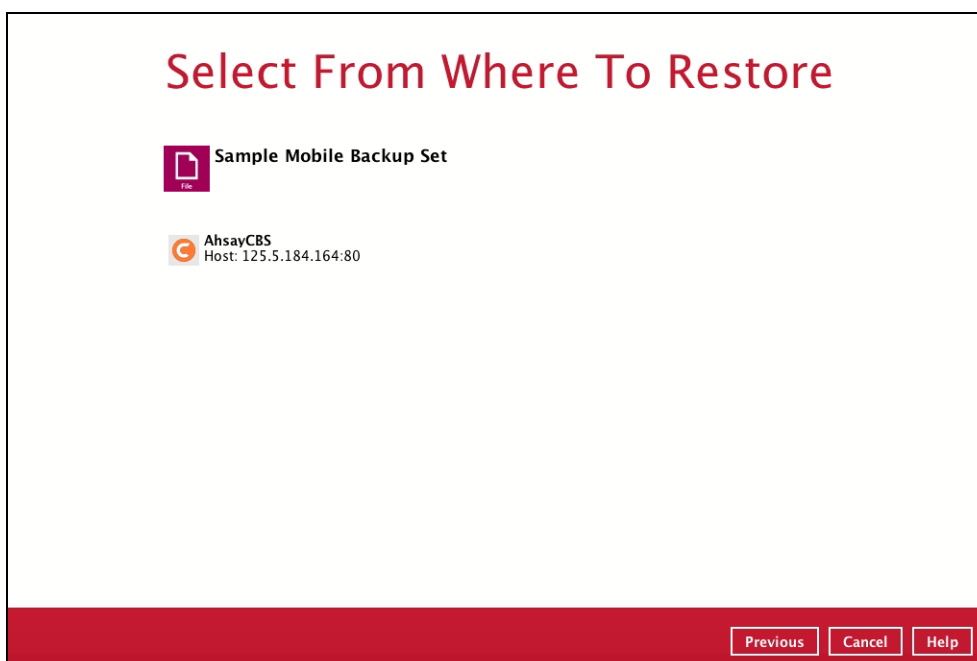
1. Click the **Restore** icon on the main interface of AhsayOBM.



2. All the available backup sets for restore will be listed. Select the backup set that you would like to restore data from.



3. Select where you would like to restore your data from.



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:

Select Your Files To Be Restored

Select what to restore

Choose from files as of job 12/15/2020 Latest

Show filter

Folders

- AhsayCBS
 - /
 - Users

Name Size Date modified

Search

Items per page 50 Page 1 / 1

Previous Next Cancel Help

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

Select what to restore

Choose from files as of job 12/15/2020 Latest

Choose from files as of job

Choose from ALL files

Name

Folders

- AhsayCBS
 - /
 - Users

Select what to restore

Choose from files as of job 12/15/2020 Latest

Show filter

12/15/2020

Name

Folders

- AhsayCBS
 - /
 - Users

Select what to restore

Choose from files as of job 12/15/2020 Latest

Show filter

Latest

14:35

Name

Folders

- AhsayCBS
 - /
 - Users

- 

Select what to restore

Choose from ALL files

Show filter

Folders

AhsayCBS

/

Users

admin

Documents

Backup

Redmi

1607783467556

blocks

2020-12-13-23-3

0

1607950400668

Name	Size	Date modified
000000.jpg	262KB	10/02/2020 23:44
000001.heic	7MB	10/14/2020 15:43
000002.heic	5MB	10/14/2020 15:44
000003.heic	2MB	10/14/2020 15:44
000004.heic	3MB	10/14/2020 15:44
000005.heic	5MB	10/14/2020 15:45
000006.jpg	304KB	10/21/2020 10:29
000007.jpg	172KB	10/21/2020 10:33
000008.jpg	253KB	10/21/2020 10:34
000009.jpg	248KB	10/22/2020 09:50
00000a.jpg	251KB	10/22/2020 09:51
00000b.jpg	152KB	10/22/2020 14:55
00000c.jpg	115KB	10/22/2020 14:55
00000d.jpg	112KB	10/22/2020 14:56
00000e.jpg	151KB	10/22/2020 14:56
00000f.jpg	228KB	10/22/2020 17:00
000010.jpg	141KB	10/27/2020 09:30
000011.jpg	139KB	10/27/2020 09:42

Search

Items per page 50

Page 1 / 7

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

5. Select to restore the files to **Alternate location**. You can choose to restore the data to a location of your choice on the computer where AhsayOBM is running. Then, click **Next** to proceed.

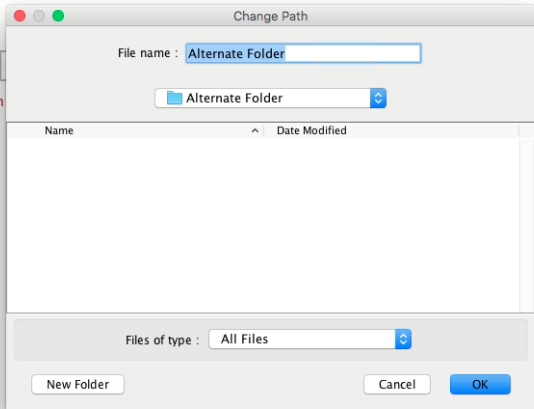
Choose Where The Files To Be Restored

Restore files to

☐ Original location

☒ Alternate location

Show advanced option



File name : Alternate Folder

Alternate Folder

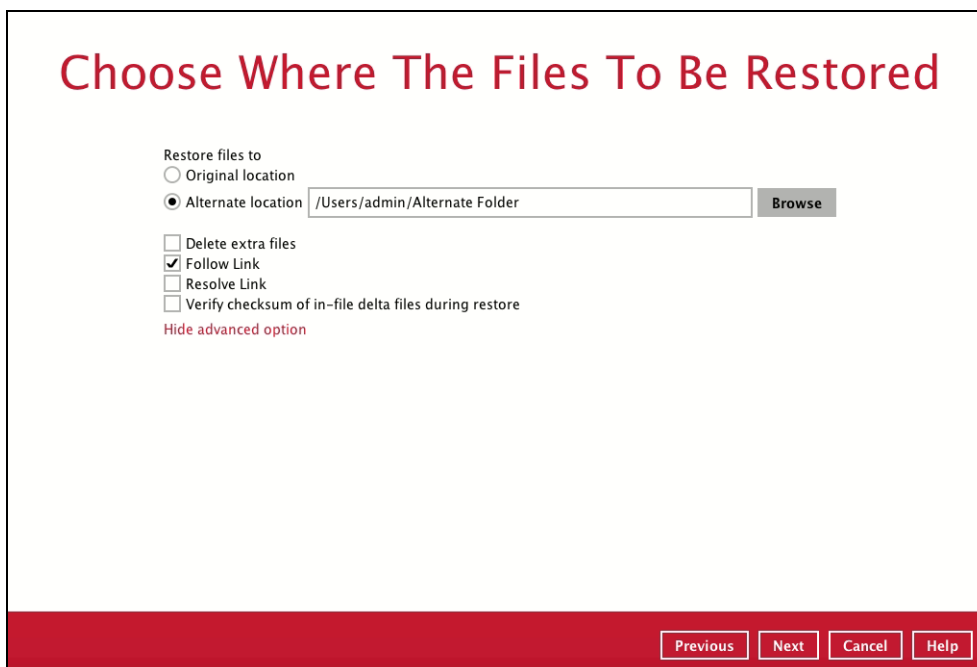
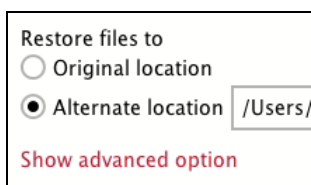
Name	Date Modified
------	---------------

Files of type : All Files

New Folder Cancel OK

Previous Next Cancel Help

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



⦿ **Delete extra files**

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

WARNING

Please exercise extra caution when enabling this feature. Consider what data in the restore source has not been backed up and what impact it would cause if those data is deleted. Prior to the data restore and synchronization, a warning message shows as the one shown below. Only clicking **Yes** will the “extra file” be deleted. You can click **Apply to all** to confirm deleting all the “extra files” at a time.

⦿ **Follow Link (Enabled by default)**

When this option is enabled, not only the symbolic link or junction point will be restored, the directories and files that the symbolic link or junction point links to will also be restored.

The table below summarizes the behaviors when a restore is performed with different settings.

Follow Link	Restore to	Behavior
Enabled	Original location	Symbolic link or junction point is restored to the original backup location. Target directories or files are also restored to the original backup location.

	Alternate location	Symbolic link or junction point is restored to the location specified. Target directories or files are also restored to the alternate location specified.
Disabled	Original location	Symbolic link or junction point is restored to the original backup location. Target directories or files are NOT restored to the original backup location.
	Alternate location	Symbolic link or junction point is restored to the location specified. Target directories or files are NOT restored to the alternate location specified.

⦿ **Resolve Link**

This option must be used in conjunction with the Follow Link option. When this option is enabled, the symbolic link, as well as the directories and files that the symbolic link links to will also be restored in the alternate location you have chosen. That means the symbolic link will point to the alternate location instead of the original location.

The table below summarizes the behaviors when a restore is performed with this option turned on and off.

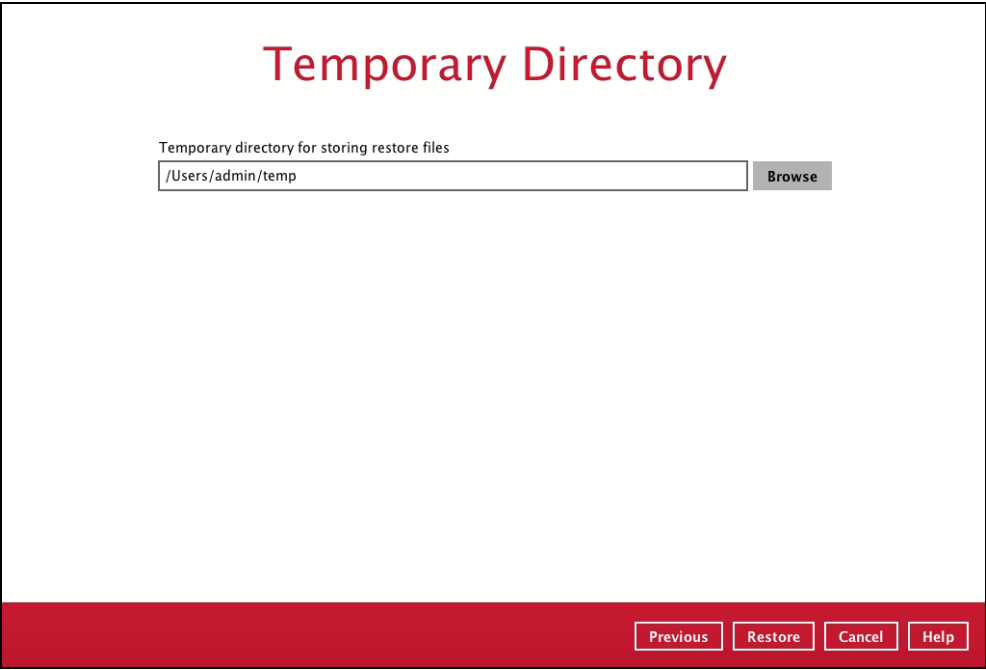
Resolve Link	Behavior
Enabled	Symbolic link is restored to the alternate location specified, with its target directories and files also restored to the same location in their relative path. Target of the link is updated to the new relative path. In other word, the link now points to the new alternate location.
Disabled	Symbolic link is restored to the alternate location specified, with its target directories and files also restored to the same location in their relative path. However, target of the link is NOT updated to the new relative path. In other word, the link still points to the original location.

⦿ **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.

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

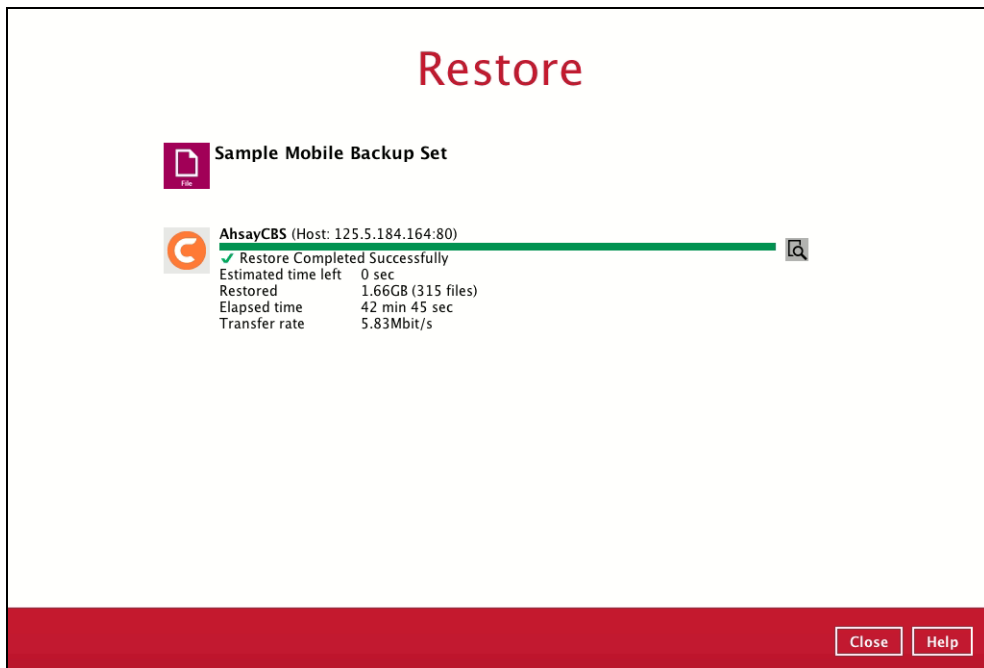
7. Select the temporary directory for storing temporary files, such as delta files, when they are being merged. By default, the temporary files are stored under the temp directory of the user profile directory. In case the same directory path does not exist in the computer you are running AhsayOBM, you have to click **Browse** to define a new location for storing the temporary files. Otherwise, you will not be able to perform a restore.




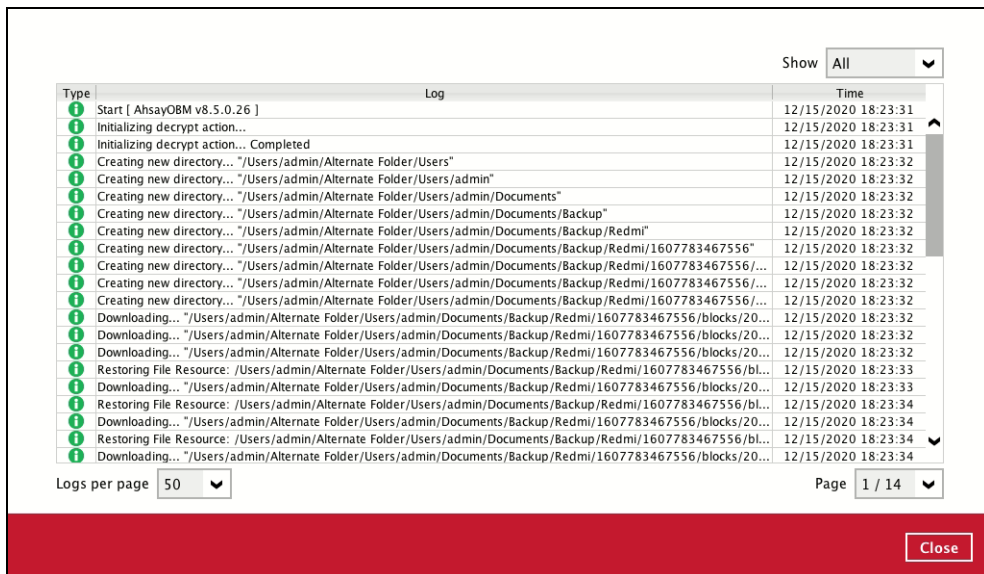
8. Click **Restore** to start the restore. The status will be shown.



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.

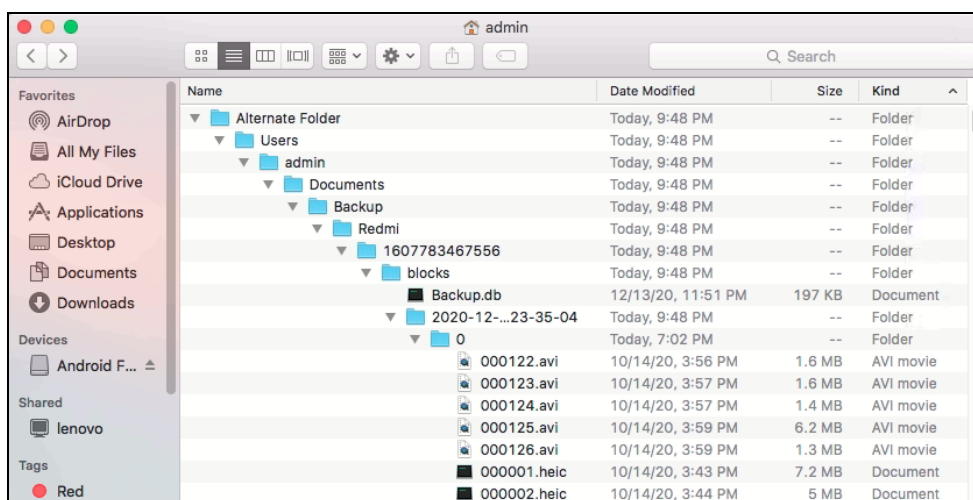


11. These are the steps to restore the restored data from the alternate location to your mobile device.

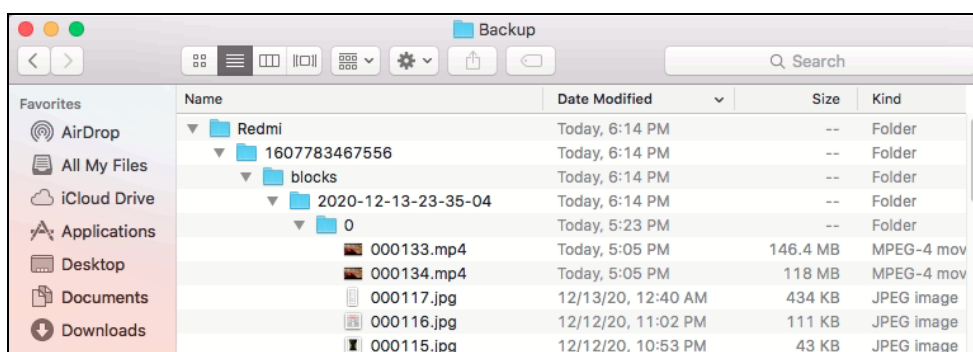
Option 1: Copy the restored data from alternate location to original location which is the **backup destination for your mobile device**.

Example:

Alternate location: **/Users/admin/Alternate Folder**



Original location: **/Users/admin/Documents/Backup**



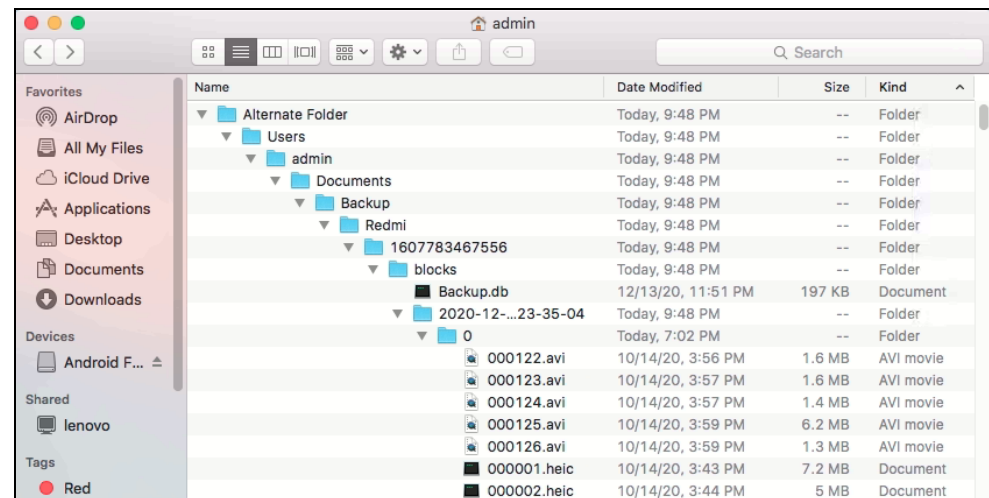
You can now use the Ahsay Mobile app to restore the photos and videos back to your mobile device.

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

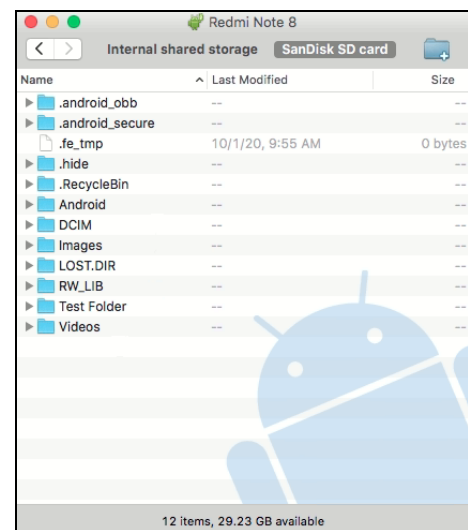
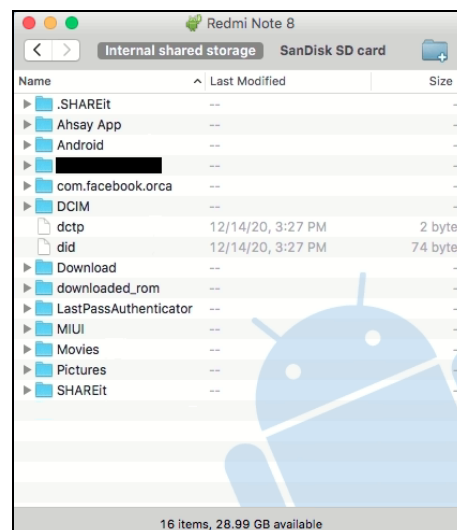
Examples:

- 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: **/Users/admin/Alternate Folder**

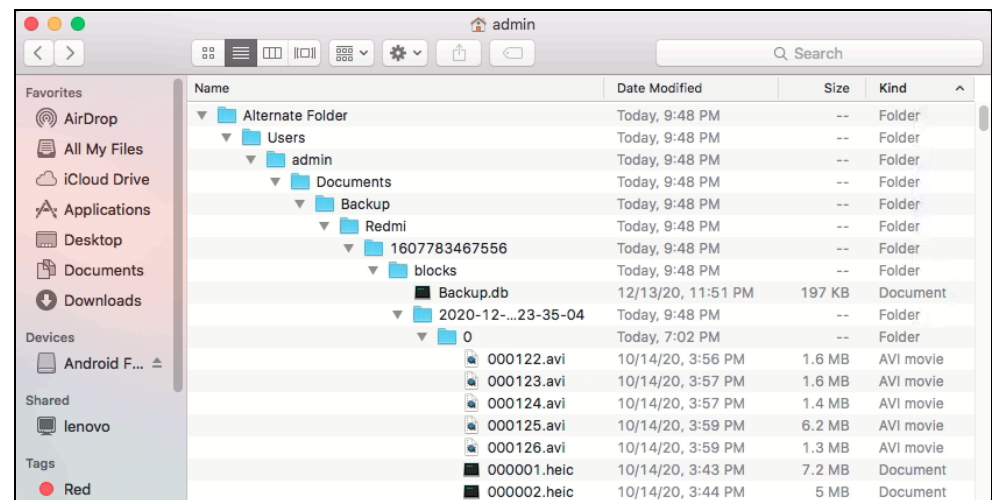


Mobile device storage: Redmi Note 8 Internal storage and SD Card

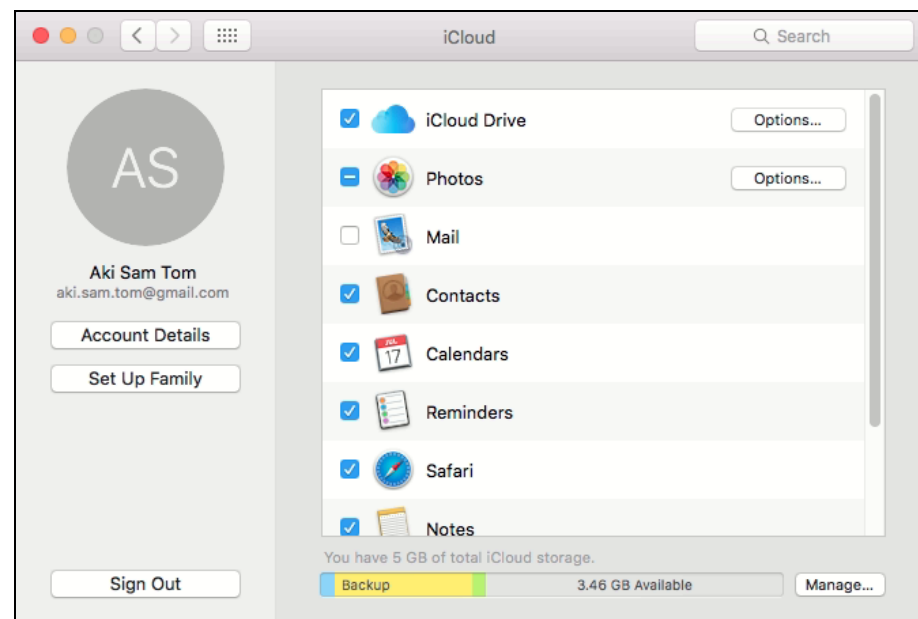


- ▶ For an iOS device, you need to transfer the restored data from the alternate location to iCloud.

Alternate location: **/Users/admin/Alternate Folder**



Upload to iCloud.



13 Contact Ahsay

13.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the Partner Portal:

<https://www.ahsay.com/partners/>

Also use the Ahsay Wikipedia for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:

<https://wiki.ahsay.com/>

13.2 Documentation

Documentations for all Ahsay products are available at:

https://www.ahsay.com/jsp/en/downloads/ahsay-downloads_documentation_guides.jsp

You can send us suggestions for improvements or report on issues in the documentation by contacting us at:

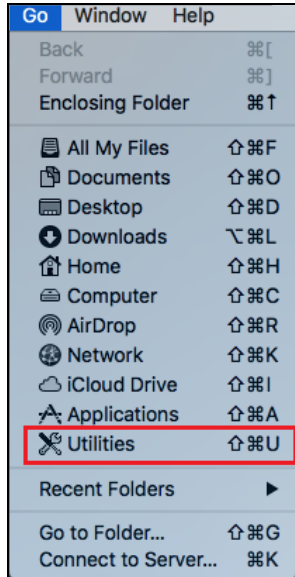
<https://www.ahsay.com/partners/>

Please specify the specific document title as well as the change required/suggestion when contacting us.

Appendix

Appendix A: Uninstall AhsayOBM

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



2. Double click the Terminal.app icon.



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

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

4. Use the command highlighted in **red** to enter the AhsayOBM folder.

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

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

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

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

```
#Shutdown Scheduler for Ahsay Online Backup Manager  
  
#Wait 5 seconds before Scheduler exits  
  
#Kill Process by Image Name:/Applications/AhsayOBM.app/jvm/bin/bJW
```

```
#Ignore Process by Image Name:

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

#Ignore Process by Image Name:

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

#Ignore Process by Image Name:

#Remove LaunchDaemons for com.AhsayOBM.scheduler from service

#Remove AhsayOBM from Your Mac OS

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

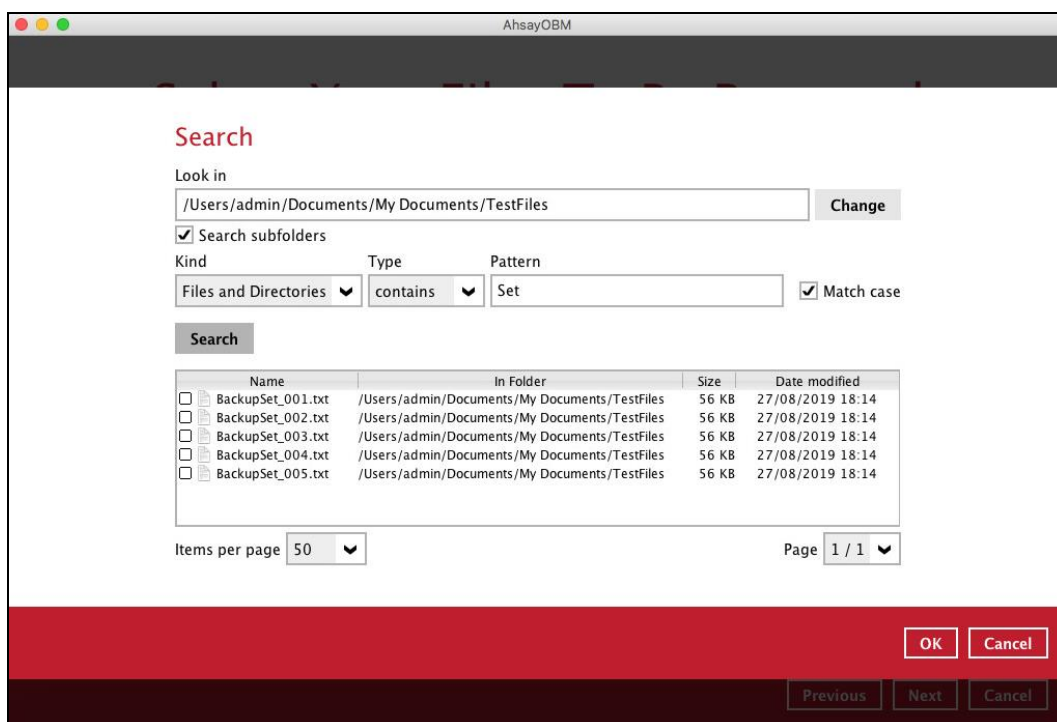
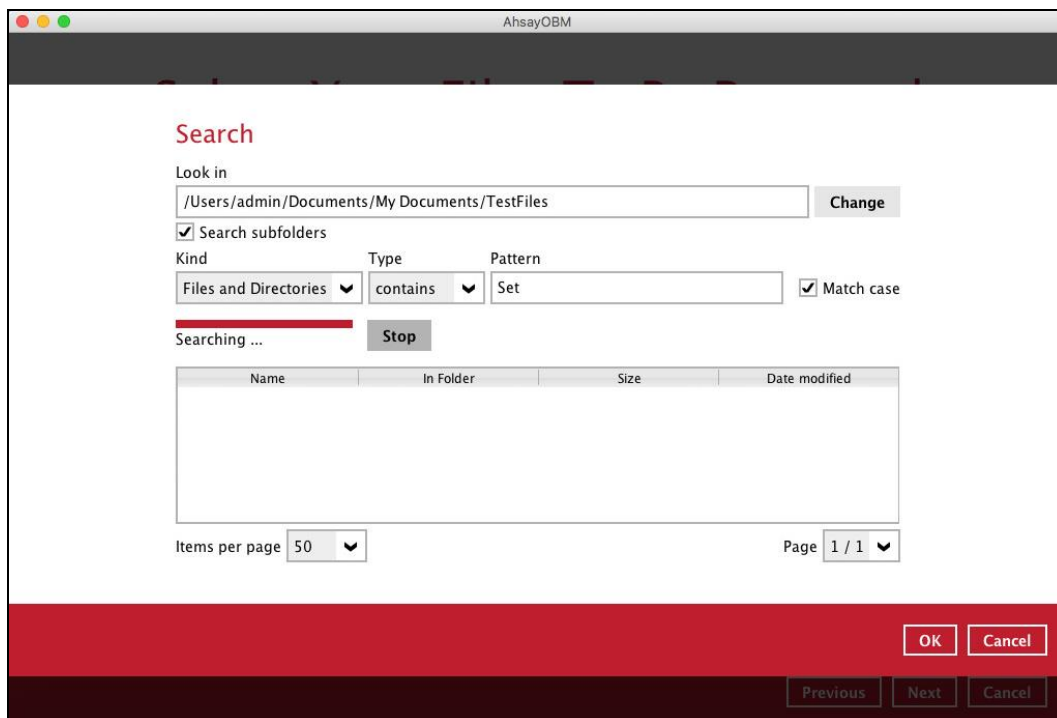
Appendix B: Example Scenarios for Restore Filter

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

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

Follow the step-by-step procedure indicated on [Restore Filter](#).

The screenshot shows the AhsayOBM Search dialog box. The title bar reads "AhsayOBM". The main heading is "Search". Below it, the "Look in" field contains the path "/Users/admin/Documents/My Documents/TestFiles" with a "Change" button to its right. A checked checkbox labeled "Search subfolders" is present. The "Kind" dropdown is set to "Files and Directories", the "Type" dropdown is set to "contains", and the "Pattern" field contains "Set". A checked checkbox labeled "Match case" is also visible. A "Search" button is located below these settings. Below the search settings is a table with four columns: "Name", "In Folder", "Size", and "Date modified". The table is currently empty. At the bottom left, there is a label "Items per page" followed by a dropdown menu showing "50". At the bottom right, there is a label "Page" followed by a dropdown menu showing "-". At the very bottom, there are two rows of buttons: the top row has "OK" and "Cancel" buttons, and the bottom row has "Previous", "Next", and "Cancel" buttons.



Explanation:

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

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

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

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

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

Follow the step-by-step procedure indicated on [Restore Filter](#).

Search

Look in
/Users/admin/Documents/My Documents/TestFiles Change

☒ Search subfolders

Kind: Files only ▼ Type: starts with ▼ Pattern: A ▼ ☒ Match case

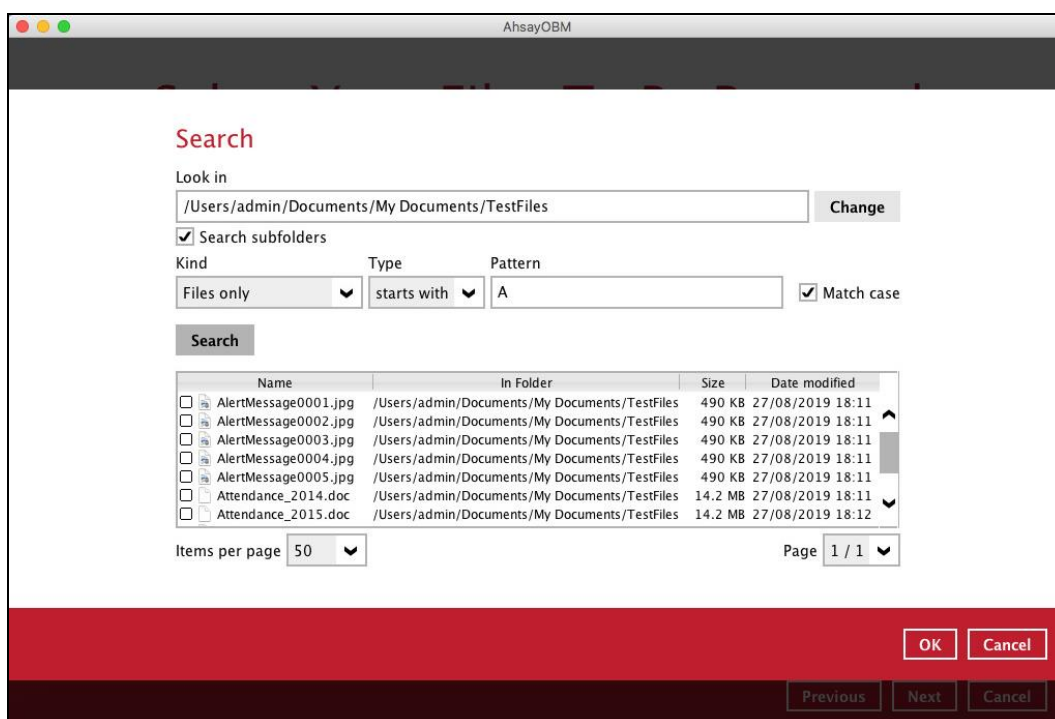
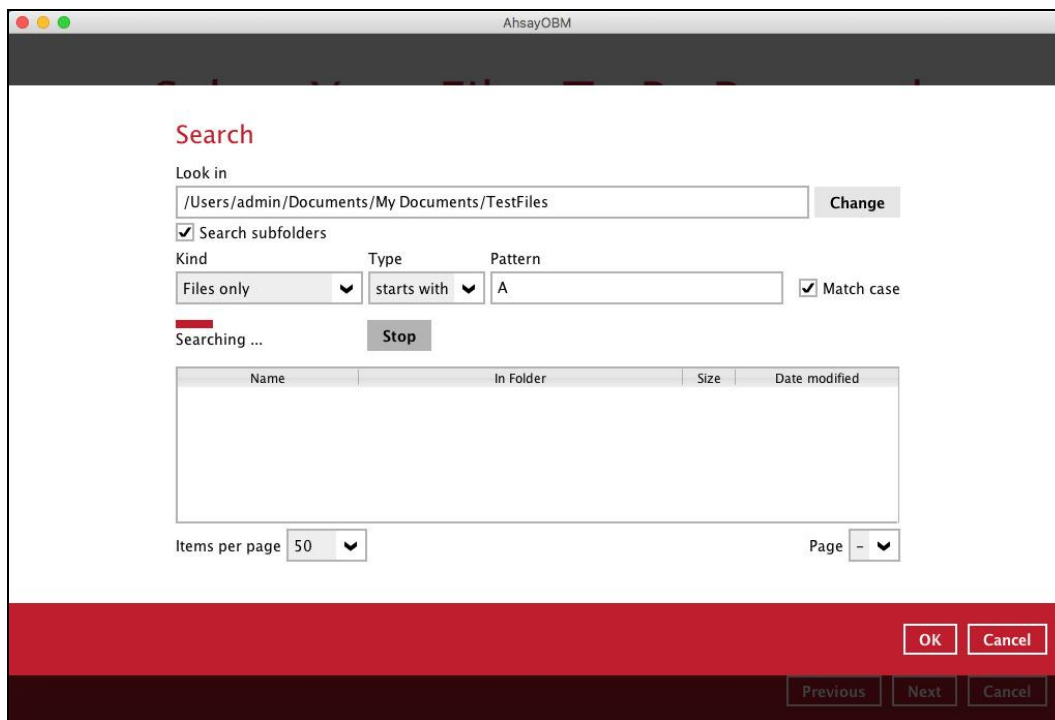
Search

Name	In Folder	Size	Date modified
------	-----------	------	---------------

Items per page: 50 ▼ Page: 1 ▼

OK Cancel

Previous Next Cancel



Explanation:

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

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

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

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

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

Follow the step-by-step procedure indicated on [Restore Filter](#).

AhsayOBM

Search

Look in

Change

☒ Search subfolders

Kind

Type

Pattern

Files and Directories

ends with

g

☒ Match case

Search

Name	In Folder	Size	Date modified
------	-----------	------	---------------

Items per page

50

Page

-

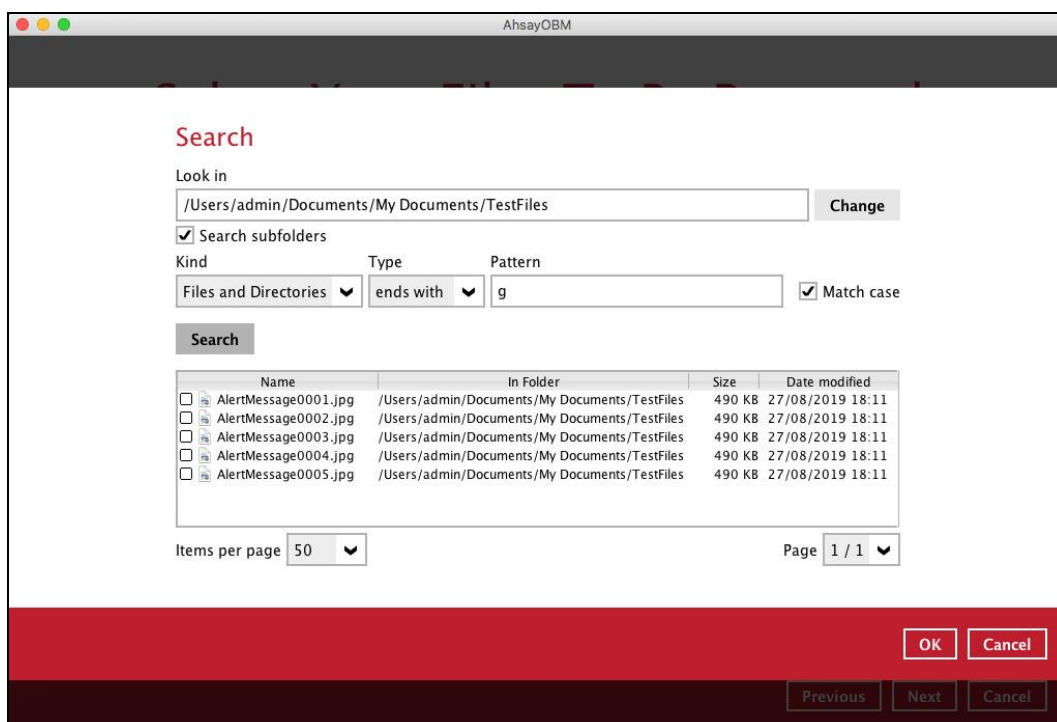
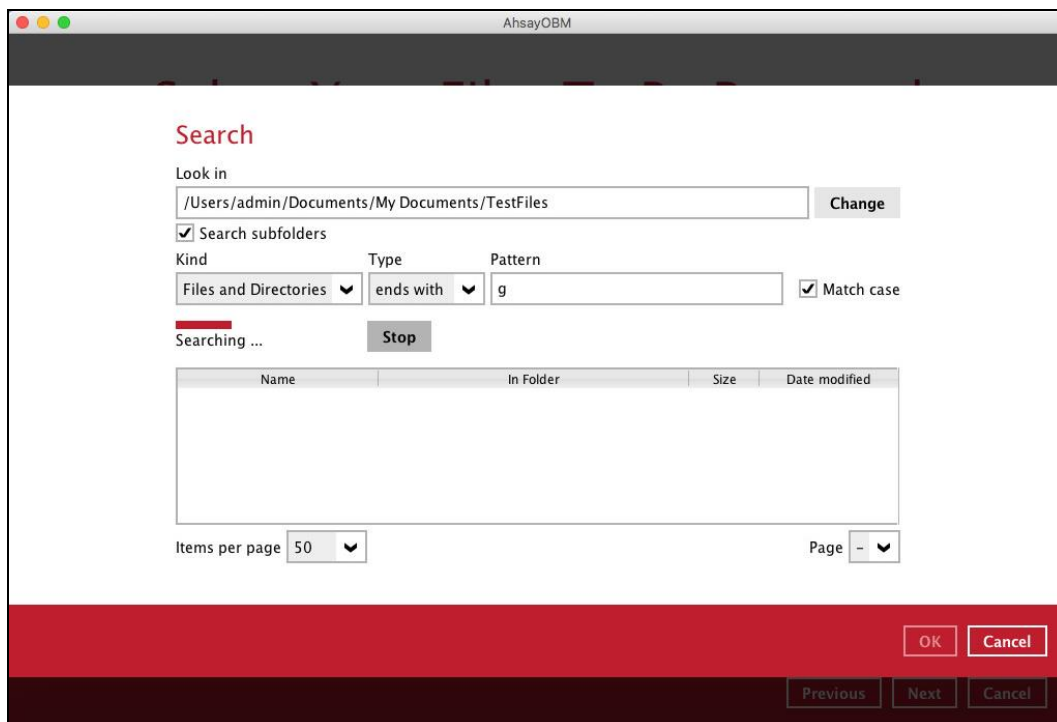
OK

Cancel

Previous

Next

Cancel



Explanation:

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

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

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

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

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

Follow the step-by-step procedure indicated on [Restore Filter](#).

Search

Look in
/Users/admin/Documents/My Documents/TestFiles Change

☒ Search subfolders

Kind: Files and Directories Type: exact Pattern: SpreadSheet_05.xlsx ☒ Match case

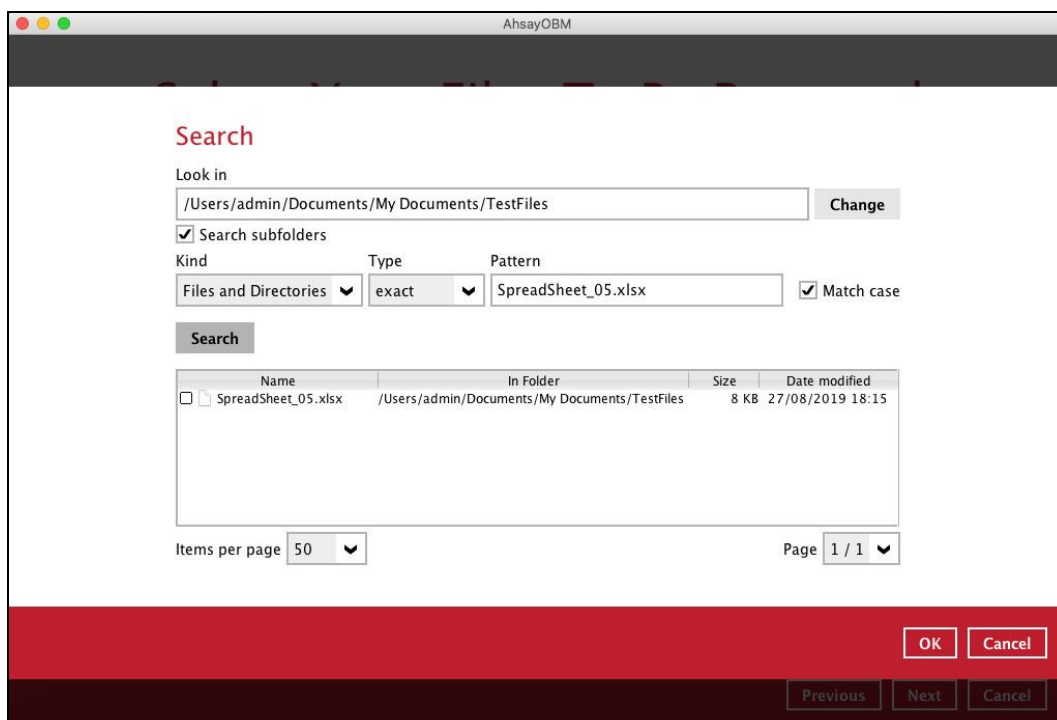
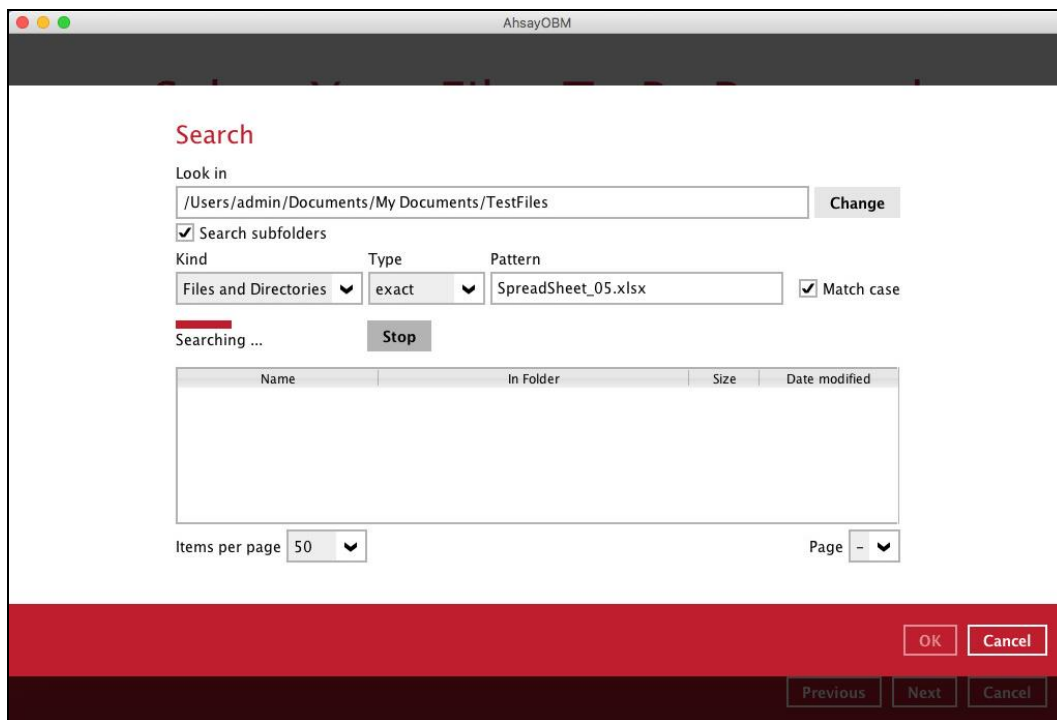
Search

Name	In Folder	Size	Date modified
------	-----------	------	---------------

Items per page: 50 Page: 1

OK Cancel

Previous Next Cancel



Explanation:

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

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

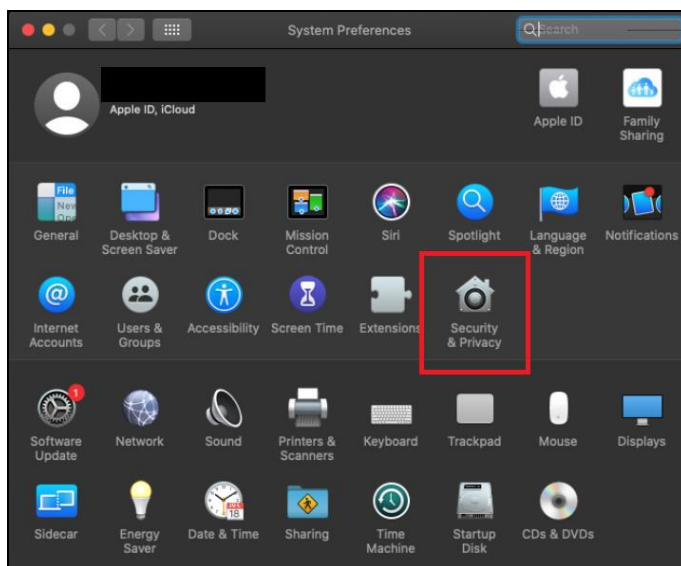
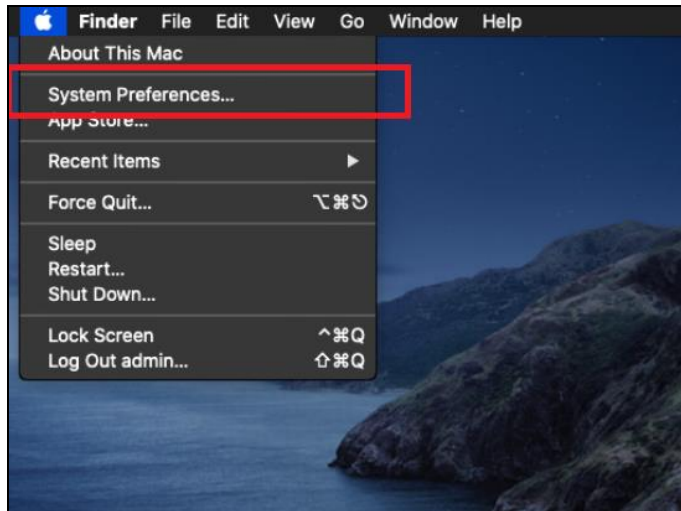
The restore filter setting includes the Search subfolder and Match case set to true. Meaning, the filter will include all available subfolders in \TestFiles upon searching. And it will strictly search only the specified pattern and case which starts with 'SpreadSheet_05.xlsx'.

Appendix C: Setting up Full Disk Access Permission

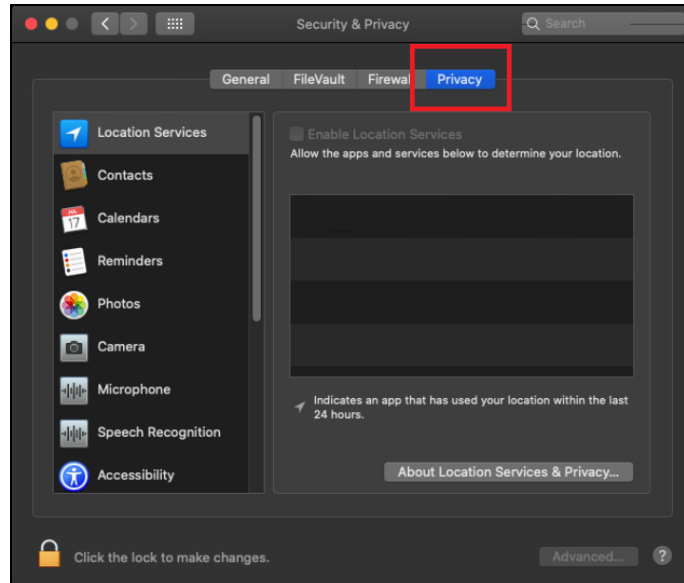
What is Full Disk Access? Full Disk Access is a new security feature in MacOS 10.15 or higher that requires some applications to be given full permission to access your protected files and have certain administrative settings available.

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

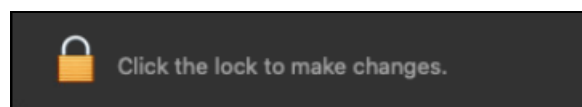
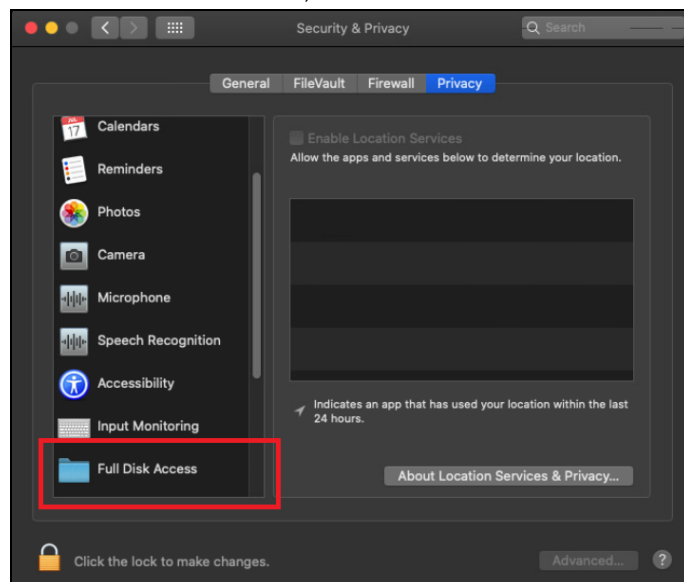
1. Open **System Preferences > Security & Privacy**.



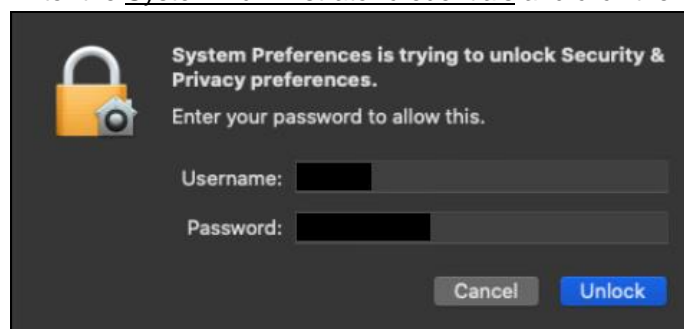
2. Select the **Privacy** tab.



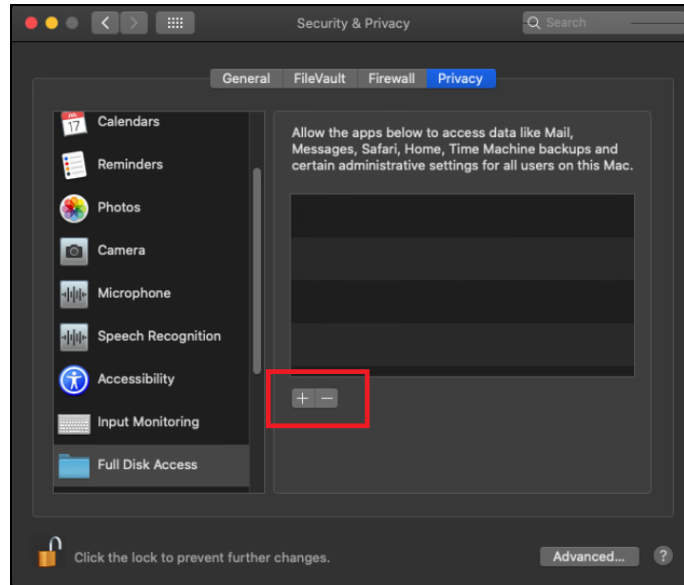
3. Select **Full Disk Access**, then click the lock icon.



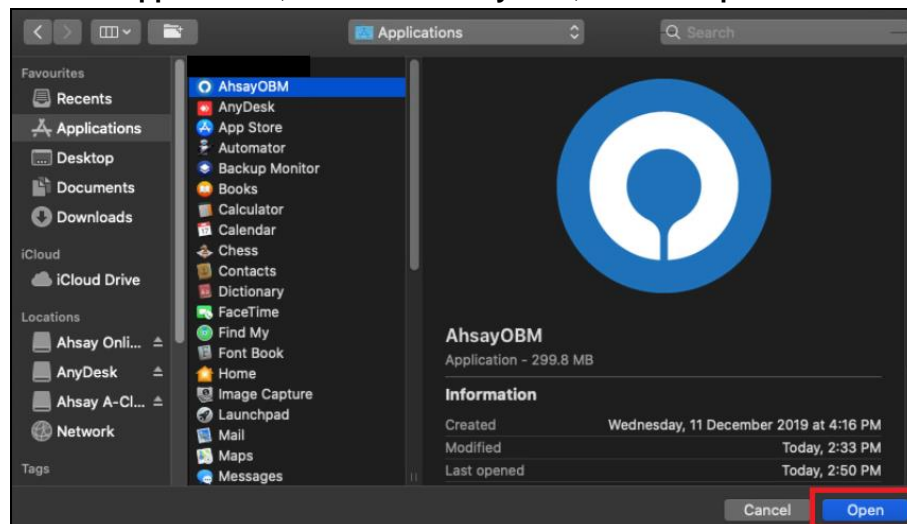
4. Enter the System Administrator credentials and click the **Unlock**.



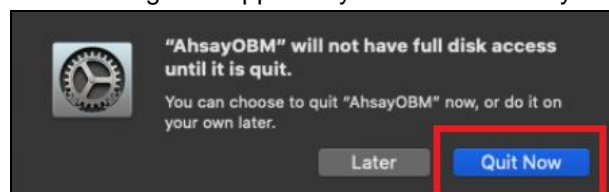
5. Click the plus icon.



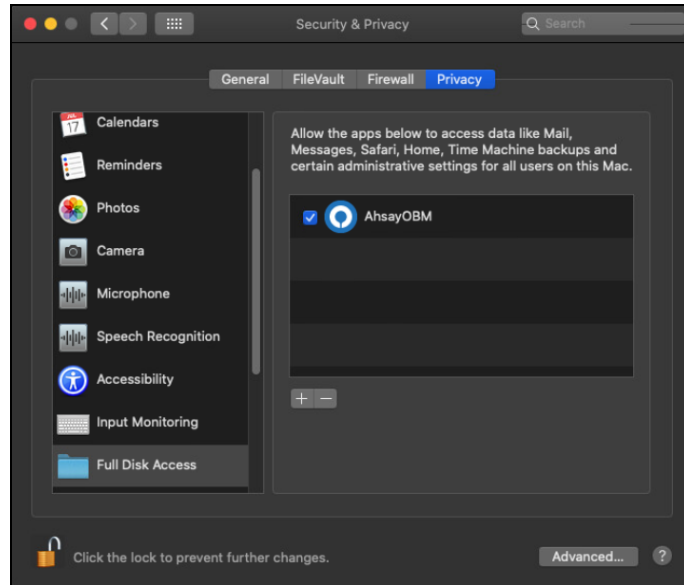
6. Click the **Applications**, then select **AhsayOBM**, and click **Open**.



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



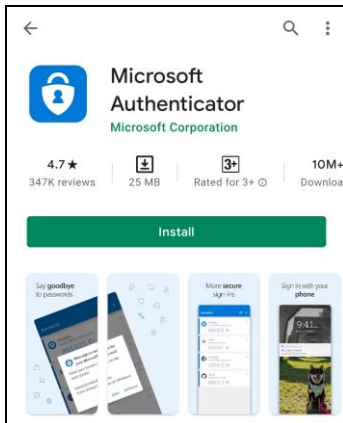
7. AhsayOBM has now Full Disk Access.



Appendix D: Example Registration of Time-based One-Time Password (TOTP) Authenticator app in Ahsay Mobile app

The following is an example of how to register a third-party TOTP authenticator app in the Ahsay Mobile app. We will use Microsoft Authenticator app as an example for our third-party TOTP Authenticator app.

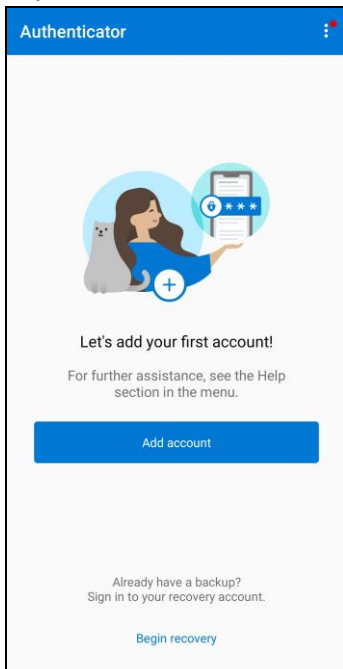
1. Download and install the Microsoft Authenticator from the Play Store for android devices or the App Store for iOS devices.



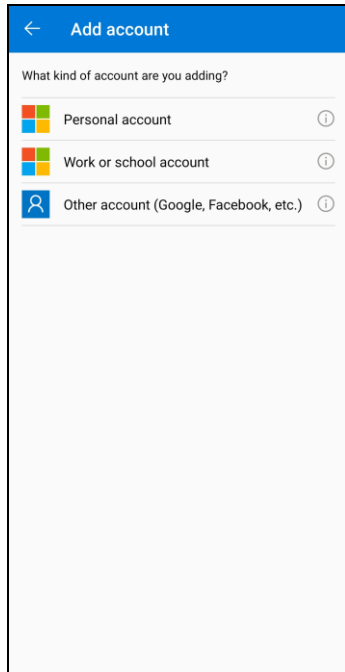
2. Launch the Microsoft Authenticator app.



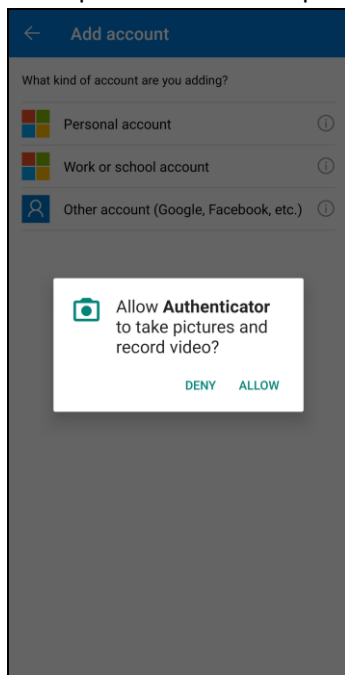
3. Tap **Add account**.



4. Select **Other account (Google, Facebook, etc.)**.



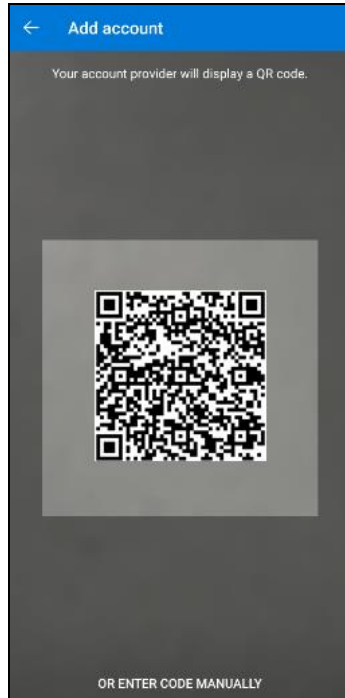
5. Allow permission to take pictures and record video.



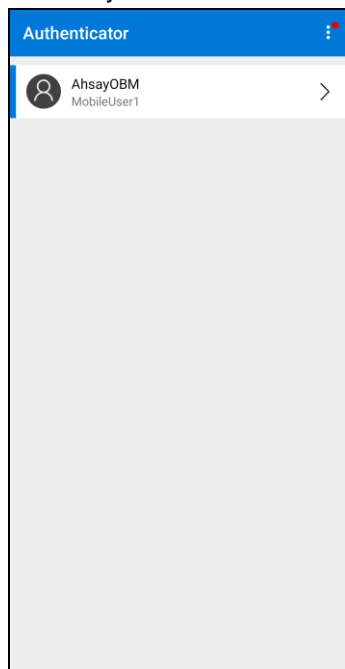
6. Setup the account. Select from the following methods: Scan the QR code or Enter code manually.

Method 1: Scan the QR code

- a. Scan the QR code on AhsayOBM.



- b. Account is successfully added to Microsoft Authenticator and registered the mobile device on AhsayOBM.

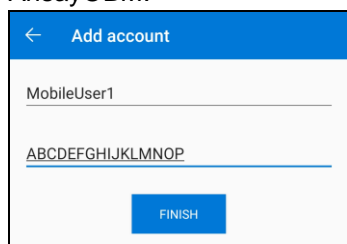


Method 2: Enter Code Manually

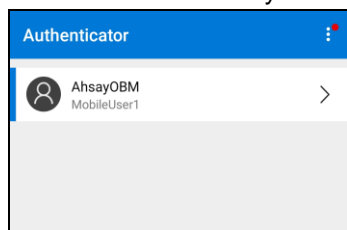
- i. Tap **OR ENTER CODE MANUALLY**.



- ii. Enter the account name and the key which is the Secret Key that is provided by AhsayOBM.



- iii. Account is successfully added to Microsoft Authenticator.



- iv. In AhsayOBM, enter the display name and one-time password generated by the Microsoft Authenticator app. Click Next to proceed.



Secret Key: 6FHC BRJM 7P33 HRXW

Enter a display name for user profile.

MobileUser1

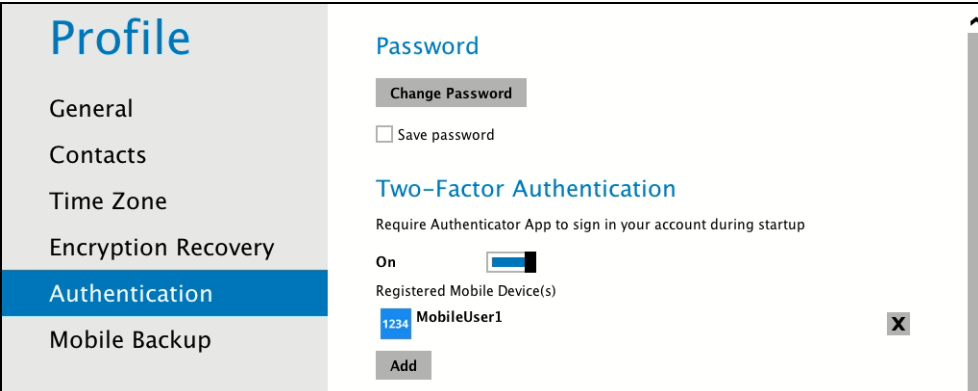
Enter the one-time password generated by Authenticator App.

386662 (00:00:18)

[Using Ahsay Mobile](#)

Skip Device Pairing Next

- v. Mobile device is successfully registered on AhsayOBM.



Profile

- General
- Contacts
- Time Zone
- Encryption Recovery
- Authentication**
- Mobile Backup

Password

[Change Password](#)

☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

On ☒

Registered Mobile Device(s)

1234	MobileUser1	X
------	-------------	-------------------

[Add](#)