

Ahsay Online Backup Manager v9

Quick Start Guide for macOS

Ahsay Systems Corporation Limited

21 March 2023

Copyright Notice

© 2023 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 365 are registered trademarks of Microsoft Corporation.

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

OpenJDK is a registered trademark of Oracle America, Inc.

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

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

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

Ubuntu is a registered trademark of Canonical Ltd.

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

Rocky is a registered trademark of Rocky Brands.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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 | Version |
|------------------|--|---------|
| 25 January 2022 | <ul style="list-style-type: none">▪ Ch. 9.5 – added Deduplication▪ Ch. 12.2 – added Migrate Data | 9.1.0.0 |
| 7 March 2022 | <ul style="list-style-type: none">▪ Ch. 12.2 – updated note for Migrate Data | 9.1.0.0 |
| 6 May 2022 | <ul style="list-style-type: none">▪ Ch. 9.5 – additional note in Command Line Tool and Temporary Directory | 9.1.4.0 |
| 8 August 2022 | <ul style="list-style-type: none">▪ Ch. 3.10 – added non-compressible file list | 9.1.0.0 |
| 3 November 2022 | <ul style="list-style-type: none">▪ Ch. 9.5 – updated Deduplication screenshots and block size choices; added backup schedule priority; added Recycle Bin instructions▪ Ch. 9.9.1 – updated screenshots and added Delete corrupted data blocks permanently description▪ Ch. 13.2 – updated screenshots due to Show backup job(s) outside retention area checkbox | 9.5.0.0 |
| 22 November 2022 | <ul style="list-style-type: none">▪ Ch. 9.5 – fixed typo in Recycle Bin | 9.5.0.0 |
| 27 January 2023 | <ul style="list-style-type: none">▪ Ch. 13.2 – updated restore instructions | 9.5.2.0 |
| 21 March 2023 | <ul style="list-style-type: none">▪ Ch. 3.3 – updated full disk access requirements▪ Appendix C – updated instructions on how to add full disk access | 9.5.4.0 |

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 | 8 |
| 2.1 | Backup Software Version Requirement..... | 8 |
| 2.2 | Network Connection..... | 8 |
| 2.3 | Android and iOS Version Requirement | 8 |
| 3 | Requirements for AhsayOBM on macOS | 9 |
| 3.1 | Hardware Requirements | 9 |
| 3.2 | Software Requirements | 9 |
| 3.3 | Full Disk Access Permission | 9 |
| 3.4 | Installation on Root Drive..... | 10 |
| 3.5 | Two-Factor Authentication Requirements | 10 |
| 3.6 | Mobile Backup Requirements | 10 |
| 3.7 | Firewall Settings | 11 |
| 3.8 | Network Bandwidth..... | 11 |
| 3.9 | ARM (M1) CPU..... | 11 |
| 3.10 | Limitations | 11 |
| 3.11 | Best Practices and Recommendations..... | 12 |
| 4 | Get Started with AhsayOBM | 13 |
| 5 | Download and Install AhsayOBM..... | 14 |
| 5.1 | Download AhsayOBM..... | 15 |
| 5.2 | Install AhsayOBM | 16 |
| 5.2.1 | Online Installation using DMG online installer..... | 16 |
| 5.2.2 | Offline Installation using TAR GZ offline installer | 21 |
| 5.3 | AhsayOBM Services..... | 26 |
| 5.3.1 | Option 1: Stop and Start | 27 |
| 5.3.2 | Option 2: Stop and Start | 27 |
| 5.4 | RunLevel Symlink Check | 29 |
| 5.5 | Mobile Backup Server (MBS) Status Check and Ahsay Mobile app Connection Check..... | 30 |
| 6 | Register device for 2FA in AhsayOBM..... | 33 |

| | | |
|----------|---|-----------|
| 6.1 | Using Ahsay Mobile Authenticator | 33 |
| 6.1.1 | Without Mobile Add-on Module..... | 33 |
| 6.1.2 | With Mobile Add-on Module..... | 45 |
| 6.2 | Using Microsoft Authenticator | 51 |
| 6.3 | Using Google Authenticator | 59 |
| 7 | Logging in to AhsayOBM | 66 |
| 7.1 | Login to AhsayOBM without 2FA | 66 |
| 7.2 | Login to AhsayOBM with 2FA using Ahsay Mobile Authenticator | 68 |
| 7.3 | Login to AhsayOBM with 2FA using Microsoft Authenticator..... | 73 |
| 7.4 | Login to AhsayOBM with 2FA using Google Authenticator..... | 76 |
| 7.5 | Login to AhsayOBM with 2FA using Twilio..... | 79 |
| 8 | Unable to log in to AhsayOBM with 2FA..... | 82 |
| 9 | AhsayOBM Overview..... | 84 |
| 9.1 | Profile | 85 |
| 9.1.1 | General | 85 |
| 9.1.2 | Contacts | 87 |
| 9.1.3 | Time Zone | 89 |
| 9.1.4 | Encryption Recovery | 90 |
| 9.1.5 | Password | 91 |
| 9.1.6 | Authentication..... | 92 |
| 9.1.7 | Security Settings | 102 |
| 9.2 | Language..... | 103 |
| 9.3 | Information..... | 104 |
| 9.4 | Backup..... | 104 |
| 9.5 | Backup Sets | 105 |
| | Backup Set Settings..... | 105 |
| | General | 106 |
| | Source..... | 107 |
| | Backup Schedule | 116 |
| | Destination | 121 |
| | Deduplication | 124 |
| | Retention Policy | 127 |
| | Command Line Tool..... | 139 |
| | Bandwidth Control..... | 143 |
| | Others | 145 |
| 9.6 | Report..... | 148 |

| | | |
|----------------------------------|---|------------|
| 9.6.1 | Backup | 149 |
| 9.6.2 | Restore..... | 153 |
| 9.7 | Restore | 155 |
| 9.8 | Settings..... | 155 |
| 9.8.1 | Proxy | 156 |
| 9.8.2 | Mobile Backup..... | 157 |
| 9.9 | Utilities | 167 |
| 9.9.1 | Data Integrity Check..... | 167 |
| Data Integrity Check Result..... | | 179 |
| Test Mode Confirmation | | 181 |
| 9.9.2 | Space Freeing Up | 183 |
| 9.9.3 | Delete Backup Data..... | 186 |
| 9.9.4 | Decrypt Backup Data..... | 192 |
| 10 | Create a Backup Set | 193 |
| 11 | Overview on Backup Process..... | 202 |
| 11.1 | Periodic Data Integrity Check Process | 203 |
| 11.2 | Backup Set Index Handling Process | 205 |
| 11.2.1 | Start Backup Job | 205 |
| 11.2.2 | Completed Backup Job | 206 |
| 11.3 | Data Validation Check Process..... | 207 |
| 12 | Run Backup Jobs | 208 |
| 12.1 | Login to AhsayOBM | 208 |
| 12.2 | Start a Manual Backup..... | 208 |
| 13 | Restore Data..... | 212 |
| 13.1 | Login to AhsayOBM | 212 |
| 13.2 | Restore Data..... | 212 |
| 13.3 | Restore Filter | 220 |
| 14 | Mobile Backup and Restore to AhsayCBS and Predefined Destination ... | 225 |
| 15 | Contact Ahsay..... | 230 |
| 15.1 | Technical Assistance | 230 |
| 15.2 | Documentation..... | 230 |
| Appendix | | 231 |
| Appendix A: | Uninstall AhsayOBM | 231 |
| Appendix B: | Example Scenarios for Restore Filter..... | 233 |
| Appendix C: | Setting up Full Disk Access Permission | 241 |
| Appendix D: | Create Free Trial Account in AhsayOBM | 245 |

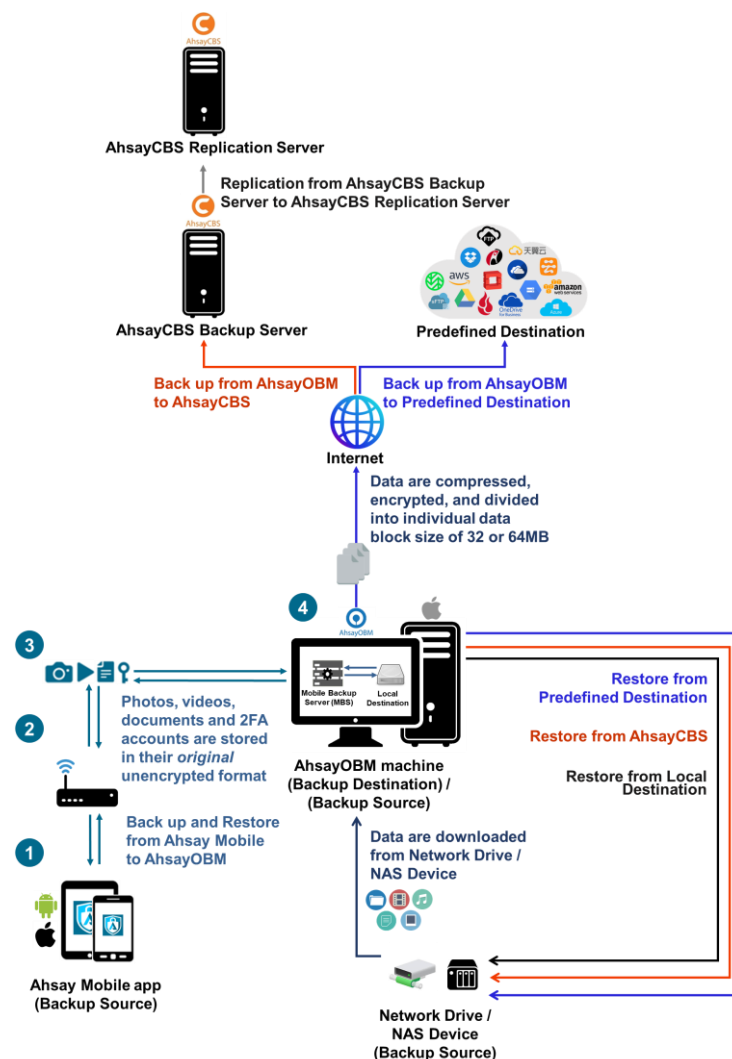
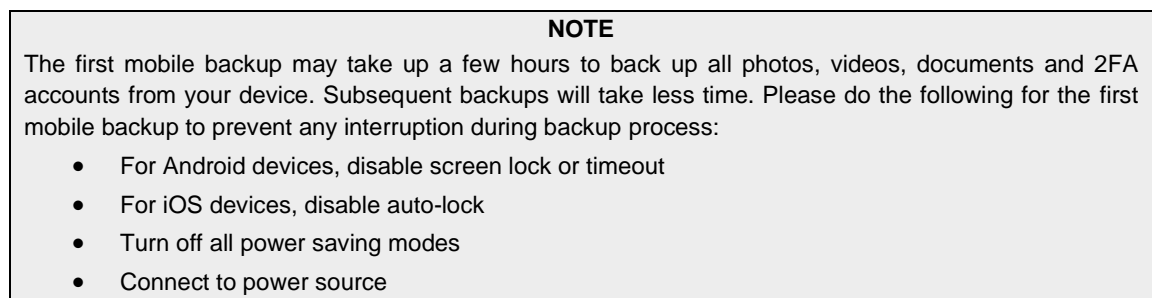
1 Overview

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 and extend protection to both Android and iOS mobile devices, 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

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.

The 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 used by other applications or services, then the MBS will automatically acquire another port(s).


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 get the below Mobile App from App Store. Once installed the Mobile App, launch it and scan the same QR code to complete the device registration.

 Mobile Backup (Add new device for backup without migration)

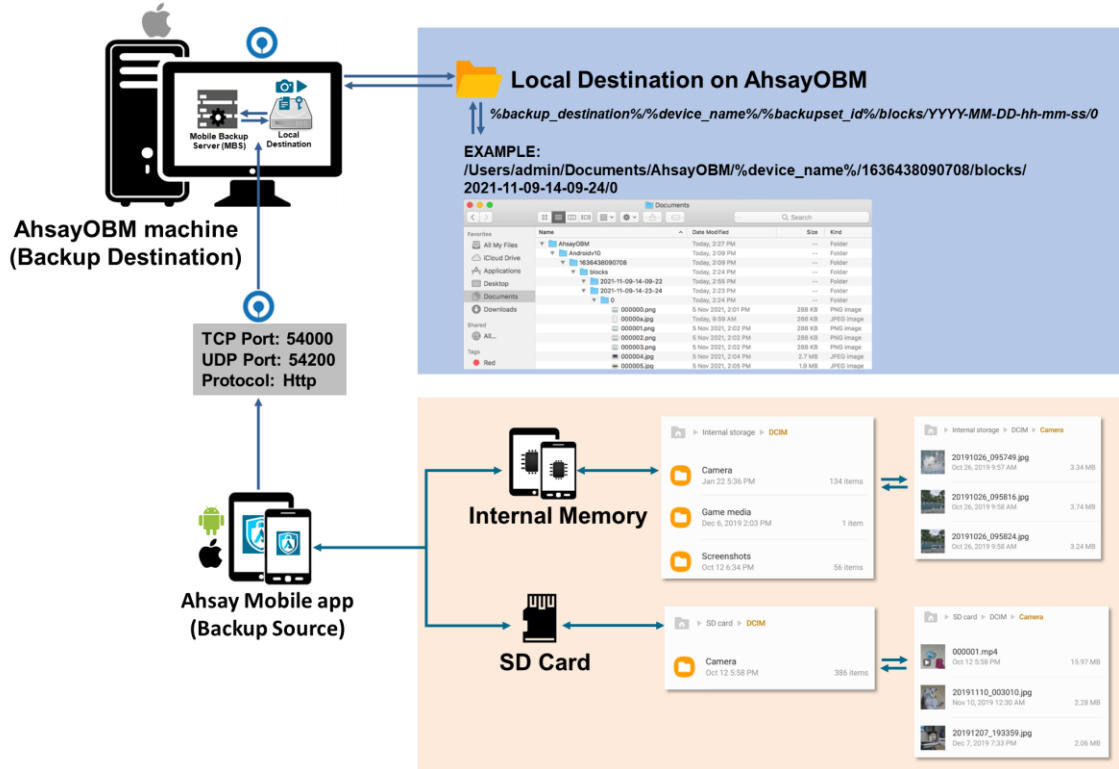




Prerequisites

- Please use the latest Mobile App version
- Please make sure below 2 ports are not blocked by any Firewall settings
TCP Port: 54000
UDP Port: 54200

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

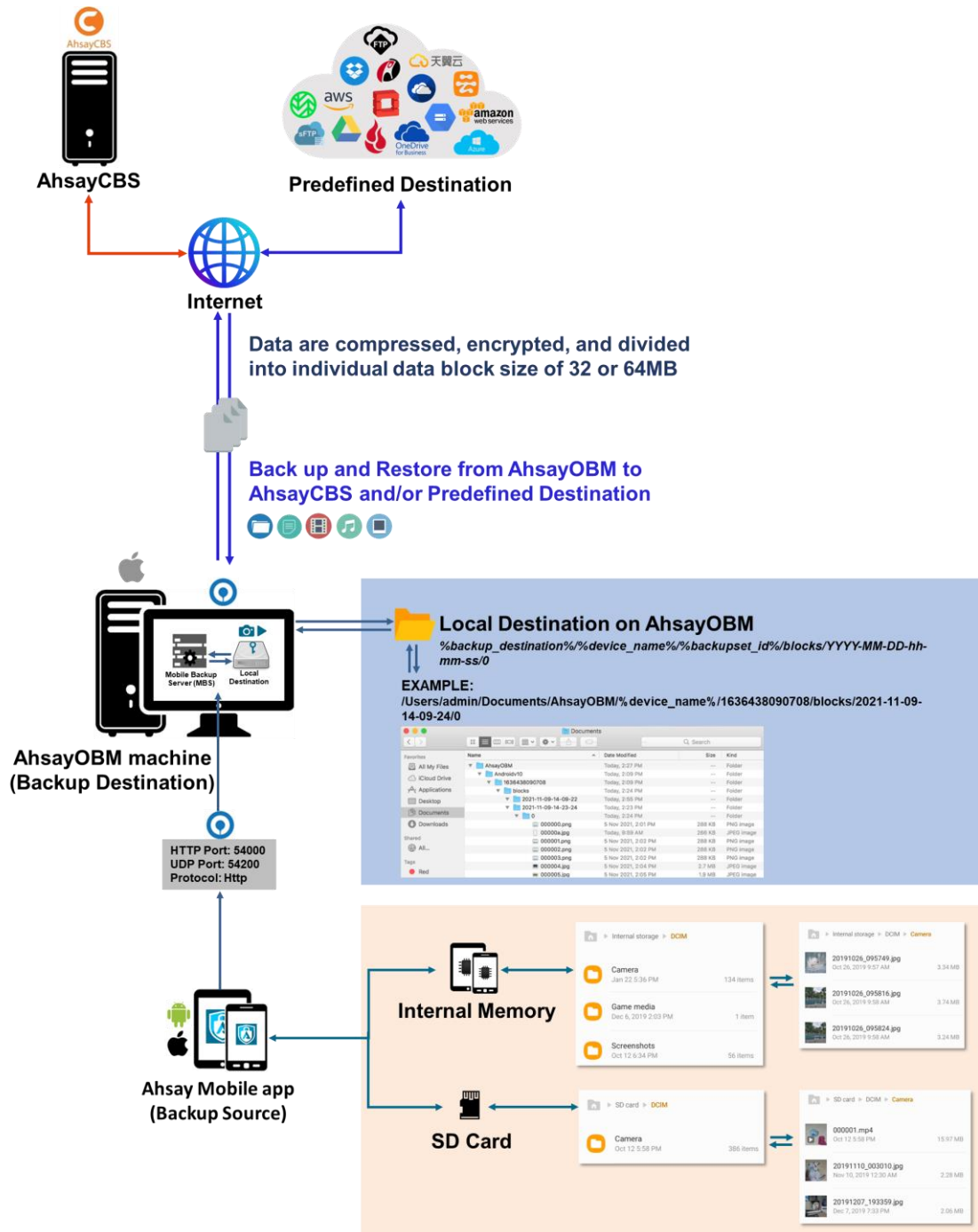


If storage of photos, videos, documents and 2FA accounts to AhsayCBS and/or Predefined Destination is required, then this can be done using AhsayOBM to perform a secondary backup and restore of the photos, videos, documents and 2FA accounts on the local drive to AhsayCBS and/or Predefined Destination.

To back up and restore photos, videos, documents and 2FA accounts from Ahsay Mobile app to AhsayOBM then AhsayCBS and/or Predefined Destination is a two-step process.

1st: Back up photos, videos, documents and 2FA accounts 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. Then back up this backup set to AhsayCBS and/or Predefined Destination.



1.4 Two-Factor Authentication

Two-Factor Authentication (2FA) supports TOTP (Time-based One-time Password) and Push notification authentications 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 the account has Two-Factor Authentication enabled, there will be an additional step necessary to login.

Upon initial login to AhsayOBM, you will have the option to set up Two-Factor Authentication, or you may skip the setup and do it later. If you proceed with the configuration of Two-Factor Authentication, it will be enabled for your account automatically. You may add more than one mobile device for authentication.

For logins with Two-Factor Authentication enabled, the authentication method that will be available will depend on the authenticator app registered during setup.

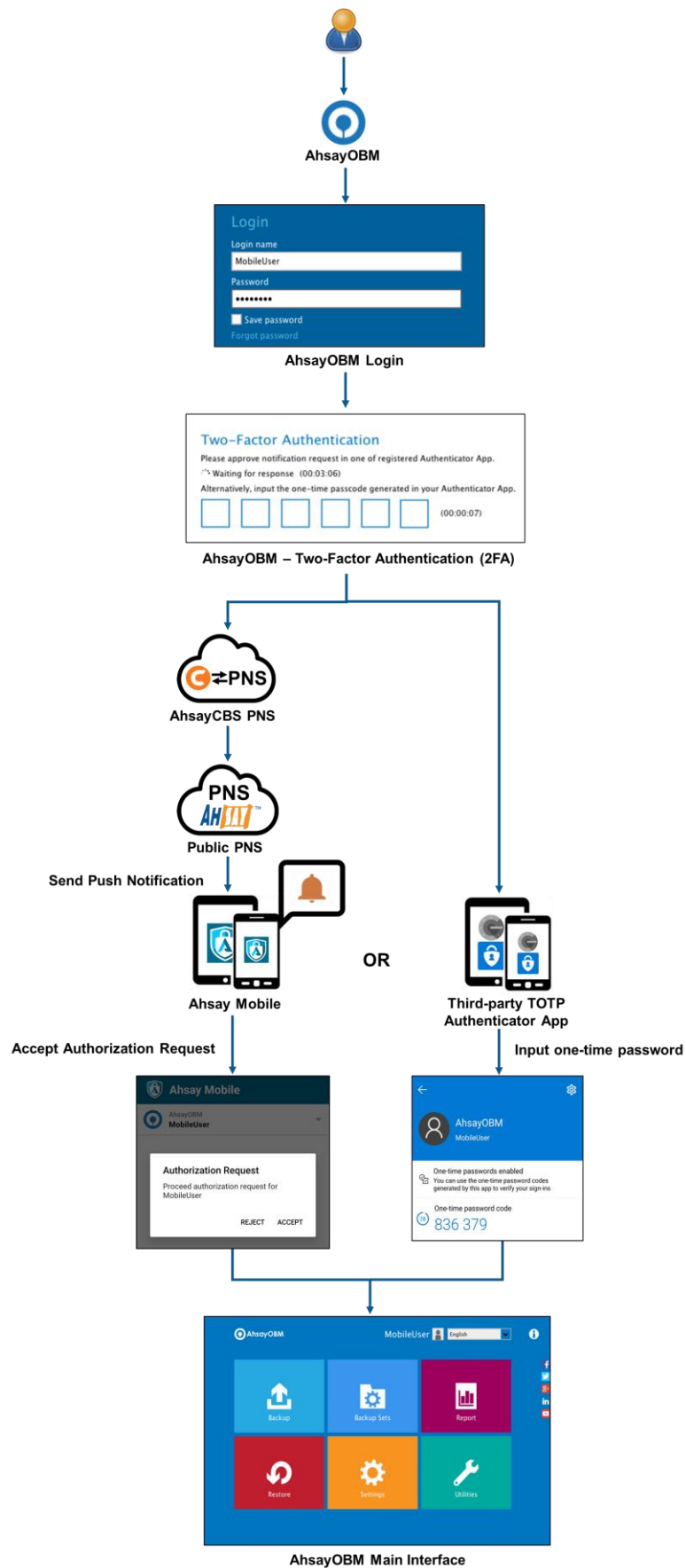
If Ahsay Mobile is used as the authenticator app:

- you will either accept the login request via push notification in the Ahsay Mobile app; or
- enter the one-time password generated in the Ahsay Mobile app

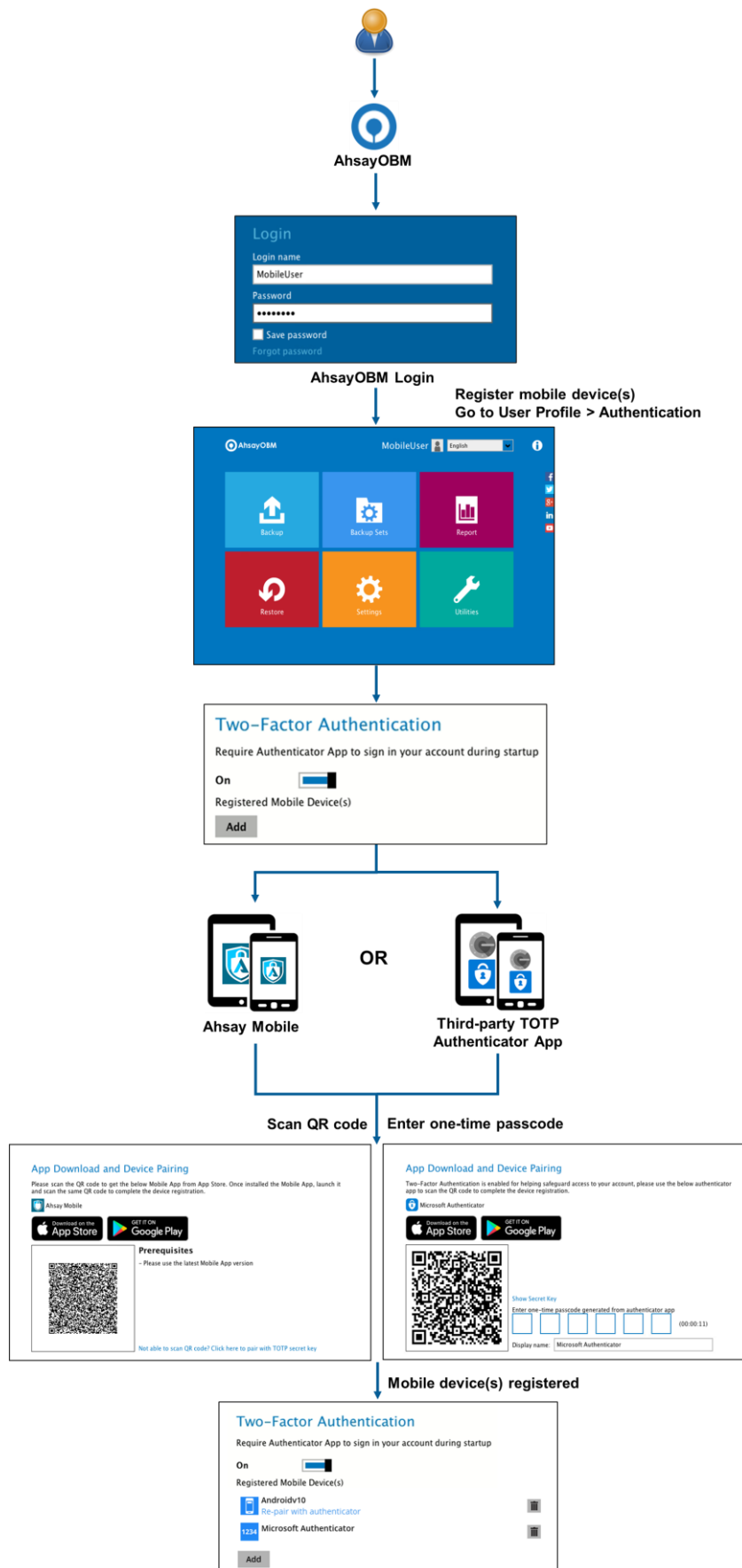
If a third-party authenticator app is used:

- you will enter the one-time password generated in the third-party authenticator (i.e., Authy, Duo, Google Authenticator, Microsoft Authenticator, LastPass Authenticator, iOS 15 Built-in Two-Factor Authenticator, etc.)

This illustrates the user login process for account with Two-Factor Authentication enabled using either the Ahsay Mobile app or a third-party authenticator app.



This illustrates the registration of mobile device(s) for Two-Factor Authentication using either the Ahsay Mobile app or a third-party authenticator app.



2 Requirements for Ahsay Mobile

2.1 Backup Software Version Requirement

- Download and install the latest version of AhsayOBM v9.0.0.0 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 devices, the Android version must be 8 or above.
- For iOS devices, the 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 9.1 or above](#)

3.2 Software Requirements

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

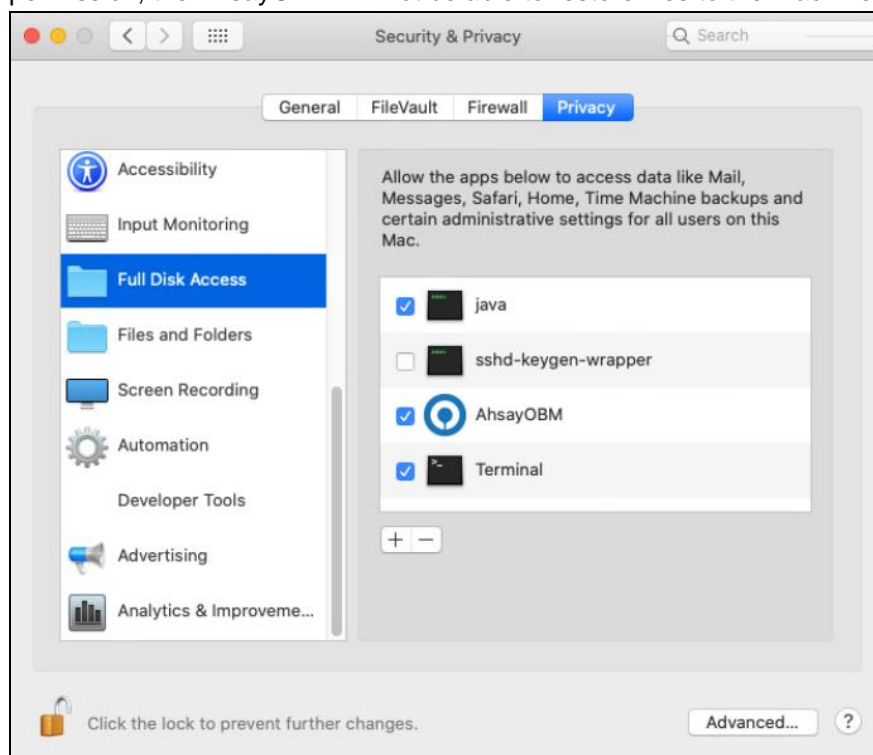
[FAQ: Ahsay Software Compatibility List \(SCL\) for version 9.1 or above](#)

3.3 Full Disk Access Permission

macOS 10.15 or higher "Full Disk Access" permission needs to be granted in:

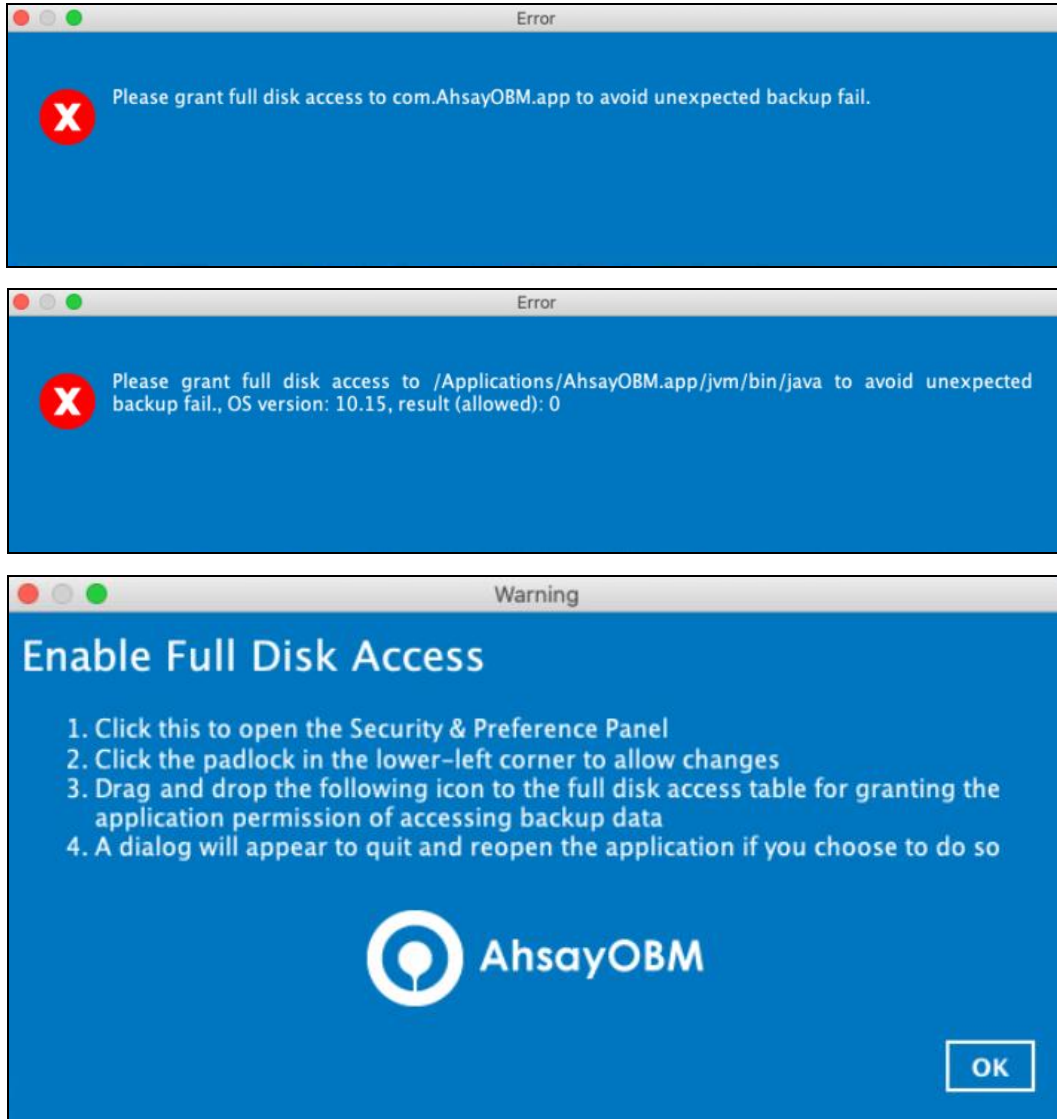
System Preferences > Security & Privacy > Privacy tab to AhsayOBM and java

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, the 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](#).

If AhsayOBM and java does not have “Full Disk Access” permission, upon opening AhsayOBM the following messages will be displayed and it will not open until the “Full Disk Access” permission is granted.



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 **Chapter 2.4** of the [Ahsay Mobile User Guide for Android and iOS](#) 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 **Chapter 2.5** of the [Ahsay Mobile User Guide for Android and iOS](#) for details of the minimum and recommended requirements for installing the Ahsay Mobile app.

3.7 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.

3.8 Network Bandwidth

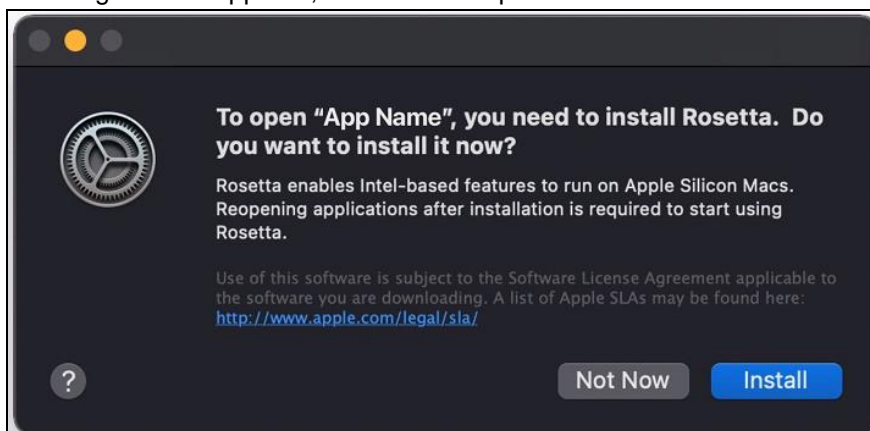
10 Mbps or above connection speed.

3.9 ARM (M1) CPU

For AhsayOBM running on macOS 11 or above on ARM (M1) CPU machine, the installation of Rosetta 2 is required that enables applications built for Intel CPU to run on an ARM (M1) CPU machine:

<https://support.apple.com/en-hk/HT211861>

If AhsayOBM is installed and run for the first time on macOS 11 or above on ARM (M1) CPU machine, there will be a pop-up message that requests installation of Rosetta. When the following window appears, click **Install** to proceed.



3.10 Limitations

- Resource Fork Files – Resource fork files cannot be restored with AhsayOBM installation on macOS 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.

- Non-compressible files – the following is a list of non-compressible files:

| Archive | Audio | | Graphics | Video | | |
|---------|-------|------|----------|-------|-------|-------|
| .7z | .aac | .ac3 | .gif | .3gp | .asf | .avi |
| .bz2 | .aifc | .amr | .jfif | .divx | .ivf | .m1v |
| .gz | .flac | .m4a | .jpeg | .m4v | .mkv | .mov |
| .rar | .mka | .mp2 | .jpg | .mp2v | .mp4 | .mpe |
| .xz | .mp3 | .mpa | .png | .mpeg | .mpg | .mpv2 |
| .zip | .ogg | .ra | .wim | .mts | .qt | .rmvb |
| | .rm | .snd | .wmp | .rv | .smil | .swf |
| | .ssm | .wma | .wmz | .vob | .webm | .wm |
| | | | | .wmd | .wmv | |

3.11 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
- 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 consider 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 six (6) major parts to get you started with using AhsayOBM.

Download and Install

Download and Install AhsayOBM on your macOS machine

Launch the App

Launch and log in to AhsayOBM

Set up 2FA and/or Mobile Backup

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

Create a Backup Set

Create a backup set according to your preference

Run Backup Jobs

Run the backup job 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.



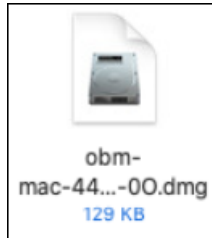
2. In the **macOS** section under the **AhsayOBM** tab of the download page, you can choose between two installation methods:
 - Online installation using DMG online installer
 - Offline installation using TAR GZ offline installer



5.2 Install AhsayOBM

5.2.1 Online Installation using DMG online installer

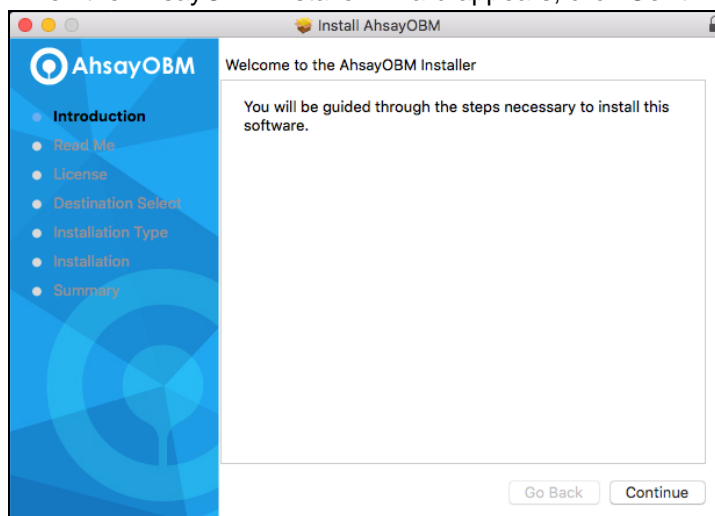
1. Launch the online installation package file you have downloaded from the download section above.



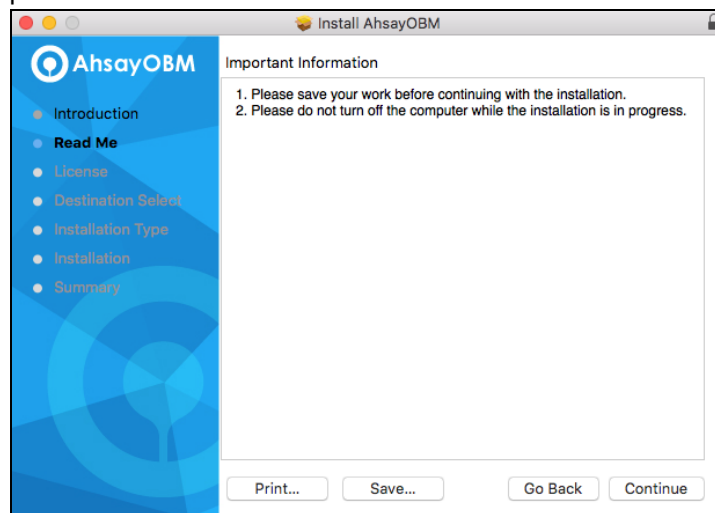
2. The Ahsay Online Backup Manager window will appear. You will see another file named "obm.pkg". Double-click on the "obm.pkg" file.




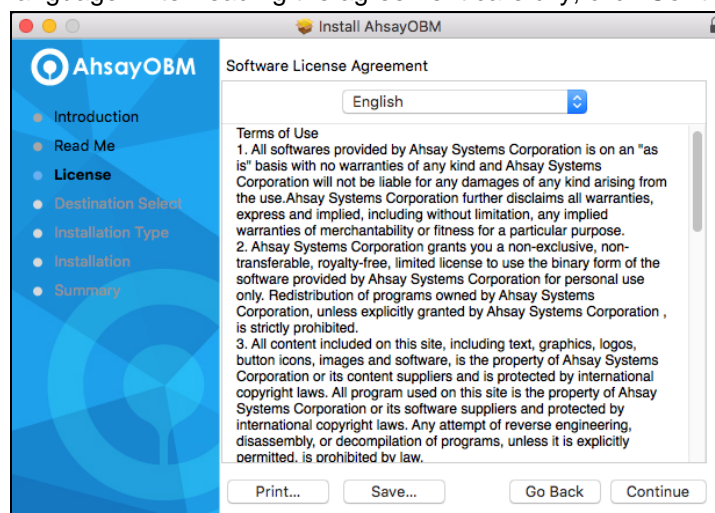
3. When the AhsayOBM Installer wizard appears, click **Continue** to proceed.



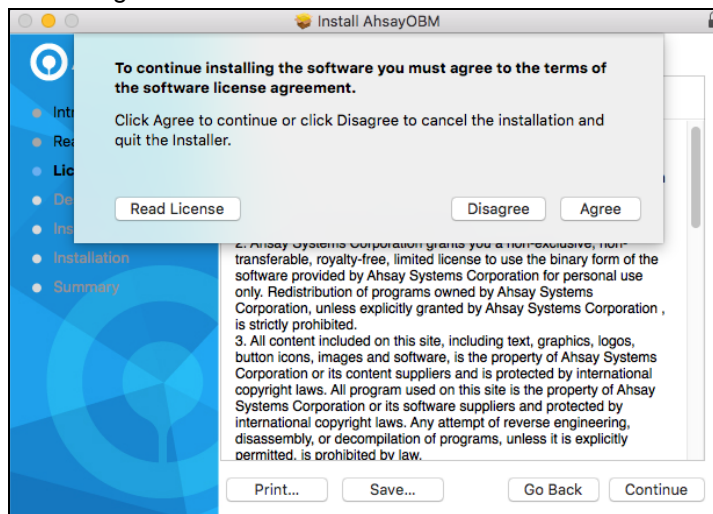
4. When the Important Information screen appears, read the information then click **Continue** to proceed.



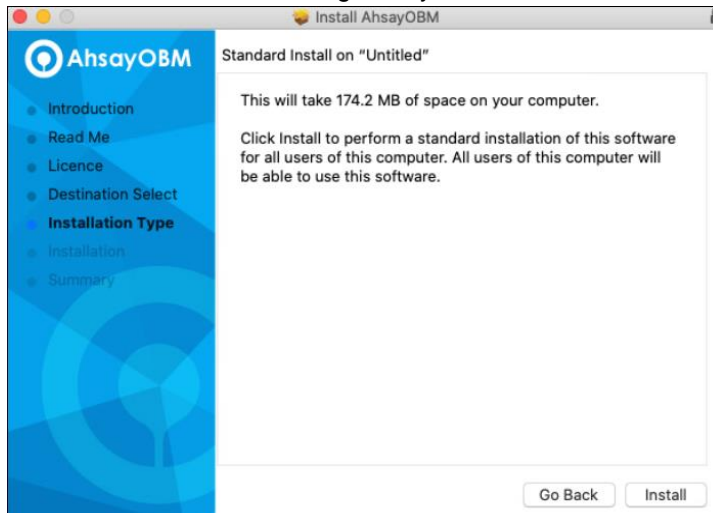
5. When the Software License Agreement appears, the agreement content will be displayed in English by default. If you prefer to read it in a different language, click  to change the language. After reading the agreement carefully, click **Continue** to proceed.



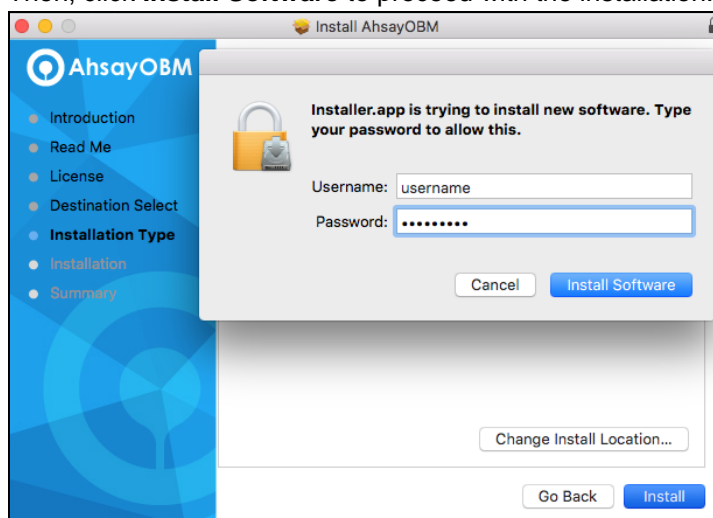
6. The following message will appear in a pop-up window. Click **Agree** to accept the software license agreement.



7. Click **Install** to start installing AhsayOBM to the default location, i.e. "Untitled" in this example.



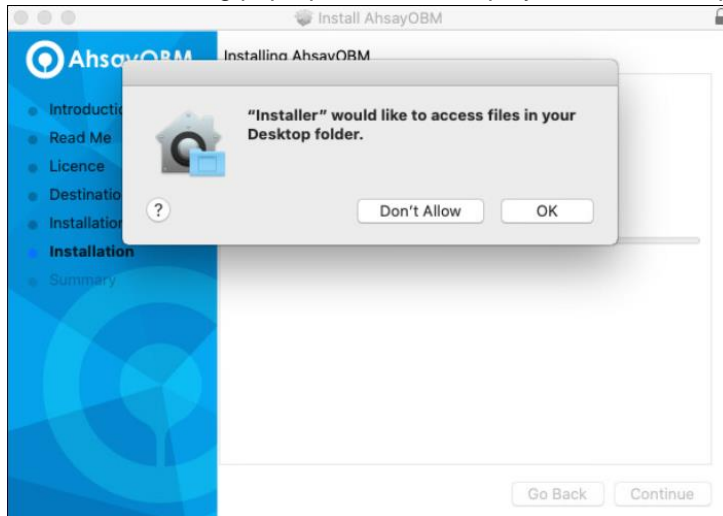
8. The following message will appear in a pop-up window. Enter your macOS login credentials. Then, click **Install Software** to proceed with the installation.



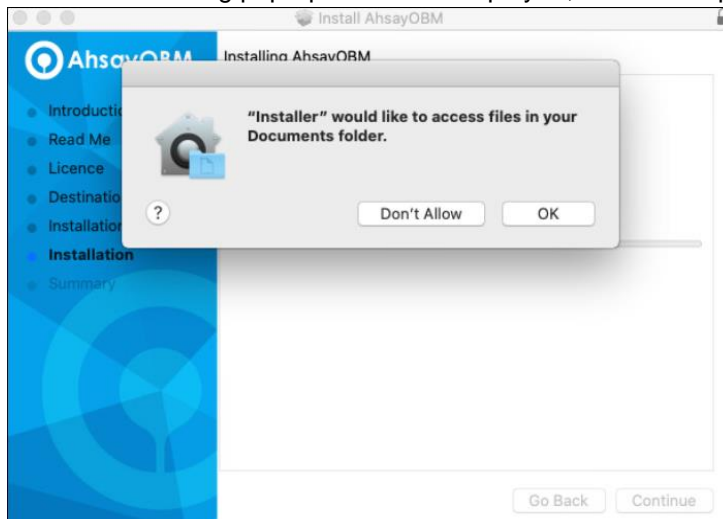
NOTE

The pop-up windows on **Steps 9, 10, and 11** are only applicable on macOS 10.15 or above. Otherwise, proceed to **Step 12**.

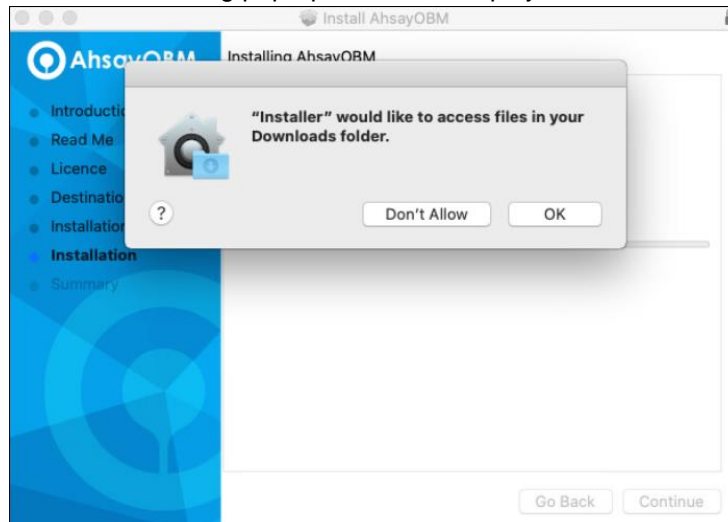
9. When the following pop-up window is displayed, click **OK** to proceed.



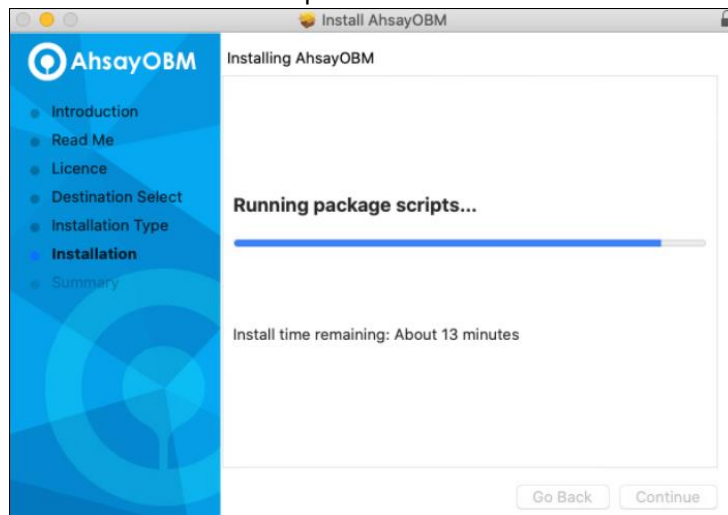
10. When the following pop-up window is displayed, click **OK** to proceed.



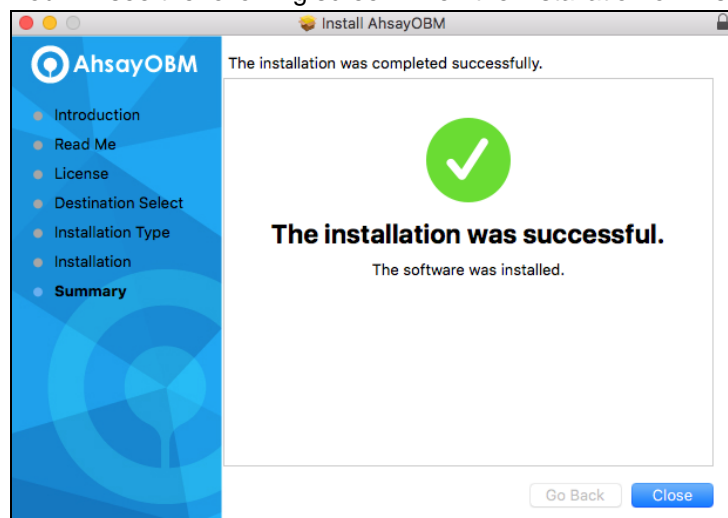
11. When the following pop-up window is displayed, click **OK** to continue with the installation.



12. Wait until the installation process is finished.



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

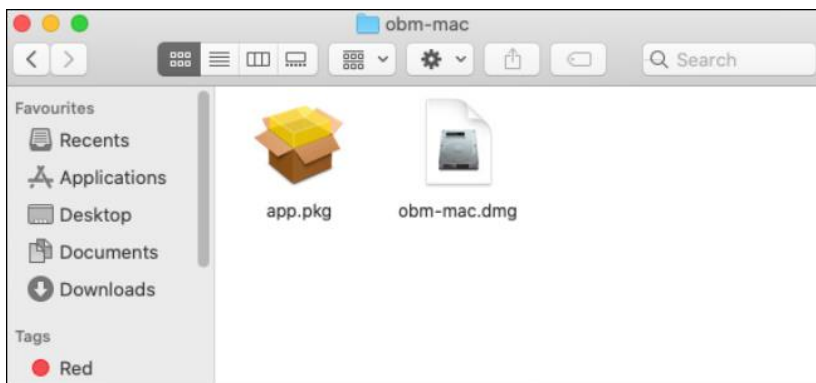
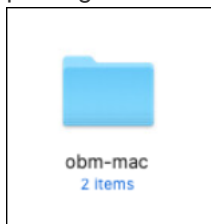


5.2.2 Offline Installation using TAR GZ offline installer

1. Double-click on the “obm-mac.tar” file you have downloaded to expand the installation package.



2. A new folder named “obm-mac” will be created. Open the folder to access the installation package file.



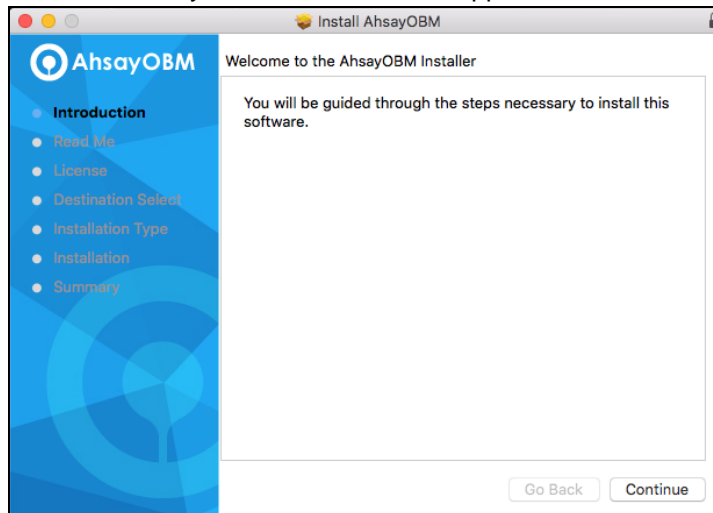
3. Double-click on the “obm-mac.dmg” file.



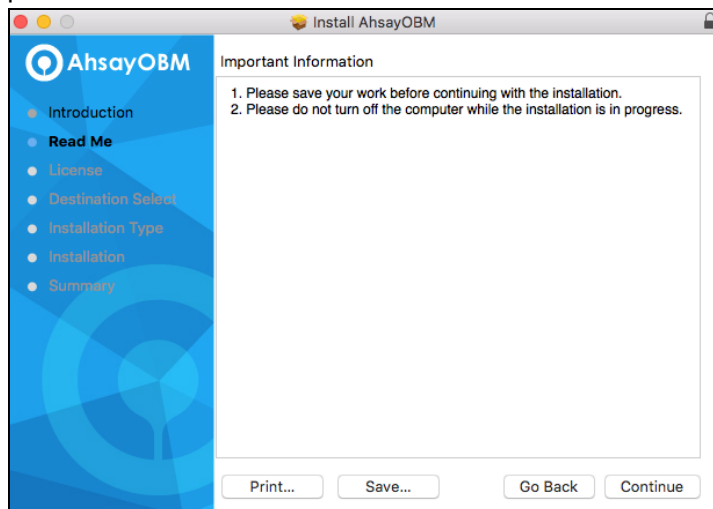
4. The Ahsay Online Backup Manager window will appear. You will see another file named “obm.pkg”. Double-click on the “obm.pkg” file to start the installation process.




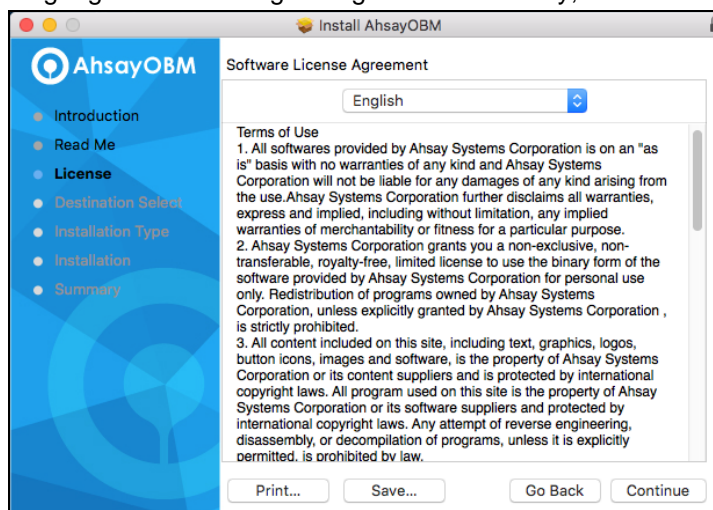
5. When the AhsayOBM Installer wizard appears, click **Continue** to proceed.



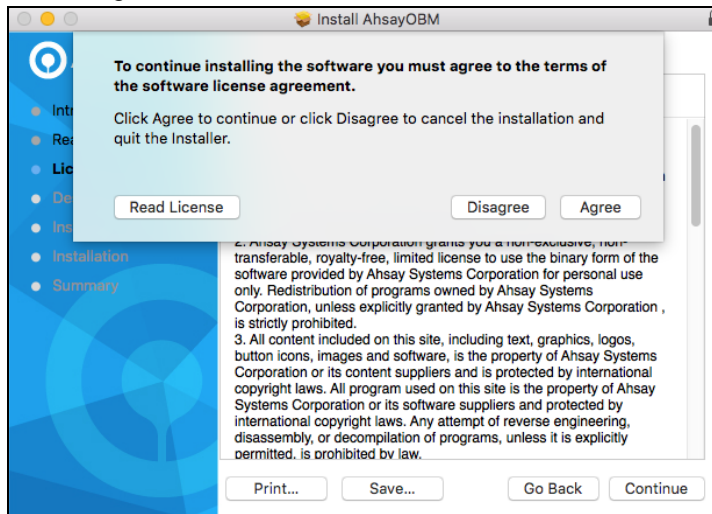
6. When the Important Information screen appears, read the information then click **Continue** to proceed.



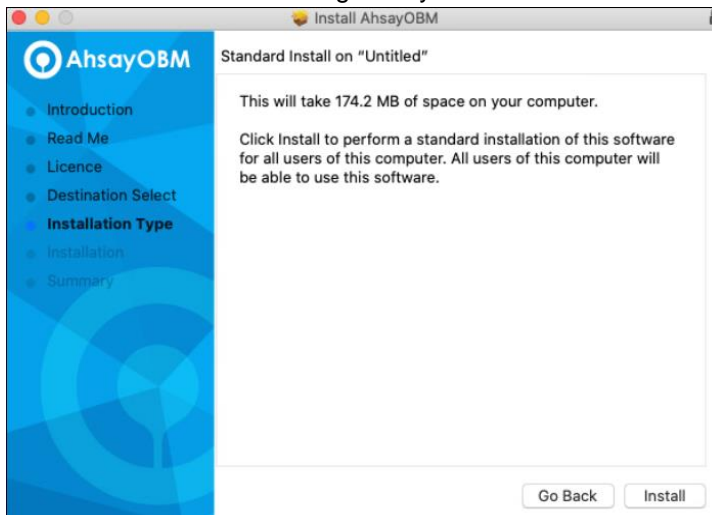
7. When the Software License Agreement appears, the agreement content will be displayed in English by default. If you prefer to read it in a different language, click  to change the language. After reading the agreement carefully, click **Continue** to proceed.



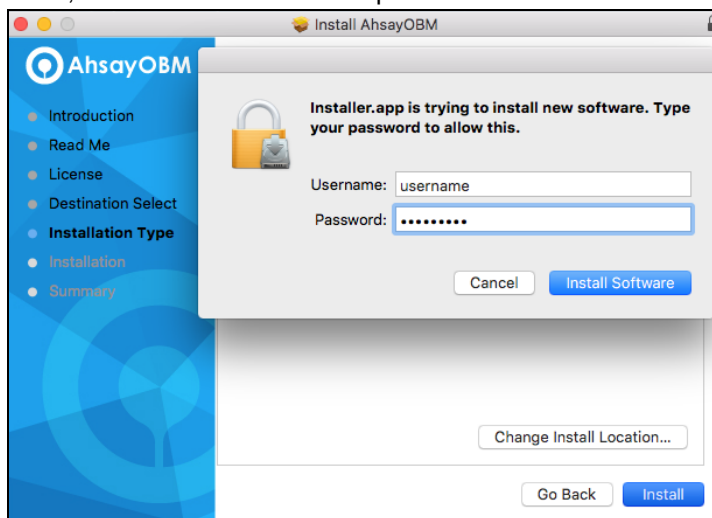
8. The following message will appear in a pop-up window. Click **Agree** to accept the software license agreement.



9. Click **Install** to start installing AhsayOBM to the default location, i.e. "Untitled" in this example.



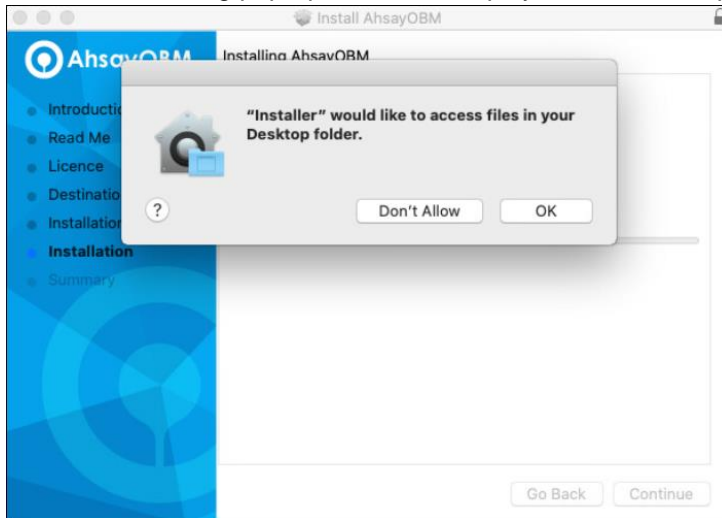
10. The following message will appear in a pop-up window. Enter your macOS login credentials. Then, click **Install Software** to proceed with the installation.



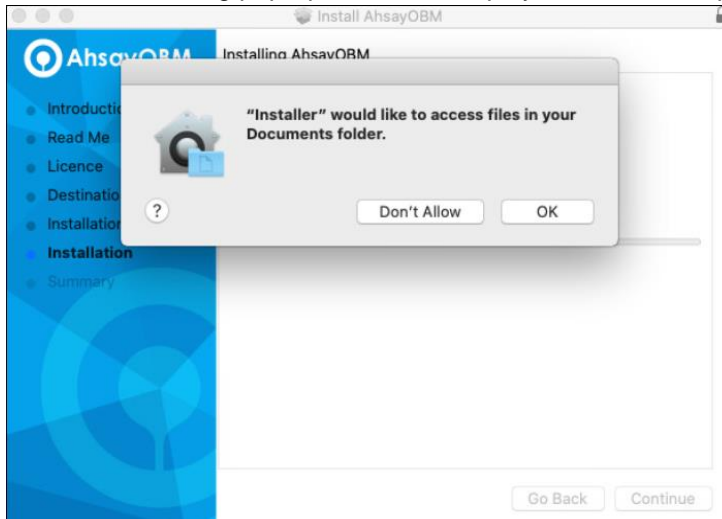
NOTE

The pop-up windows on **Steps 11, 12, and 13** are only applicable on macOS 10.15 or above. Otherwise, proceed to **Step 14**.

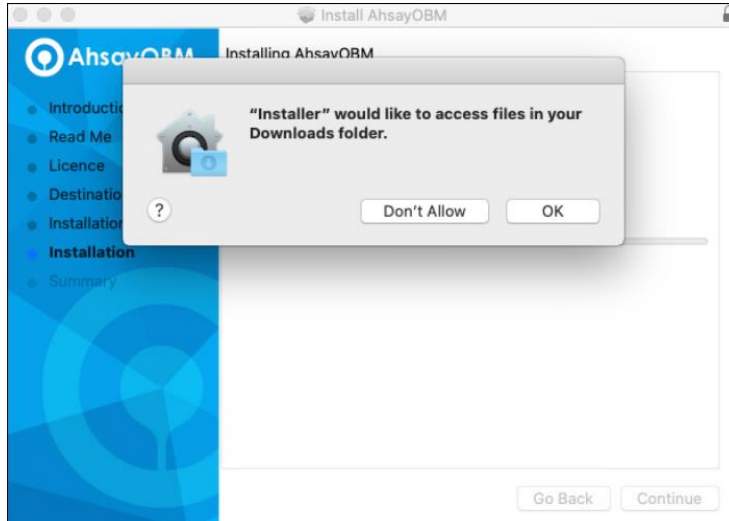
11. When the following pop-up window is displayed, click **OK** to proceed.



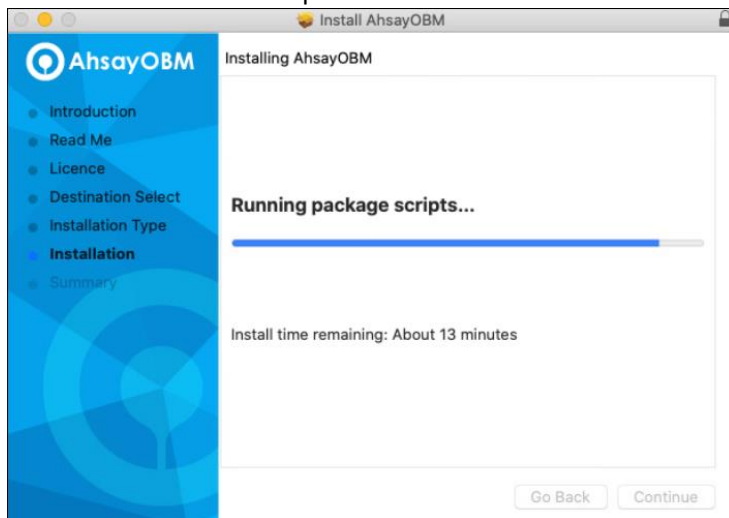
12. When the following pop-up window is displayed, click **OK** to proceed.



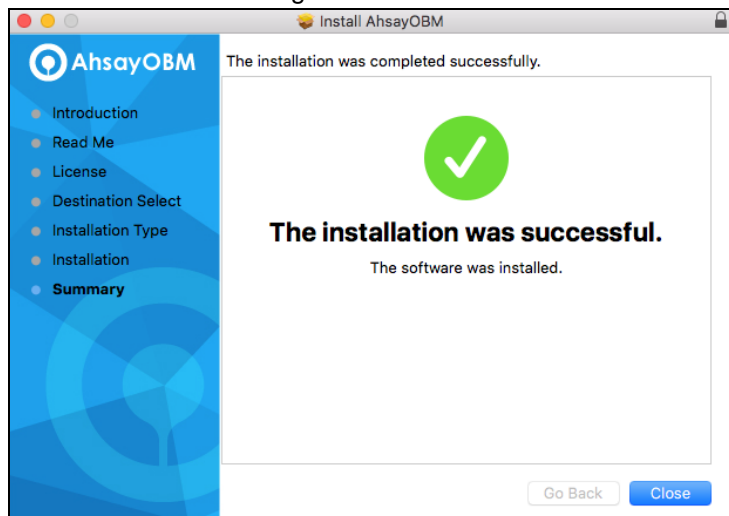
13. When the following pop-up window is displayed, click **OK** to continue with the installation.



14. Wait until the installation process is finished.



15. 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.

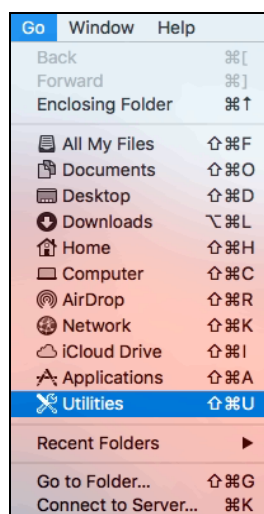
| Function | Description |
|---|---|
| Continuous Backups (Windows platform only) | Ensures that Continuous backups are run according to the backup interval. |
| Reminder (Windows platform only) | Ensures that a reminder popup is displayed when the last time a backup was run exceeded the tolerance period. |
| 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 will be created to the scheduler startup script:

/Applications/AhsayOBM.app/bin/com.cb.scheduler.plist

This will allow the AhsayOBM Scheduler Service to automatically start 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**.

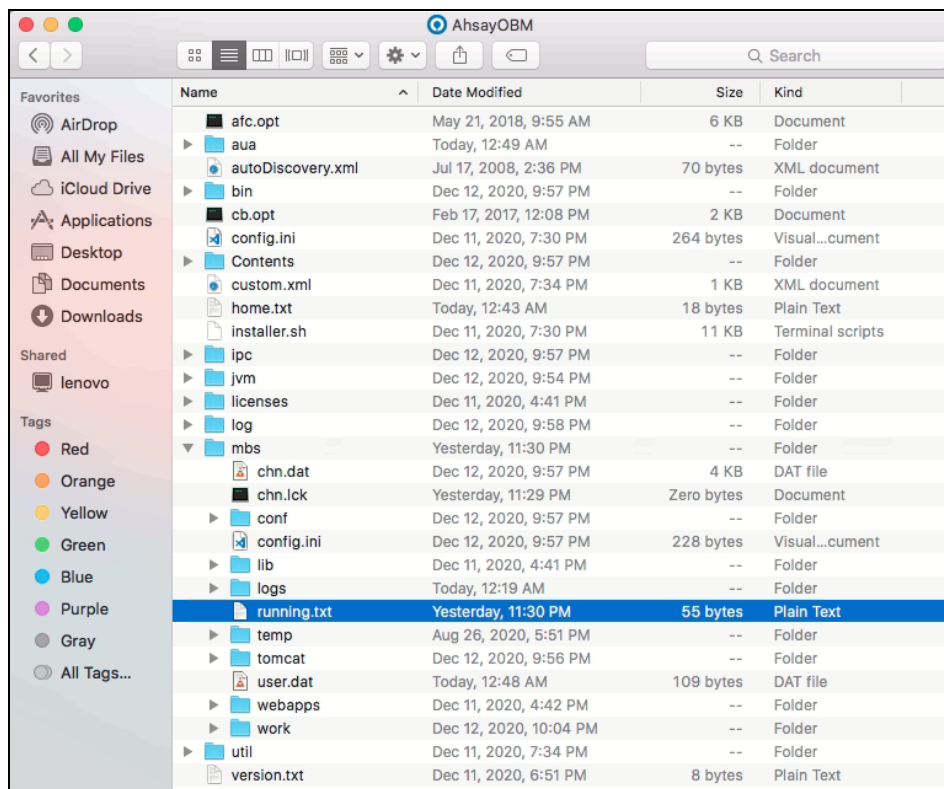
```
admins-Mac:~ admin$ ls -la /Library/LaunchDaemons/
total 16
drwxr-xr-x+ 62 root wheel 2108 Apr  5 01:56 ..
lrwxr-xr-x  1 root wheel 53 May 15 03:07 com.AhsayOBM.scheduler.plist ->
/Applications/AhsayOBM.app/bin/com.cb.scheduler.plist
admins-Mac:~ admin$
```

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:

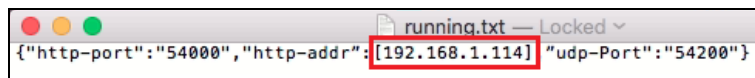
1. Check HTTP port, IP address and UDP port in the **running.txt** file. Go to mbs folder.
Example: /Applications/AhsayOBM.app/mbs



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::6a:a8:6d:ff:fe29:58%en1 prefixlen 64 duplicated scopeid 0x5
    inet 192.168.1.114 netmask 0xffffffff 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
```

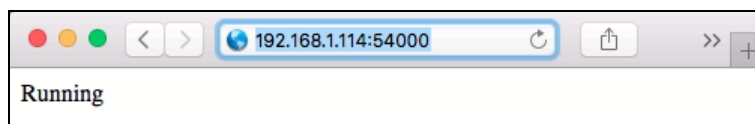
```

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 0 127.0.0.1.54050 *.* 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.

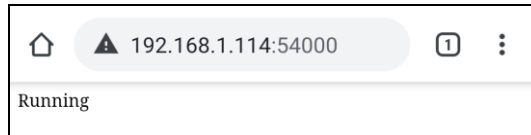
In the AhsayOBM machine



6. To run a connection test between the mobile device and machine open a browser in your mobile device and type the IP address followed by 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 Register device for 2FA in AhsayOBM

There are two types of Authenticator that can be used to register a device for 2FA in AhsayOBM:

- Ahsay Mobile Authenticator
- Third-party TOTP Authenticator (e.g., Microsoft Authenticator, Google Authenticator, Authy, Duo, LastPass Authenticator, iOS 15 Built-in Two-Factor Authenticator, etc.)

The 2FA registration steps using the different types of authenticator will be discussed in this chapter.

- [Using Ahsay Mobile Authenticator](#)
 - Supports two types of authentication:
 - i) Push Notification
 - ii) TOTP
 - Can be configured to support two 2FA modes:
 - i) Push Notification and TOTP (default mode); or
 - ii) TOTP only
- [Using Microsoft Authenticator](#)
- [Using Google Authenticator](#)

6.1 Using Ahsay Mobile Authenticator

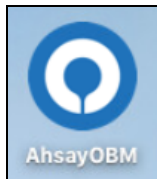
To register a device for 2FA in AhsayOBM using Ahsay Mobile, here are the two scenarios:

- [Without Mobile Add-on Module](#)
- [With Mobile Add-on Module](#)

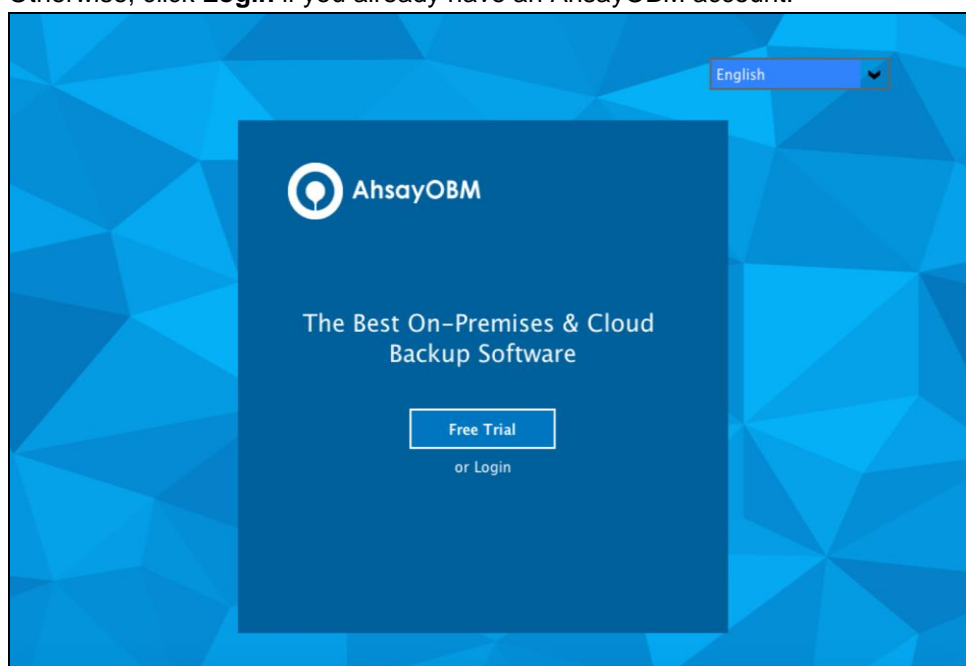
6.1.1 Without Mobile Add-on Module

To register a device for 2FA without Mobile Add-on Module, 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.



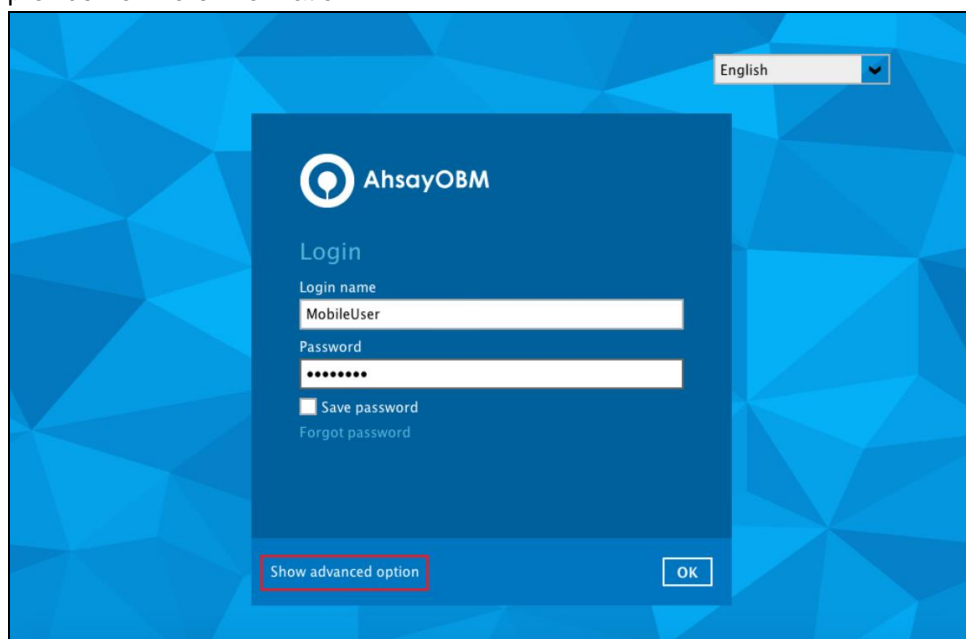
2. The Free Trial Registration option may be displayed when you login for the first time. If you want to create a free trial account please proceed to [Appendix E](#). Otherwise, click **Login** if you already have an AhsayOBM account.



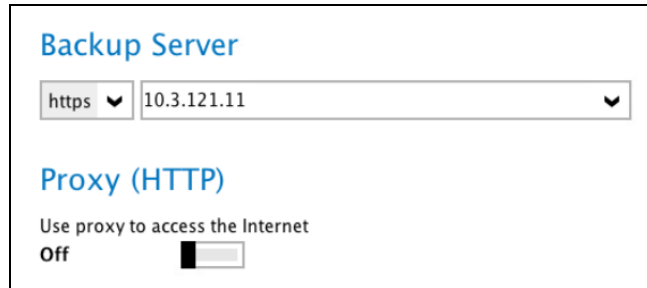
NOTE

The **Free Trial** registration option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

3. The **Show advanced option** may not be available if the backup server settings are already setup by your backup service provider. Please contact your backup service provider for more information.

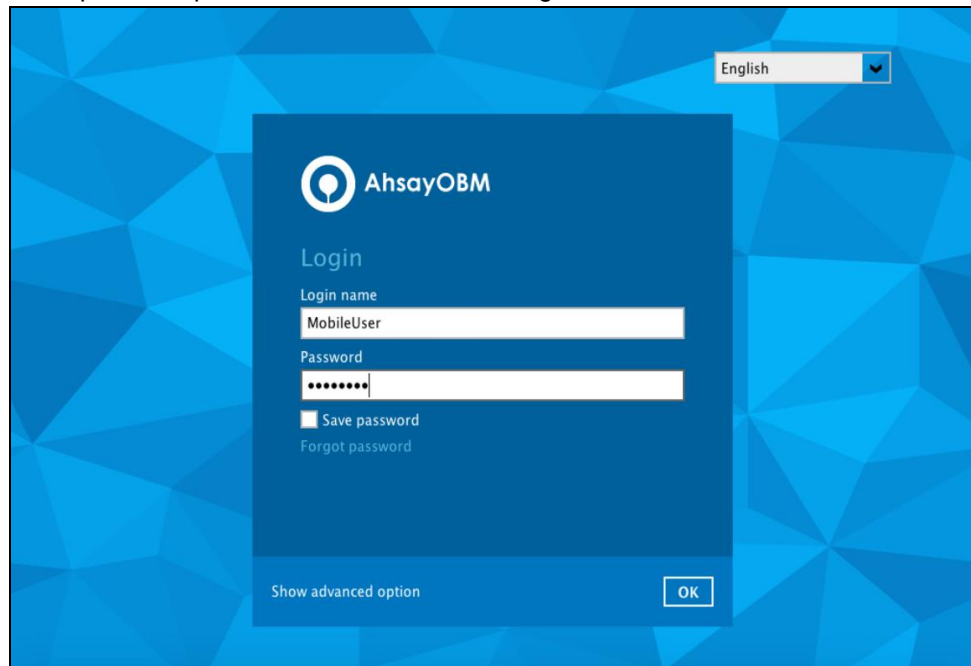


If **Show advanced option** is clicked, this will be displayed.



The screenshot shows a configuration window titled "Backup Server". It contains a dropdown menu set to "https" and a text field with the IP address "10.3.121.11". Below this is a section titled "Proxy (HTTP)" with the text "Use proxy to access the Internet" and a toggle switch labeled "Off".

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



The screenshot shows the AhsayOBM Login dialog box. It has a blue background with a geometric pattern. The dialog box is white with a blue header containing the AhsayOBM logo and name. Below the header, it says "Login". There are two input fields: "Login name" with the text "MobileUser" and "Password" with masked characters. Below the password field is a checkbox labeled "Save password" and a link labeled "Forgot password". At the bottom of the dialog box, there is a "Show advanced option" link and an "OK" button. In the top right corner of the background window, there is a language dropdown menu set to "English".

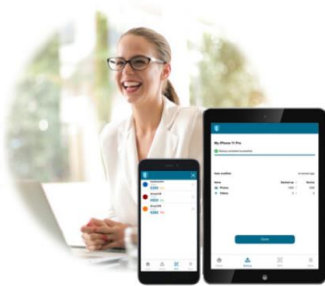
NOTE

The **Save password** option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

5. You will have the option to set up your 2FA. Click **Setup Now**.


New Ahsay Mobile App, Free of Charge!

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.



[Skip Feature Setup](#)[Setup Now](#)

If you do not want to set up the 2FA feature, click the **Skip Feature Setup** link. If you click **Yes** in the pop-up message that will be displayed, it will skip to **step 8**. Otherwise, click **No** to continue with the set-up of the 2FA feature.




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.



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


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

App Download and Device Pairing

Please scan the QR code to get the below Mobile App from App Store. Once installed the Mobile App, launch it and scan the same QR code to complete the device registration.

 Ahsay Mobile





Prerequisites

– Please use the latest Mobile App version

[Not able to scan QR code? Click here to pair with TOTP secret key](#)

7. Ahsay Mobile supports two types of authentication method:

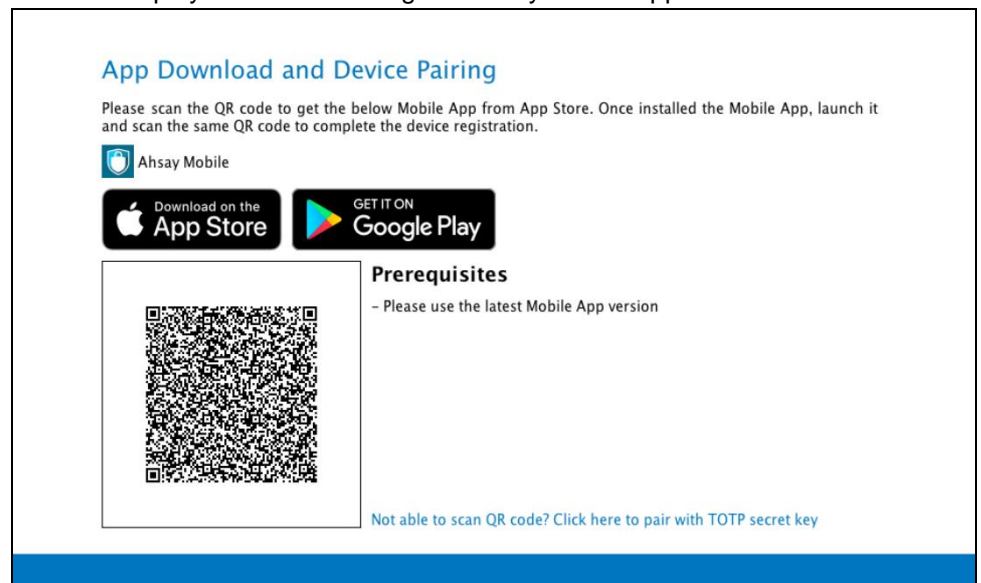
- Push Notification
- TOTP

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)

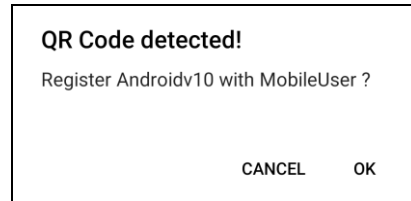
- i. To configure Push Notification and TOTP 2FA with Ahsay Mobile, simply scan the displayed QR code using the Ahsay Mobile app.



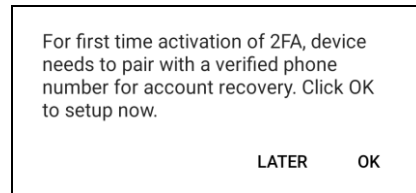
- ii. In this example, the Ahsay Mobile app is installed on a mobile device named "Androidv10".



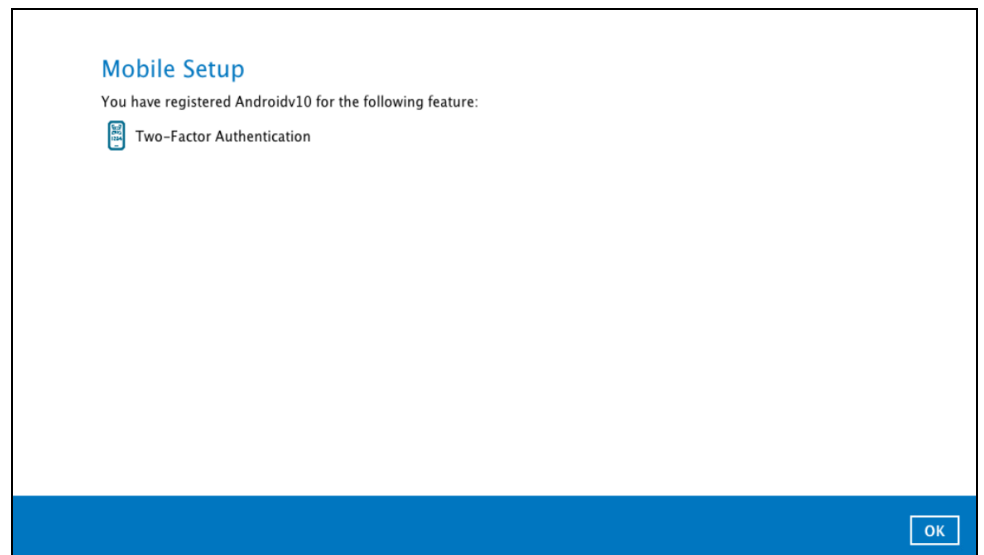
Tap **OK** to continue.



Once the device is successfully paired, the following message will be displayed in the Ahsay Mobile app. You can set up a recovery number here that will be used in case of "Authentication Recovery" procedure by tapping **OK**. Otherwise, tap **LATER** to set it up later on.

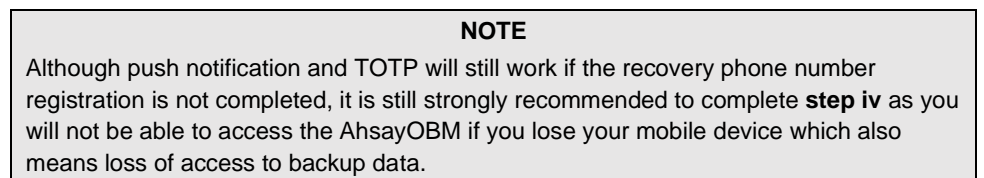


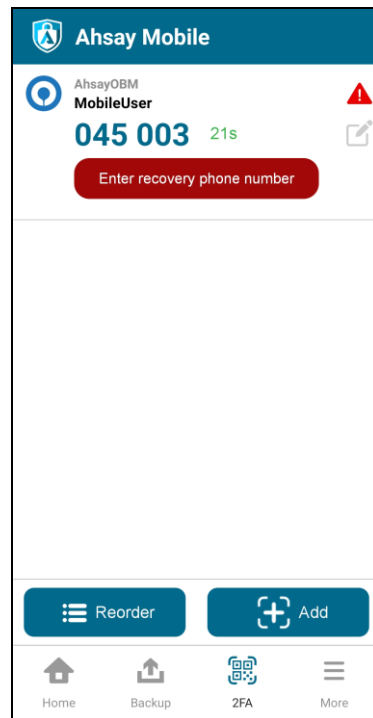
- iii. After successful scan of the QR code, you have now registered Ahsay Mobile for Push Notification and TOTP 2FA. Click **OK** to continue.



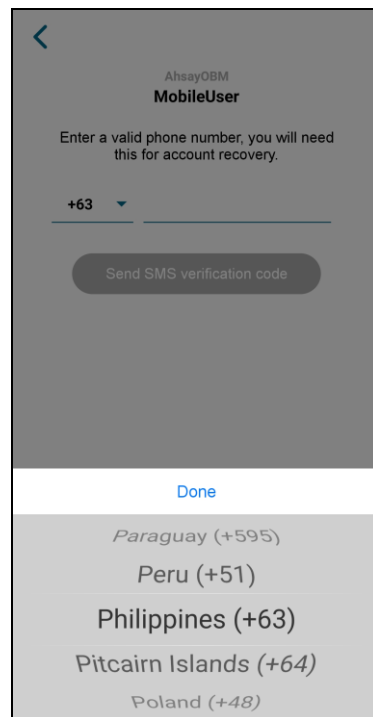
Phone number verification for account recovery

- iv. In the Ahsay Mobile app, go to 2FA then enter the phone number for account recovery. Tap **Enter recovery phone number**.

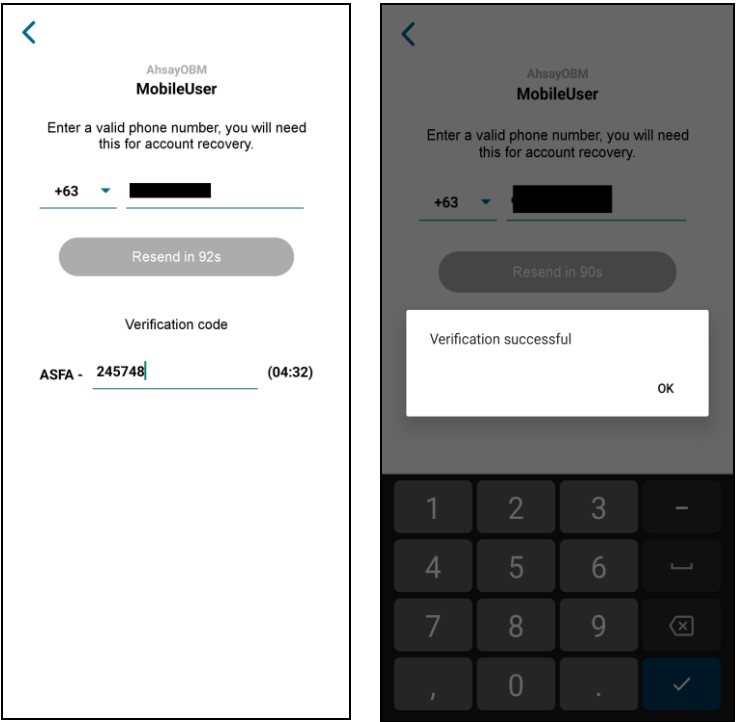




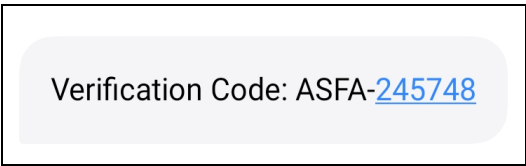
Select your country code and enter your phone number. Tap **Send SMS verification code**.



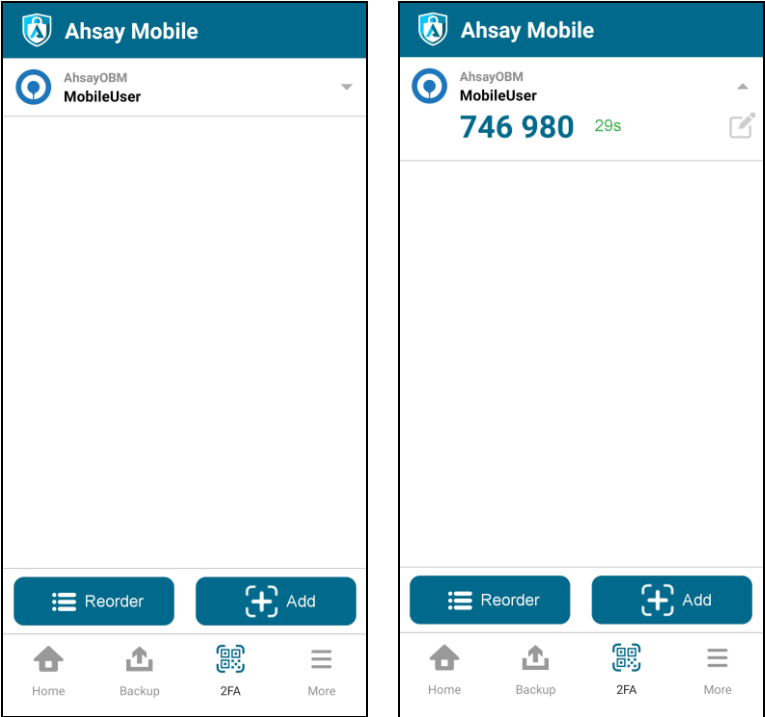
Enter the verification code sent to your mobile device.



Example of verification code:

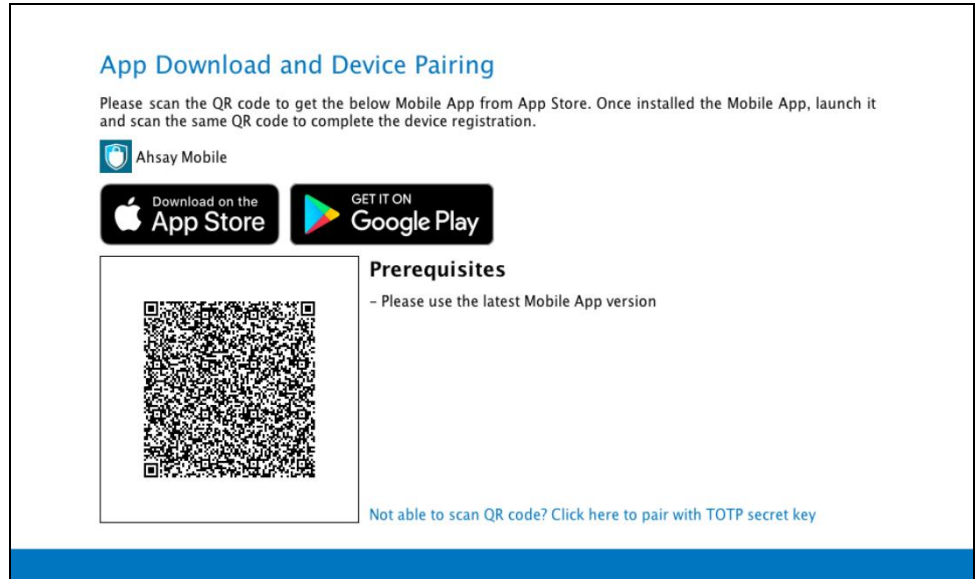


Your phone number for account recovery is successfully verified.

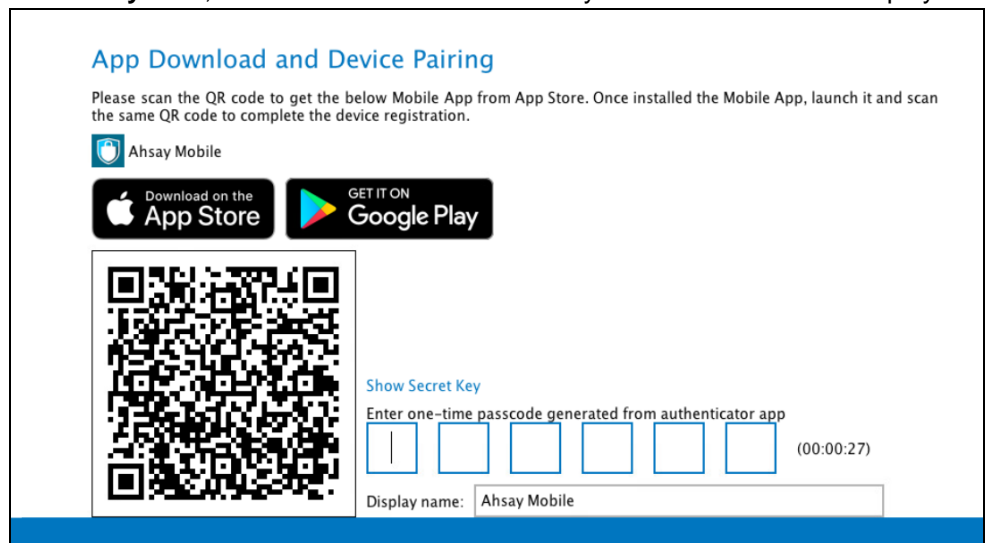


TOTP only

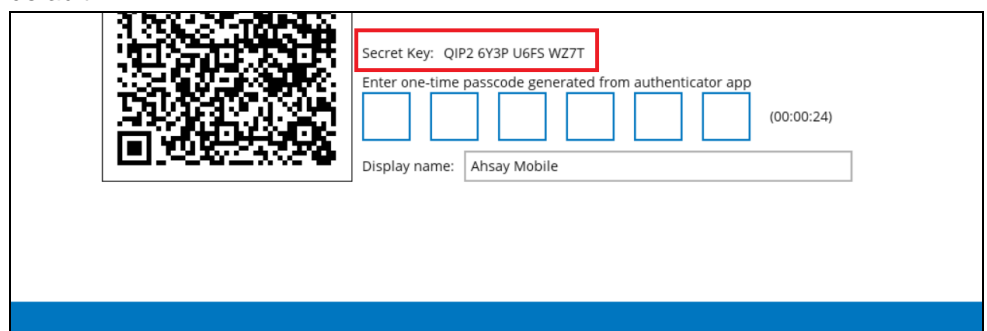
- i. To configure a TOTP only 2FA with Ahsay Mobile, click the **“Not able to scan QR code? Click here to pair with TOTP secret key”** link.



- ii. After clicking the **“Not able to scan QR code? Click here to pair with TOTP secret key”** link, the QR code for the TOTP only authenticator will be displayed.



To show the secret key, click the **Show Secret Key** link to display the 16-character alphanumeric secret key. The display name will be “Ahsay Mobile” by default.



- iii. In the Ahsay Mobile app, go to **2FA**. Tap the **Not able to scan QR code?** link.

The left screenshot shows the 'Ahsay Mobile' app interface. It has a blue header with the app logo and name. Below the header, it says 'Scan the QR code displayed in your application (supports two-factor authentication, mobile device backup etc.)'. There is a large black square representing the QR code. At the bottom, there is a blue 'Cancel' button and a red-bordered link that says 'Not able to scan QR code?'. The right screenshot shows a dialog box titled 'Connect using Secret Key'. It has a close button (X) in the top left. Below the title, it says 'Key in the Secret Key provided by the app'. There are two input fields: 'Username' and 'Secret Key'. At the bottom, there is a grey 'Connect' button and a blue link that says 'Scan QR Code'.


- iv. Enter the Username and Secret Key shown in the AhsayOBM then tap **Connect**. Once the device is paired successfully, click **OK** to continue.



The left screenshot shows the 'Connect using Secret Key' dialog box. The 'Username' field is filled with 'Ahsay Mobile' and the 'Secret Key' field is filled with dots. At the bottom, there is a blue 'Connect' button and a blue link that says 'Scan QR Code'. The right screenshot shows the same dialog box, but with a white message box in the center that says 'Device paired successfully' and an 'OK' button. The 'Connect' button is now greyed out.


- v. Enter the one-time passcode from the Ahsay Mobile app.

App Download and Device Pairing

Please scan the QR code to get the below Mobile App from App Store. Once installed the Mobile App, launch it and scan the same QR code to complete the device registration.

 Ahsay Mobile





[Show Secret Key](#)
Enter one-time passcode generated from authenticator app

5

1

8

2

7


3


(00:00:27)


Display name:

Cancel

Example of the one-time passcode generated by Ahsay Mobile:

 Ahsay Mobile

 AhsayOBM
MobileUser

 TOTP (Manual input)
Ahsay Mobile
518 273 27s

Reorder

Add

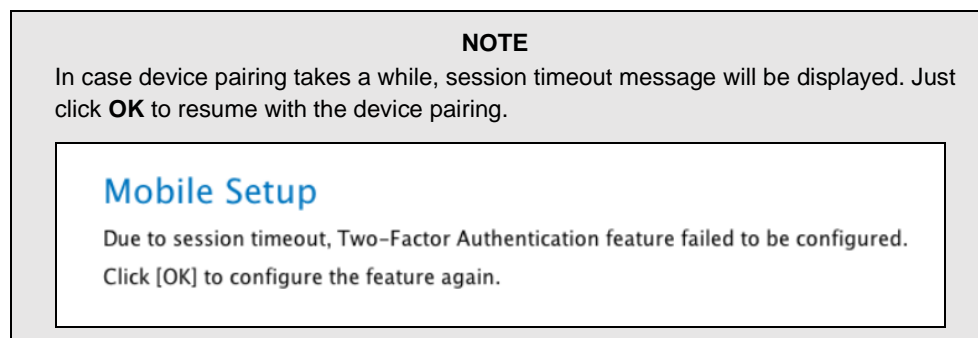
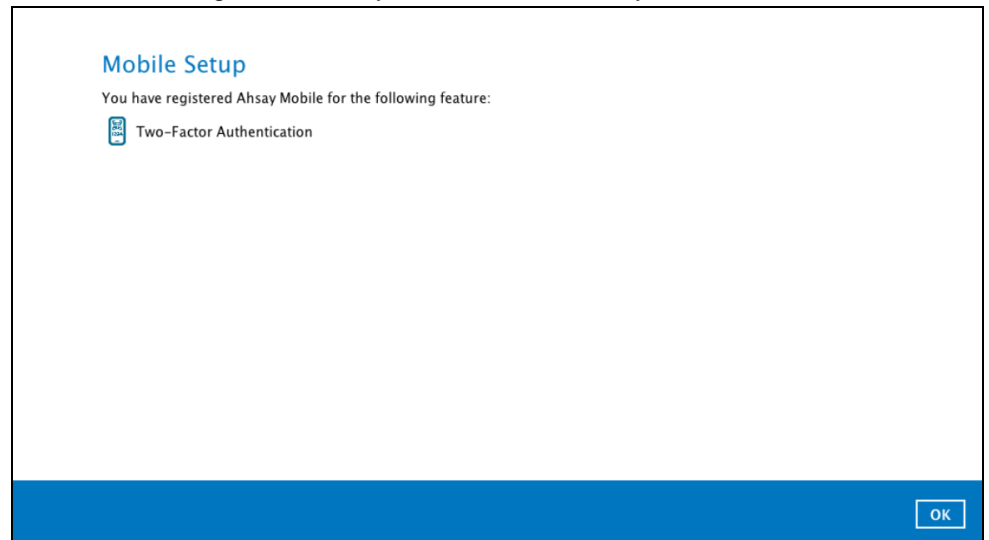
Home

Backup

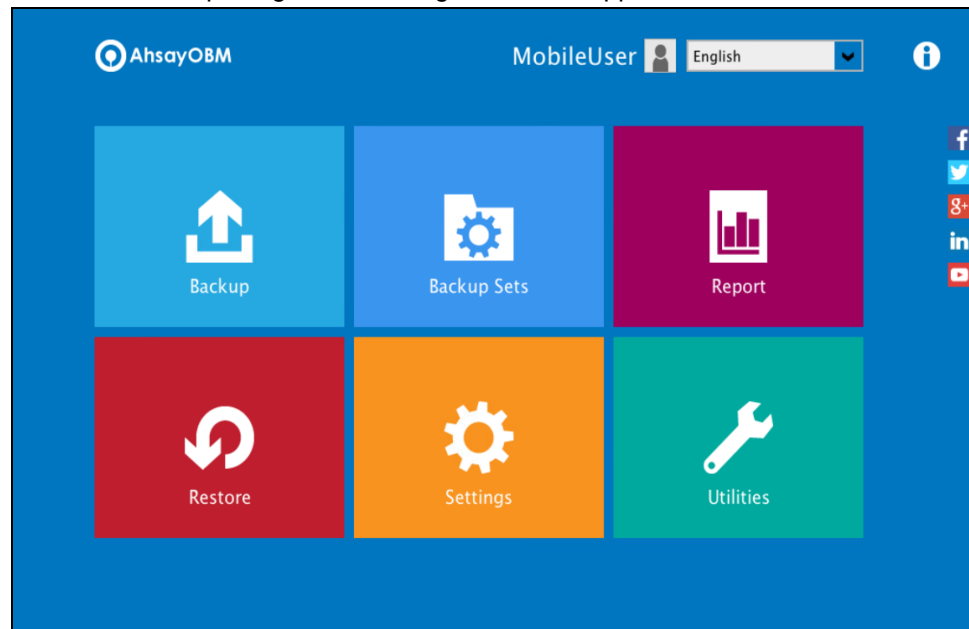
2FA

More

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



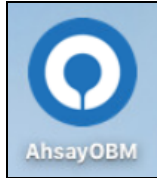
8. After successful pairing, the following screen will appear.



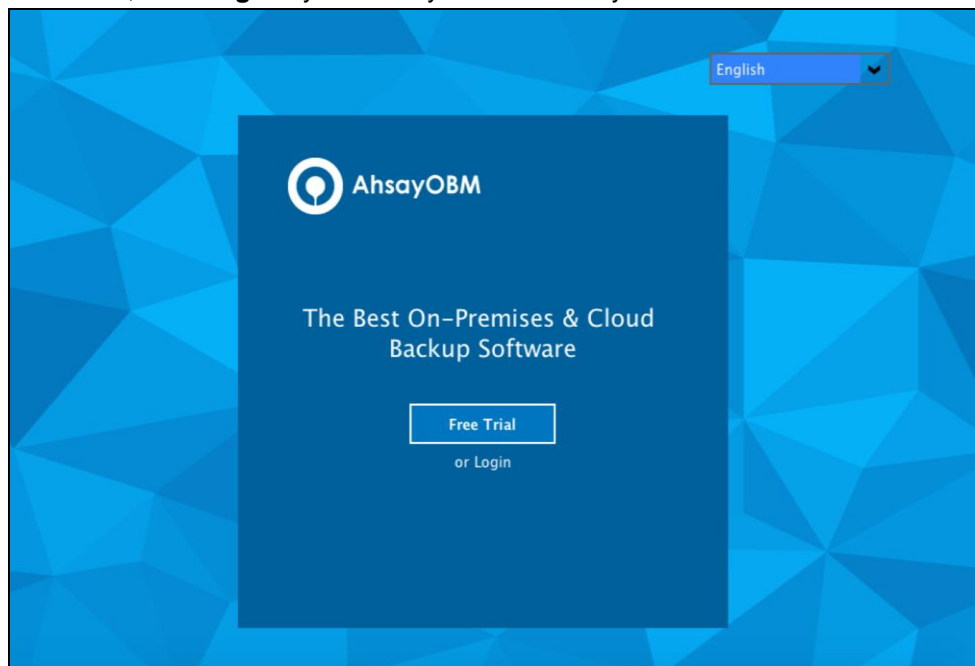
6.1.2 With Mobile Add-on Module

To register a device for 2FA 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.



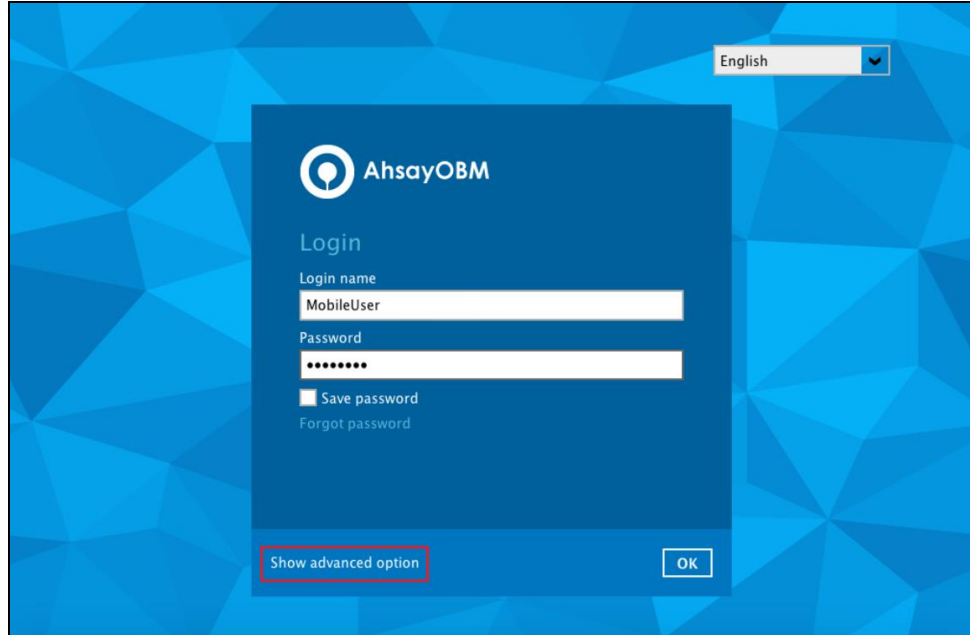
2. The Free Trial Registration option may be displayed when you login for the first time. If you want to create a free trial account please proceed to [Appendix E](#). Otherwise, click **Login** if you already have an AhsayOBM account.



NOTE

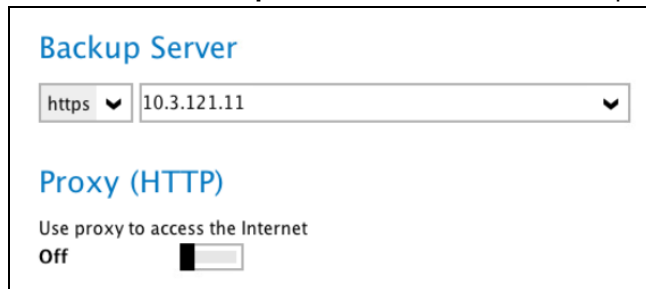
The **Free Trial** registration option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

3. The **Show advanced option** may not be available if the backup server settings are already setup by your backup service provider. Please contact your backup service provider for more information.



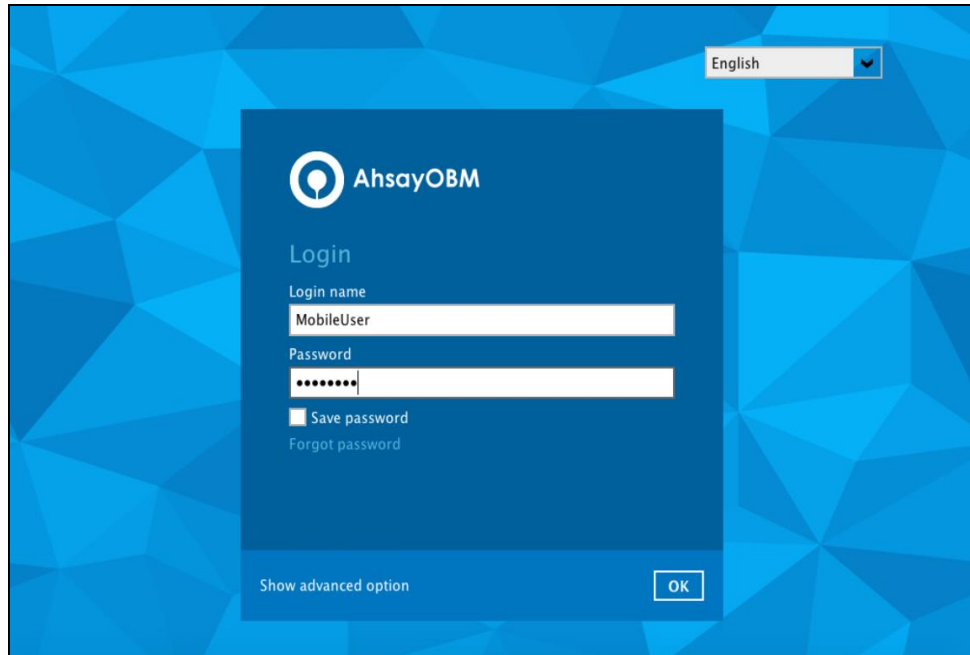
The image shows the AhsayOBM login interface. At the top right, there is a language dropdown menu set to 'English'. The central part of the screen features the AhsayOBM logo and the word 'Login'. Below this, there are input fields for 'Login name' (containing 'MobileUser') and 'Password' (masked with dots). There is a 'Save password' checkbox and a 'Forgot password' link. At the bottom of the login panel, the 'Show advanced option' button is highlighted with a red rectangle. An 'OK' button is located at the bottom right of the login panel.

If **Show advanced option** is clicked, this will be displayed.



The image shows the 'Backup Server' settings dialog. It has a title 'Backup Server'. Below the title, there is a dropdown menu for the protocol (set to 'https') and a text input field for the IP address (containing '10.3.121.11'). Below this, there is a section titled 'Proxy (HTTP)' with the text 'Use proxy to access the Internet'. At the bottom, there is a toggle switch for 'Off'.

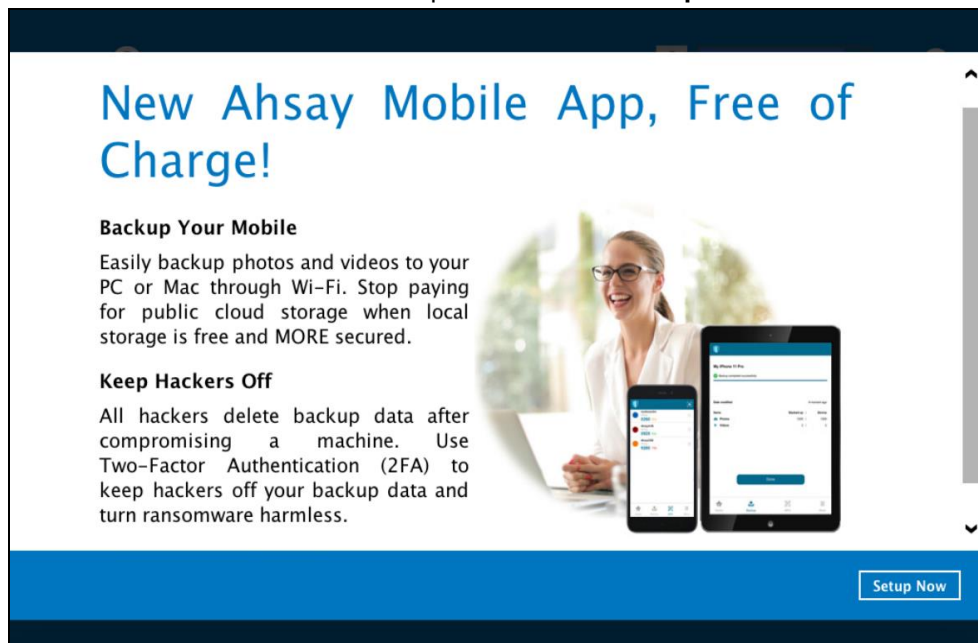
4. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.

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 word 'Login'. Below the logo, there are two input fields: 'Login name' with the text 'MobileUser' and 'Password' with masked characters. There are also checkboxes 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.

NOTE

The **Save password** option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.


5. You will have the option to set up your 2FA and 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 has a white background with a blue header and footer. The main text is in blue. Below the title, there are two sections: 'Backup Your Mobile' and 'Keep Hackers Off'. The 'Backup Your Mobile' section describes backing up photos and videos to a PC or Mac through Wi-Fi. The 'Keep Hackers Off' section describes using Two-Factor Authentication (2FA) to protect backup data. To the right of the text is a circular image of a smiling woman with glasses, with a smartphone and a tablet displaying the app interface in front of her. At the bottom right, there is a 'Setup Now' button.


6. Download the Ahsay Mobile app from the App Store / Google Play Store. Ensure that the displayed Prerequisites are met.

App Download and Device Pairing

Please scan the QR code to get the below Mobile App from App Store. Once installed the Mobile App, launch it and scan the same QR code to complete the device registration.

 Ahsay Mobile



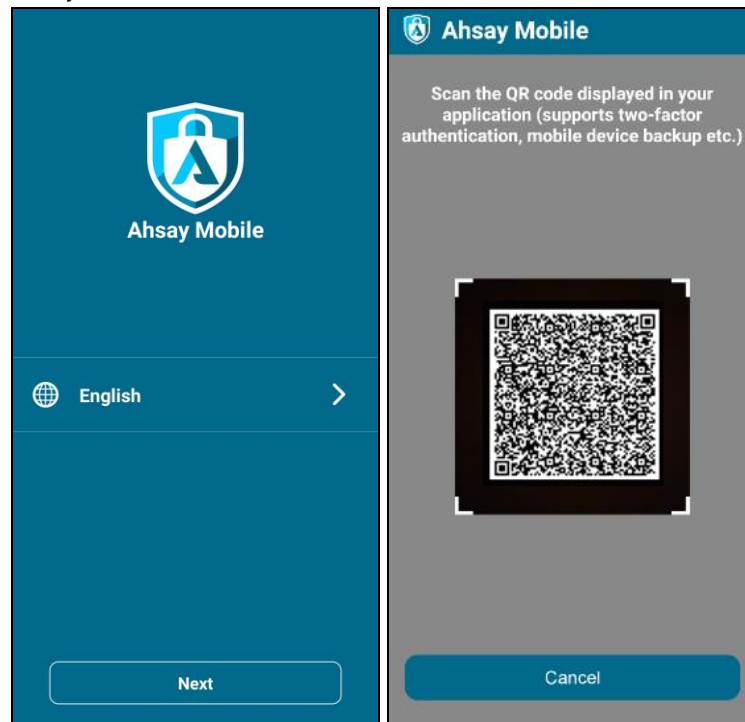


Prerequisites

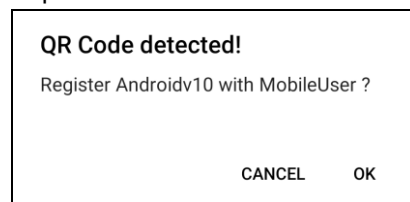
- Please use the latest Mobile App version
- Please make sure below 2 ports are not blocked by any Firewall settings
TCP Port: 54000
UDP Port: 54200

[Not able to scan QR code? Click here to pair with TOTP secret key](#)

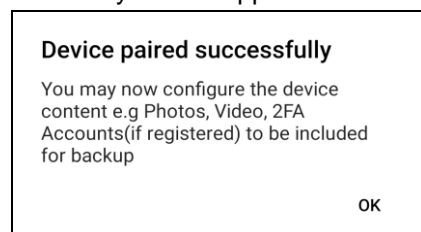
7. By using the Ahsay Mobile app, tap **Next** and scan the QR code displayed in AhsayOBM.



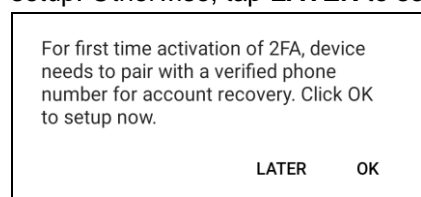
Tap **OK** to continue.



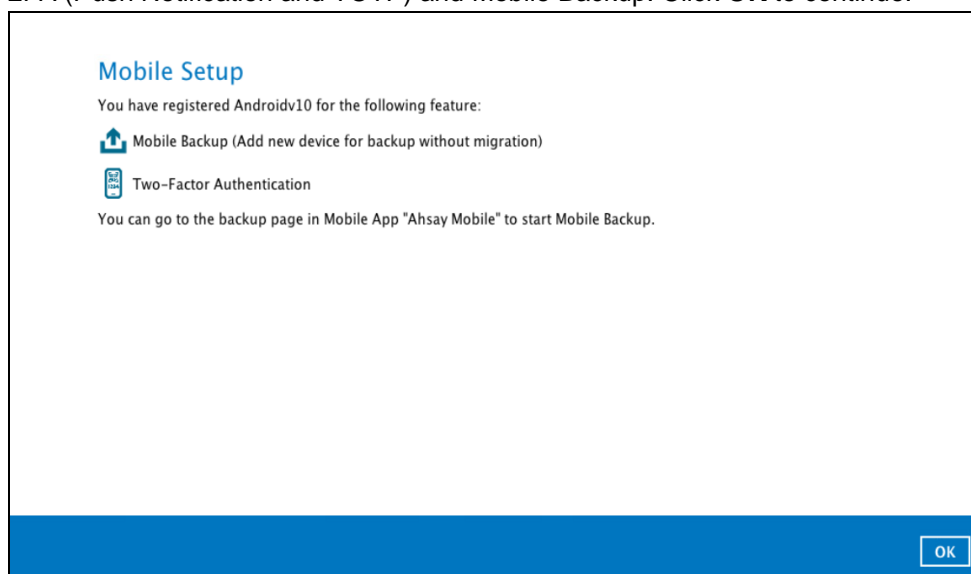
Once the device is successfully paired, the following message will be displayed in the Ahsay Mobile app. Click **OK** to continue.



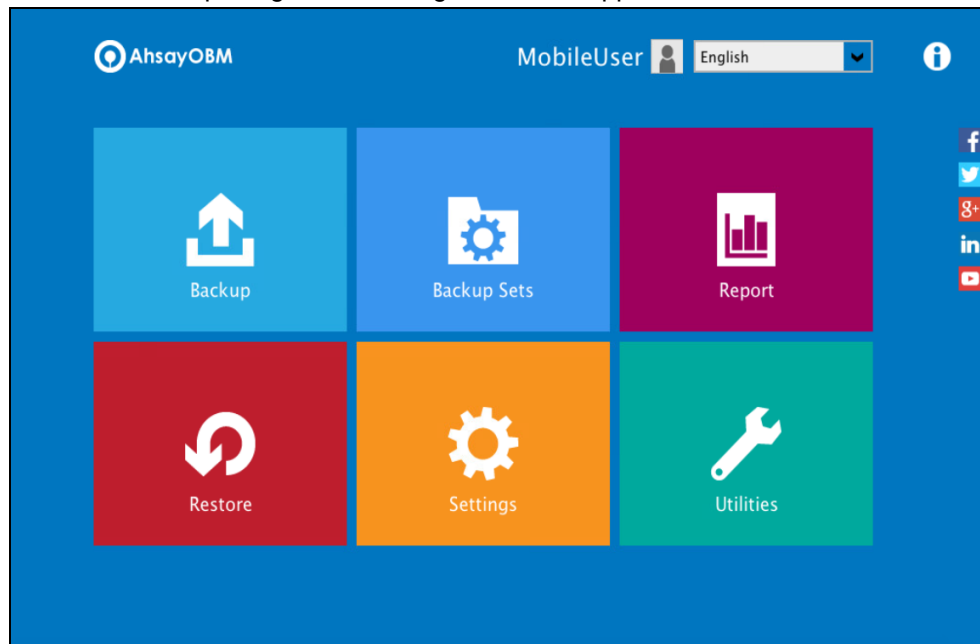
Once the device is successfully paired, the following message will be displayed in the Ahsay Mobile app. You can set up a recovery number here that will be used in case of the “Authentication Recovery” procedure by tapping **OK**. You may refer to [Phone number verification for account recovery](#) in **Chapter 6.1.1** for the following setup. Otherwise, tap **LATER** to set it up later on.



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



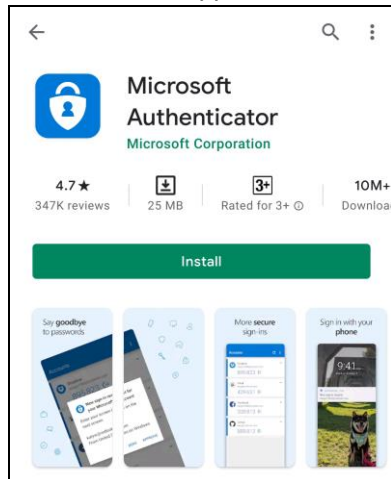
9. After successful pairing, the following screen will appear.



6.2 Using Microsoft Authenticator

To register a device for TOTP 2FA in AhsayOBM using Microsoft Authenticator, please follow the steps below:

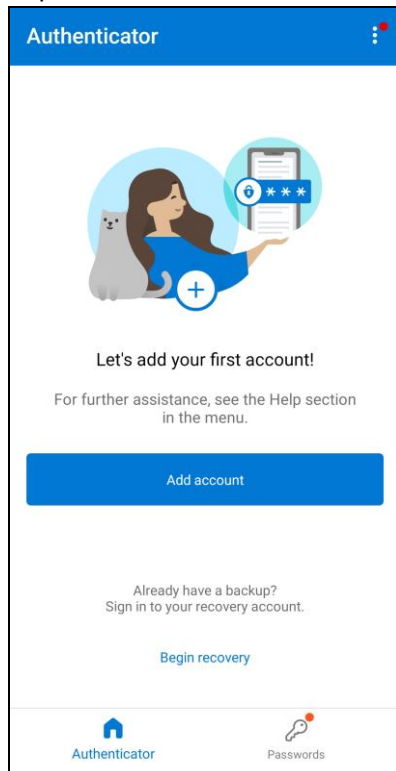
1. Download and install the Microsoft Authenticator from the Play Store for Android devices or the App Store for iOS devices.



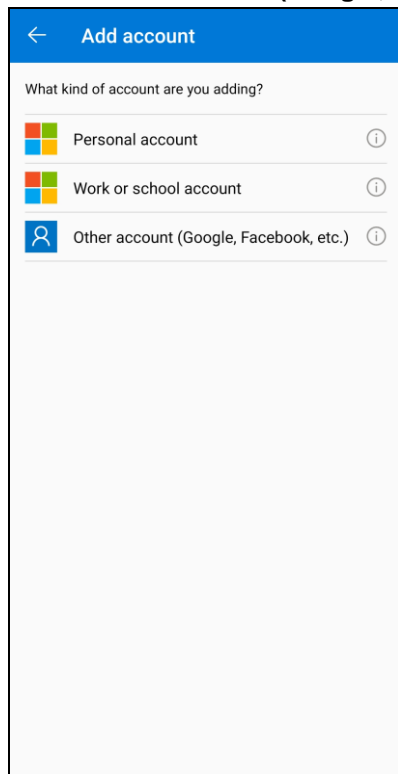
2. Launch the Microsoft Authenticator app.



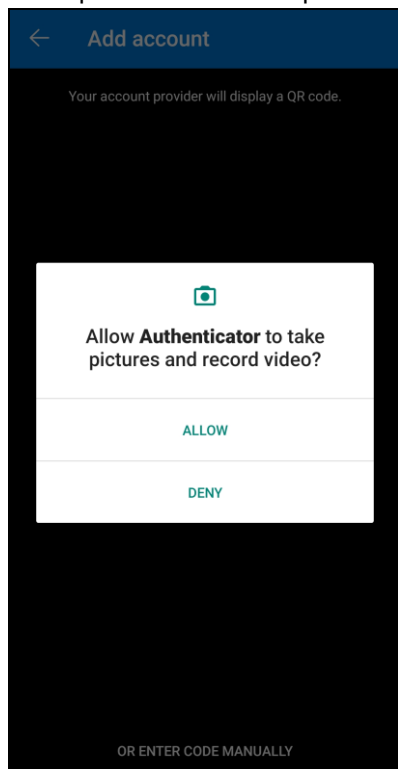
3. Tap **Add account**.



4. Select **Other account (Google, Facebook, etc.)**.



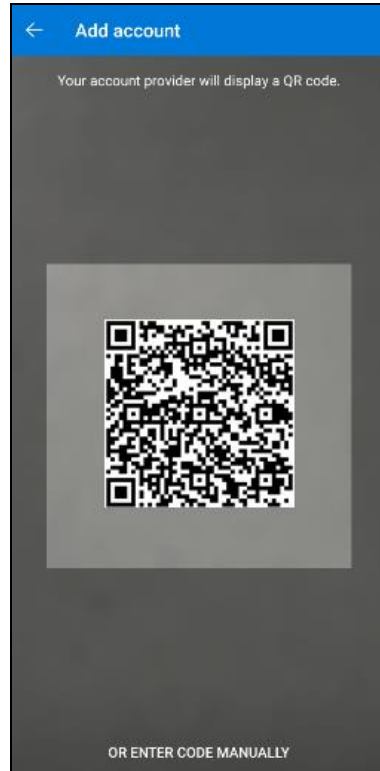
5. Allow permission to take pictures and record video.



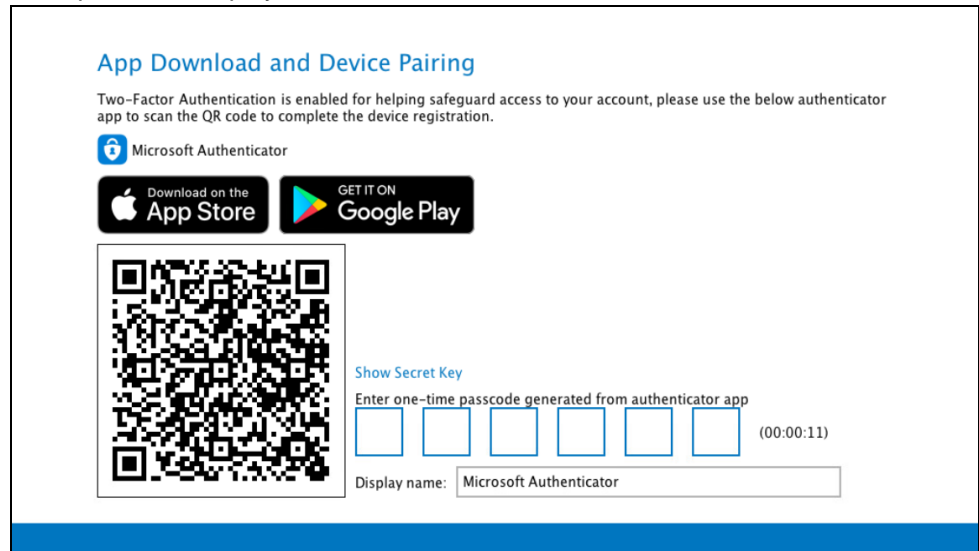
6. Set up the account by selecting from the following methods: Scan the QR code or Enter code manually.

Method 1: Scan the QR code

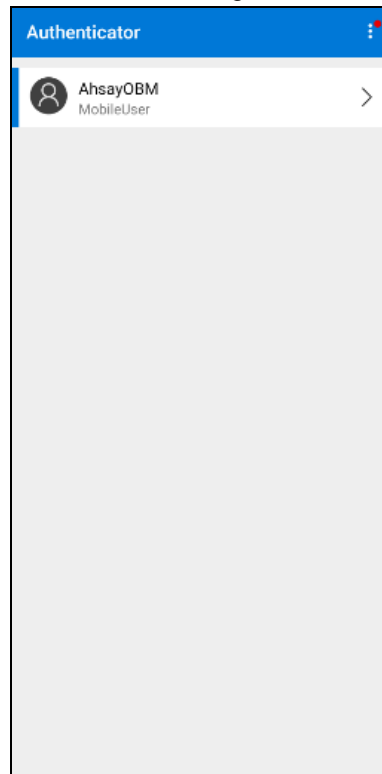
- i. Scan the QR code on AhsayOBM.



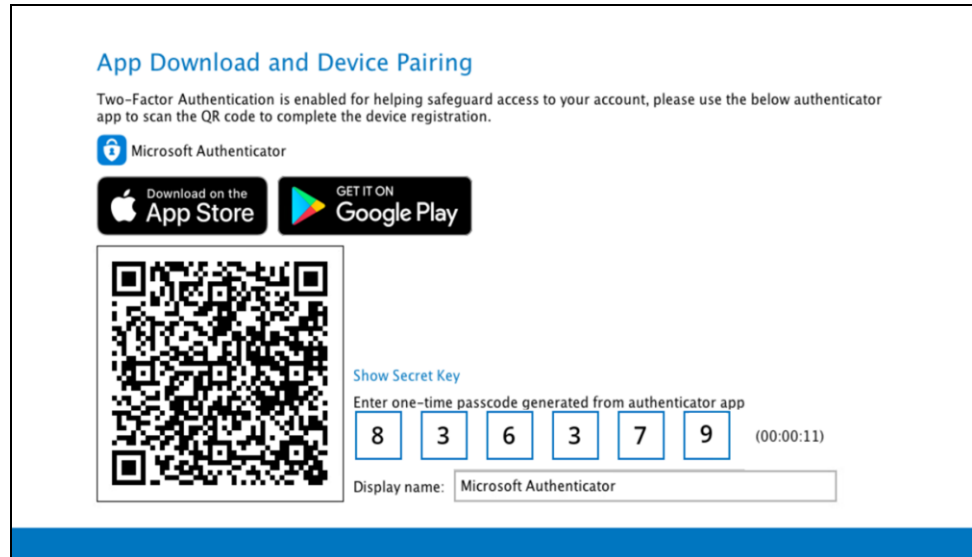
Example of the displayed QR code:



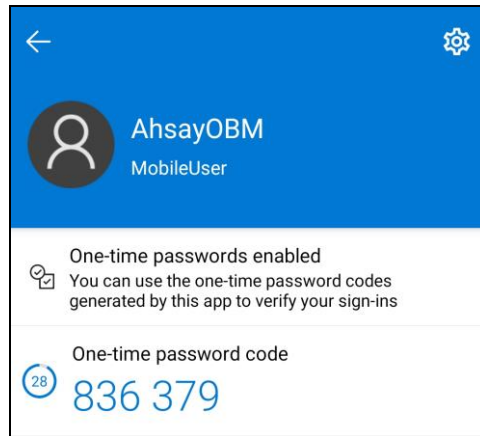
- ii. The AhsayOBM account is successfully added to Microsoft Authenticator and the mobile device is registered in AhsayOBM.



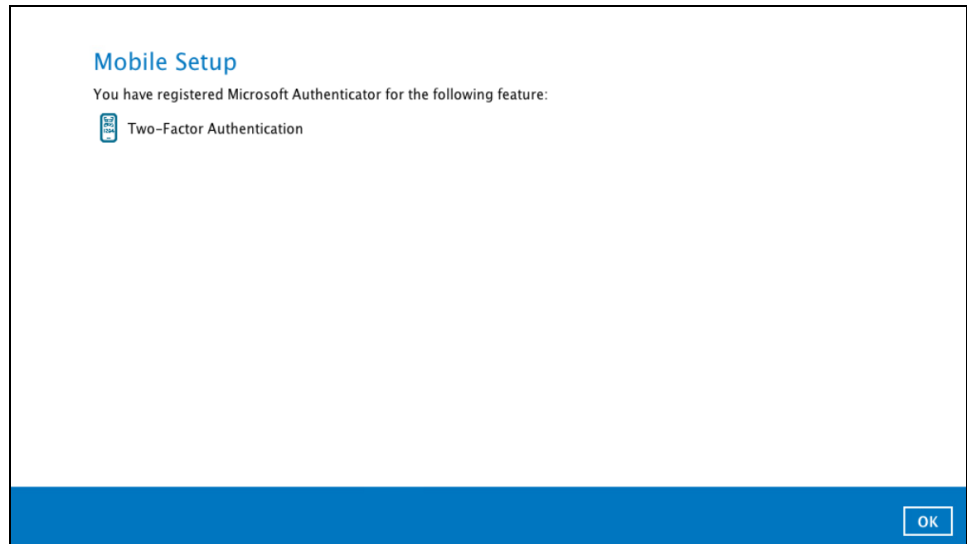
- iii. Once the account is added to Microsoft Authenticator, enter the one-time passcode generated from the authenticator app to AhsayOBM.



Example of the one-time passcode generated:



- iv. The device is successfully registered for TOTP 2FA in AhsayOBM using Microsoft Authenticator. Click **OK** to continue.

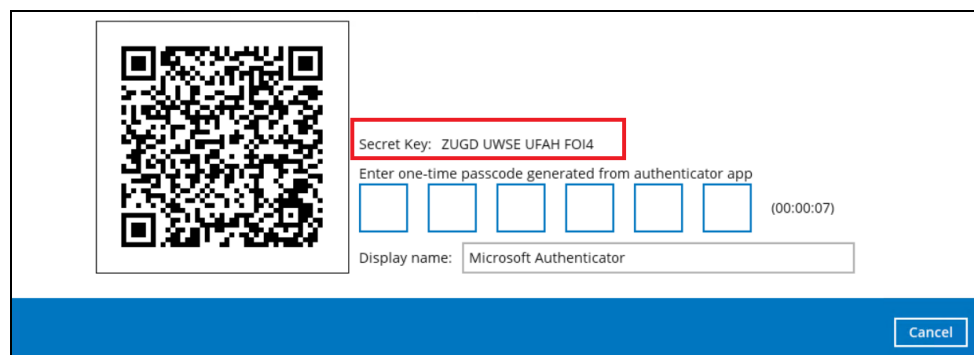
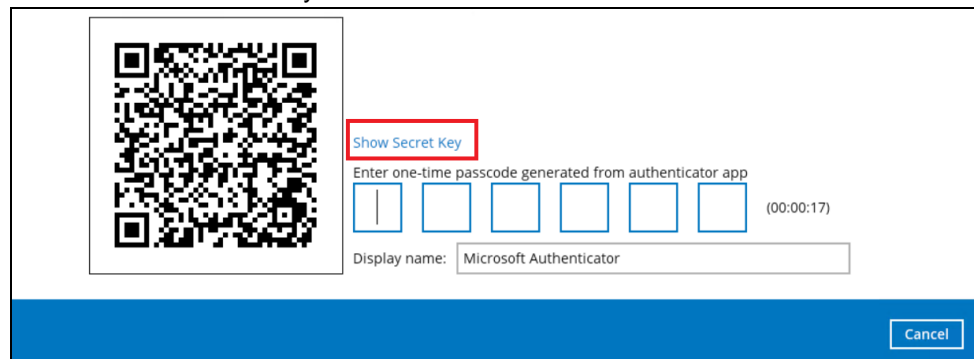


Method 2: Enter Code Manually

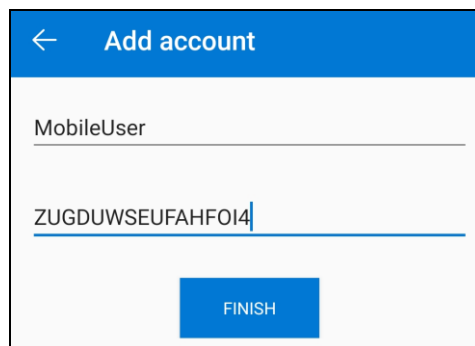
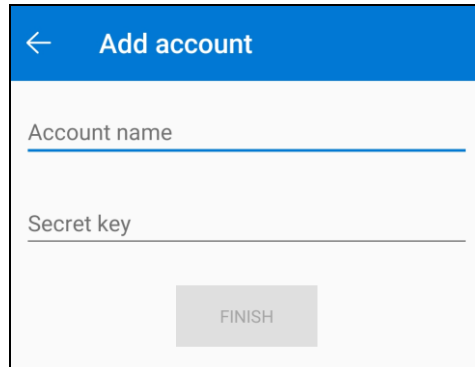
- i. Tap **OR ENTER CODE MANUALLY**.



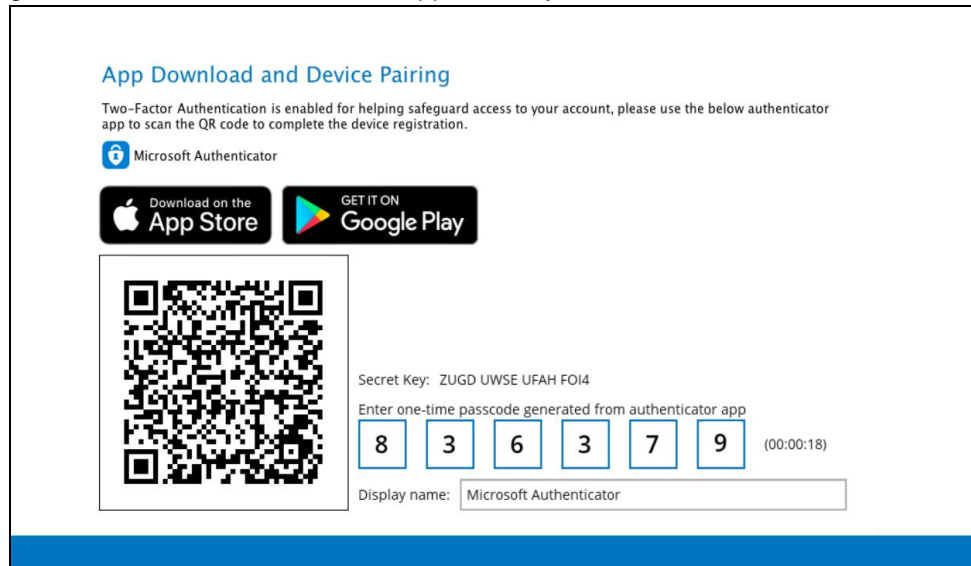
- ii. Click the **Show Secret Key** link in the AhsayOBM to display the Secret Key which must be entered manually in the Microsoft Authenticator.



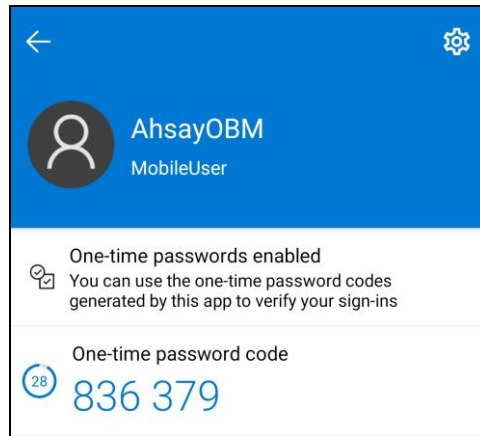
- iii. On the Microsoft Authenticator app, input an account name, then enter the displayed Secret Key in the AhsayOBM. Tap **FINISH** to proceed.



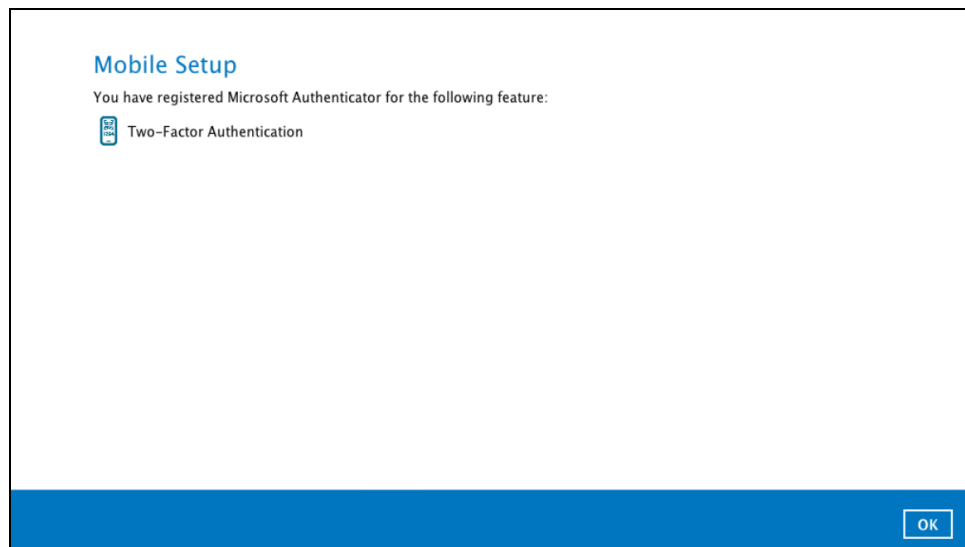
- iv. Once the account is added to Microsoft Authenticator, enter the one-time passcode generated from the authenticator app to AhsayOBM.



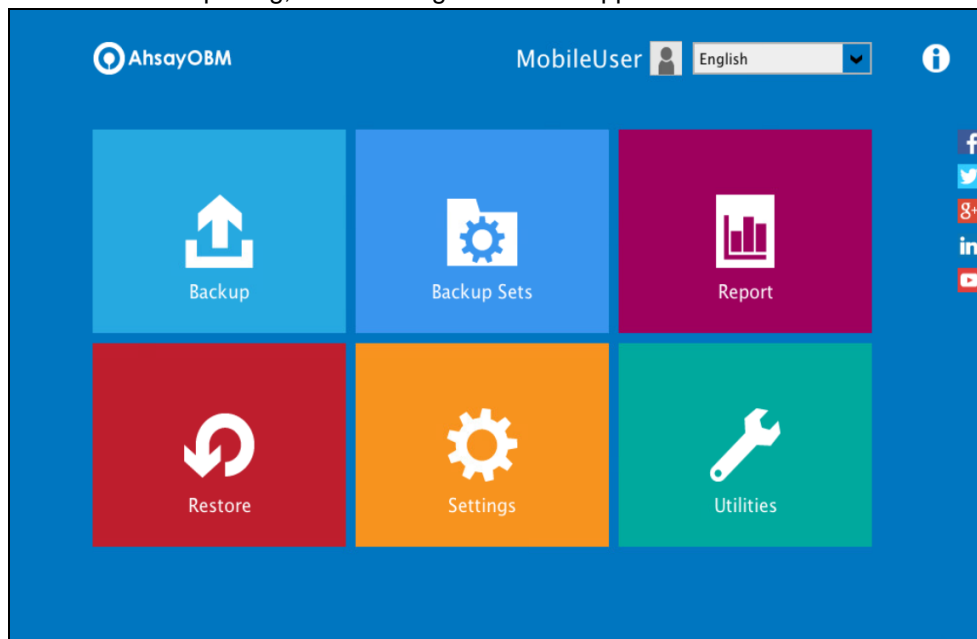
Example of the one-time passcode generated:



- v. The device is successfully registered for TOTP 2FA in AhsayOBM using Microsoft Authenticator. Click **OK** to continue.



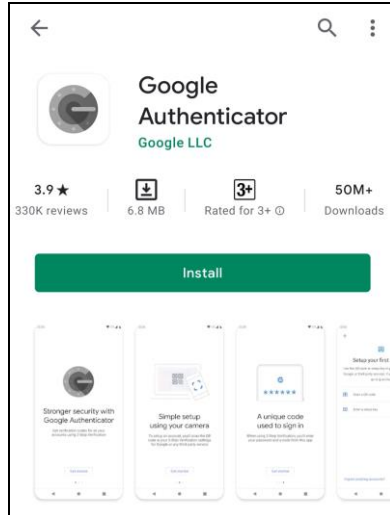
7. After successful pairing, the following screen will appear.



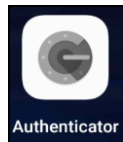
6.3 Using Google Authenticator

To register a device for TOTP 2FA in AhsayOBM using Google Authenticator, please follow the steps below:

1. Download and install the Google Authenticator from the Play Store for Android devices or the App Store for iOS devices.



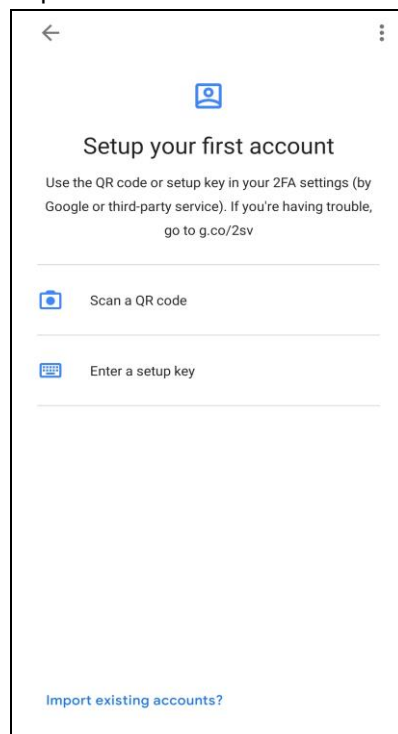
2. Launch the Google Authenticator app.



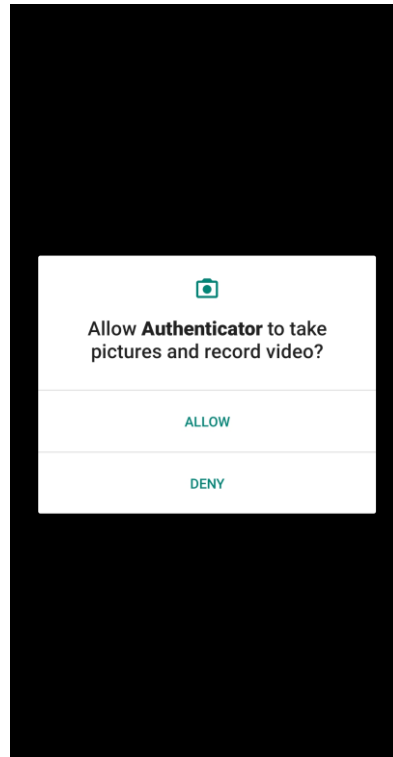
3. Set up the account by selecting from the following methods: Scan the QR code or Enter a setup key manually.

Method 1: Scan the QR code

- i. Tap **Scan a QR code**.



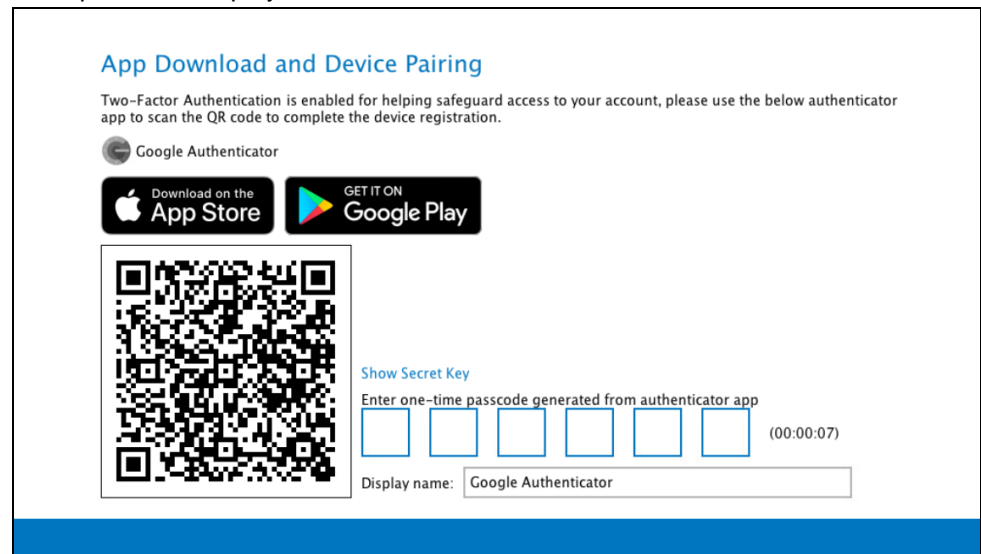
- ii. Allow permission to take pictures and record video.



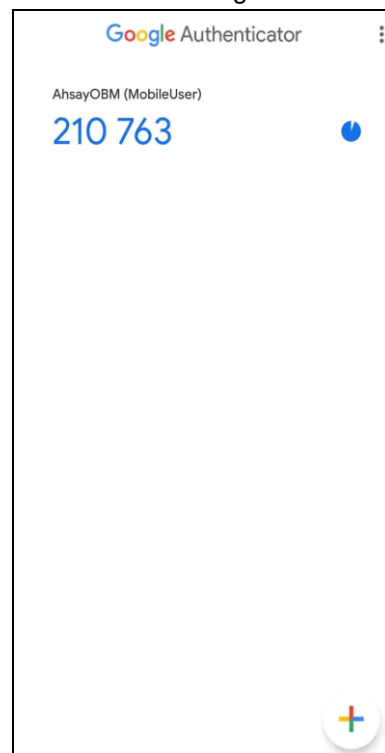
- iii. Scan the QR code on AhsayOBM.



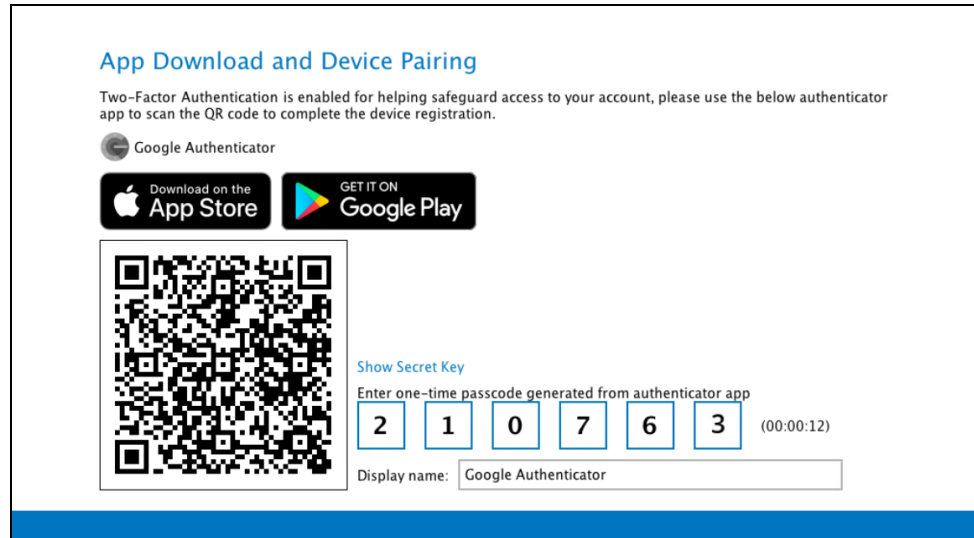
Example of the displayed QR code:



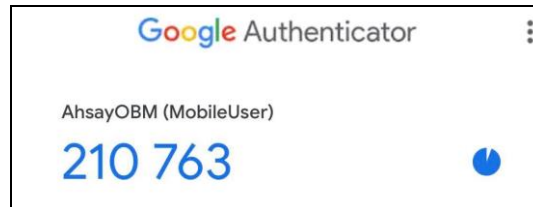
- iv. The AhsayOBM account is successfully added to Google Authenticator and the mobile device is registered in AhsayOBM.



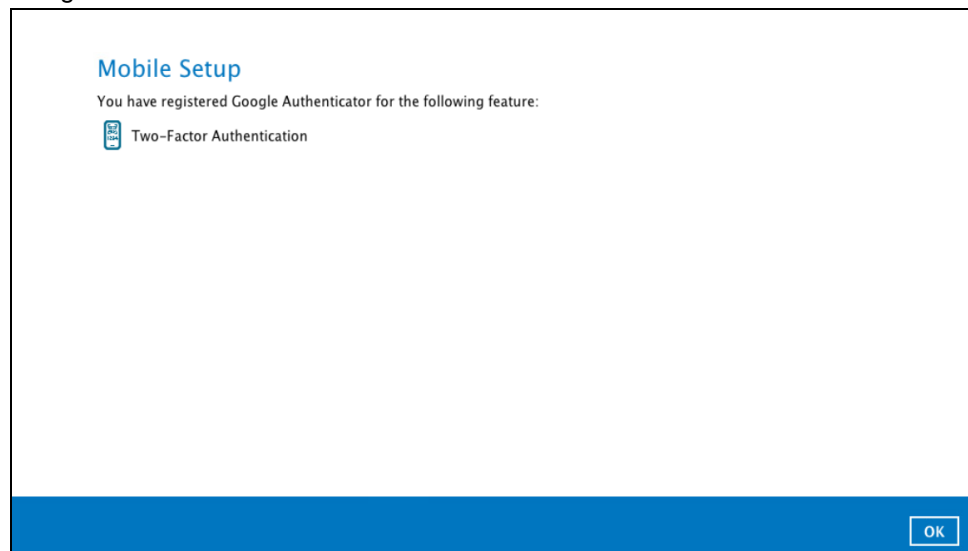
- v. Once the account is added to Google Authenticator, enter the one-time passcode generated from the authenticator app to AhsayOBM.



Example of the one-time passcode generated:

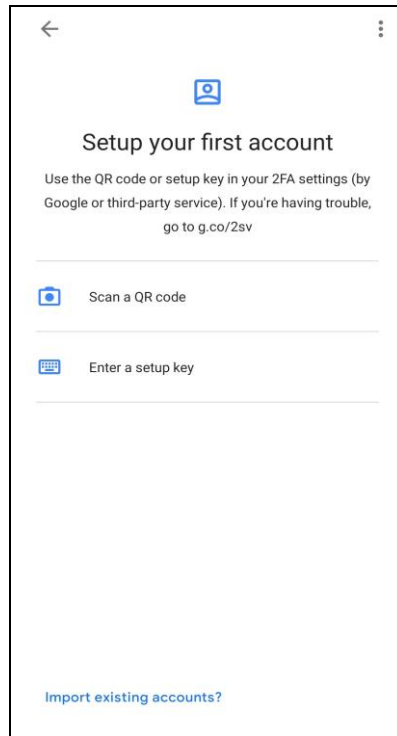


- vi. The device is successfully registered for TOTP 2FA in AhsayOBM using Google Authenticator. Click **OK** to continue.

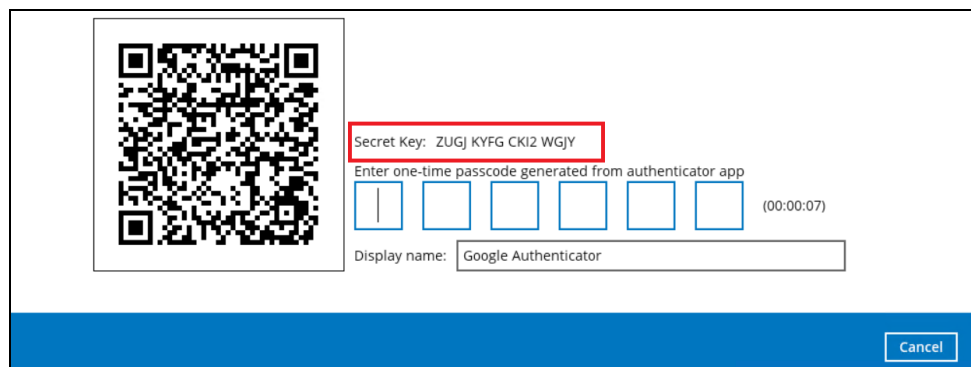


Method 2: Enter a setup key manually

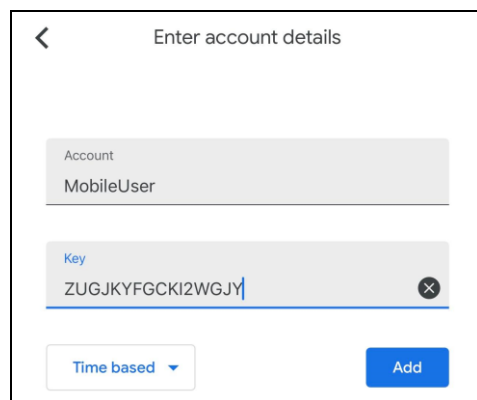
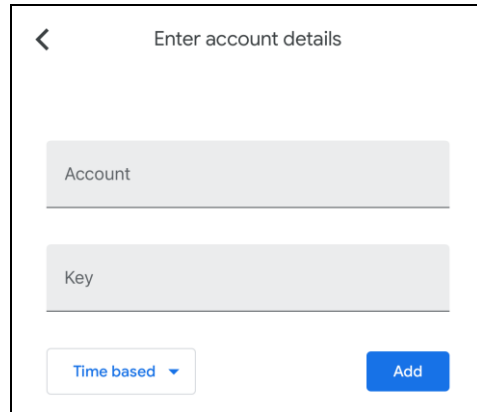
- i. Tap **Enter a setup key**.



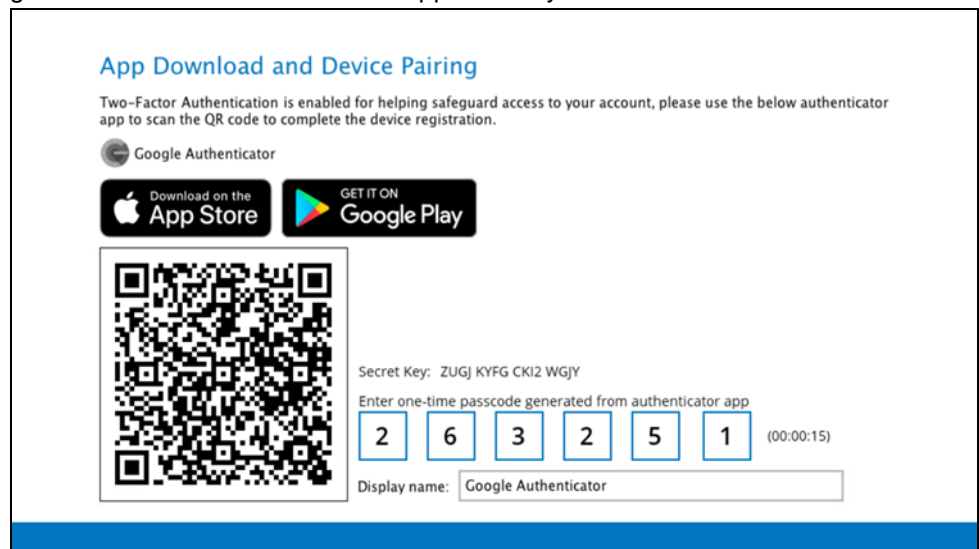
- ii. Click the **Show Secret Key** link in the AhsayOBM to display the Secret Key which must be entered manually on the Google Authenticator.



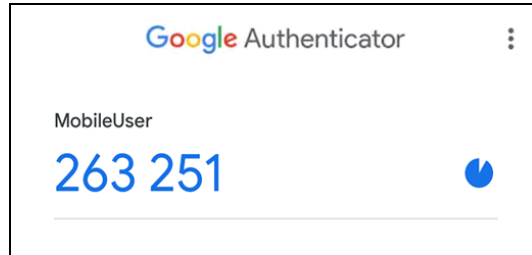
- iii. On the Google Authenticator app, input an account name, then enter the displayed Secret Key in the AhsayOBM. Tap **Add** to proceed.



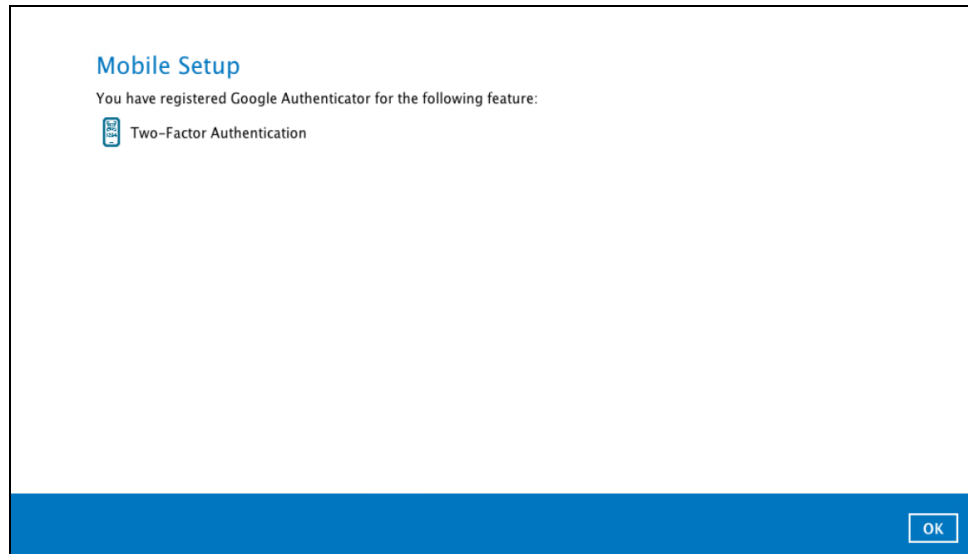
- iv. Once the account is added to Google Authenticator, enter the one-time passcode generated from the authenticator app to AhsayOBM.



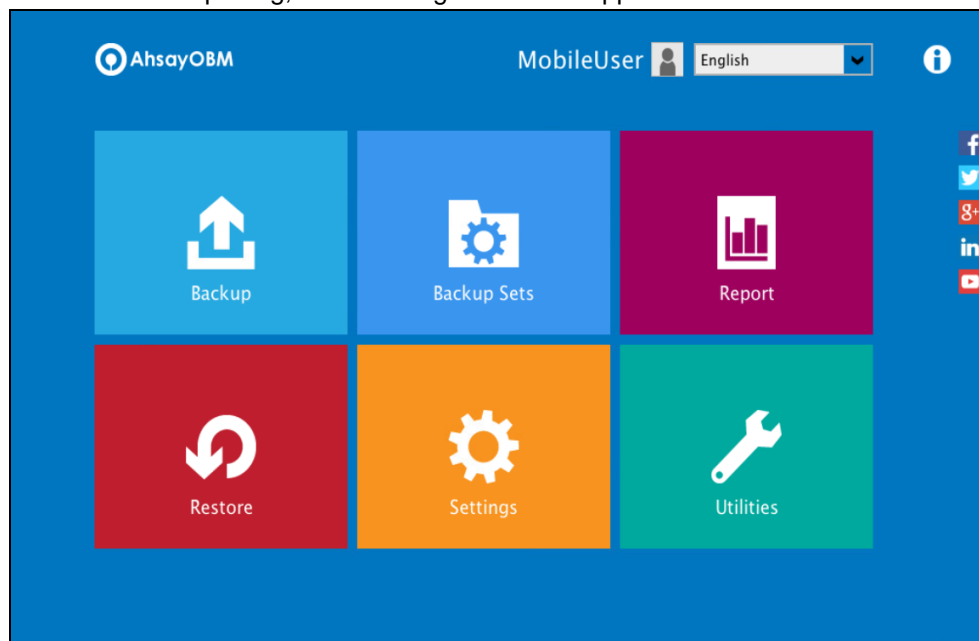
Example of the one-time passcode generated:



- v. The device is successfully registered for TOTP 2FA in AhsayOBM using Google Authenticator. Click **OK** to continue.



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



7 Logging in to AhsayOBM

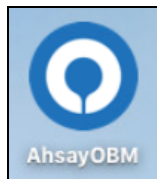
Login steps without 2FA and with 2FA using the different types of authenticator will be discussed in this chapter.

- [Login to AhsayOBM without 2FA](#)
- [Login to AhsayOBM with 2FA using Ahsay Mobile Authenticator](#)
 - Push Notification and TOTP 2FA
 - TOTP only 2FA
- [Login to AhsayOBM with 2FA using Microsoft Authenticator](#)
- [Login to AhsayOBM with 2FA using Google Authenticator](#)
- [Login to AhsayOBM with 2FA using Twilio](#)

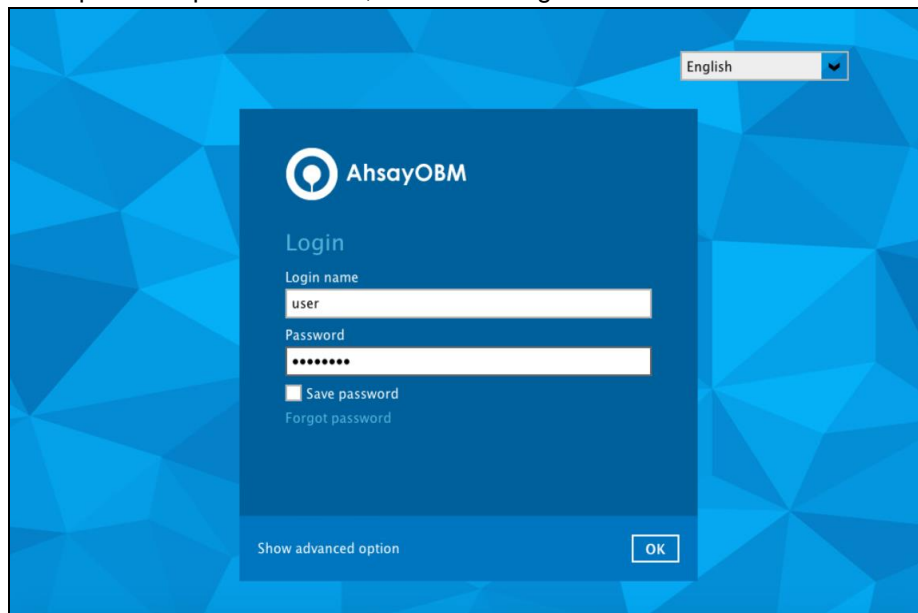
7.1 Login to AhsayOBM without 2FA

When logging in to AhsayOBM without two-factor authentication, please follow the steps below:

1. Double-click the icon to launch the application.



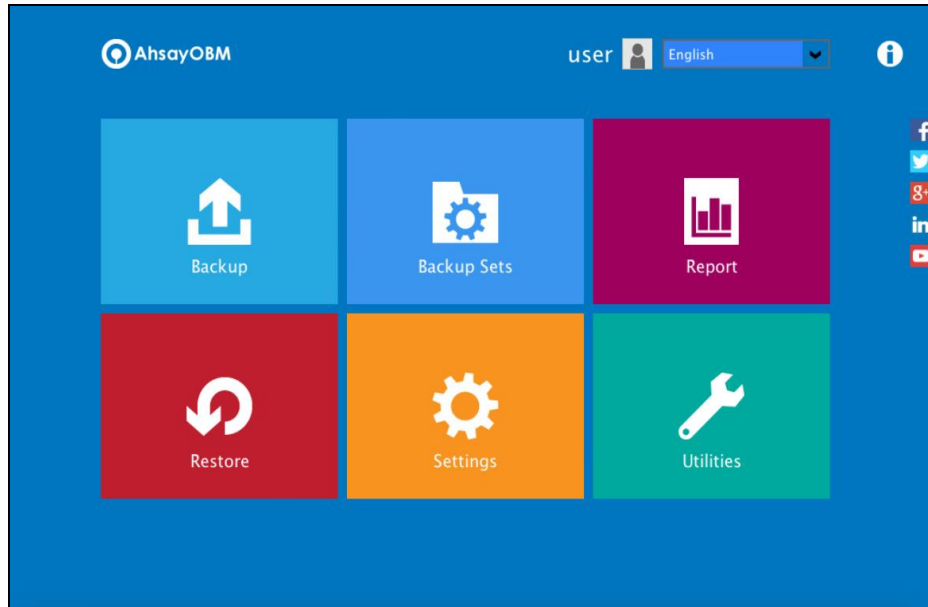
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.

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

NOTE

The **Save password** option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

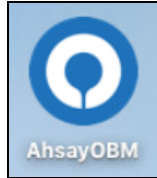
3. After successful login, the following screen will appear.



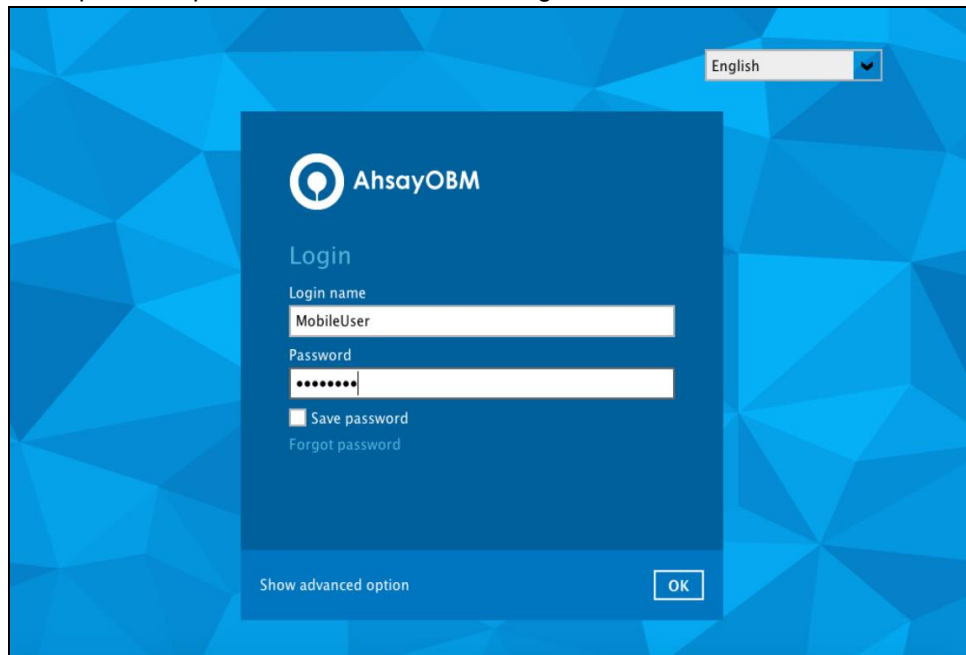
7.2 Login to AhsayOBM with 2FA using Ahsay Mobile Authenticator

When logging in to AhsayOBM with two-factor authentication using Ahsay Mobile Authenticator, please follow the steps below:

1. 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 log in.

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

NOTE

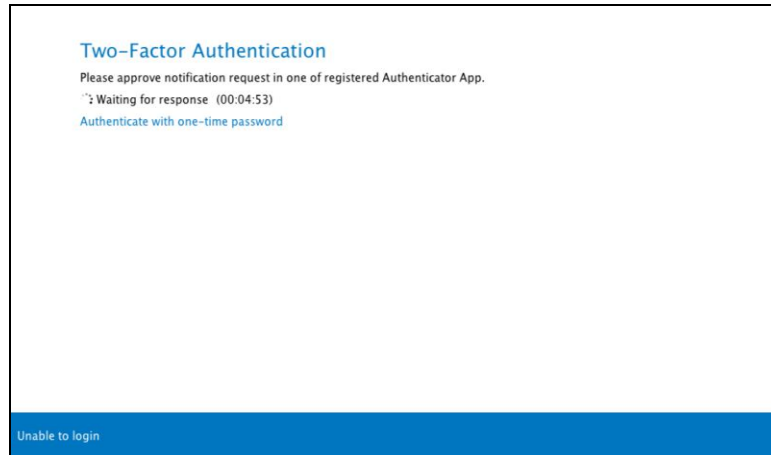
The **Save password** option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

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

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

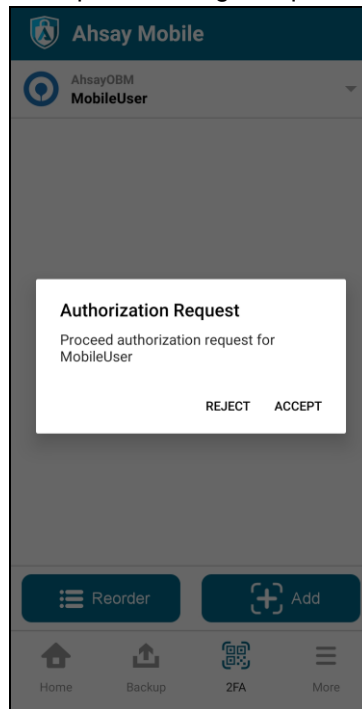
- **Push Notification and TOTP (default mode)**

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

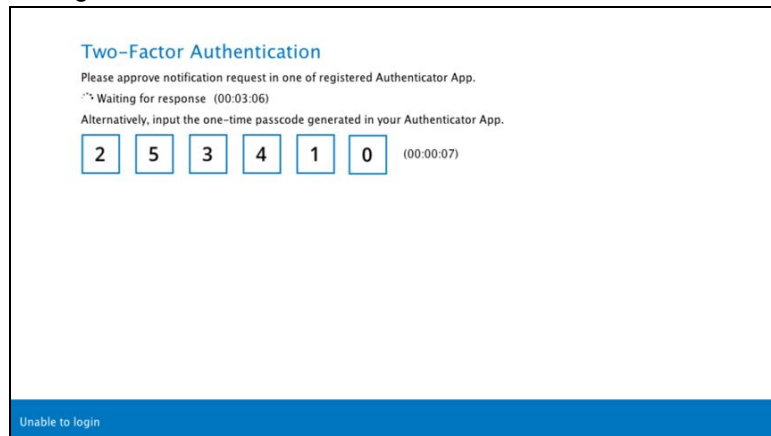


Push notification is the default 2FA mode. Accept the login request on the Ahsay Mobile app to complete the login.

Example of the login request sent to the Ahsay Mobile:

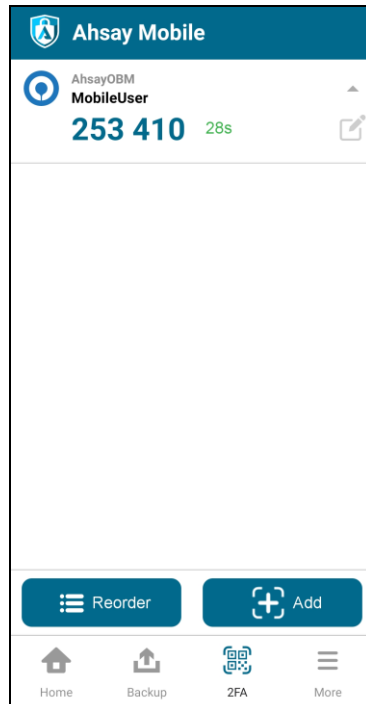


However, if push notification is not working or you prefer to use one-time password instead, click the “**Authenticate with one-time password**” link, then input the one-time password generated from Ahsay Mobile to complete the login.



The image shows a 'Two-Factor Authentication' screen. At the top, it says 'Two-Factor Authentication' in blue. Below that, it says 'Please approve notification request in one of registered Authenticator App.' and 'Waiting for response (00:03:06)'. Then it says 'Alternatively, input the one-time passcode generated in your Authenticator App.' Below this is a row of six input boxes containing the digits 2, 5, 3, 4, 1, and 0. To the right of these boxes is a timer '(00:00:07)'. At the bottom of the screen, there is a blue bar with the text 'Unable to login'.

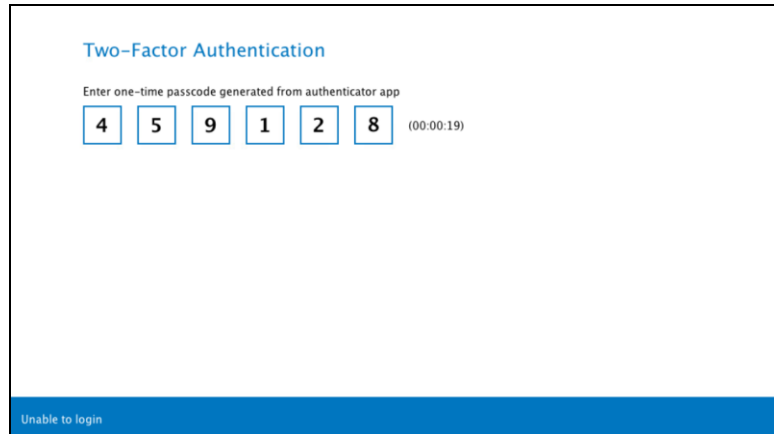
Example of the one-time password generated by Ahsay Mobile:



- **TOTP only**

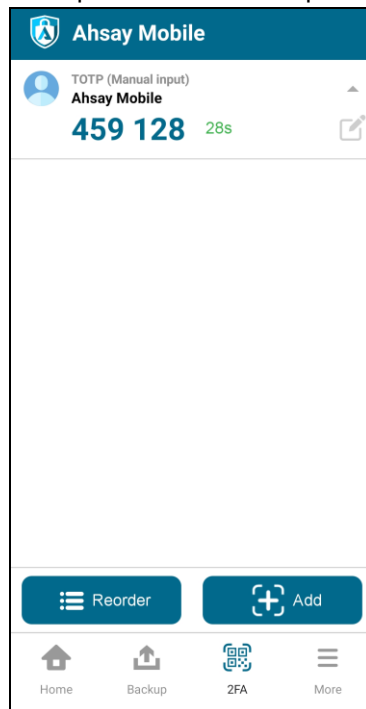
Example of the 2FA alert screen on AhsayOBM after login with correct username and password.

Input the one-time password generated by Ahsay Mobile to complete the login.



The screenshot shows a 'Two-Factor Authentication' screen. At the top, it says 'Two-Factor Authentication' in blue. Below that, it says 'Enter one-time passcode generated from authenticator app'. There are six input boxes containing the digits 4, 5, 9, 1, 2, and 8. To the right of these boxes is a timer showing '(00:00:19)'. At the bottom of the screen, there is a blue bar with the text 'Unable to login'.

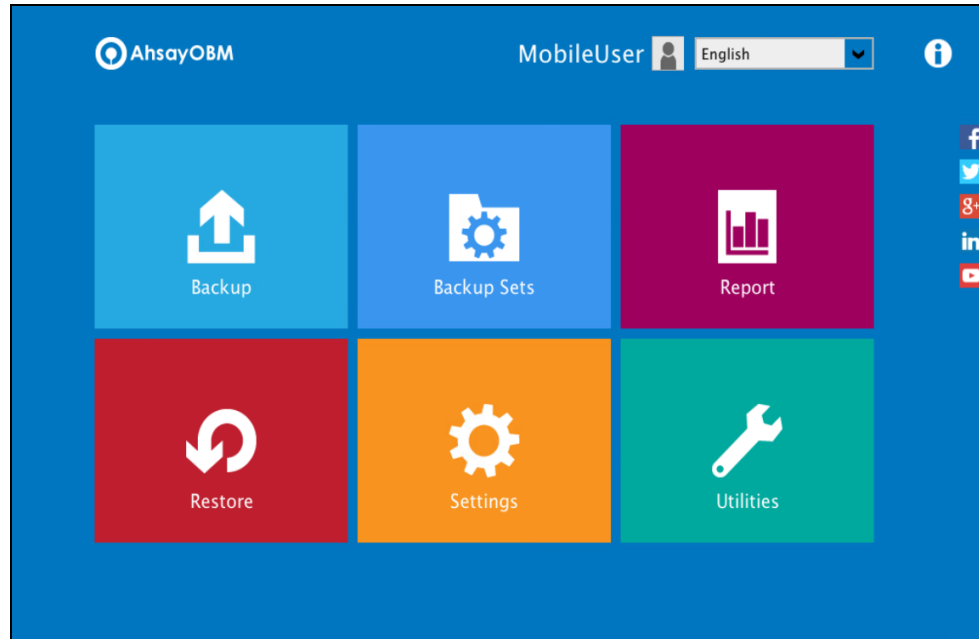
Example of the one-time password generated by Ahsay Mobile:



NOTE

If you are unable to log in using any of the authentication method, please refer to [Chapter 8 Unable to log in to AhsayOBM with 2FA](#).

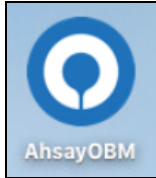
4. After successful login, the following screen will appear.



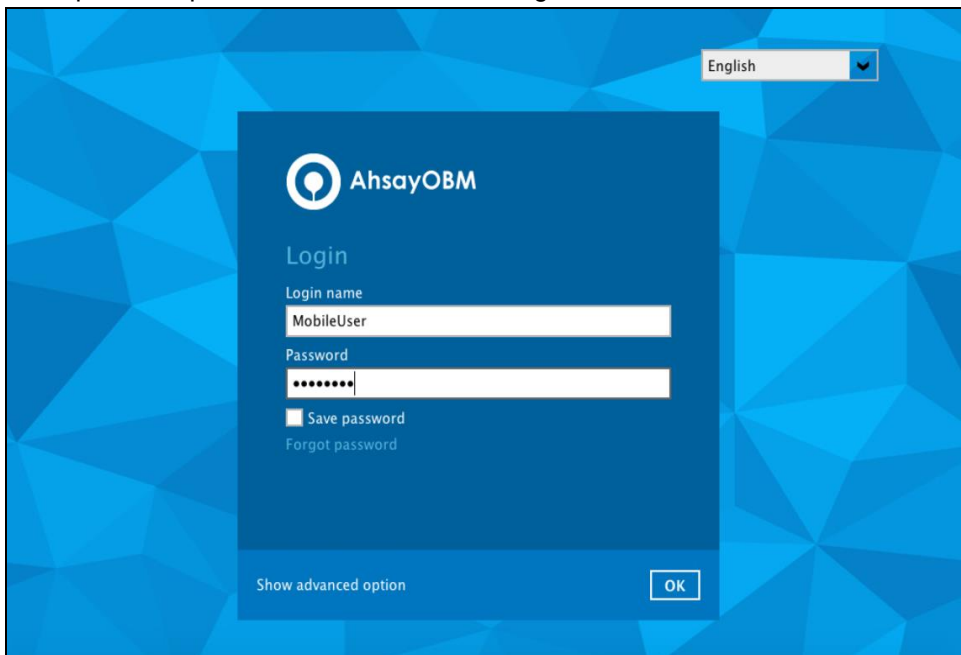
7.3 Login to AhsayOBM with 2FA using Microsoft Authenticator

When logging in to AhsayOBM with two-factor authentication using Microsoft Authenticator, please follow the steps below:

1. 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 log in.

The image shows the AhsayOBM login screen. The background is a blue geometric pattern. In the center is a dark blue rectangular box with the AhsayOBM logo and the word 'AhsayOBM' at the top. Below this is the word 'Login'. There are two input fields: 'Login name' with the text 'MobileUser' and 'Password' with a masked password '*****'. Below the password field is a checkbox labeled 'Save password' and a link 'Forgot password'. At the bottom of the box are two buttons: 'Show advanced option' and 'OK'. In the top right corner of the login box, there is a language dropdown menu set to 'English'.

NOTE

The **Save password** option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

3. Enter the one-time passcode generated from the Microsoft Authenticator app.


Two-Factor Authentication


Enter one-time passcode generated from authenticator app


(00:00:00)


Unable to login

Example of the one-time passcode generated:

← 

 **AhsayOBM**
MobileUser

 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
836 379

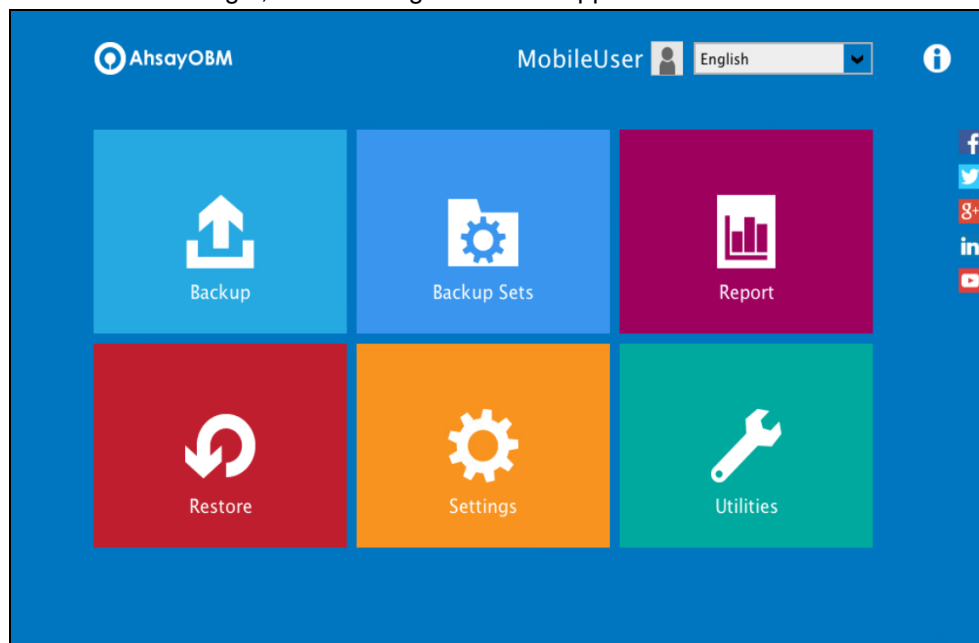
Two-Factor Authentication

Enter one-time passcode generated from authenticator app

(00:00:07)

Unable to login

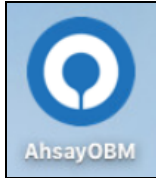
4. After successful login, the following screen will appear.



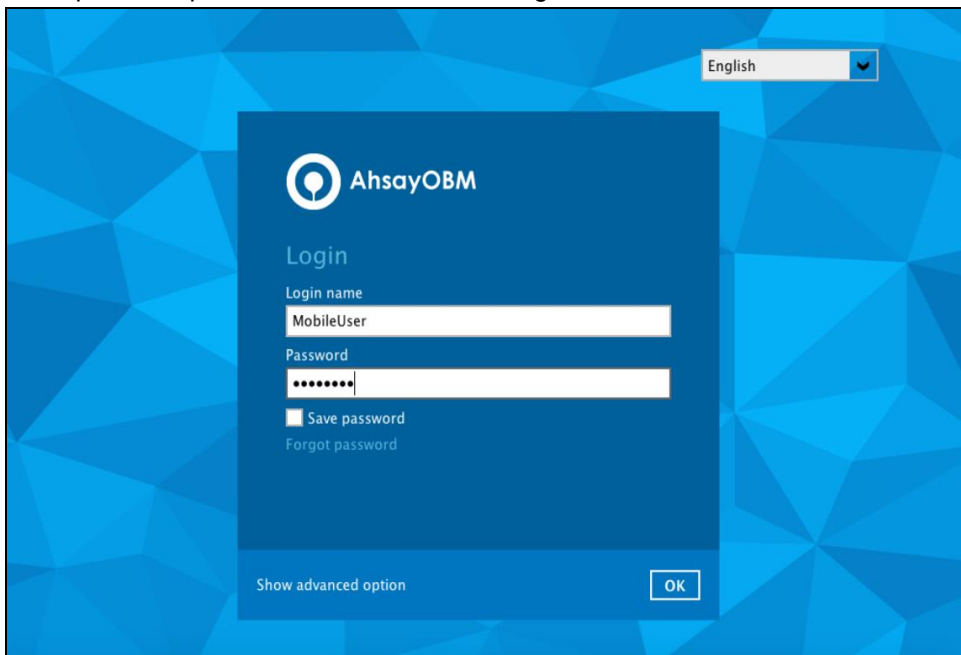
7.4 Login to AhsayOBM with 2FA using Google Authenticator

When logging in to AhsayOBM with two-factor authentication using Google Authenticator, please follow the steps below:

1. 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 log in.

The image shows the AhsayOBM login screen. The background is a blue geometric pattern. In the center is a dark blue rectangular box with the AhsayOBM logo and the word 'AhsayOBM' in white. Below the logo, the word 'Login' is written in white. There are two input fields: 'Login name' with the text 'MobileUser' and 'Password' with a masked password '*****'. Below the password field is a checkbox labeled 'Save password' and a link 'Forgot password'. At the bottom of the box, there is a link 'Show advanced option' and an 'OK' button. In the top right corner of the screen, there is a language dropdown menu set to 'English'.

NOTE

The **Save password** option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

3. Enter the one-time passcode generated from the Google Authenticator app.

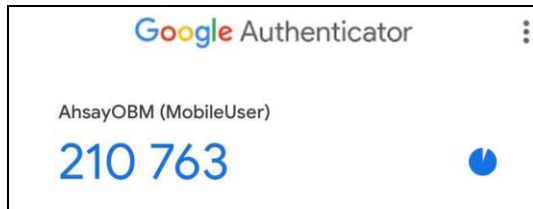
Two-Factor Authentication

Enter one-time passcode generated from authenticator app

(00:00:00)

Unable to login

Example of the one-time passcode generated:



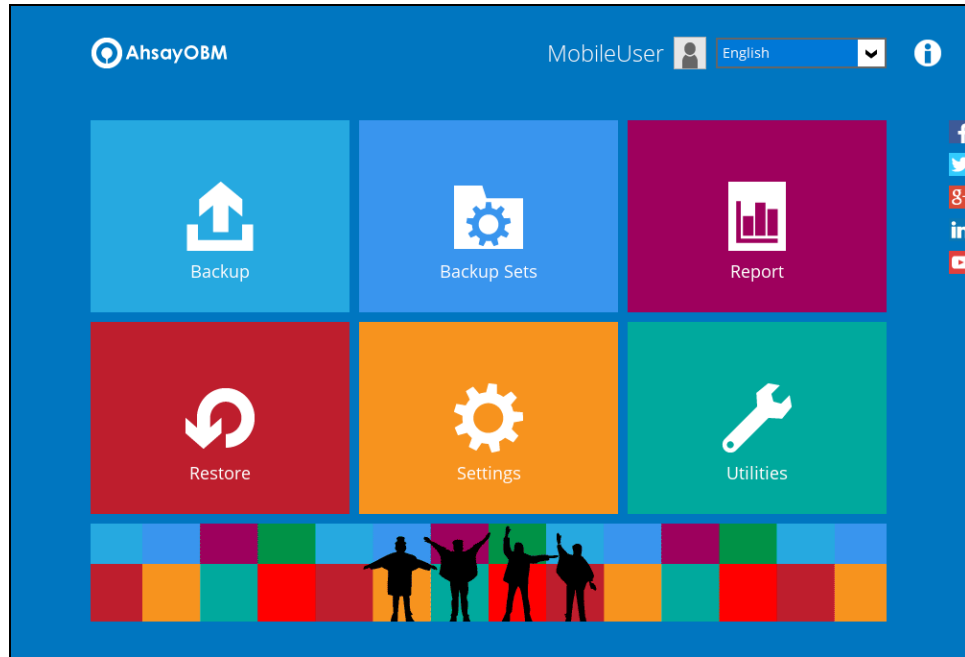
Two-Factor Authentication

Enter one-time passcode generated from authenticator app

(00:00:24)

Unable to login

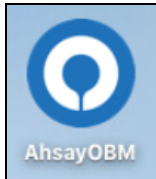
4. After successful login, the following screen will appear.



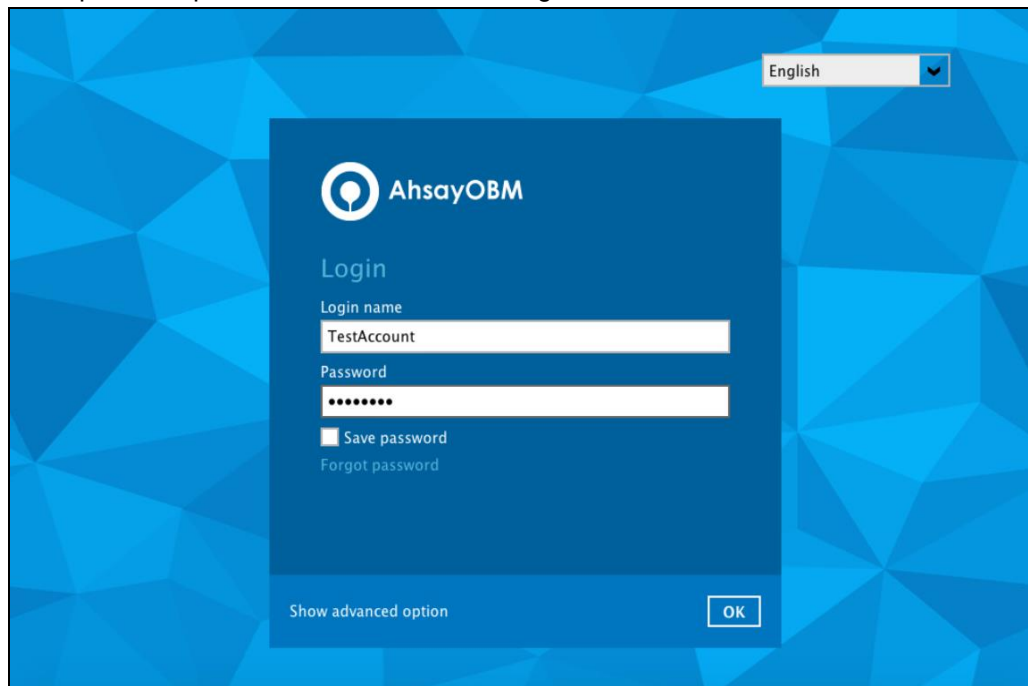
7.5 Login to AhsayOBM with 2FA using Twilio

When logging in to AhsayOBM for user accounts using Twilio, please follow the steps below:

1. 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 log in.

The image shows the AhsayOBM login screen. The background is a blue geometric pattern. In the top right corner, there is a language dropdown menu set to 'English'. In the center, there is a dark blue login box. Inside the box, the AhsayOBM logo and name are at the top. Below that is the word 'Login'. There are two input fields: 'Login name' with the text 'TestAccount' and 'Password' with masked characters. Below the password field is a checkbox labeled 'Save password' and a link 'Forgot password'. At the bottom of the login box, there is a link 'Show advanced option' and an 'OK' button.


NOTE

The **Save password** option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

3. Select your phone number to receive the passcode.

Two-Factor Authentication

Please select phone number to receive passcode via SMS message to continue login.

 Philippines (+63) - *****6123

CancelHelp

4. Enter the passcode and click **Verify** to log in.

Two-Factor Authentication

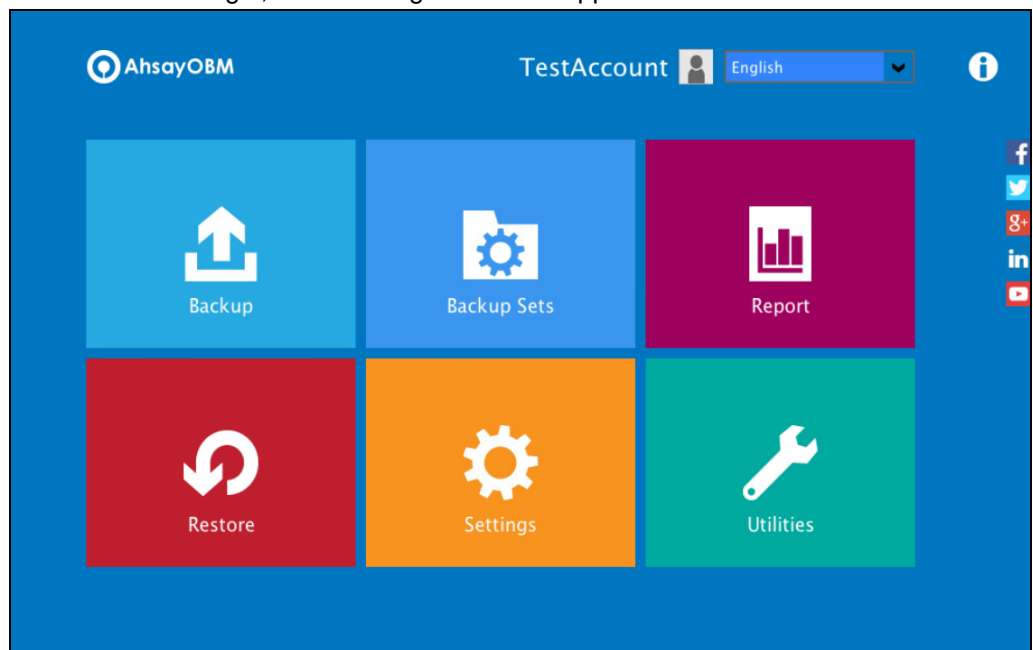
SMS message with a passcode was already sent to the phone number Philippines (+63) - *****6123
Please enter the passcode to continue login.

XIUA - (00:04:30)

Resend passcode

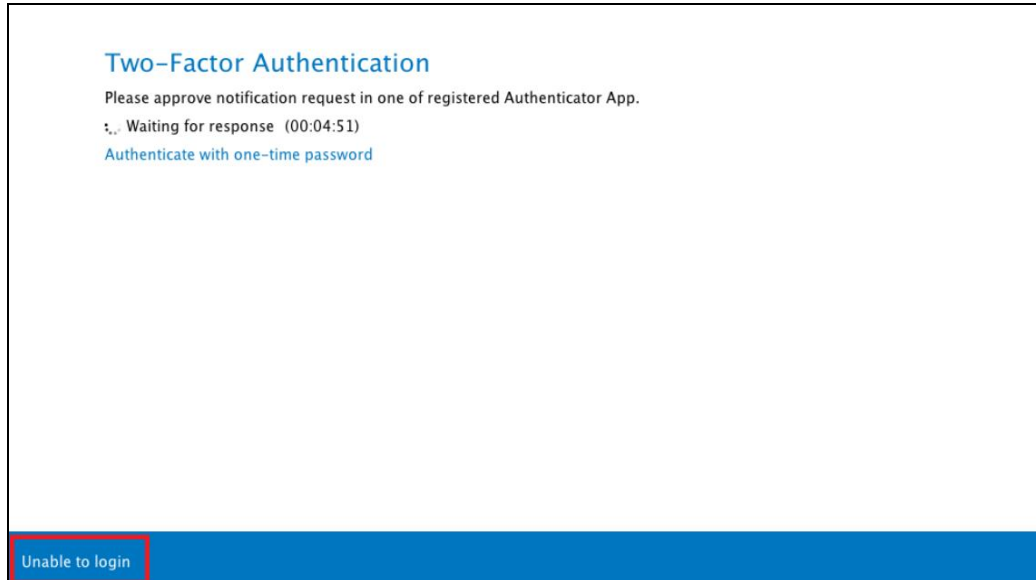
VerifyCancelHelp

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



8 Unable to log in to AhsayOBM with 2FA

AhsayOBM supports **Unable to login** feature for users who were not able to accept the notification request from the Ahsay Mobile app and/or cannot obtain the TOTP code from Ahsay Mobile on the subsequent login to AhsayOBM.

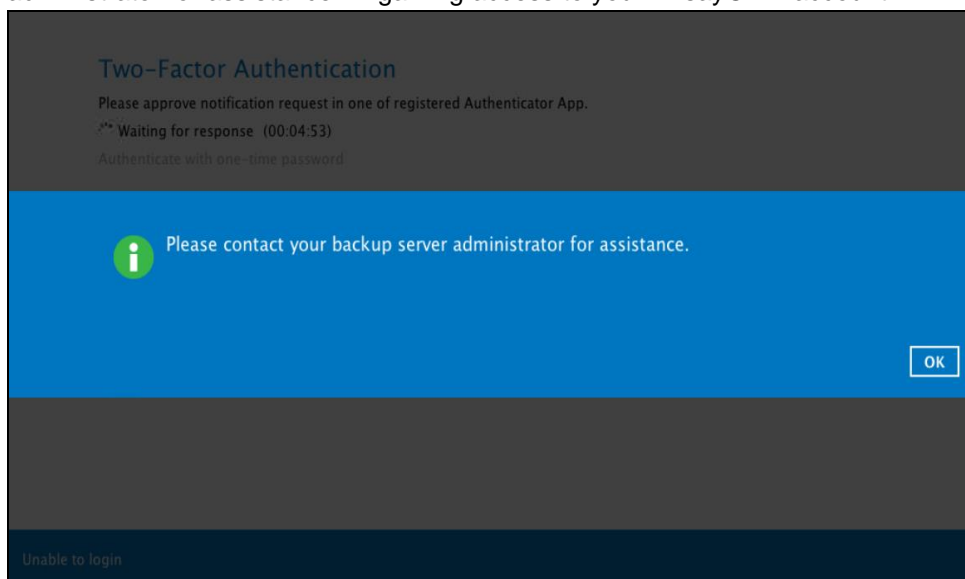


Here are the three scenarios after clicking the **Unable to login** link:

- [No recovery number was registered on Ahsay Mobile for the 2FA account](#)
- ["Authentication Recovery" procedure](#)
- [Unable to perform the "Authentication Recovery" procedure](#)

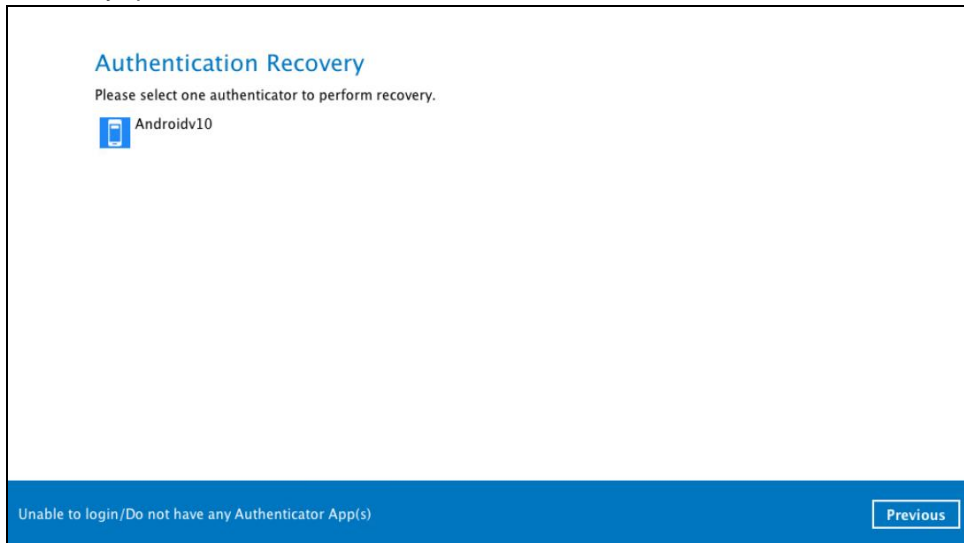
1. No recovery number was registered on Ahsay Mobile for the 2FA account

If no recovery number was registered on Ahsay Mobile for the 2FA account, then the following message will be displayed "Please contact your backup server administrator for assistance" in gaining access to your AhsayOBM account.



2. "Authentication Recovery" procedure

If a recovery number was registered on Ahsay Mobile for the 2FA account, then select the registered mobile device to perform the following "Authentication Recovery" procedure.

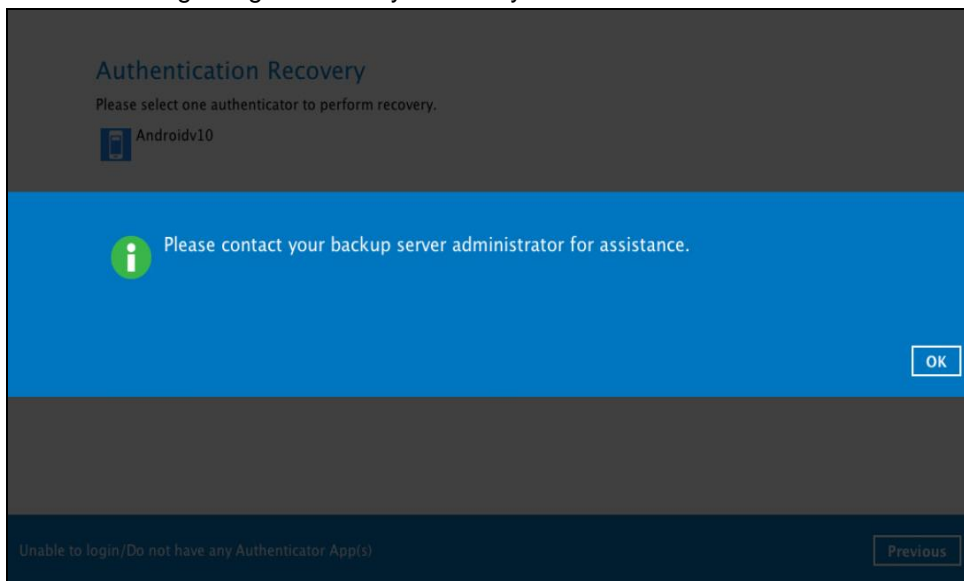


NOTE

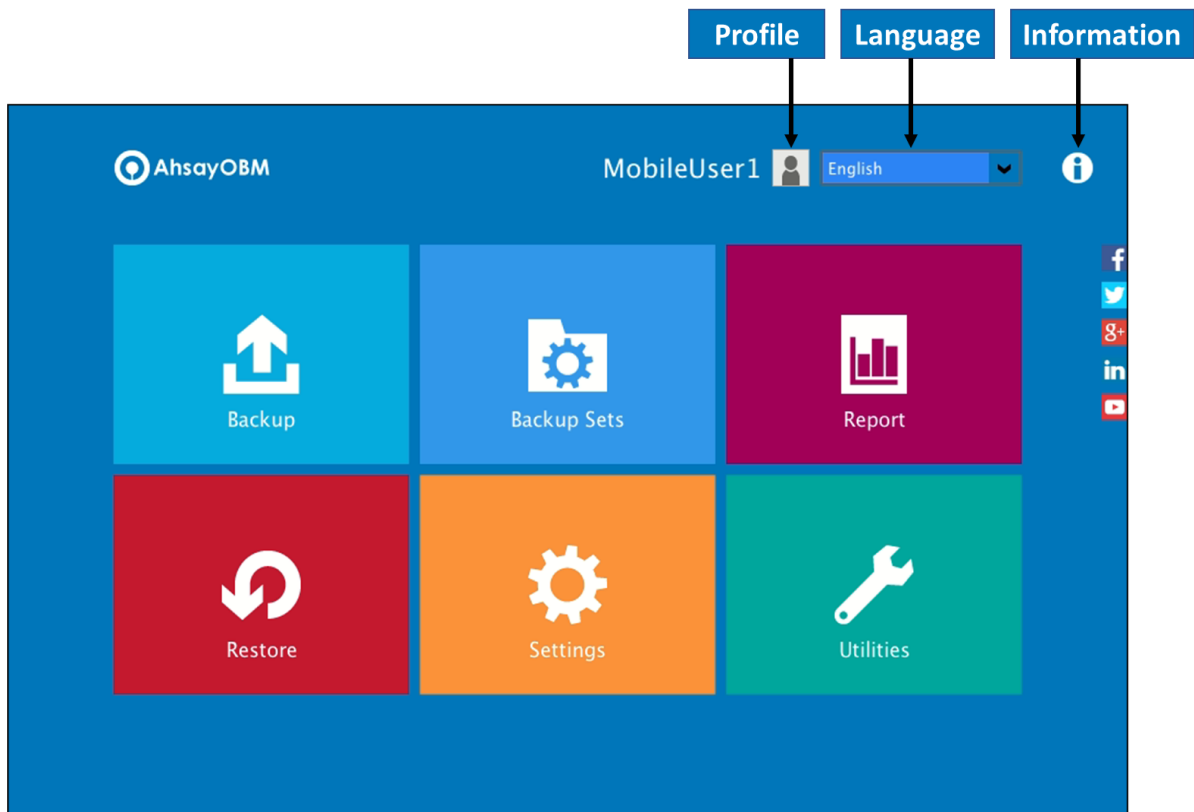
For the detailed steps in performing Authentication Recovery, please refer to the **Appendix A: Troubleshooting Login** of the [Ahsay Mobile User Guide for Android and iOS](#).

3. Unable to perform the "Authentication Recovery" procedure

If you are not able to perform the "Authentication Recovery" procedure, click the **Unable to login/Do not have any Authenticator App(s)** link, then the following message will be displayed "Please contact your backup server administrator for assistance" in gaining access to your AhsayOBM account.



9 AhsayOBM Overview

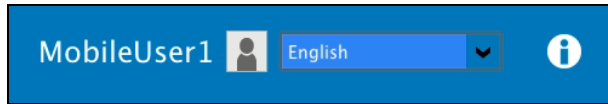


AhsayOBM main interface has nine (9) icons that can be accessed by the user:

- [Profile](#)
- [Language](#)
- [Information](#)
- [Backup](#)
- [Backup Sets](#)
- [Report](#)
- [Restore](#)
- [Settings](#)
- [Utilities](#)

9.1 Profile

The **Profile** icon shows the settings that can be modified by the user. The features that will be shown will depend on 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 seven (7) 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](#)
- ◉ [Security Settings](#) (Only shown for backup accounts created prior to AhsayOBM v8.5.0.0 and using Twilio for two-factor authentication.)

9.1.1 General

The General tab displays the user's information.

A screenshot of the 'User Information' form within the 'Profile' section. The left sidebar shows 'General' as the selected tab, with other options like 'Contacts', 'Time Zone', 'Encryption Recovery', and 'Authentication'. The main area is titled 'User Information' and contains two fields: 'Login name' with the value 'MobileUser1' and 'Display name' with an empty text input box. At the bottom right of the form are 'Save' and 'Cancel' buttons.

| 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
- Security Settings

User Information

Login name MobileUser1
Display name

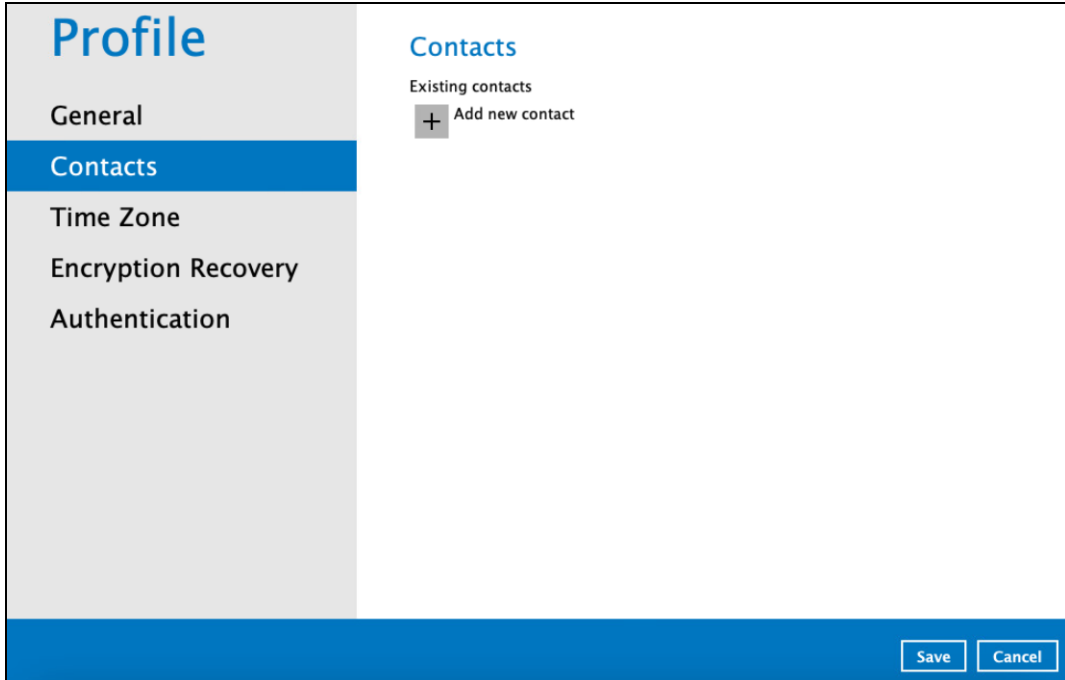
Last Successful Login

Time: 12/14/2020 19:57 (PHT)
IP address: 175.176.32.185
Phone number (MFA): 63-
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 log in. |
| 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. |

9.1.2 Contacts

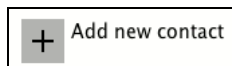
This refers to the contact information of the user. You can also add multiple contacts or modify existing contact information. Having this filled in will help in sending backup and daily reports and even recovered backup set encryption key in case it was forgotten or lost.



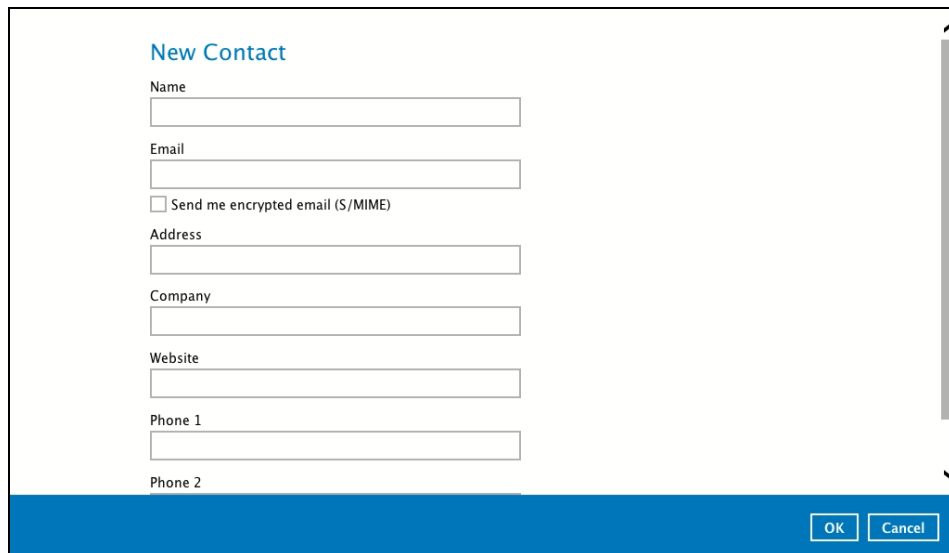
The screenshot shows a web interface for a user profile. On the left is a sidebar with the title 'Profile' and several menu items: 'General', 'Contacts' (which is highlighted with a blue background), 'Time Zone', 'Encryption Recovery', and 'Authentication'. The main content area on the right is titled 'Contacts' in blue. Below this title, it says 'Existing contacts' and then a button with a plus sign and the text 'Add new contact'. At the bottom right of the main content area, there are two buttons: 'Save' and 'Cancel'.

To add a new contact, follow the instructions below:

1. Click the **[+]** button 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', and 'Authentication'. The main content area is titled 'Contacts' and shows 'Existing contacts' with a list containing one entry: 'samplename' with email 'sample_email@mail.com'. Below this is an 'Add' button. At the bottom right, there are 'Save' and 'Cancel' buttons. The page has a blue footer bar.

Profile

General

Contacts

Time Zone

Encryption Recovery

Authentication

Contacts

Existing contacts

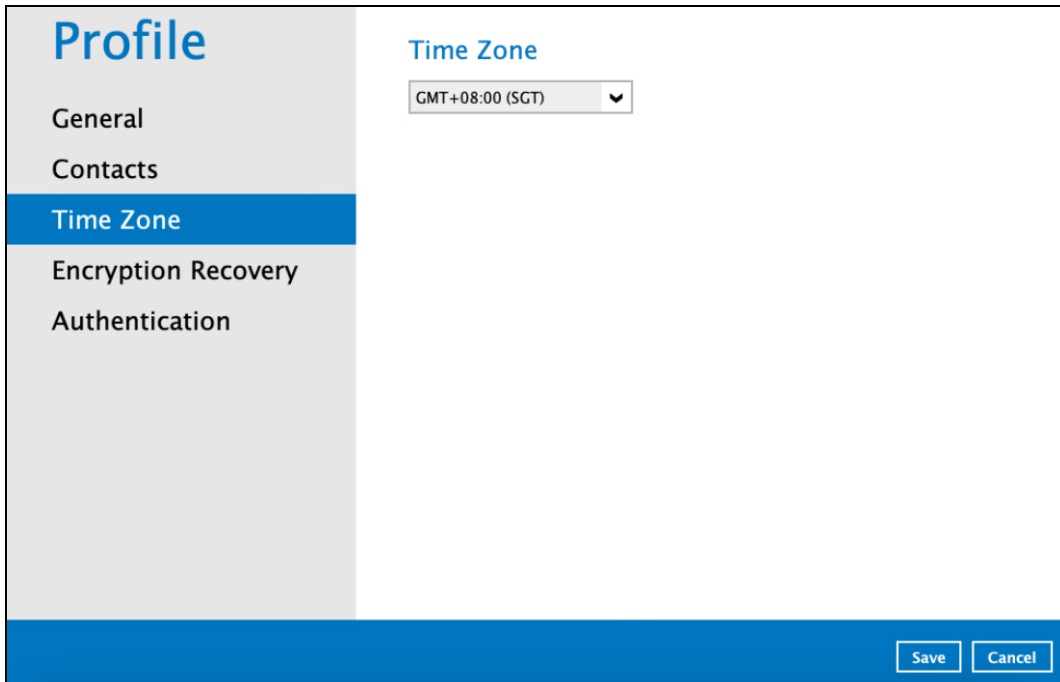
 samplename
sample_email@mail.com

Add

Save Cancel

9.1.3 Time Zone

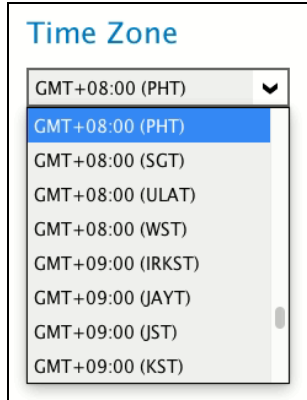
The time zone indicated.



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' (which is highlighted with a blue background), 'Encryption Recovery', and 'Authentication'. The main content area is titled 'Time Zone' in blue. Below the title is a dropdown menu currently showing 'GMT+08:00 (SGT)'. At the bottom right of the main area are two buttons: 'Save' and 'Cancel'.

To modify the time zone, follow the instructions below:

1. Select from the dropdown list.



This screenshot shows the 'Time Zone' dropdown menu expanded. The title 'Time Zone' is at the top. The dropdown list contains the following options: 'GMT+08:00 (PHT)', '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)'. The first option, 'GMT+08:00 (PHT)', is currently selected and highlighted in blue.

2. Click **Save** to save the updated time zone

9.1.4 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

Encryption Recovery

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

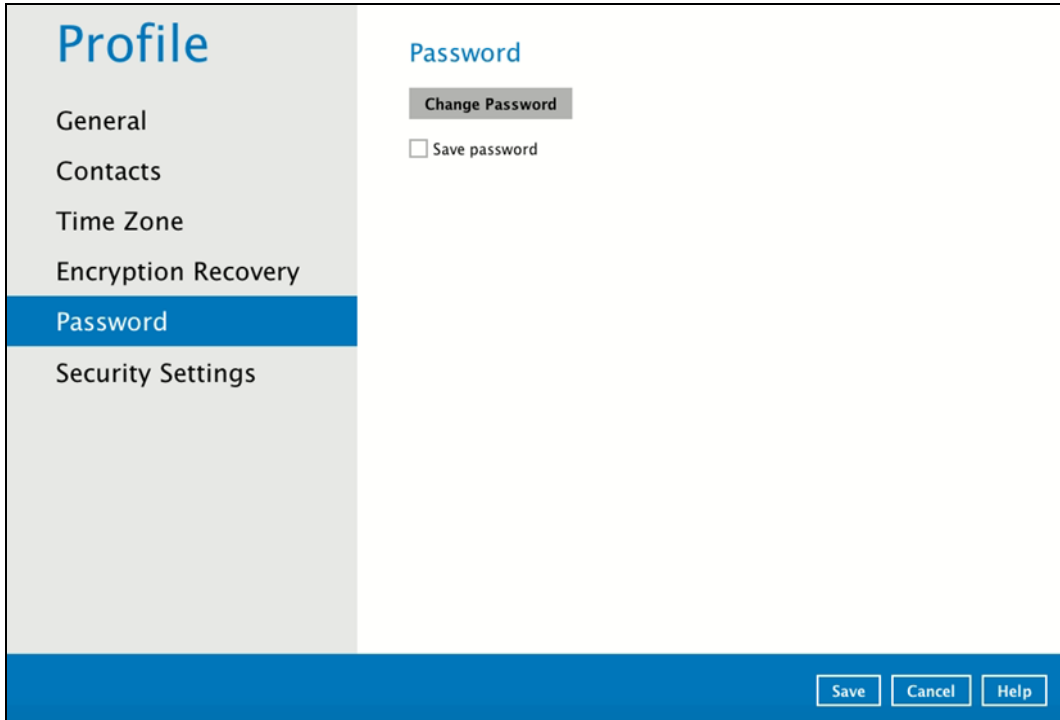
On ☒

SaveCancel

9.1.5 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 in AhsayOBM. On the left is a sidebar menu with options: General, Contacts, Time Zone, Encryption Recovery, Password (highlighted in blue), 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 of the main area are three buttons: 'Save', 'Cancel', and 'Help'.

NOTE

The **Save password** option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

9.1.6 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 **Chapter 6.3.1** of the [Ahsay Mobile User Guide for Android and iOS](#) for the detailed step-by-step procedure.

- [Remove one or more device\(s\)](#) registered for Two-Factor Authentication (2FA).
- [Re-pair](#) mobile device with AhsayOBM account.
- View details of the “[Last Successful Login](#)” for Password Lock and Two-Factor Authentication (2FA).

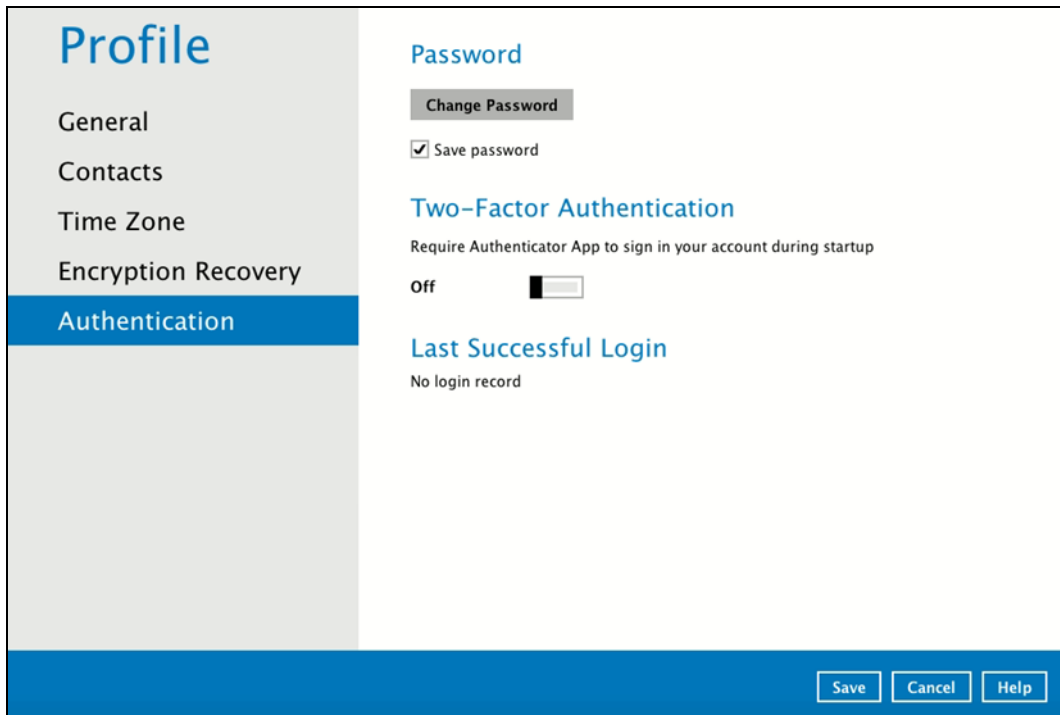
NOTE

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, LastPass Authenticator, iOS 15 Built-in Two-Factor Authenticator, etc.).

The screenshot shows the 'Profile' page of the Ahsay Mobile app. On the left is a sidebar menu with options: General, Contacts, Time Zone, Encryption Recovery, and Authentication (which is highlighted in blue). The main content area is titled 'Authentication' and contains three sections: 'Password' with a 'Change Password' button and a 'Save password' checkbox; 'Two-Factor Authentication' with a toggle switch currently set to 'Off' and the text 'Require Authenticator App to sign in your account during startup'; and 'Last Successful Login' showing 'No login record'. At the bottom right of the page are three buttons: 'Save', 'Cancel', and 'Help'.

Password

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



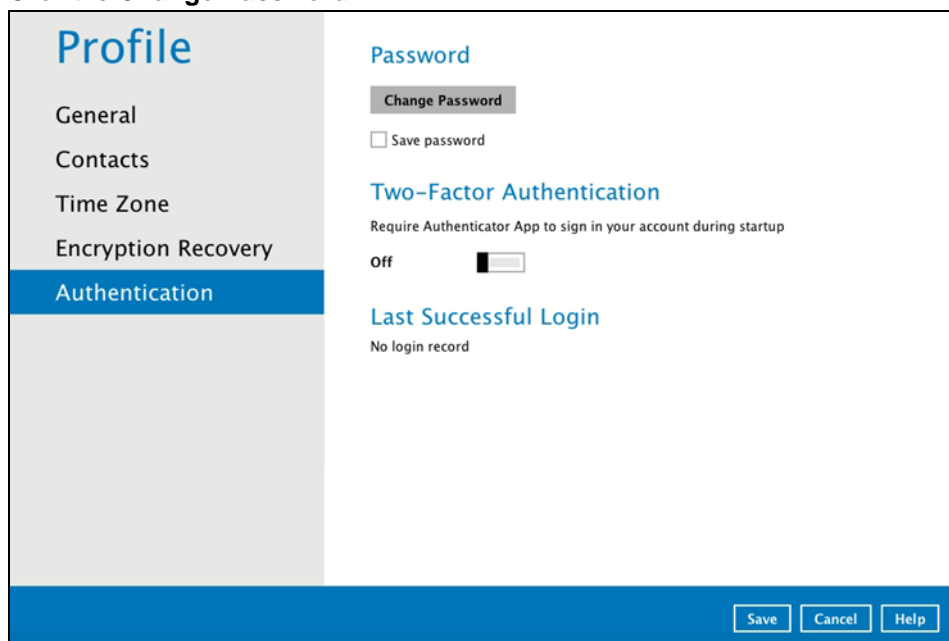
The screenshot shows the 'Profile' page with a sidebar on the left containing links: General, Contacts, Time Zone, Encryption Recovery, and Authentication (which is highlighted in blue). The main content area is titled 'Password' and includes a 'Change Password' button. Below this is a checkbox labeled '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.

NOTE

The **Save password** option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

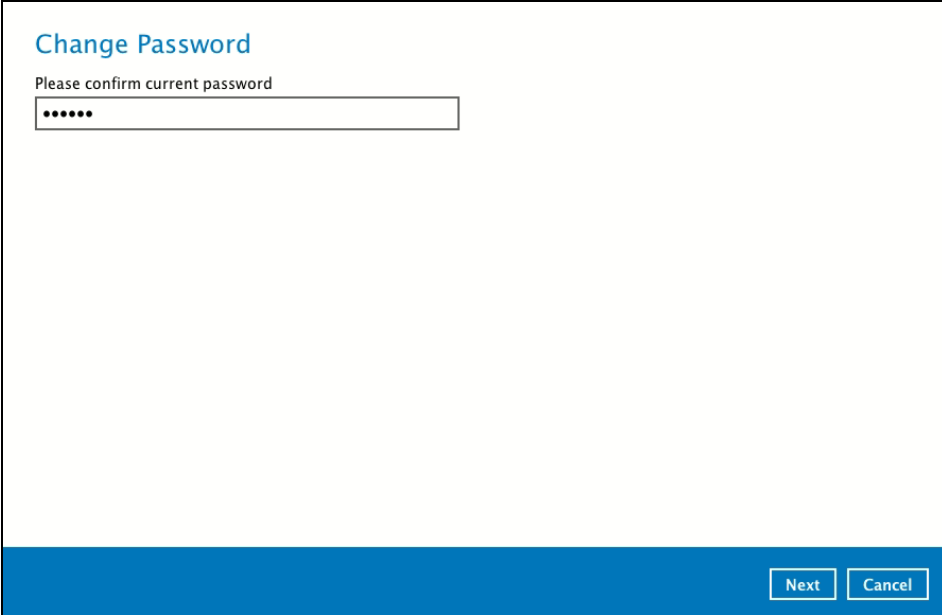
To change the password, follow the instructions below:

1. Click the **Change Password**.



This screenshot is identical to the one above, but the 'Change Password' button is highlighted with a grey border to indicate it should be clicked. The 'Save password' checkbox is now unchecked.

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".

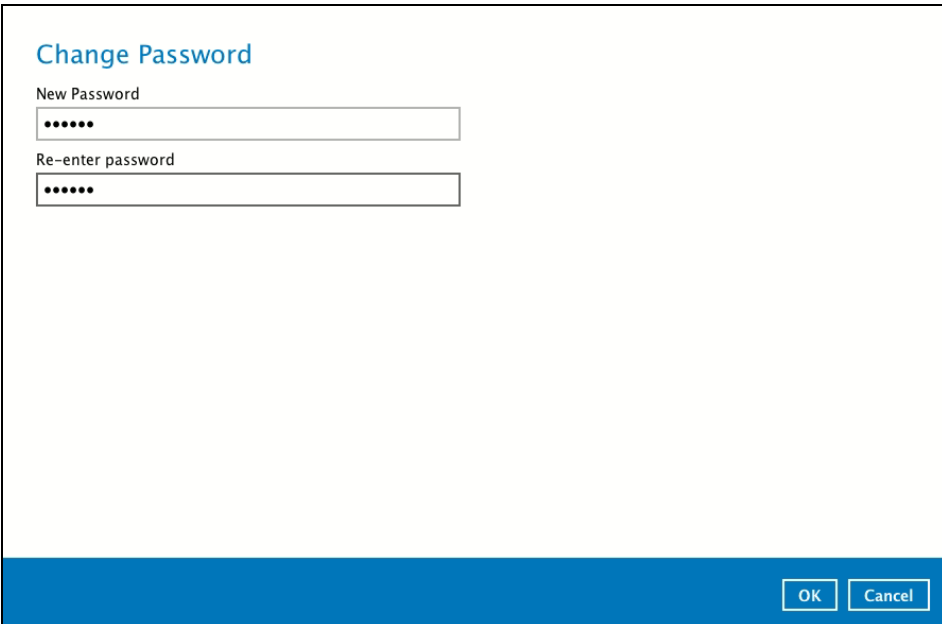
Change Password

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.

The screenshot shows a web interface for user profile settings. On the left is a sidebar with the title 'Profile' and a list of menu items: 'General', 'Contacts', 'Time Zone', 'Encryption Recovery', and 'Authentication'. The 'Authentication' item is highlighted with a blue background. The main content area on the right is divided into three sections. The first section, 'Password', includes a 'Change Password' button and a checkbox for 'Save password'. The second section, 'Two-Factor Authentication', has the subtitle 'Require Authenticator App to sign in your account during startup' and a toggle switch currently set to 'Off'. The third section, 'Last Successful Login', shows the text 'No login record'. At the bottom right of the page, there are three buttons: 'Save', 'Cancel', and 'Help'.

Profile

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

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](#)

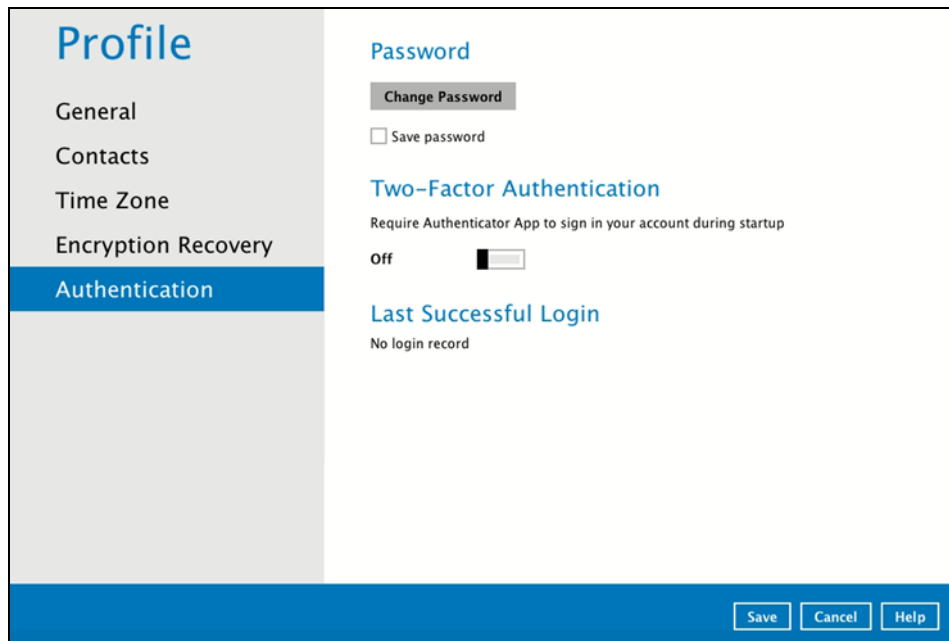
Two-Factor Authentication

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 **Profile > Authentication > Two-Factor Authentication**.



The screenshot shows the 'Profile' page with the 'Authentication' tab selected. Under the 'Two-Factor Authentication' section, the toggle switch is in the 'Off' position. The 'Save' button is visible at the bottom right.

Profile

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

Password

[Change Password](#)

☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

Off ☐

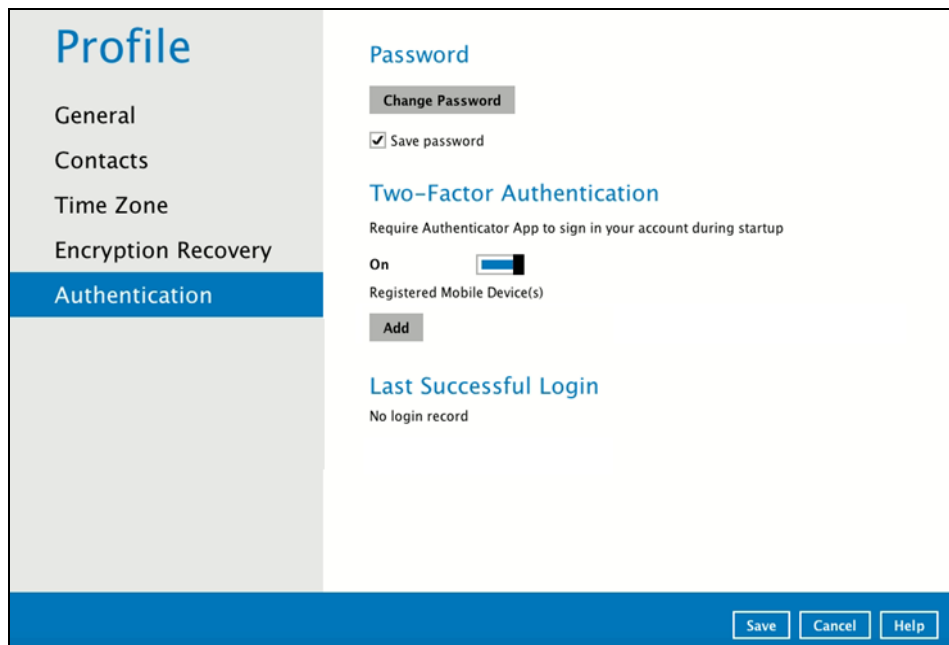
Last Successful Login

No login record

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

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 **Chapter 6.3.1** of the [Ahsay Mobile User Guide for Android and iOS](#).



The screenshot shows the 'Profile' page with the 'Authentication' tab selected. Under the 'Two-Factor Authentication' section, the toggle switch is in the 'On' position. The 'Add' button is visible below the 'Registered Mobile Device(s)' label. The 'Save' button is visible at the bottom right.

Profile

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

Password

[Change Password](#)

☒ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

On ☒

Registered Mobile Device(s)


[Add](#)

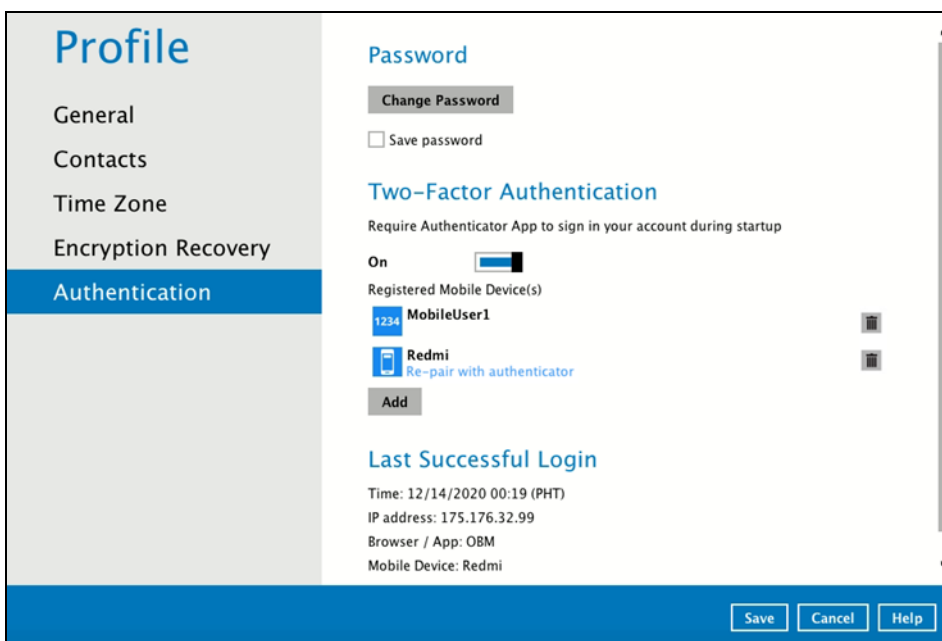
Last Successful Login

No login record

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

To remove a mobile device, follow the instructions below:

1. Click the  button on the left side of the registered mobile device. In this example, we are going to delete the mobile device named "MobileUser1".



Profile

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

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 
- Redmi [Re-pair with authenticator](#) 

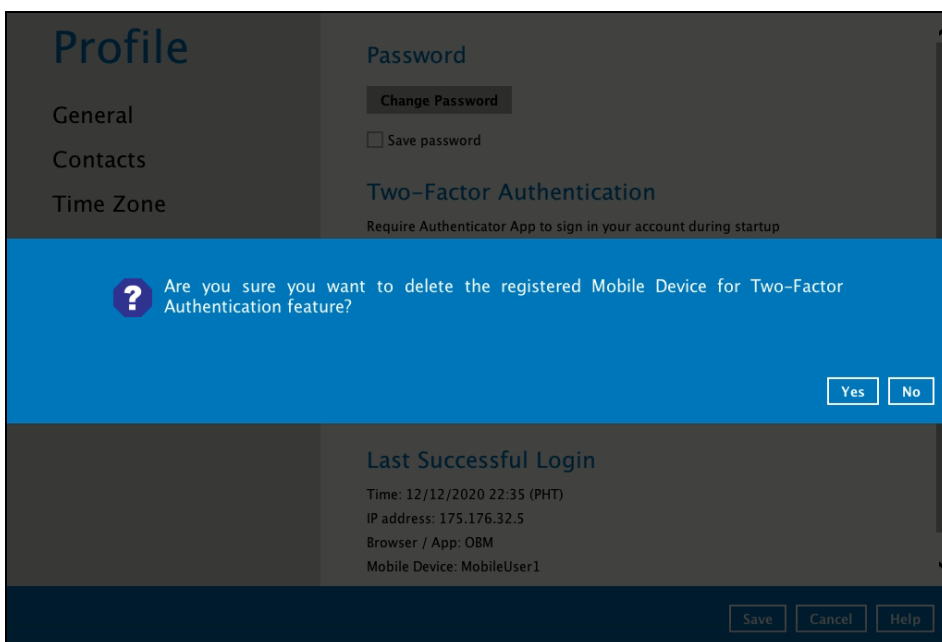
[Add](#)

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


Password

[Change Password](#)

☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

 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**

Password

[Change Password](#)

☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

On ☐

Registered Mobile Device(s)

Redmi
[Re-pair with authenticator](#)

[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](#)

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, and Authentication (which is highlighted in blue). 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' and a list of registered mobile devices including 'MobileUser1' and 'Redmi'; and 'Last Successful Login' showing details for a login on 12/14/2020. At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons.

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

This screenshot is identical to the previous one, but the toggle switch for 'Two-Factor Authentication' is now set to 'Off'. The rest of the interface, including the sidebar, other settings, and the login history, remains the same.

Re-pair with authenticator

AhsayOBM supports “Re-pair with authenticator” feature that enables user to re-pair their AhsayOBM account with Ahsay Mobile Authenticator as long as the mobile device used for the 2FA is still registered in the AhsayOBM. This feature is used when:

1. The registered profile for the 2FA is removed from the Ahsay Mobile app
2. The Ahsay Mobile app is accidentally uninstalled from the mobile device

The screenshot displays the 'Profile' page of the AhsayOBM application. The left sidebar contains navigation links: 'General', 'Contacts', 'Time Zone', 'Encryption Recovery', and 'Authentication' (which is highlighted in blue). The main content area is divided into three sections: 'Password', 'Two-Factor Authentication', and 'Last Successful Login'. In the 'Two-Factor Authentication' section, the toggle switch is turned 'On'. Below this, a list of 'Registered Mobile Device(s)' shows one device named 'Androidv10'. A red rectangular box highlights the 'Re-pair with authenticator' link next to the device name. There is also a trash icon to the right of the device name. At the bottom of the page, there are 'Save' and 'Cancel' buttons.

Profile

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

Password

Change Password



☐ Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

On ☒

Registered Mobile Device(s)

-  Androidv10 **Re-pair with authenticator** 

Add

Last Successful Login

Time: 03/09/2021 16:13 (HKT)
IP address: 10.3.121.13
Browser / App: OBM
Mobile Device: Ahsay Mobile

Save Cancel

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 the 'Authentication' tab selected. The 'Last Successful Login' section displays the following information:

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

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

The screenshot shows the 'Profile' page with the 'Authentication' tab selected. The 'Last Successful Login' section displays the following information:

| Field | Value |
|---------------|-------|
| Time | |
| IP address | |
| Browser / App | |
| Mobile Device | |

9.1.7 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.

Profile

- General
- Contacts
- Time Zone
- Encryption Recovery
- Password
- Security Settings**

Security Settings

Phone numbers for SMS authentication

- Philippines (+63) - [redacted], Verified ✕

Add

Save **Cancel** **Help**

1. Click the **Add** button.

Add

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

Security Settings

Please enter a new phone number for SMS authentication

Philippines (+63) ▼ [redacted]

Add **Cancel**

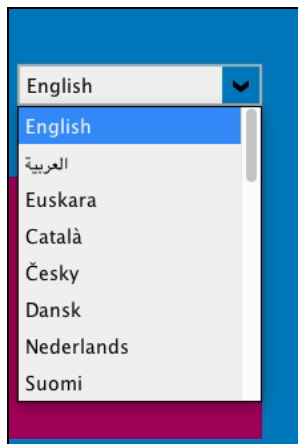
3. Click the **Save** button to save the phone number.

The screenshot shows the 'Profile' settings page with a sidebar on the left containing links: General, Contacts, Time Zone, Encryption Recovery, Password, and Security Settings (which is highlighted in blue). The main content area is titled 'Security Settings' and includes a section for 'Phone numbers for SMS authentication'. This section contains two entries: 'Philippines (+63) - [redacted], Verified' and 'Philippines (+63) - [redacted], Not verified', each with a delete icon (X). Below these is an 'Add' button. At the bottom right of the page are three buttons: 'Save', 'Cancel', and 'Help'.

9.2 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.



9.3 Information

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





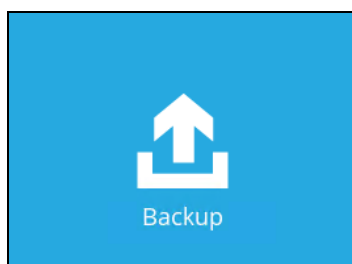
| | |
|-------------------------------|---|
| Version | 9.0.0.0 |
| Virtual Machine Vendor | OpenJDK 64-Bit Server VM Version 25.181-b13 Oracle Corporation |
| Live Threads | 13 (Current) / 20 (Peak) |
| Daemon Threads | 9 |
| Total Threads Started | 55 |
| Heap Size | 98,560 kbytes (Current) / 1,864,192 kbytes (Maximum) |
| Operating System Architecture | Mac OS X Version 10.12 x86_64 |
| Number of Processors | 4 |
| Committed Virtual Memory | 7,099,840 kbytes |
| Physical Memory | 9,066,516 kbytes (Free) / 16,777,216 kbytes (Total) |
| Swap Space | 0 kbyte (Free) / 0 kbyte (Total) |
| VM Arguments | -Djava.library.path=/Applications/AhsayOBM.app/Contents/MacOS -Xrs -Xms128m -Xmx2048m -XX:MaxDirectMemorySize=512m -Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=/Applications/AhsayOBM.app/bin:/Applications/AhsayOBM.app/bin/MacX84 |
| Class Path | /Applications/AhsayOBM.app/bin:/Applications/AhsayOBM.app/bin/ |

© 2021 Ahsay Systems Corporation. All Rights Reserved.

Close

9.4 Backup

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



For instructions on how to start a backup, refer to [Chapter 12 Run Backup Jobs](#).

9.5 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 10 Create a Backup Set](#).

Backup Set Settings

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

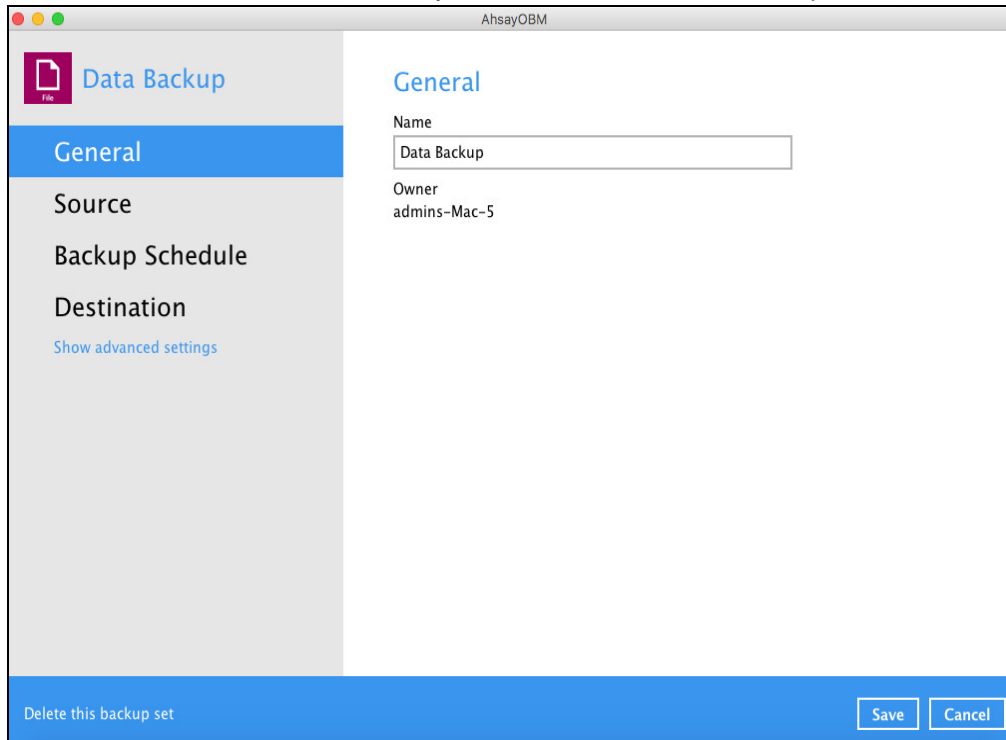
- [General](#)
- [Source](#)
- [Backup Schedule](#)
- [Destination](#)

(Advanced settings)

- [Deduplication](#)
- [Retention Policy](#)
- [Command Line Tool](#)
- [Bandwidth Control](#)
- [Others](#)

General

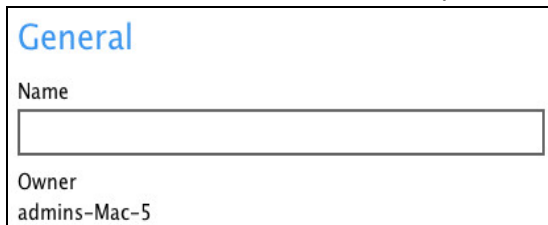
This feature allows the user to modify the current name of the backup set.



The screenshot shows a window titled "AhsayOBM" with a sidebar on the left and a main content area on the right. The sidebar has a "Data Backup" header with a file icon and a list of options: "General" (highlighted in blue), "Source", "Backup Schedule", "Destination", and a link "Show advanced settings". The main content area is titled "General" and contains two fields: "Name" with a text input field containing "Data Backup", and "Owner" with a text input field containing "admins-Mac-5". At the bottom of the window is a blue bar with the text "Delete this backup set" 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 window. It shows the "Name" field with a text input box. Below it is the "Owner" field with the text "admins-Mac-5".

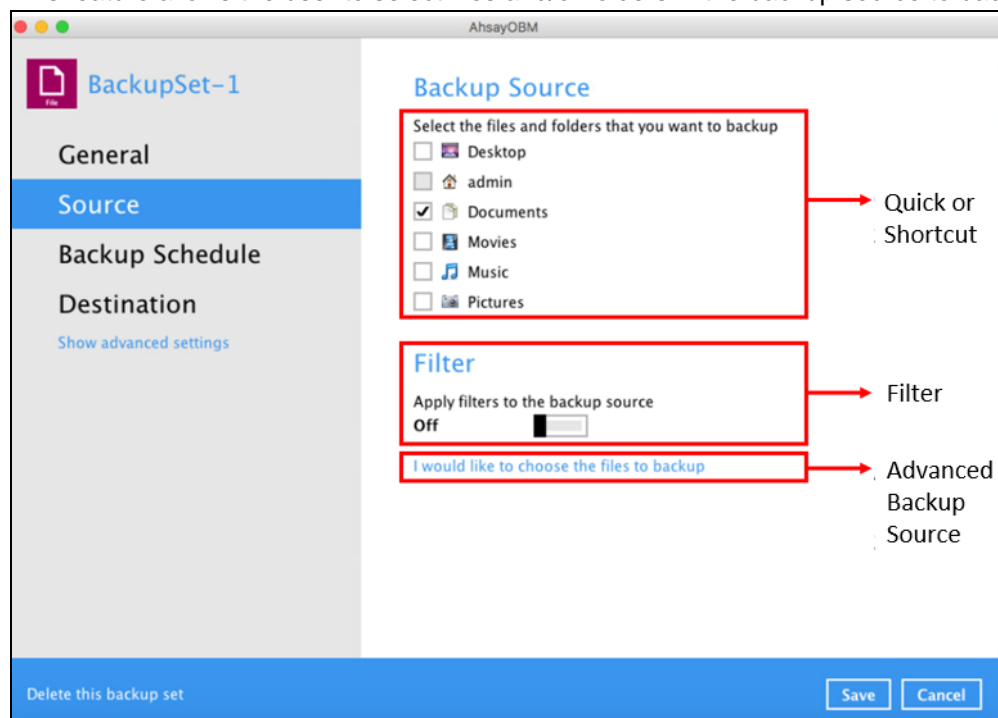
2. Click the **Save** button to save the updated backup set name.

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><i>\$UserProfile/admin/Desktop</i></p> |
| admin |  | <p>If admin is selected, all files and/or folders located in the following locations will be backed up:</p> <p><i>\$UserProfile/admin</i></p> <p><i>\$UserProfile/Library</i></p> <p>If the Follow Link is enabled, the following locations will also be included to the backup job:</p> <p><i>\$UserProfile/LocalStorage</i></p> <p><i>\$UserProfile/Applications</i></p> <p><i>\$UserProfile/admin/Downloads</i></p> <p><i>\$UserProfile/admin/Library</i></p> <p><i>\$UserProfile/admin/temp</i></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><i>\$UserProfile/admin/Documents</i></p> |
| Movies |  | <p>If Movies is selected, all files and/or folders located in the following location will be backed up:</p> <p><i>\$UserProfile/admin/Movies</i></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 **[+]** button to create a filter.

Existing filters

 Add new filter

3. Assign a desired name to the backup filter.

New Backup Filter

Name


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.

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

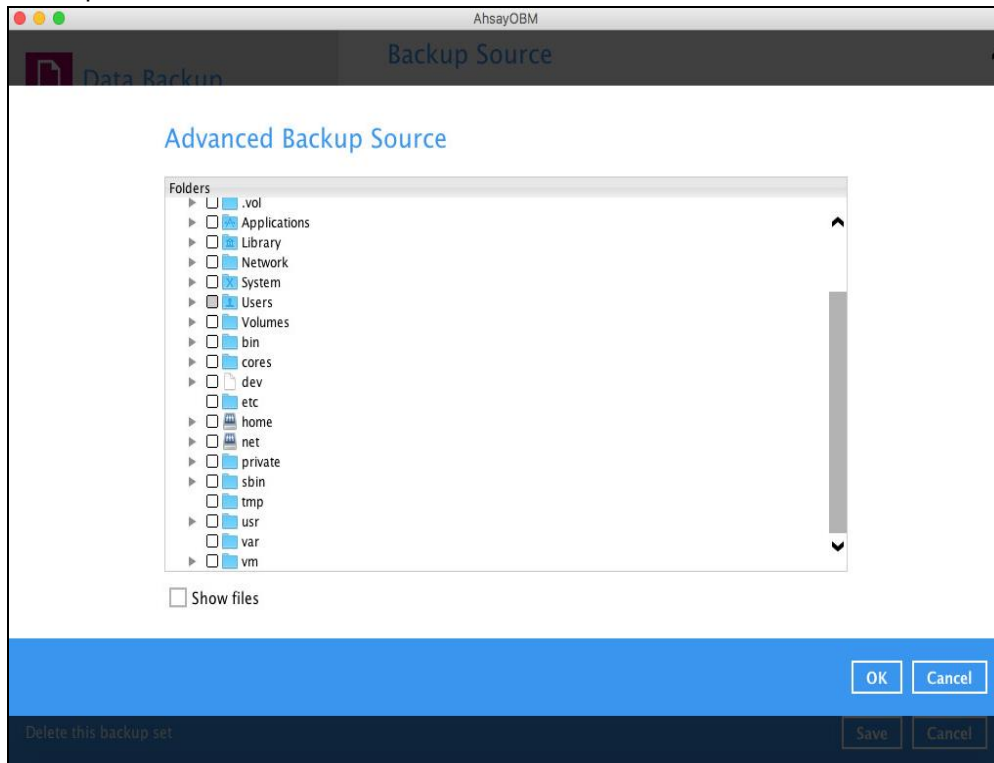
Existing filters

 **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.

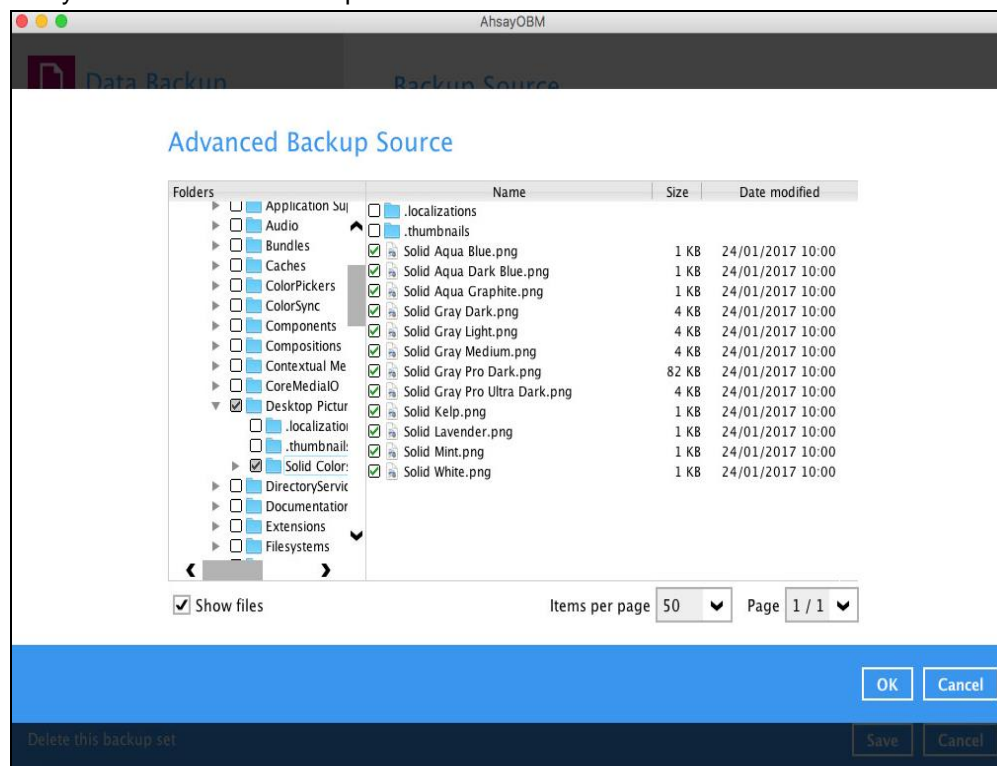


To select files and/or folders using the Advanced Backup Source, follow the steps below:

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.



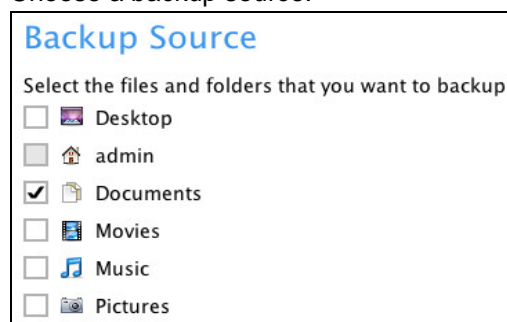
3. Click the **OK** button to save the selection, then click the **Save** button to store settings.

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:

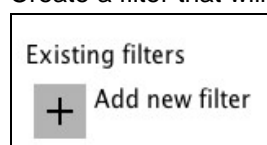
Scenario 1 (Quick or Shortcut + Filter)

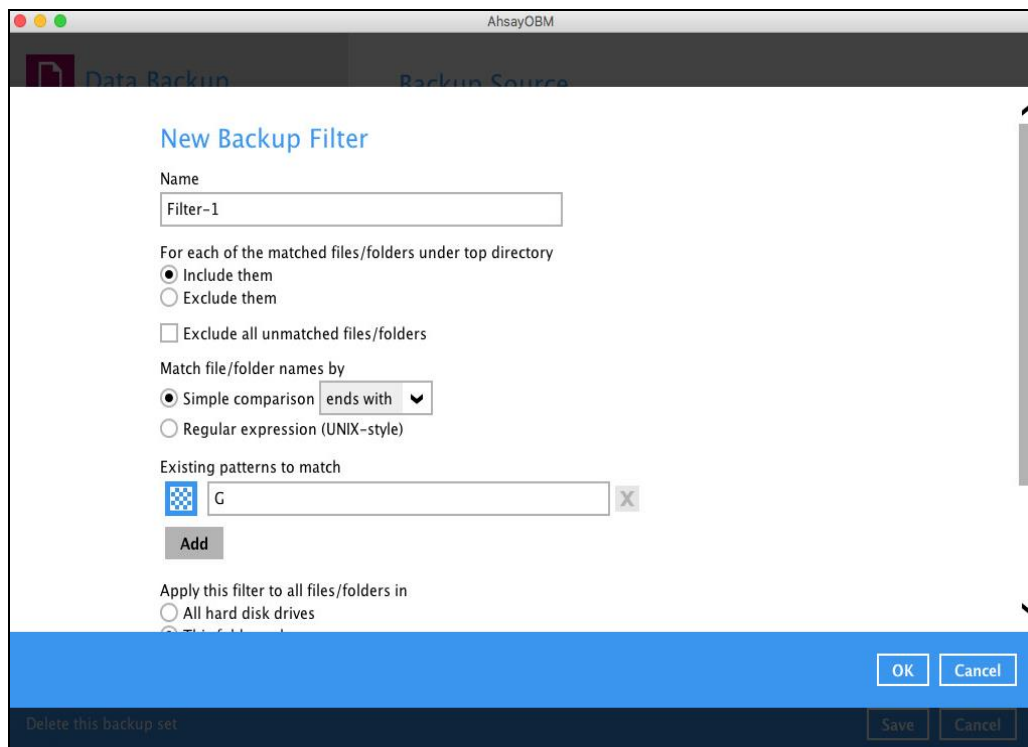
You can use the Quick or Shortcut option and apply filter to the selected backup source at the same time. To use this type of combination, follow the steps below:

1. Choose a backup source.



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



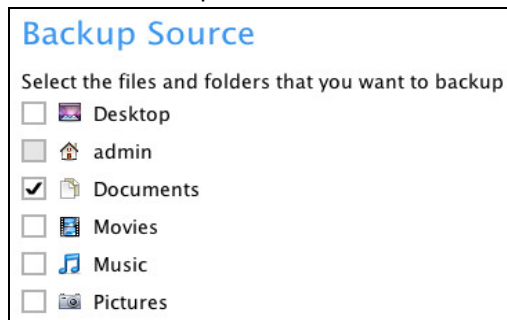


3. Click the **OK** button to save the created filter, then click the **Save** button to store settings.

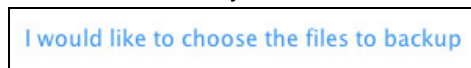
Scenario 2 (Quick or Shortcut + Advanced Backup Source)

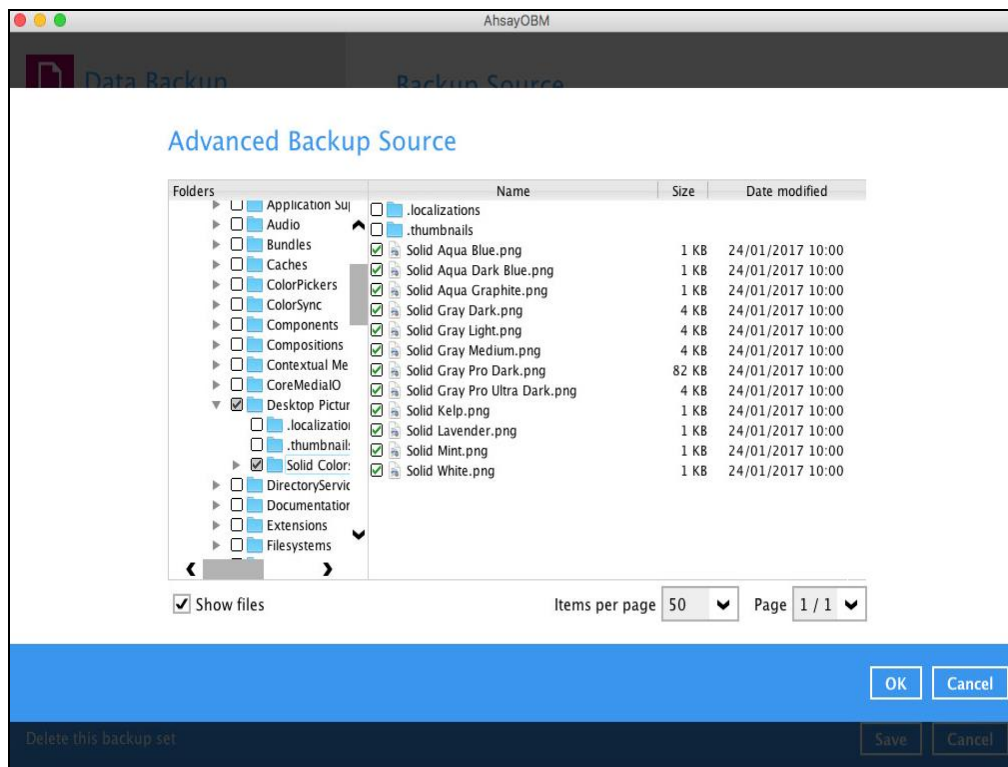
You can use the Quick or Shortcut option and select files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

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.



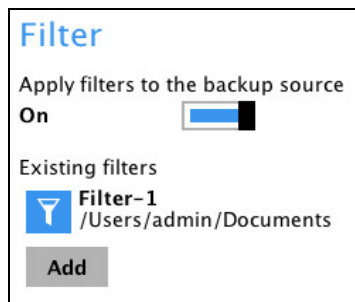


3. Click the **OK** button to save the selection, then click the **Save** button to save settings.

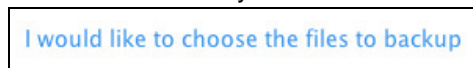
Scenario 3 (Filter + Advanced Backup Source)

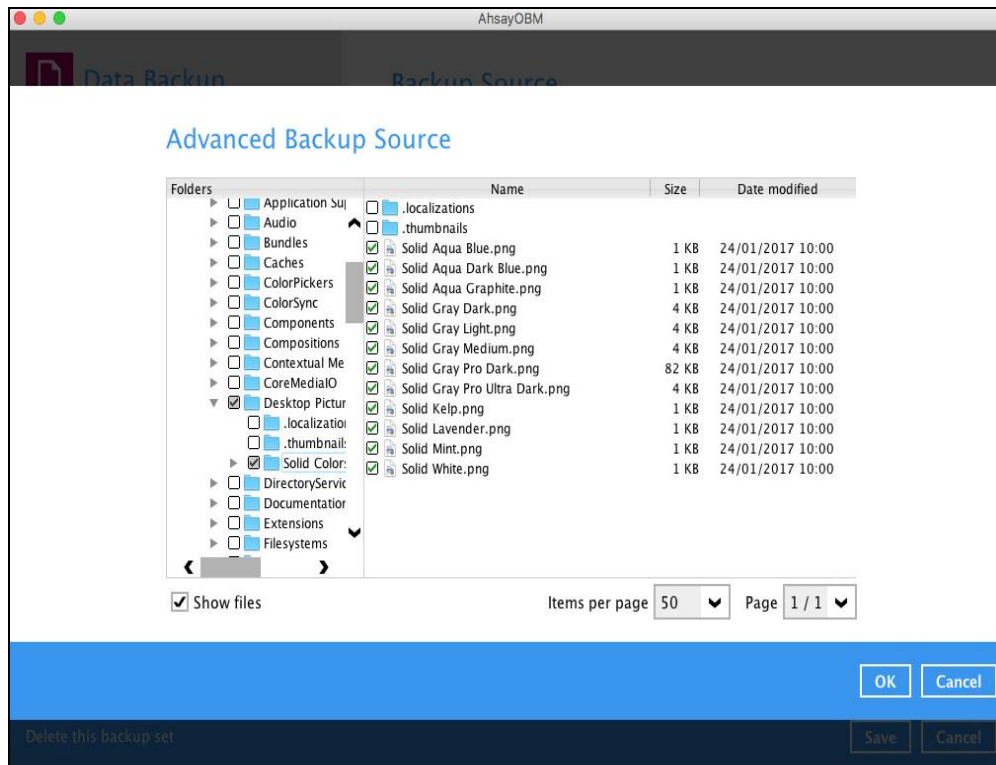
You can use the filter backup source and select files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

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.

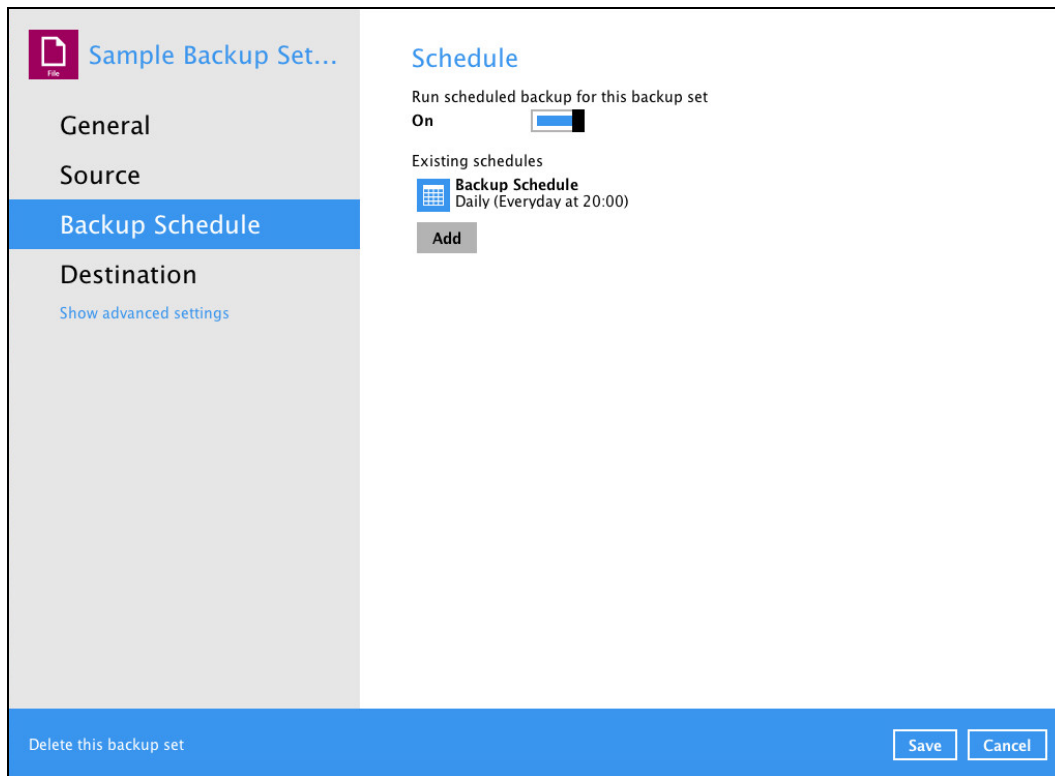




3. Click the **OK** button to save the selection, then click the **Save** button to save settings.

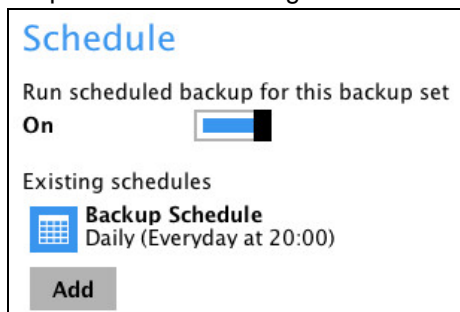
Backup Schedule

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

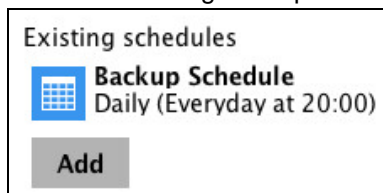


To configure a backup schedule, follow the steps below:

1. Swipe the lever to the right to turn on the backup schedule setting.



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



3. In the New Backup Schedule window, configure the following backup schedule settings.

- **Name** – the name of the backup schedule.
- **Type** – the type of the backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.

- **Daily** – the time of the day or 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

1 minute

2 minutes

3 minutes

4 minutes

5 minutes

6 minutes

10 minutes

12 minutes

30 minutes

1 hour

2 hours

3 hours

4 hours

6 hours

8 hours

12 hours

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

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

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

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

NOTE

For backup sets with multiple backup schedules configured **at the same time**, this will be the order of priority to determine which schedule will be run:

1. Backup type: Full > Differential

While for Schedules that have selectable Backup Type:

- IBM Lotus Domino: Database > Log
- MS Exchange Server: Database > Log File
- MS SQL Server: Full > Differential > Incremental (VSS Backup Mode)
Full > Differential > Transaction Log (ODBC Backup Mode)
- MS Hyper-V: Full > Incremental
- Oracle Database: Database > Log
- ShadowProtect: Complete > Differential > Incremental
- VMWare: Full > Incremental

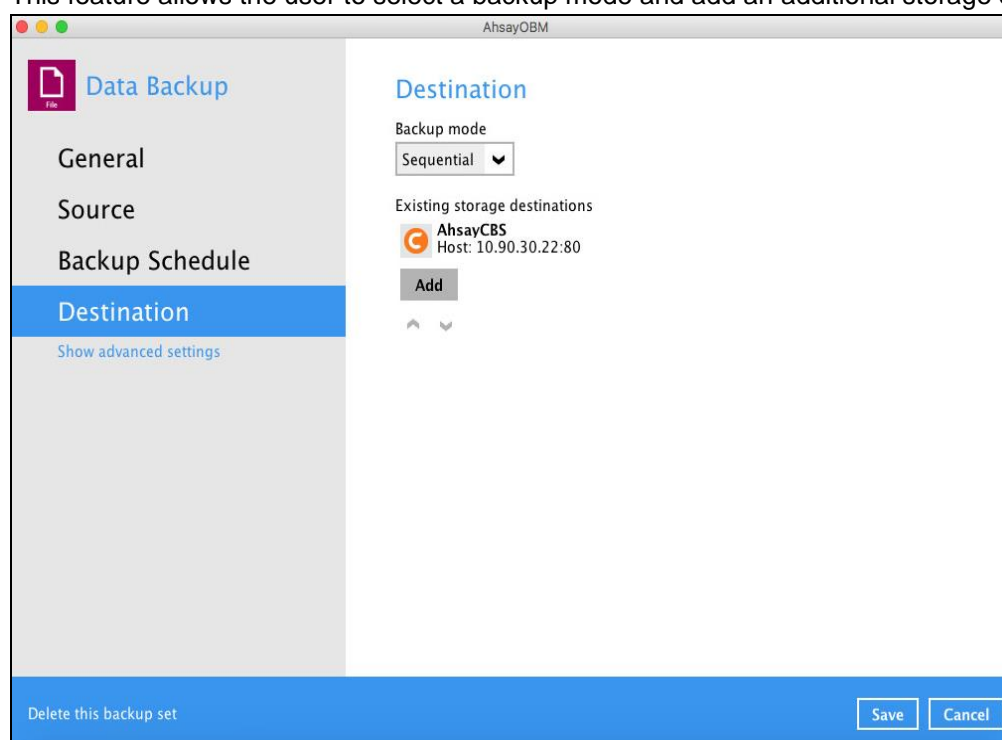
2. Stop: after X hours > after Y hours > until full backup completed (where $X < Y$)
3. Run Retention Policy after backup: enabled > disabled
4. Schedule type: Daily > Weekly > Monthly > Custom
5. Creation order

Examples:

- a. If there are 2 backup schedules with Full backup type and with Stop after 2 hours and 4 hours respectively. The backup schedule with Stop after 2 hours will be run.
- b. If there are 2 backup schedules with any Run Retention Policy enabled, it will have priority and execute that Schedule in this instance and ignore Schedule Type prioritization.
- c. For backup sets with backup schedules Daily and Weekly, the Daily backup schedule will be run.

Destination

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



There are two (2) 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

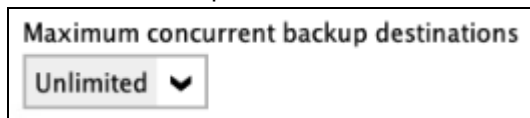
| Backup mode | Pros | Cons |
|-------------------|---|--|
| Sequential | <ul style="list-style-type: none">➤ Takes less resources in the local machine (e.g., memory, CPU, bandwidth, etc.) to complete a backup job. | <ul style="list-style-type: none">➤ Backup job is slower than in concurrent mode since 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 modify the Backup mode, follow the steps below:

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



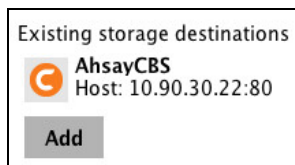
4. If "Concurrent" is selected, click the drop-down button to select the no. of maximum concurrent backup destinations.



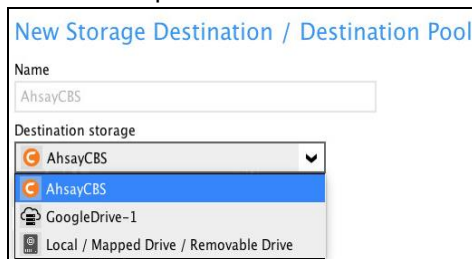
5. Click the **Save** button to save the selected backup mode.

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

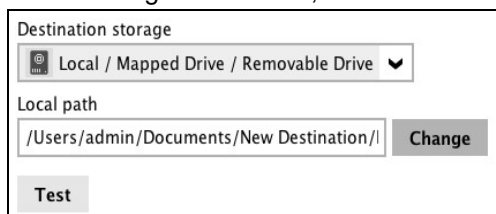
1. Click the **Add** button.



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

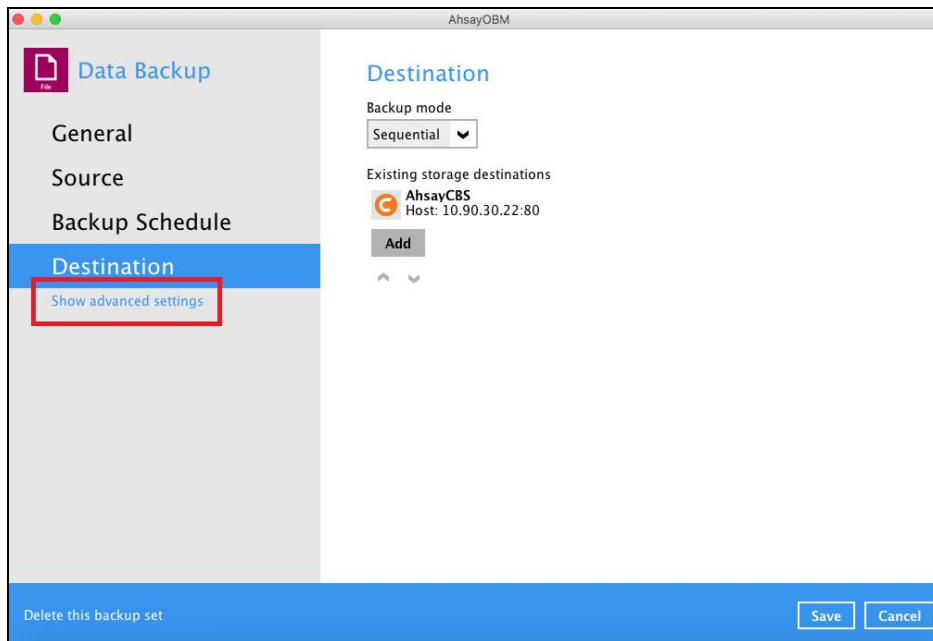


3. If the Local / Mapped Drive / Removable Drive is selected, click the **Change** button to select a new storage destination, then click the **Test** button to validate access to it.



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.

To continue on with the menu, click the **Show advanced settings** link to modify the **Deduplication**, **Retention Policy**, **Command Line Tool**, **Bandwidth Control**, and other configurable items under the **Others** tab.



Deduplication

Starting with AhsayOBM v9.0.0.0 or above, the In-File Delta feature (i.e., Incremental, Differential and Full) will be replaced with Deduplication. This feature is **On (enabled)** by default.

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

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

AhsayOBM

Data Backup

General

Source

Backup Schedule

Destination

Deduplication

Retention Policy

Command Line Tool

Bandwidth Control

Others

[Hide advanced settings](#)

Delete this backup set

Save Cancel

Deduplication

Enable Deduplication
On

Deduplication scope

☐ Same file path within the same backup set

☒ All files within the same backup set

Block size

64 k - 256 k (optimal settings) Bytes

☐ Migrate existing data to latest version

There are two (2) types of Deduplication scope:

| Deduplication Scope | Description |
|--|--|
| Same file path within the same backup set | Deduplication will be applied to the duplicated contents within a file during the current backup job |
| All files within the same backup set | Deduplication will be applied across different files in the backup set. |

Migrate Data

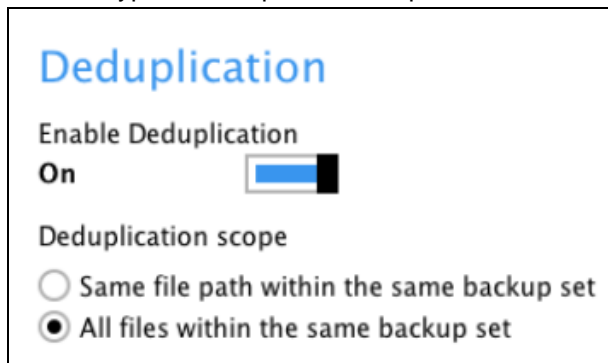
When this option is enabled, the existing data will be migrated to the latest version during a backup job. This option is disabled by default.

Migrate Data

☐ Migrate existing data to latest version

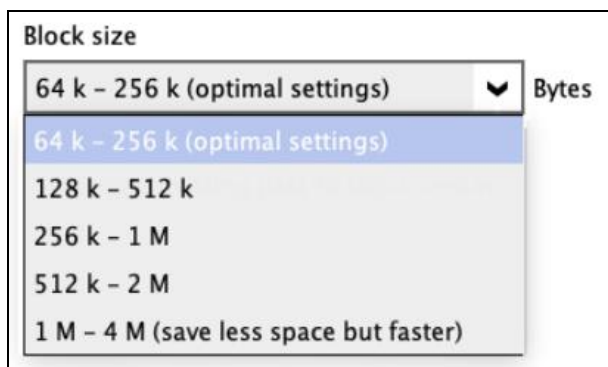
To configure the Deduplication settings, follow the steps below:

1. Select a type of Deduplication scope.

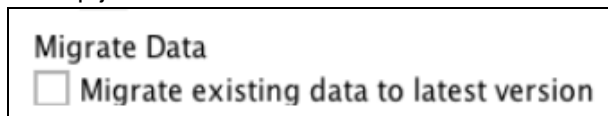


2. Click the drop-down button to select the block size that will be used for the deduplication data block.

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



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



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

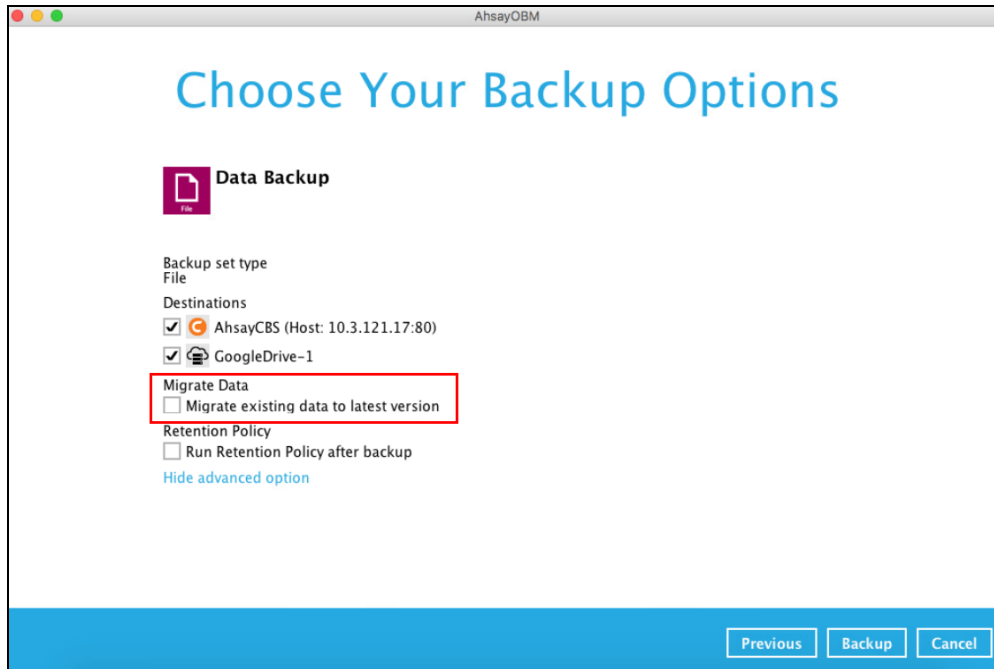
NOTE

For more details about the **Deduplication** feature, refer to the [AhsayCBS v9 New Features Supplemental document](#).

Run Backup Job

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

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

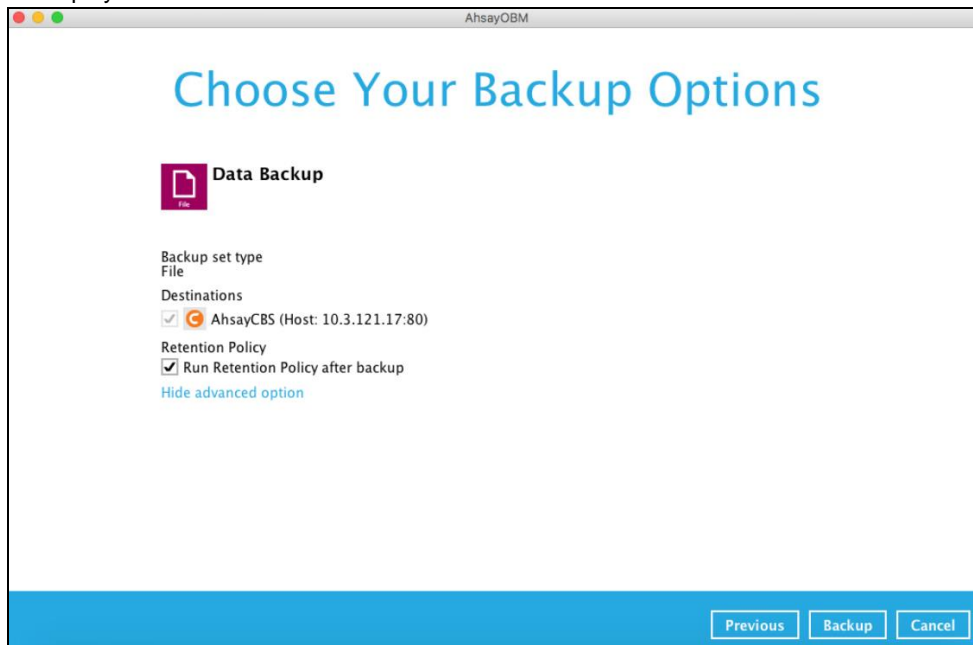


The screenshot shows a window titled "AhsayOBM" with the heading "Choose Your Backup Options". Below the heading is a "Data Backup" icon. The configuration options are as follows:

- Backup set type: File
- Destinations:
 - ☒ AhsayCBS (Host: 10.3.121.17:80)
 - ☒ GoogleDrive-1
- Migrate Data:
 - ☐ Migrate existing data to latest version
- Retention Policy:
 - ☐ Run Retention Policy after backup

A red rectangle highlights the "Migrate Data" section. At the bottom right are buttons for "Previous", "Backup", and "Cancel". A link "Hide advanced option" is located below the Retention Policy section.

Below is an example of a backup set with Deduplication setting **disabled**, the **Migrate Data** option will not be displayed.



The screenshot shows a window titled "AhsayOBM" with the heading "Choose Your Backup Options". Below the heading is a "Data Backup" icon. The configuration options are as follows:

- Backup set type: File
- Destinations:
 - ☒ AhsayCBS (Host: 10.3.121.17:80)
- Retention Policy:
 - ☒ Run Retention Policy after backup

The "Migrate Data" option is not present. At the bottom right are buttons for "Previous", "Backup", and "Cancel". A link "Hide advanced option" is located below the Retention Policy section.

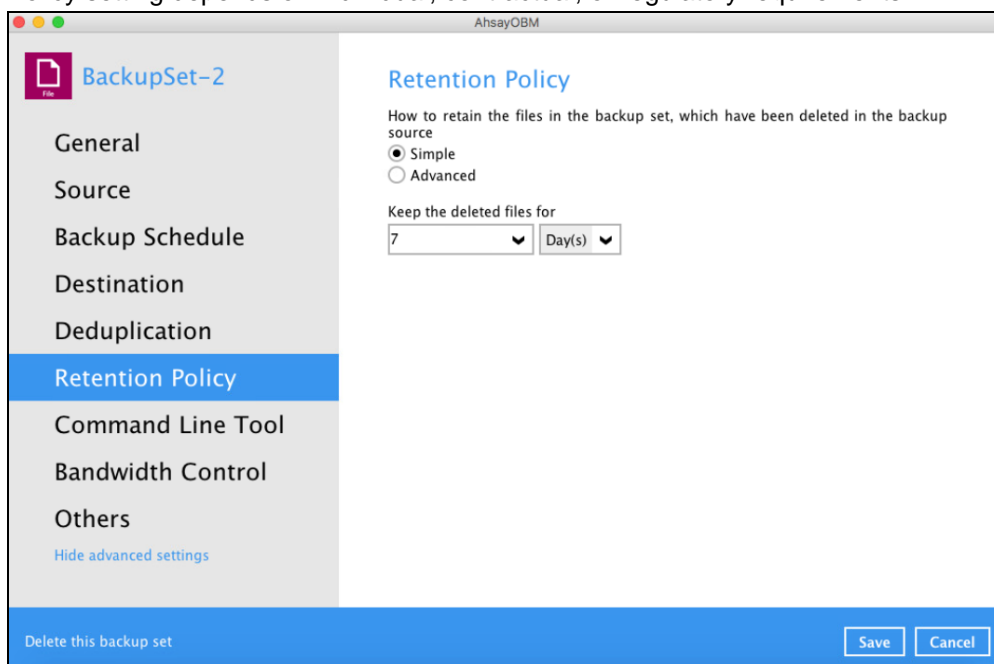
Retention Policy

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 before 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.



The screenshot shows the 'Retention Policy' configuration window for 'BackupSet-2' in the AhsayOBM application. The left sidebar contains a list of settings: General, Source, Backup Schedule, Destination, Deduplication, Retention Policy (highlighted), Command Line Tool, Bandwidth Control, and Others. The main area is titled 'Retention Policy' and contains the following text: 'How to retain the files in the backup set, which have been deleted in the backup source'. There are two radio buttons: 'Simple' (selected) and 'Advanced'. Below this, it says 'Keep the deleted files for' followed by a text input field containing '7' and a dropdown menu set to 'Day(s)'. 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.

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

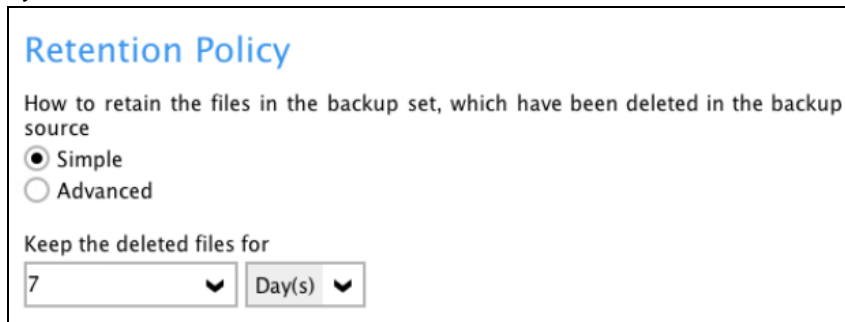
| Control | Simple | Advanced |
|--------------------------|--|---|
| Backup Jobs | Can keep the deleted files within 1 to 365 backup job(s) | Not applicable |
| Days | Can keep the deleted files within 1 to 365 day(s) | Can keep the deleted files within 1 to 365 day(s) |
| Type | Not applicable | <ul 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. Go to Backup Sets, then select a backup set.
2. Click the **Retention Policy** tab in the Backup Set Settings.
3. Select **Simple** from the options, then click the drop-down button to define the number of day(s) or job(s) which the deleted files will be retained. This is configured as seven (7) days by default.

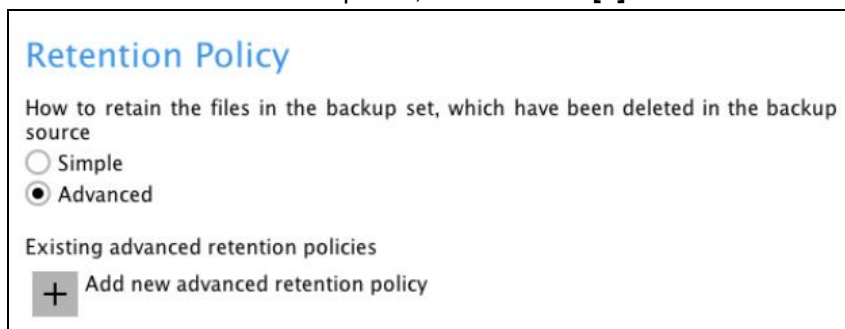


The screenshot shows the 'Retention Policy' configuration window. It has a title 'Retention Policy' in blue. Below the title is a subtitle 'How to retain the files in the backup set, which have been deleted in the backup source'. There are two radio buttons: 'Simple' (selected) and 'Advanced'. Below the radio buttons is a section 'Keep the deleted files for' with a text input field containing '7' and a dropdown menu showing 'Day(s)'.

4. Click the **Save** button to save the configured Retention Policy settings.

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

1. Go to Backup Sets, then select a backup set.
2. Click the **Retention Policy** tab in the Backup Set Settings.
3. Select **Advanced** from the options, then click the **[+]** button to create.



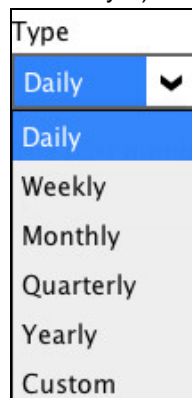
The screenshot shows the 'Retention Policy' configuration window with 'Advanced' selected. It has a title 'Retention Policy' in blue. Below the title is a subtitle 'How to retain the files in the backup set, which have been deleted in the backup source'. There are two radio buttons: 'Simple' and 'Advanced' (selected). Below the radio buttons is a section 'Existing advanced retention policies' with a button labeled '+ Add new advanced retention policy'.

4. Assign a desired name to the Retention Policy.



The screenshot shows the 'New Retention Policy' configuration window. It has a title 'New Retention Policy' in blue. Below the title is a section 'Name' with a text input field containing 'Daily-1'.

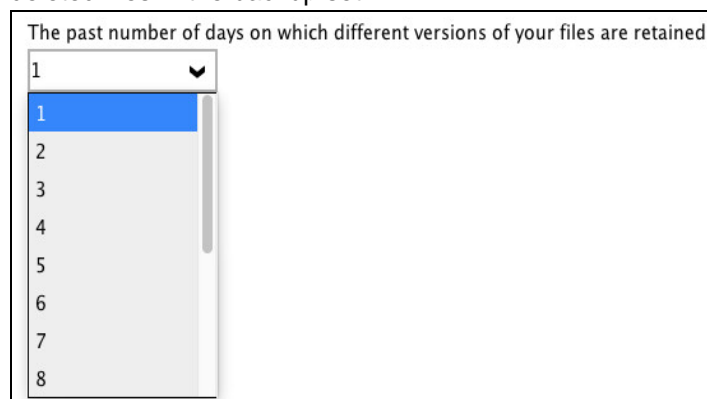
5. Click the drop-down button to choose a Retention Type (e.g., Daily, Weekly, Monthly, Quarterly...).



A screenshot of a dropdown menu titled "Type". The menu is open, showing a list of retention types: Daily, Weekly, Monthly, Quarterly, Yearly, and Custom. The "Daily" option is currently selected and highlighted in blue.

| Type |
|-----------|
| Daily |
| Weekly |
| Monthly |
| Quarterly |
| Yearly |
| Custom |

6. Click the drop-down button to specify the period on which the Retention Area will keep the deleted files in the backup set.



A screenshot of a dropdown menu titled "The past number of days on which different versions of your files are retained". The menu is open, showing a list of numbers from 1 to 8. The number "1" is currently selected and highlighted in blue.

| The past number of days on which different versions of your files are retained |
|--|
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |
| 6 |
| 7 |
| 8 |

7. Click the **OK** button to store the configured advanced Retention Policy, then click the **Save** button to store the settings.

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

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

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.






Retention Policy

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

☐ Simple

☒ Advanced

Existing advanced retention policies

-  **Daily-1**
Daily
-  **Weekly-1**
Weekly
-  **Monthly-1**
Monthly
-  **Quarterly-1**
Quarterly
-  **Yearly-1**
Yearly

Add

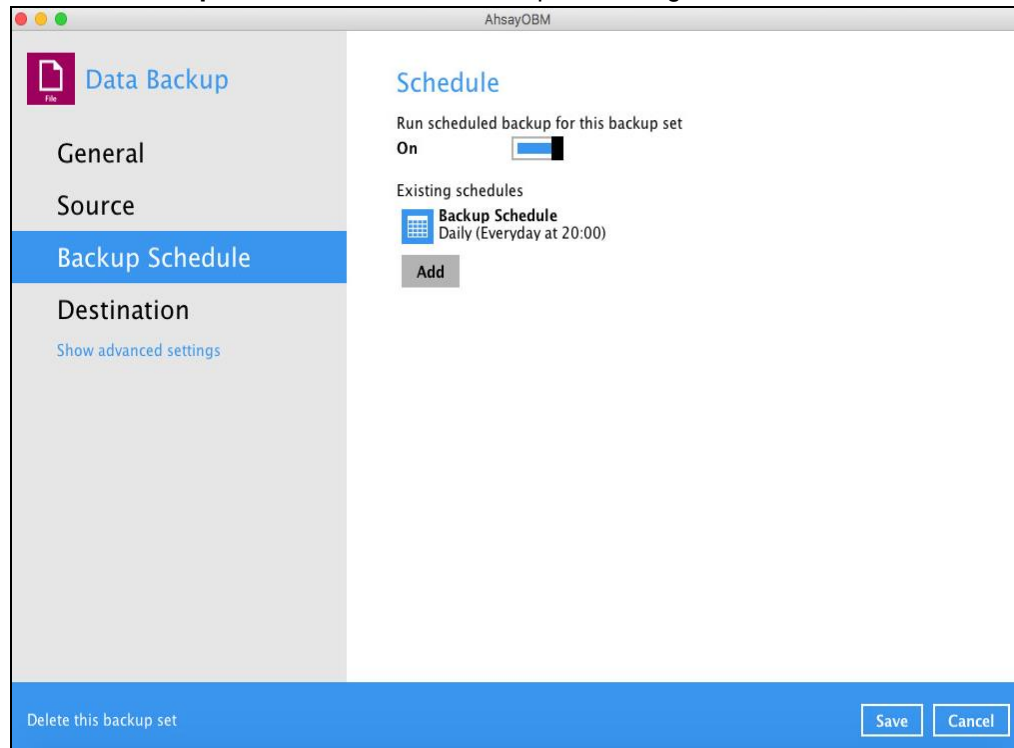
There are three (3) ways to run the Retention Policy job:

- Backup Scheduler
- Manual Backup
- Space Freeing Up

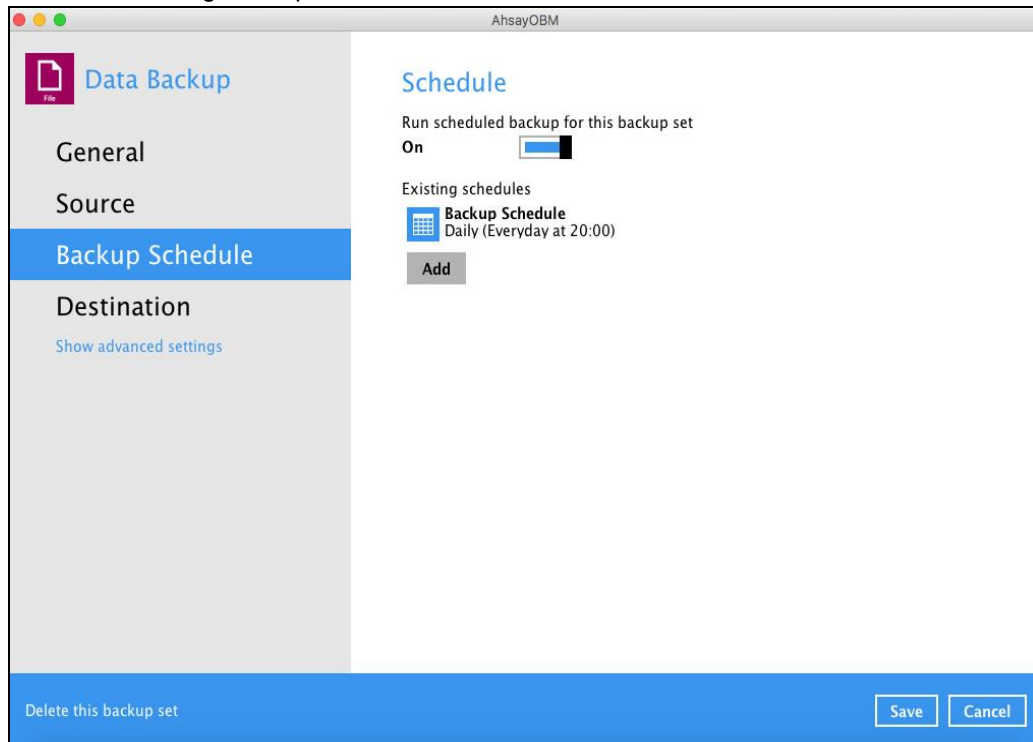
Backup Scheduler (Recommended)

To run a Retention Policy job after a scheduled backup job, follow the steps below:

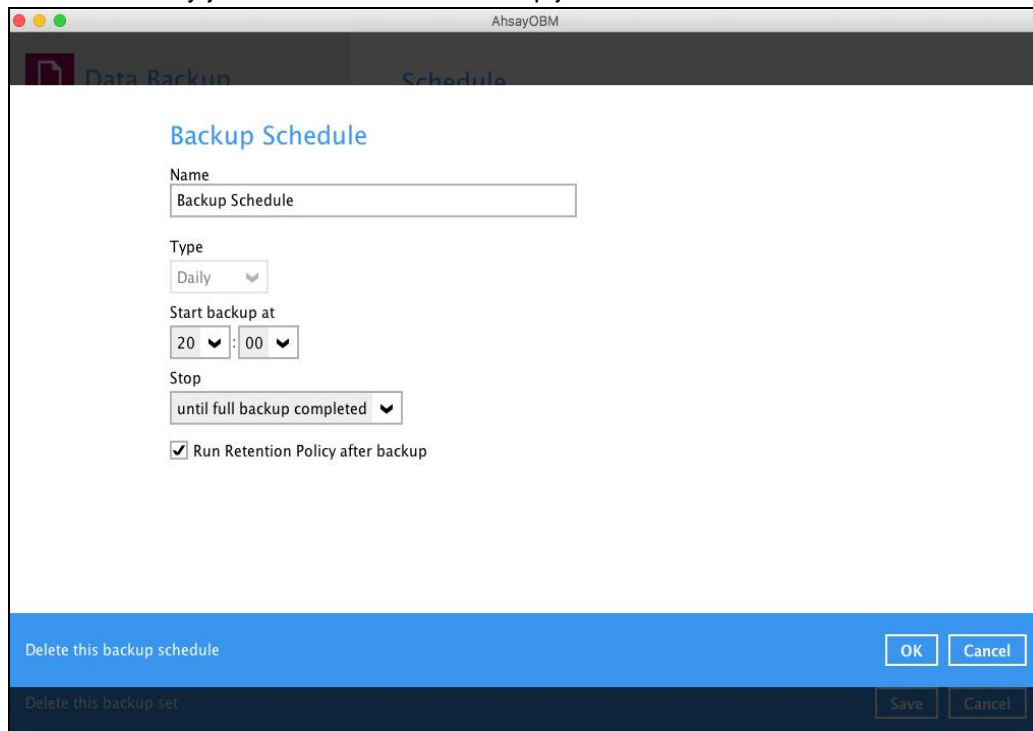
1. Click the **Backup Schedule** tab in the backup set settings.



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.



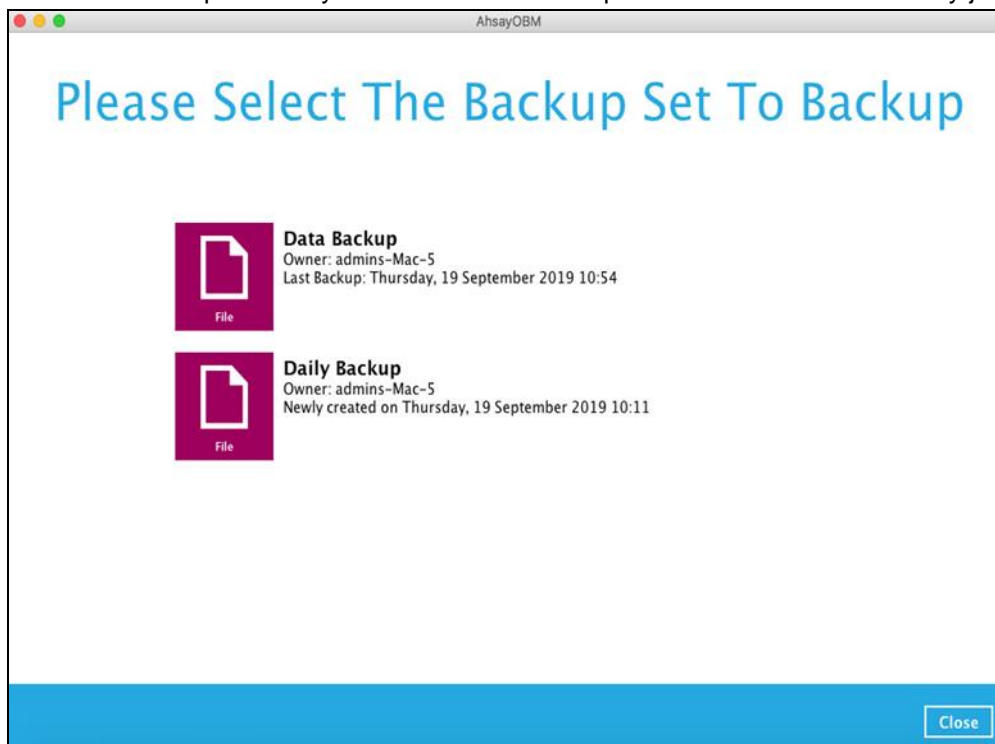
Manual Backup

To run a Retention Policy job after a manual backup, follow the steps below:

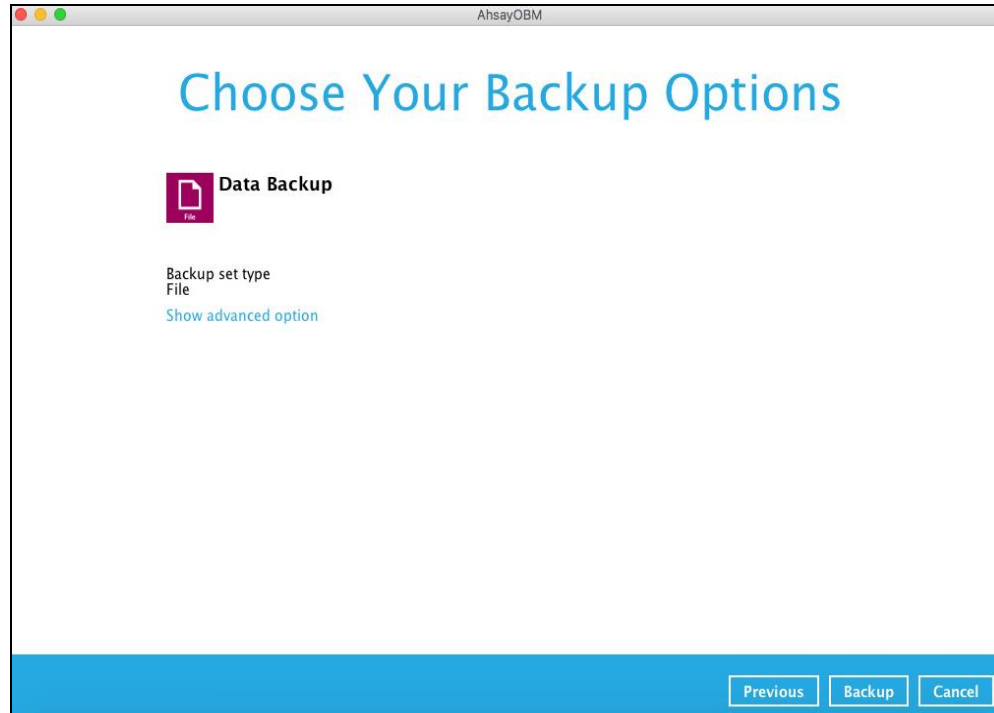
1. Click the **Backup** icon in the AhsayOBM main interface.



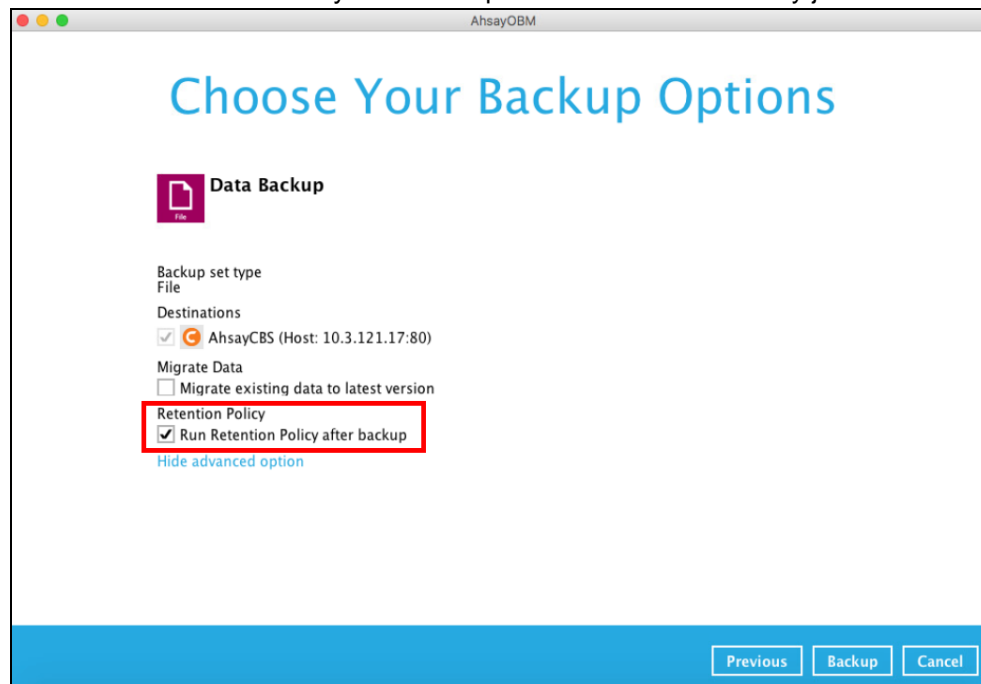
2. Select the backup set that you would like to back up and run the Retention Policy job on.



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



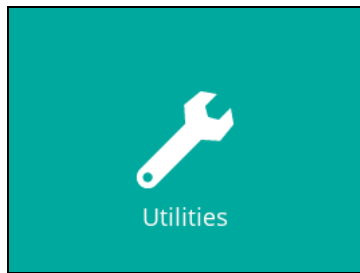
4. Select 'Run Retention Policy after backup' to run a Retention Policy job after a backup job.



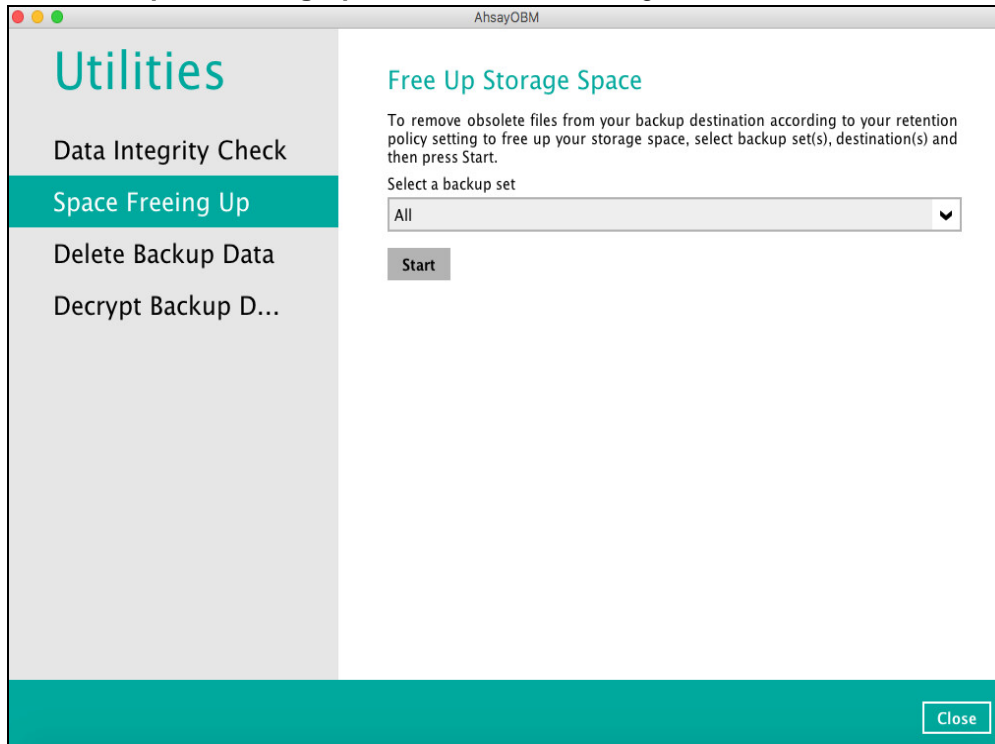
Space Freeing Up

To run a Retention Policy job manually via backup client interface, follow the steps below:

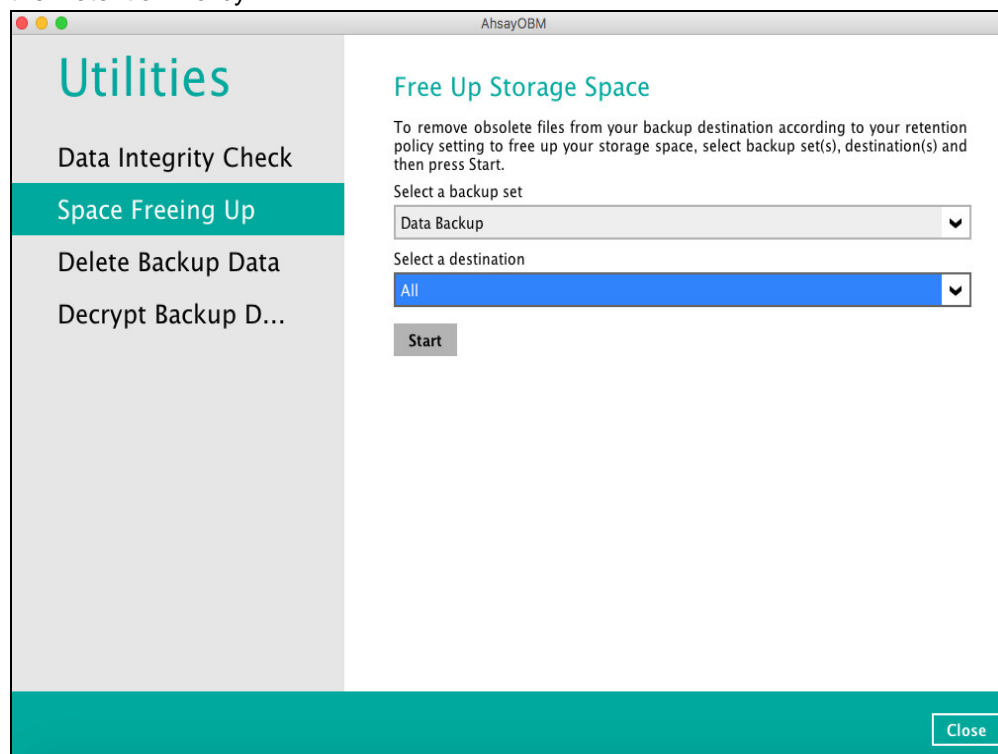
1. Click the **Utilities** icon in the AhsayOBM interface.



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.



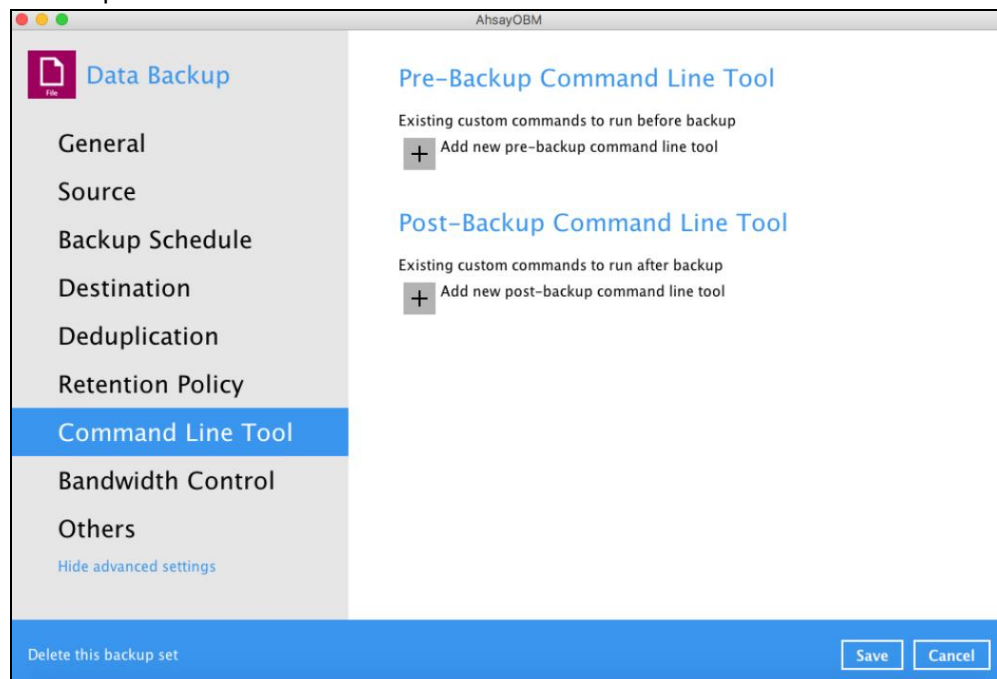
NOTE

For more details about Space Freeing Up, refer to [Chapter 9.9.2 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 [Chapter 9.6 Report](#).

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 **[+]** 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

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.

| AhsayOBM | | |
|--|-----|---------------------|
| Type | Log | Time |
| Start [AhsayOBM v9.0.0.46] | | 12/11/2021 13:25:24 |
| Saving encrypted backup set encryption keys to server... | | 12/11/2021 13:25:24 |
| Start Backup ... [Migrate Delta: Incremental] | | 12/11/2021 13:25:25 |
| Using Temporary Directory /Users/admin/.obm/temp/1636606806827/OBS@1636606824692 | | 12/11/2021 13:25:25 |
| Start running pre-commands | | 12/11/2021 13:25:27 |
| [Pre-Backup-1] ls -la | | 12/11/2021 13:25:27 |
| [Pre-Backup-1] total 24 | | 12/11/2021 13:25:28 |
| [Pre-Backup-1] drwx-----+ 8 admin staff 272 Nov 12 13:21 . | | 12/11/2021 13:25:28 |
| [Pre-Backup-1] drwxr-xr-x+ 18 admin staff 612 Sep 21 17:09 .. | | 12/11/2021 13:25:28 |
| [Pre-Backup-1] -rw-r--r--@ 1 admin staff 10244 Nov 12 13:22 .DS_Store | | 12/11/2021 13:25:28 |
| [Pre-Backup-1] -rw----- 1 admin staff 0 Jan 25 2017 .localized | | 12/11/2021 13:25:28 |
| [Pre-Backup-1] drwx----- 4 admin staff 136 Nov 9 14:27 AhsayOBM | | 12/11/2021 13:25:28 |
| [Pre-Backup-1] drwxr-xr-x@ 5 admin staff 170 Nov 12 13:20 Latest version | | 12/11/2021 13:25:28 |
| [Pre-Backup-1] drwxr-xr-x 3 admin staff 102 Sep 14 11:22 MobileBackup | | 12/11/2021 13:25:28 |
| [Pre-Backup-1] drwxr-xr-x@ 5 admin staff 170 Nov 12 13:20 New updates | | 12/11/2021 13:25:28 |
| Finished running pre-commands | | 12/11/2021 13:25:28 |
| Downloading server file list... | | 12/11/2021 13:25:28 |
| Downloading server file list... Completed | | 12/11/2021 13:25:29 |
| Reading backup source from hard disk... | | 12/11/2021 13:25:30 |

Logs per page 50

Page 1 / 663

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:

- Click the **[+]** button.

Post-Backup Command Line Tool

Existing custom commands to run after backup

+

Add new post-backup command line tool

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

New Post-Backup Command Line Tool

Name

Post-Backup-1


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

Working Directory

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

Command

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

- 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.

AhsayOBM

Show All

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

Logs per page 50
Page 4 / 4

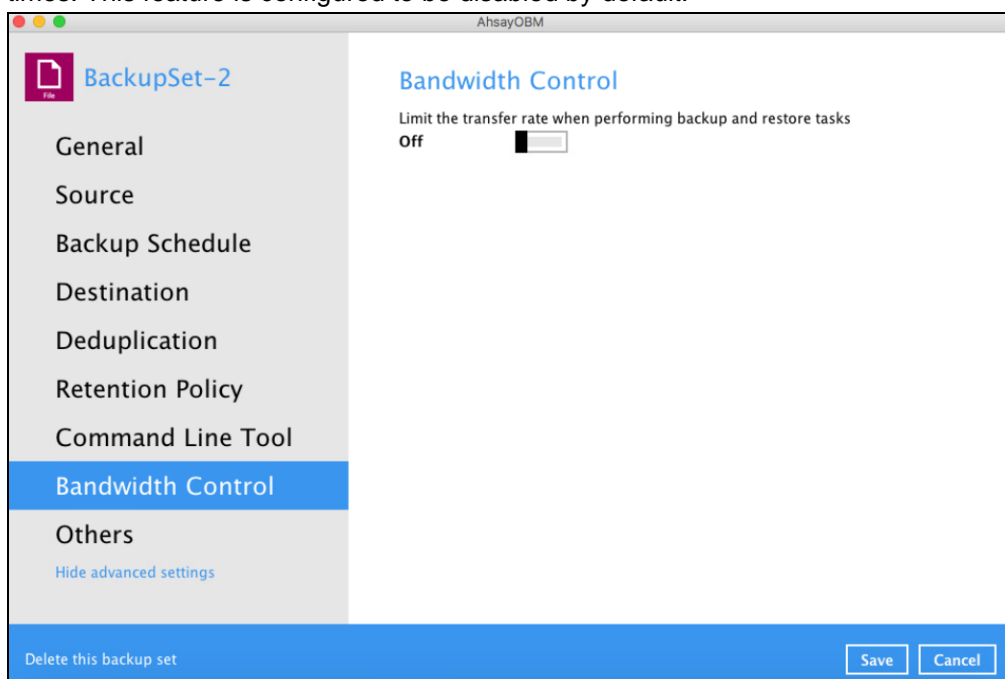
Close

NOTE

- Multiple Pre-backup and Post-backup commands can be created in the Command Line Tool.
- Errors from Pre-backup and Post-backup commands will only be flagged as a warning and will not cause an error. The warning may be viewed in the logs.
- To trigger a job warning, Pre-backup and Post-backup commands must output a message to stderr. It is not possible to cause a job "Error" message to be logged.

Bandwidth Control

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



There are two (2) types of bandwidth control:

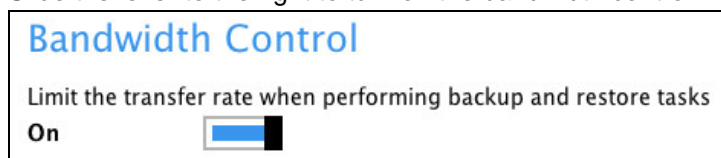
| Bandwidth Control Type | Description |
|------------------------|--|
| Independent | Each backup and restore has its assigned bandwidth. |
| Share | All backup and restore operations are sharing the same assigned bandwidth. |

NOTE

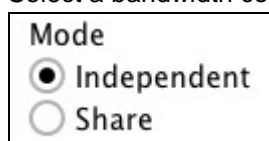
Share mode does not support performing backup job on multiple destinations concurrently.

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

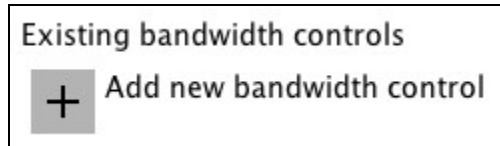
1. Slide the lever to the right to turn on the bandwidth control.



2. Select a bandwidth control mode.

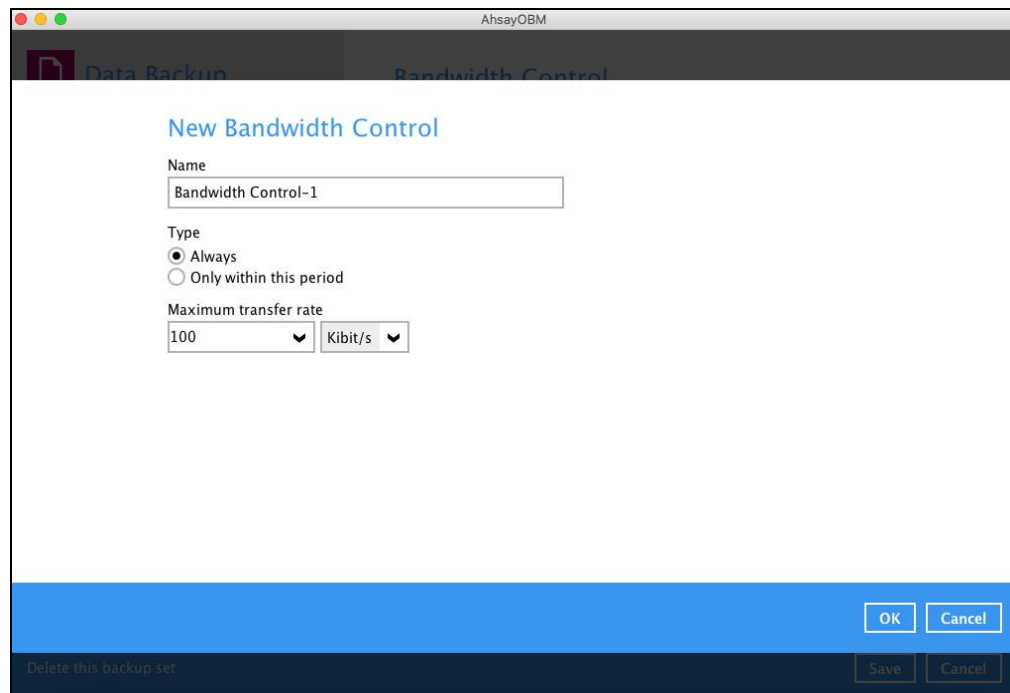


3. Click the **[+]** button to create a modified bandwidth control.



4. Complete the following fields:

- **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**: A text input field with "Bandwidth Control-1" entered.
- Type**: Two radio buttons. "Always" is selected (indicated by a filled circle), and "Only within this period" is unselected (indicated by an empty circle).
- Maximum transfer rate**: A text input field with "100" entered, followed by a dropdown menu currently showing "Kibit/s".

At the bottom of the dialog, there is a blue bar with "OK" and "Cancel" buttons. Below this bar, in a dark footer, is the text "Delete this backup set" followed by "Save" and "Cancel" buttons.

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

Others

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

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

Temporary Directory

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



The screenshot shows a window titled "Temporary Directory". Inside, it says "Temporary directory for storing backup files". There is a text input field containing "/Users/admin/temp" and a "Change" button to its right. Below the input field, it displays "53.88GB free out of total 79.2GB space in /Users/admin/temp". At the bottom, there is a checkbox labeled "Remove temporary files after backup" which is checked.

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 job. The index files are synchronized to each individual backup destination at the end of each backup job.

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

NOTES

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.


The message below will be displayed if the path to the temporary directory is inaccessible. Click OK then proceed to correct the temporary directory path.

Temporary directory does not exist! Temporary Directory = "/temporary"

OK

To change the temporary directory, follow the steps below:

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



The 'Temporary Directory' window shows the current path as '/Users/admin/temp'. Below the path field, it displays '53.88GB free out of total 79.2GB space in /Users/admin/temp'. A checkbox labeled 'Remove temporary files after backup' is checked. A 'Change' button is located to the right of the path field.

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

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.



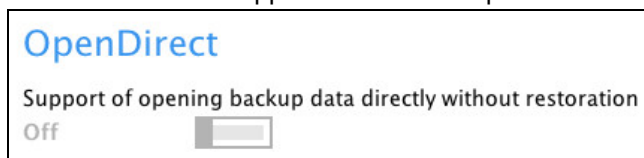
The 'Follow Link' window shows the 'Follow link of the backup files' toggle switch is turned 'On'.

NOTE

This feature is only applicable for File Backup Sets.

OpenDirect

This feature is not supported on macOS platform.

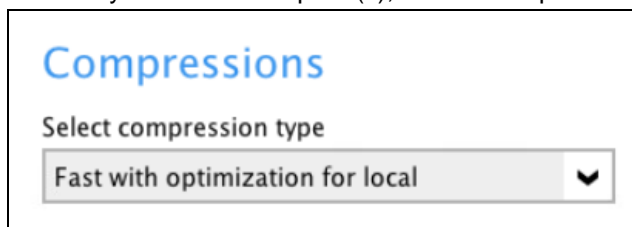


The 'OpenDirect' window shows the 'Support of opening backup data directly without restoration' toggle switch is turned 'Off'.

Compressions

When this feature is enabled, the AhsayOBM will compress all files before it is backed up to the backup destination(s).

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



The 'Compressions' window shows a dropdown menu for 'Select compression type' with 'Fast with optimization for local' selected.

The following are the four (4) compression types:

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

NOTE

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

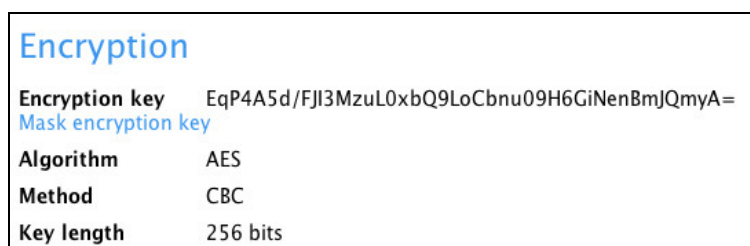
Encryption

This feature allows the user to view the current encryption settings. The encryption settings can only be enabled or disabled during the creation of backup set.



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

1. Go to Backup Sets, then select a backup set.
2. Click the **Others** tab in the backup set settings.
3. In the Encryption, click the 'Unmask encryption key' link to display the encryption key of the backup set.



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 10 Create a Backup Set](#).

Recycle Bin

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

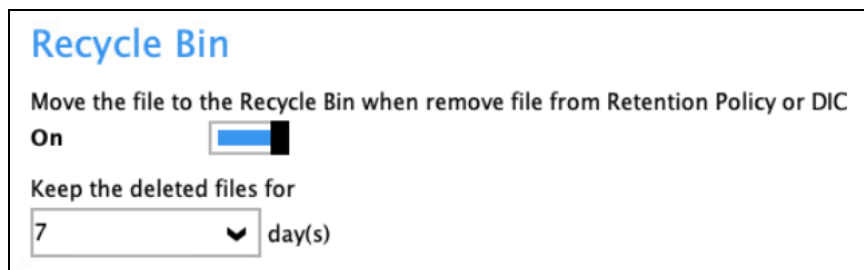
This is how the Recycle Bin will treat deleted data:

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

WARNING

When reverting index, new data will be lost.

This is enabled by default set with 7 days.

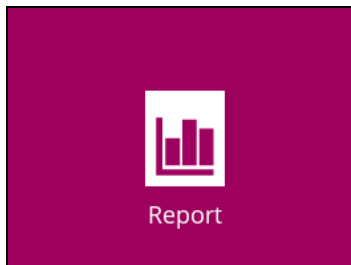


To set the number of days, follow the steps below:

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

9.6 Report

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



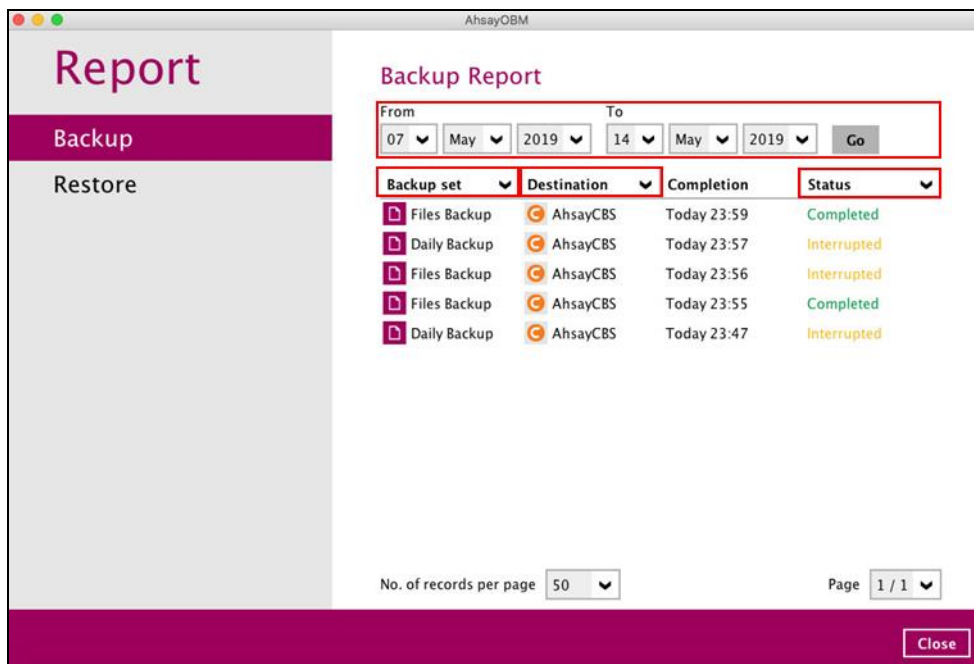
There are two (2) options available for this feature:

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

9.6.1 Backup

This feature displays the backup report logs for each backup set. There are four (4) filters that can be applied on this feature:

- Date
- Backup set
- Destination
- Status



The screenshot shows the AhsayOBM application window with the 'Report' section selected. The 'Backup Report' sub-section is active, displaying a table of backup logs. The table has four columns: 'Backup set', 'Destination', 'Completion', and 'Status'. The 'Status' column uses color coding: green for 'Completed' and yellow for 'Interrupted'. The table lists six backup sets, alternating between 'Files Backup' and 'Daily Backup', all using 'AhsayCBS' as the destination. The completion times are listed as 'Today' followed by a time. At the bottom of the window, there is a 'No. of records per page' dropdown set to 50, a 'Page' indicator showing '1 / 1', and a 'Close' button.

| 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 |

Date

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

Backup Report

From

08 May 2019

To

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 |

Backup set

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

Backup Report

From

08 May 2019

To

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 |

Destination

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

| 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 |

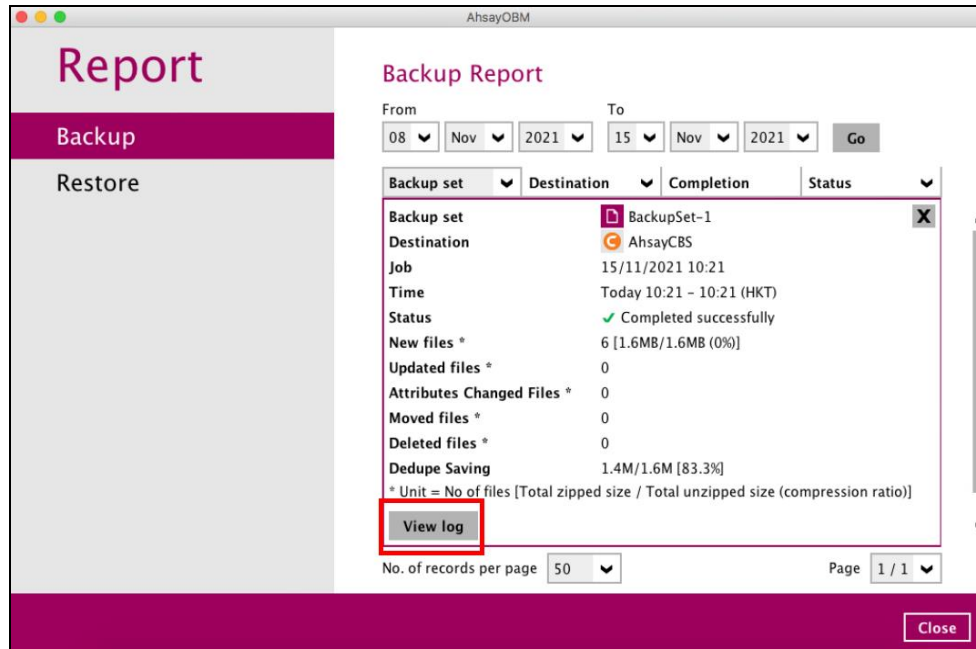
Status

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

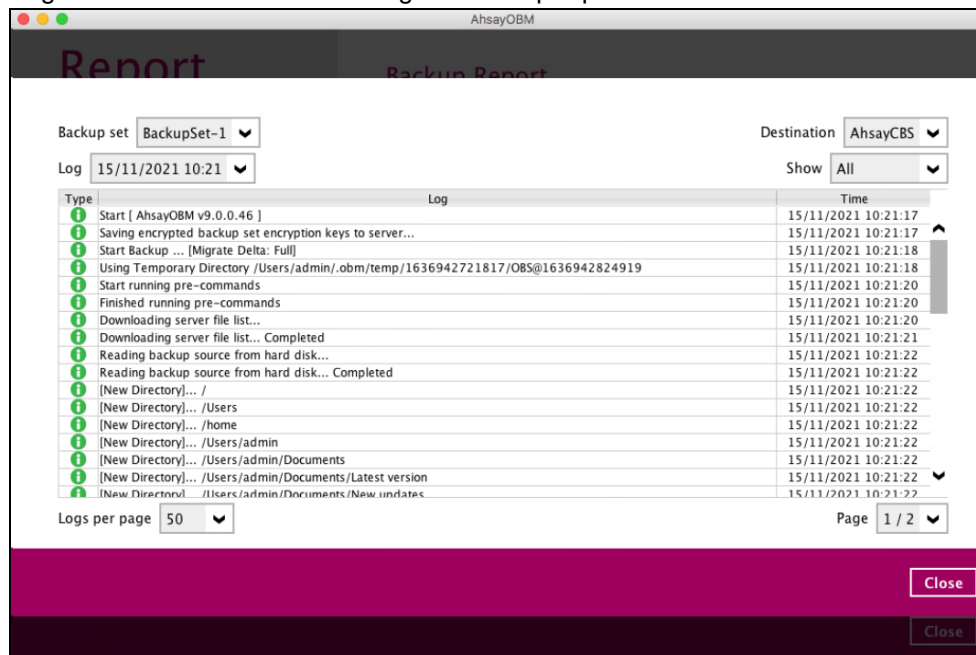
| Backup Report | | | |
|-----------------|---------------|------------------|---------------------------|
| From | | To | |
| 08 | May | 2019 | 15 May 2019 Go |
| Backup set | Destination | Completion | Status |
| Files Backup | Local-1 | Today 01:11 | Status |
| Files Backup | GoogleDrive-1 | Today 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 |

To view the backup log, follow the instructions below:

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



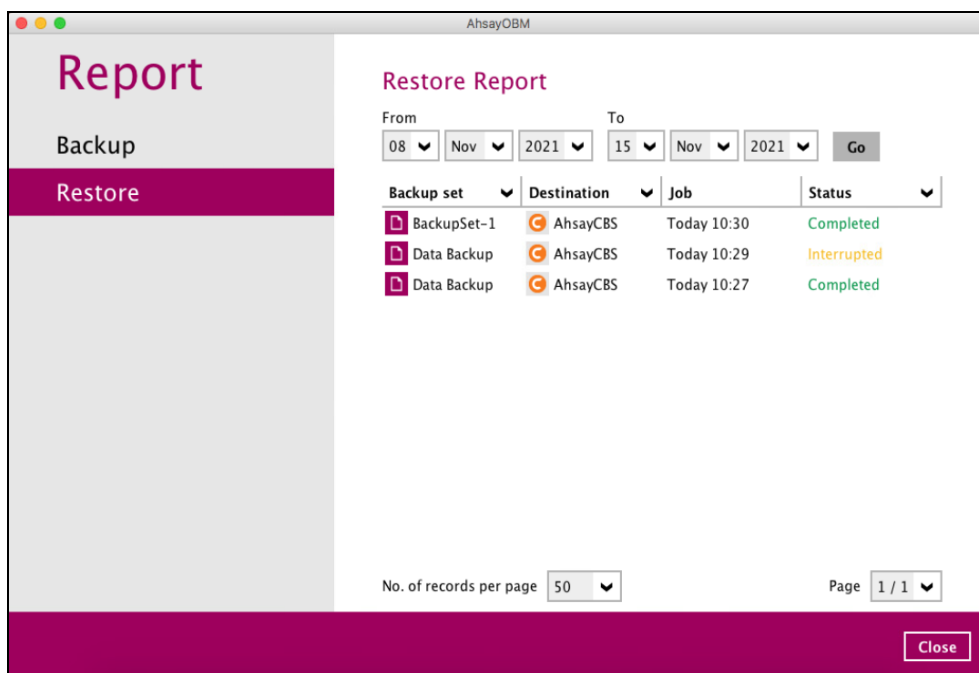
2. The Backup set, Destination, Log Date and Time, Status, the number of Logs per page, and Page can be filtered when viewing the backup report.



9.6.2 Restore

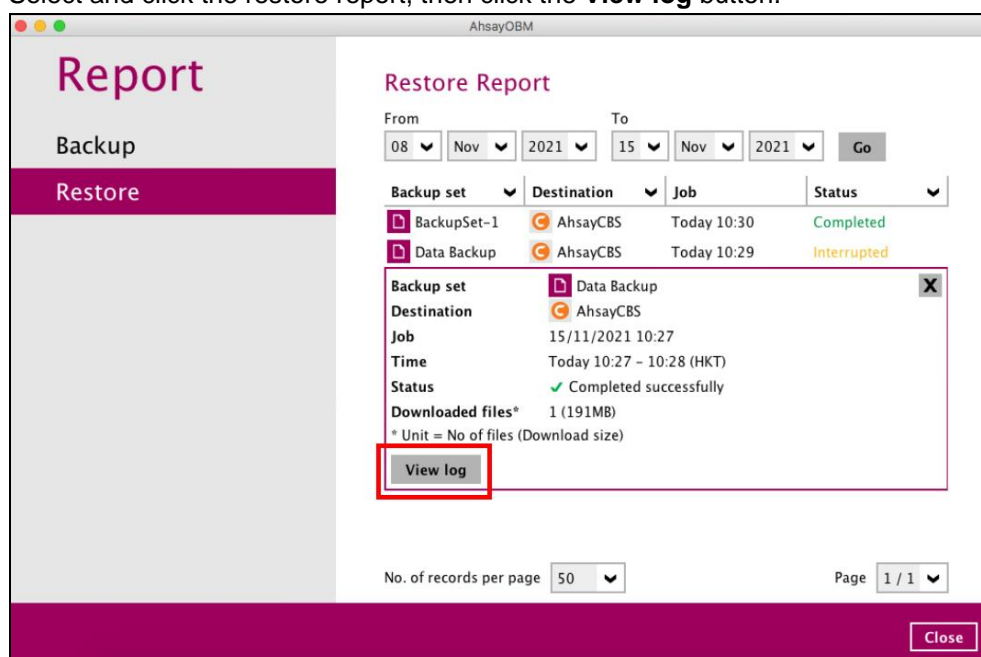
This feature displays the restore report logs for each backup set. Similar to the **Backup** tab, this feature also consists of the following filters:

- Date
- Backup Set
- Destination
- Status



To view the restore log, follow the instructions below:

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



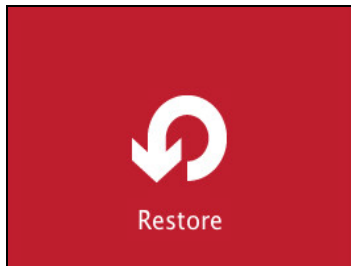
- The Backup set, Destination, Log Date and Time, Status, the number of Logs per page, and Page can be filtered when viewing the restore report.

The screenshot shows the 'Restore Report' window in AhsayOBM. At the top, there are filters for 'Backup set' (set to 'Data Backup'), 'Log' (set to '15/11/2021 10:27'), and 'Show' (set to 'All'). Below these filters is a table of logs. The table has three columns: 'Type', 'Log', and 'Time'. The logs are listed with their corresponding times. At the bottom of the window, there are controls for 'Logs per page' (set to 50) and 'Page' (set to 1 / 171). There are also 'Close' buttons at the bottom right.

| Type | Log | Time |
|--|-----|---------------------|
| Start [AhsayOBM v9.0.0.46] | | 15/11/2021 10:27:40 |
| Same file "/Library/Application Support/App Store/adoption.plist" exists already. | | 15/11/2021 10:27:43 |
| "/Library/Application Support/App Store/adoption.plist" contains the same file resource. Skip restore file resource. | | 15/11/2021 10:27:43 |
| Same file "/Library/Application Support/CrashReporter/AnonymousIdentifier_564D93C1-F73D-354A-60EA-A9F8787... | | 15/11/2021 10:27:44 |
| "/Library/Application Support/CrashReporter/AnonymousIdentifier_564D93C1-F73D-354A-60EA-A9F878789.pli... | | 15/11/2021 10:27:44 |
| Same file "/Library/Application Support/CrashReporter/AnonymousIdentifier_564DE085-D581-8958-1575-SA1C1FC... | | 15/11/2021 10:27:44 |
| "/Library/Application Support/CrashReporter/AnonymousIdentifier_564DE085-D581-8958-1575-SA1C1FC9614.pli... | | 15/11/2021 10:27:44 |
| Existing item found (overwrite)... /Library/Application Support/CrashReporter/DiagnosticMessagesHistory.plist | | 15/11/2021 10:28:06 |
| Downloading... "/Library/Application Support/CrashReporter/DiagnosticMessagesHistory.plist" (Total 190 bytes) | | 15/11/2021 10:28:06 |
| Restoring File Resource: /Library/Application Support/CrashReporter/DiagnosticMessagesHistory.plist | | 15/11/2021 10:28:06 |
| Same file "/Library/Application Support/CrashReporter/mtmd_564DE085-D581-8958-1575-SA1C1FCE9614.plist" e... | | 15/11/2021 10:28:06 |
| "/Library/Application Support/CrashReporter/mtmd_564DE085-D581-8958-1575-SA1C1FCE9614.plist" contains th... | | 15/11/2021 10:28:06 |
| Same file "/Library/Application Support/CrashReporter/ReportCrash_564DE085-D581-8958-1575-SA1C1FCE9614.... | | 15/11/2021 10:28:06 |
| "/Library/Application Support/CrashReporter/ReportCrash_564DE085-D581-8958-1575-SA1C1FCE9614.plist" cont... | | 15/11/2021 10:28:06 |
| Same file "/Library/Application Support/CrashReporter/softwareupdate_download_service_564DE085-D581-8958-1... | | 15/11/2021 10:28:06 |
| "/Library/Application Support/CrashReporter/softwareupdate_download_service_564DE085-D581-8958-1575-SA1C... | | 15/11/2021 10:28:06 |
| Same file "/Library/Application Support/CrashReporter/softwareupdate_downloaded_564D93C1-F73D-354A-60EA-A9F8787... | | 15/11/2021 10:28:06 |

9.7 Restore

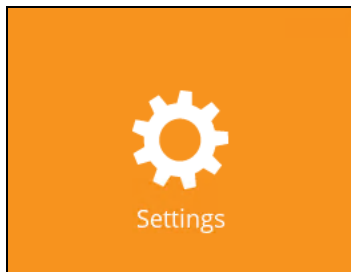
This feature is used to restore backed up files to its original or alternate location.



To restore backed up files, follow the instructions on [Chapter 13 Restore Data](#).

9.8 Settings

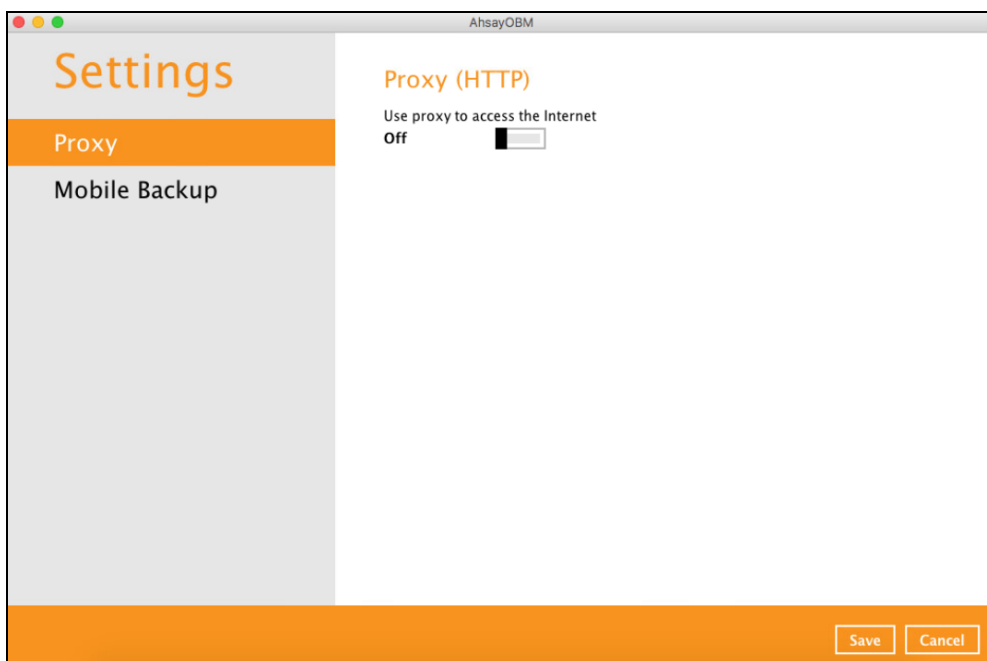
This feature allows user to enable the **Proxy Settings**.



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

- Proxy
- Mobile Backup

NOTE: The Mobile Backup tab will only be available if the mobile add-on module is enabled on the user profile. Please contact your backup service provider for details.

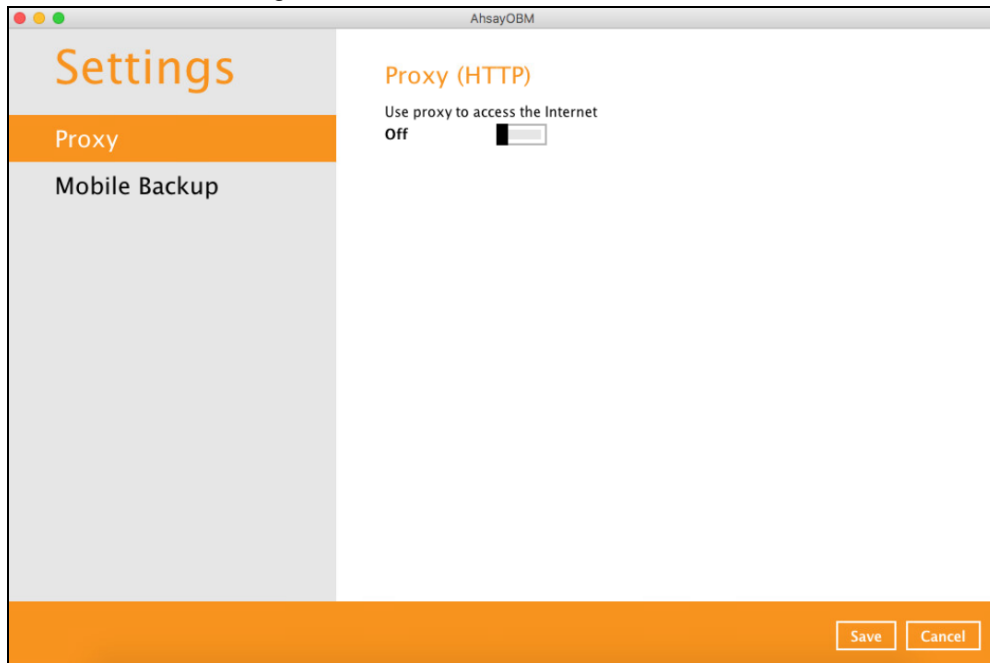


9.8.1 Proxy

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

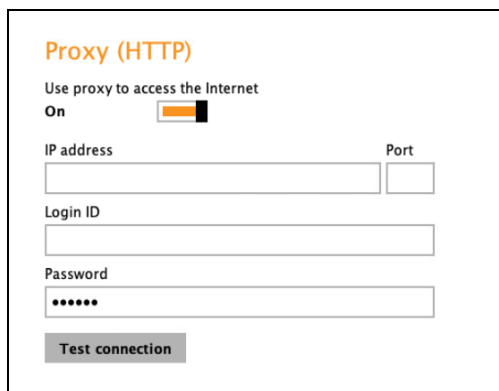
To enable the Proxy Settings, follow the instructions below:

1. Slide the lever to the right to turn it on.



2. Complete the following fields:

- IP address
- Port
- Login ID
- Password

A screenshot of the Proxy (HTTP) configuration form. The form is titled 'Proxy (HTTP)' and includes the text 'Use proxy to access the Internet'. Below this is a toggle switch currently set to 'On'. The form contains four input fields: 'IP address', 'Port', 'Login ID', and 'Password'. The 'Password' field is masked with dots. At the bottom of the form is a 'Test connection' button.

3. Click the **Test Connection** button to validate the connection.
4. Click the **Save** button to apply the settings.

9.8.2 Mobile Backup

The Mobile Backup tab is only available if the mobile add-on module is enabled on the user profile. Please contact your backup service provider for details.

You can use the Mobile backup function to:

- Add one or more device(s) registered for mobile backup.

NOTE

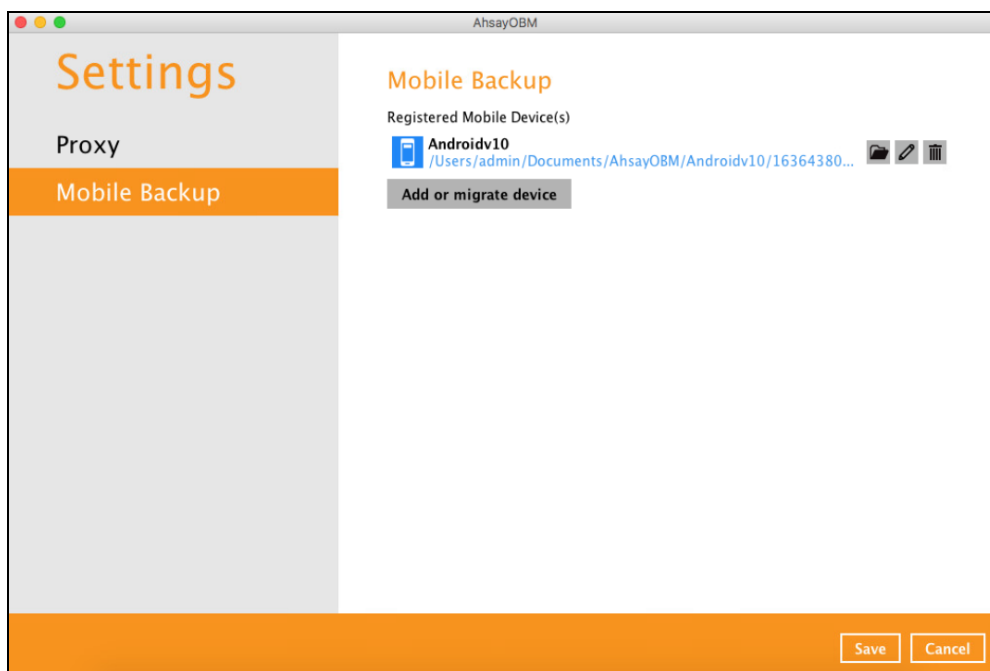
Please refer to **Chapter 7** of the [Ahsay Mobile User Guide for Android and iOS](#) for the detailed step-by-step procedure.

- [View backed up photos, videos and documents saved in the mobile backup destination.](#)
- Change the mobile backup destination to:
 - [new location in the same machine](#)
 - [new machine](#)
- [Remove one or more device\(s\) registered for mobile backup.](#)

NOTE

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

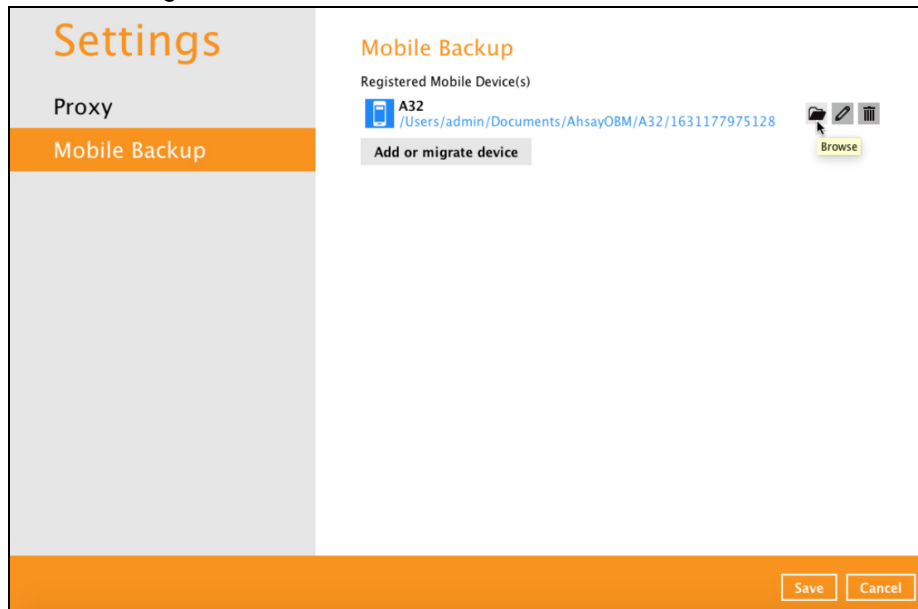
- Restore to a different mobile device on the same operating system.
- Restore to a different mobile device on another operating system, i.e., Android to iOS or iOS to Android.



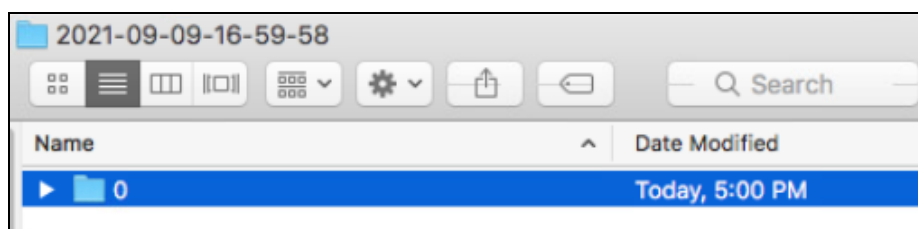
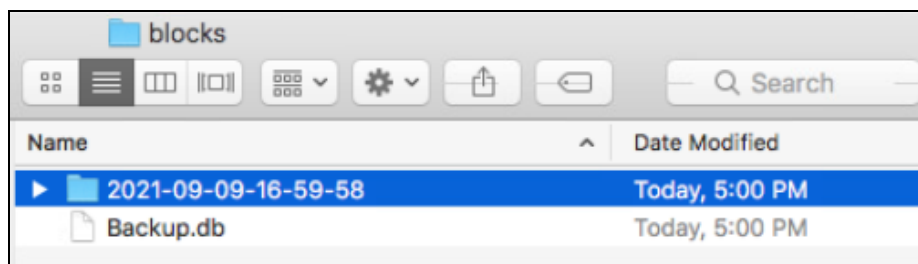
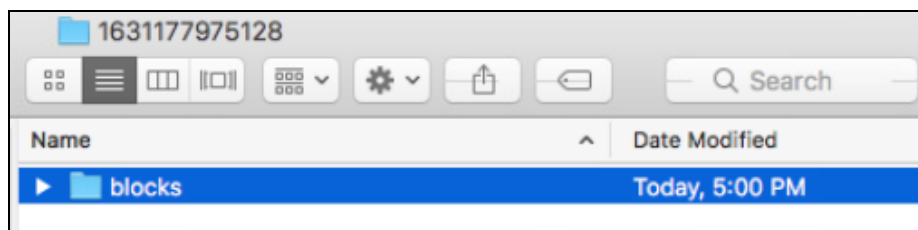
View backed up photos, videos and documents saved in the mobile backup destination

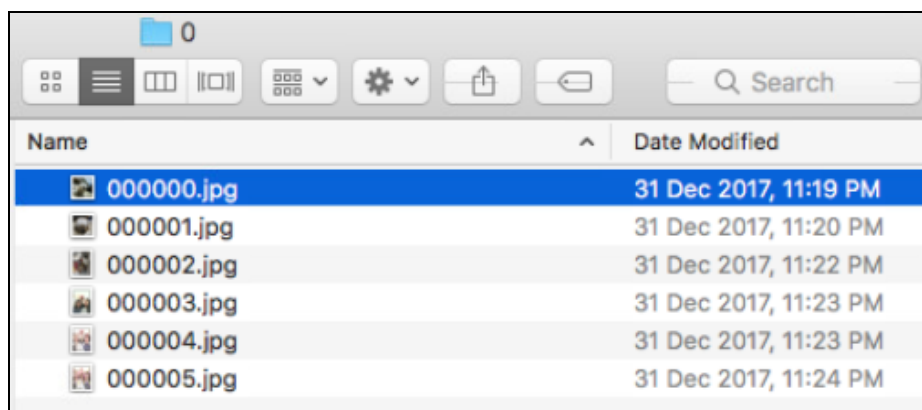
To view backed up photos, videos and documents saved in the mobile backup destination, follow the instructions below:

1. Either click the link under the registered mobile device or click the **Browse** icon on the right side of the registered mobile device.



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





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

Change mobile backup destination location to new location in the same machine

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

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

If Free up space is enabled on the Ahsay Mobile app, it is strongly recommended to copy the previously backed up photos, videos, documents and 2FA accounts to the new location to prevent missing data. As some of the backed up photos, videos, documents and 2FA accounts have already been removed from the mobile device.

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

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

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

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

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

Example: Change backup destination

from

/Users/admin/Documents/AhsayOBM/\$registered_mobile_device/\$backupsetID

to

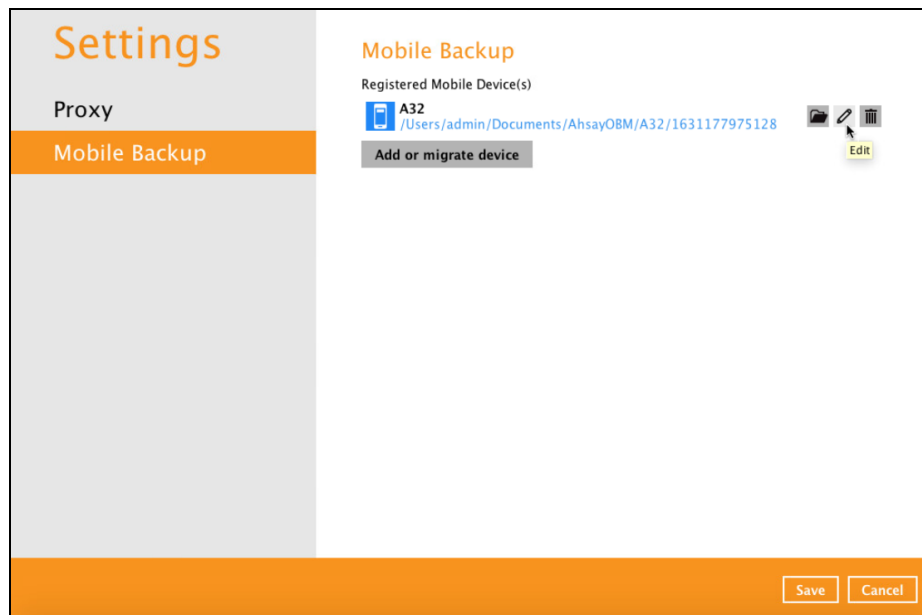
/Users/admin/Documents/MobileBackup

1. From the old location, secure a copy of the previously backed up photos, videos, documents and 2FA accounts.
2. Copy the previously backed up photos, videos, documents and 2FA accounts from the original location to the new mobile backup destination (if applicable).

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

In this example, the old mobile backup destination is

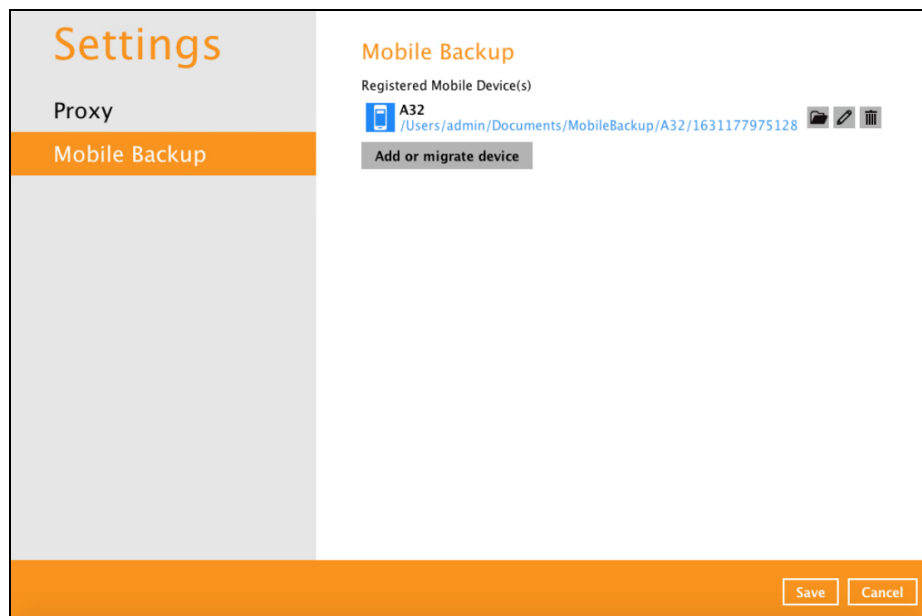
/Users/admin/Documents/AhsayOBM/\$registered_mobile_device/\$backupsetID.



4. A new screen will be displayed. Select the new mobile backup destination then click **Open**.
5. Click **Save** to store the change made.

Mobile backup destination is successfully changed to

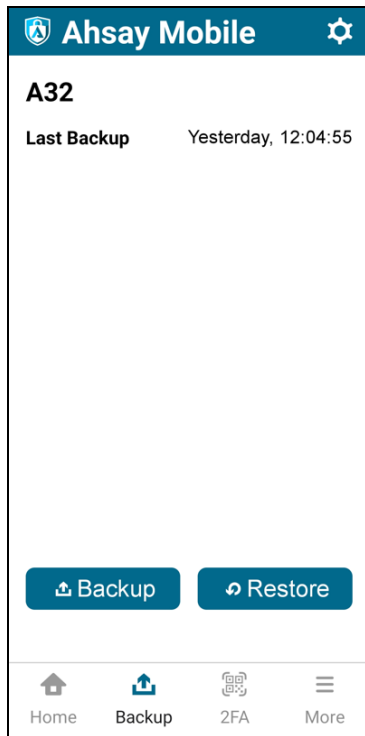
/Users/admin/Documents/MobileBackup. All mobile backups will now be saved to this destination.



NOTE

The \$registered_mobile_device and \$backupsetID will be appended automatically to the new mobile backup destination.

- Resume the backup job.



Change mobile backup destination location to new machine

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

If the machine needs upgrading, the previously backed up photos, videos, documents and 2FA accounts are still available.

If Free up space is enabled on the Ahsay Mobile app, it is strongly recommended to copy the previously backed up photos, videos and 2FA accounts to the new machine to prevent missing data. As some of the backed up photos, videos, documents and 2FA accounts have already been removed from the mobile device.

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

NOTE

- If the machine is lost/stolen, changing the mobile destination is not supported as it is required to re-register your mobile devices on AhsayOBM and perform backup of backed up photos, videos, documents and 2FA accounts.
- Changing the mobile backup destination to a new machine with a different operating system is supported, e.g. from a macOS machine to Window machine or Linux machine to macOS machine etc.

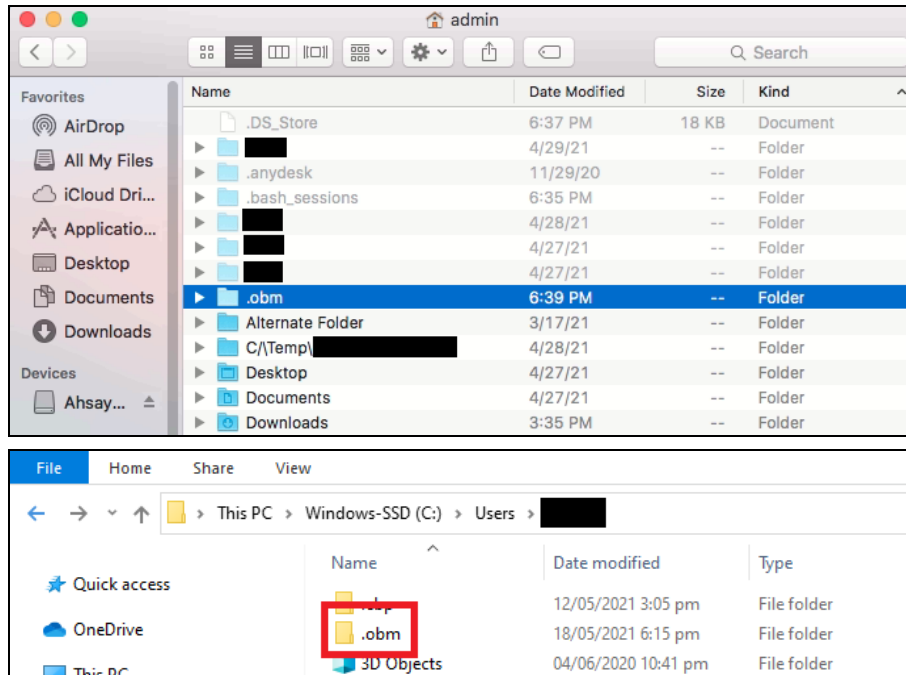
To change the mobile backup destination to a new machine, follow the instructions below:

Example: Changing the mobile backup destination from an old macOS machine to a new Windows machine.

1. On the new machine, install **AhsayOBM**.



2. Copy the **.obm** folder from the old macOS machine to the new Windows machine.

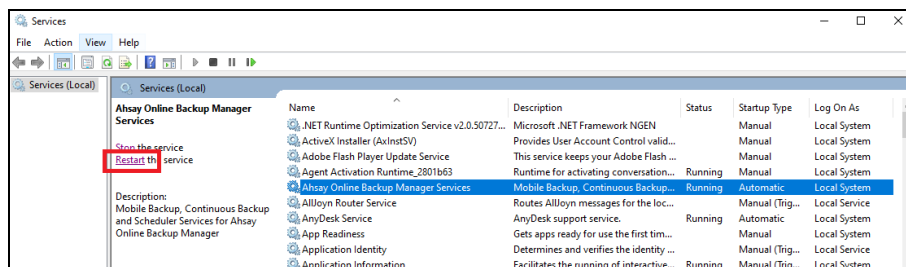


3. Copy the previously backed up photos, videos, documents and 2FA accounts from the old machine to the new mobile backup destination.

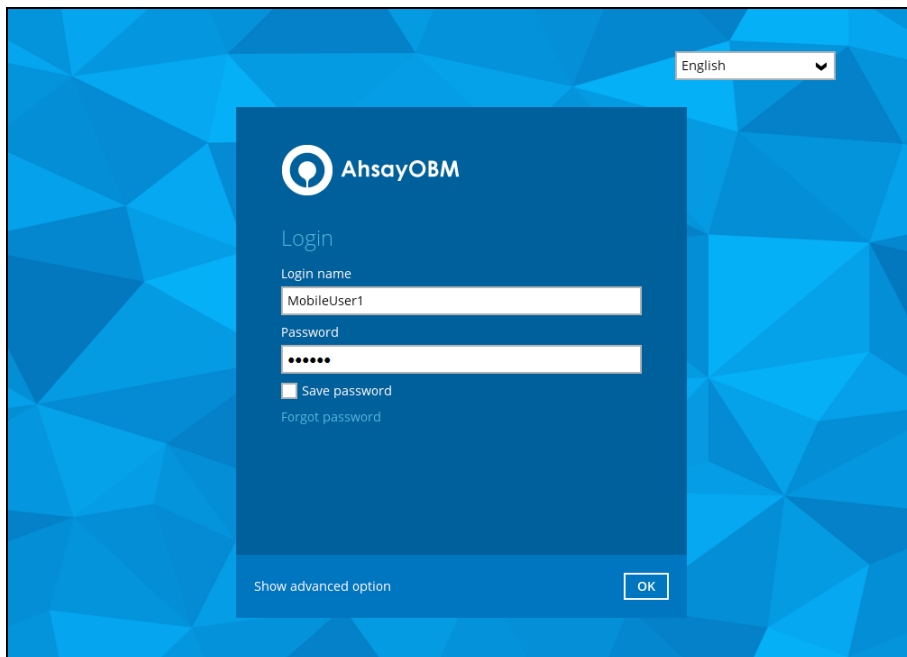
NOTE

During machine upgrade, make sure to uninstall the AhsayOBM from the old machine to avoid any interruptions while backing up on the new machine.

4. Restart the **AhsayOBM Services** because copying the **.obm** folder on a newly installed AhsayOBM will not trigger the MBS.

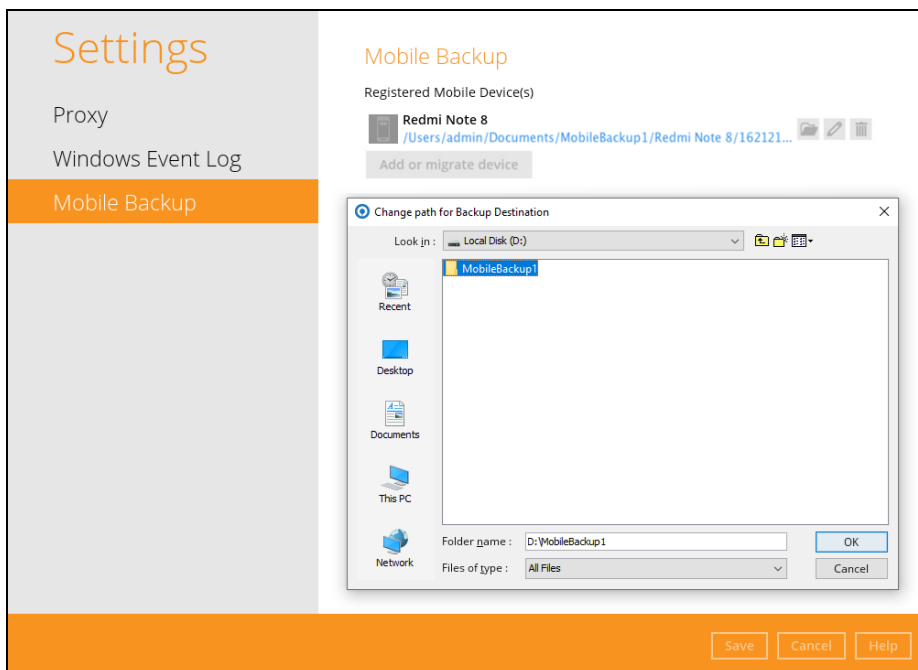


5. Login to **AhsayOBM**. Enter the login name and password of your AhsayOBM account. Then, click **OK** to login



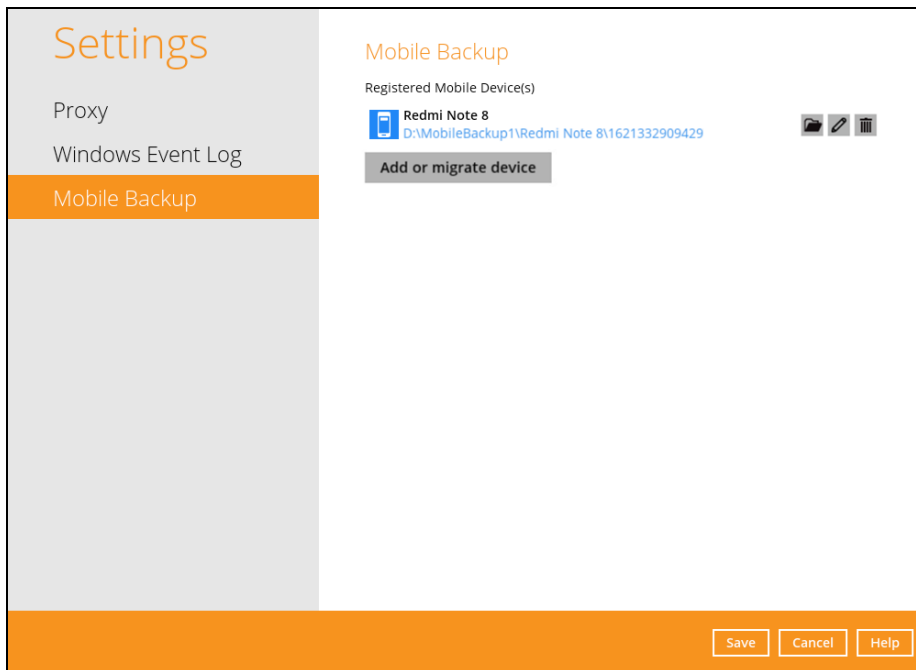
6. Go to **Settings > Mobile Backup**. Click the **Edit** icon on the right side of the registered mobile device.
7. **Change path for Backup Destination** screen will be displayed. Select the new mobile backup destination then click **OK**.

In this example, the new mobile backup destination will be **D:\MobileBackup1**.



8. Click **Save** to store the change made.

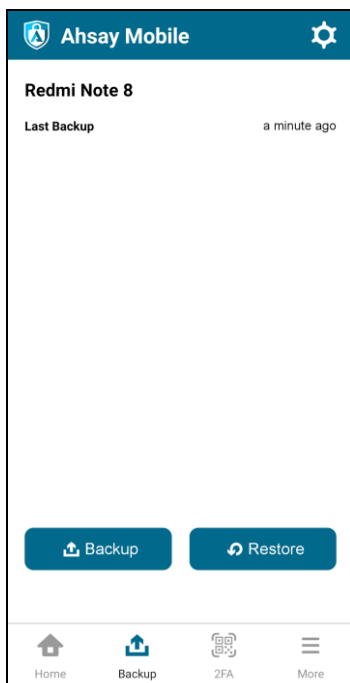
Mobile backup destination is successfully changed to **D:\MobileBackup1**. All mobile backups will now be saved to this destination.



NOTE

The \$registered_mobile_device and \$backupsetID will be appended automatically to the new mobile backup destination.

9. Resume the backup job.



NOTE

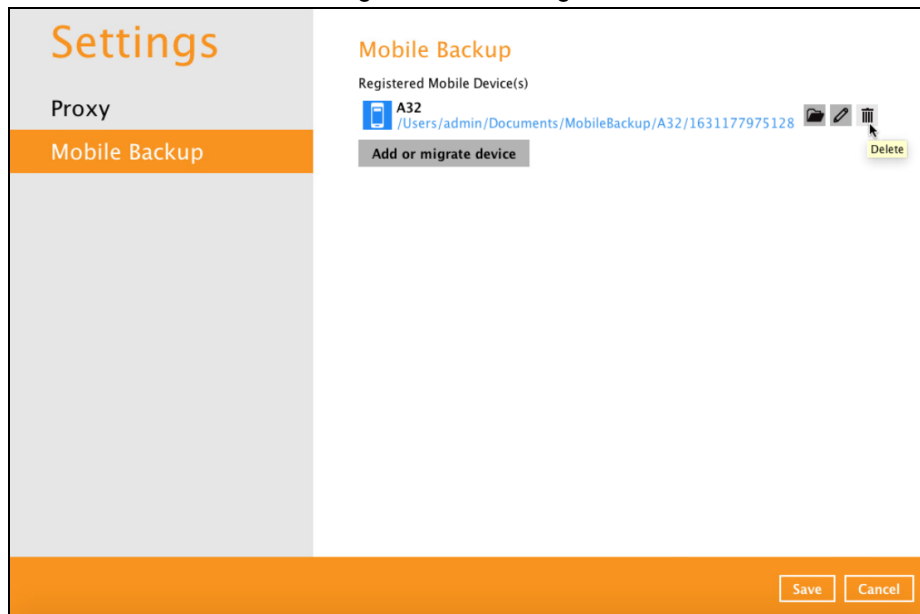
For instructions on changing the mobile backup destination of:

- a Windows machine to a macOS machine, please refer to **Chapter 10.8.3** of the [AhsayOBM v8 Quick Start Guide for Windows](#).

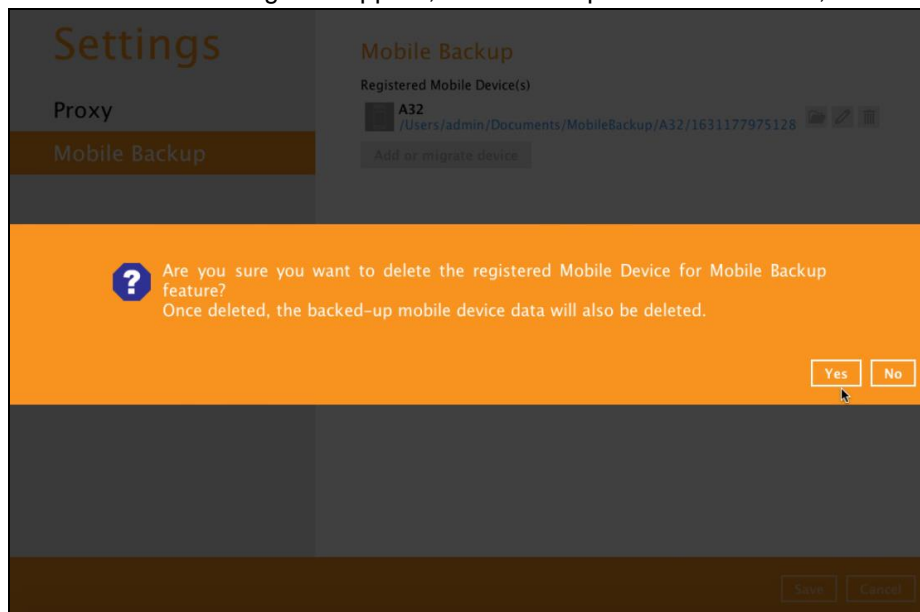
Remove one or more device(s) registered for Mobile Backup

To remove a mobile device, follow the instructions below:

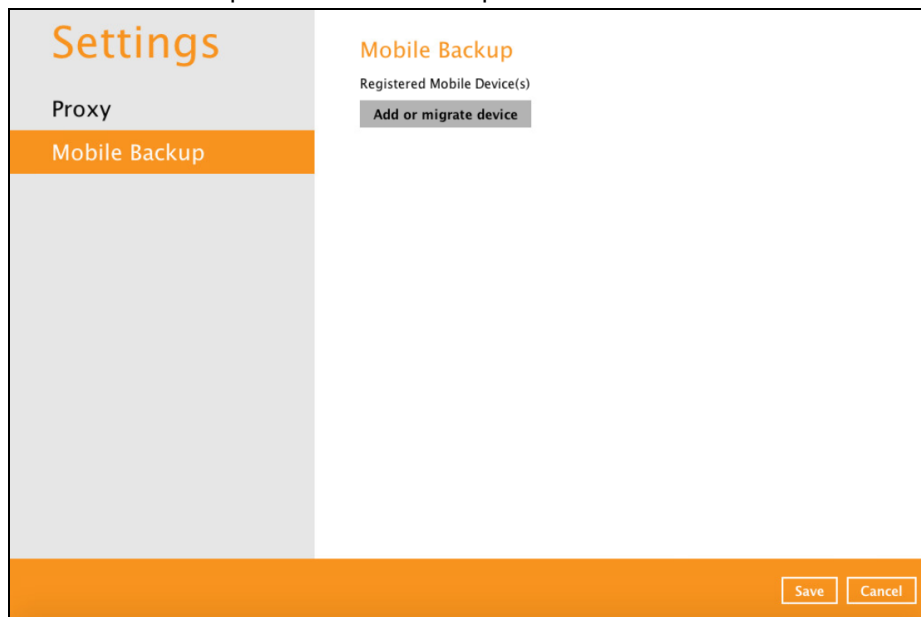
1. Click the **Delete** icon on the right side of the registered mobile device.



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

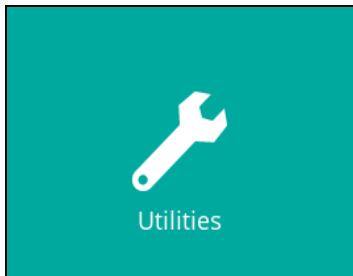


3. Mobile device is successfully removed along with any photos, videos, documents and 2FA accounts backed up in the mobile backup destination.



9.9 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.



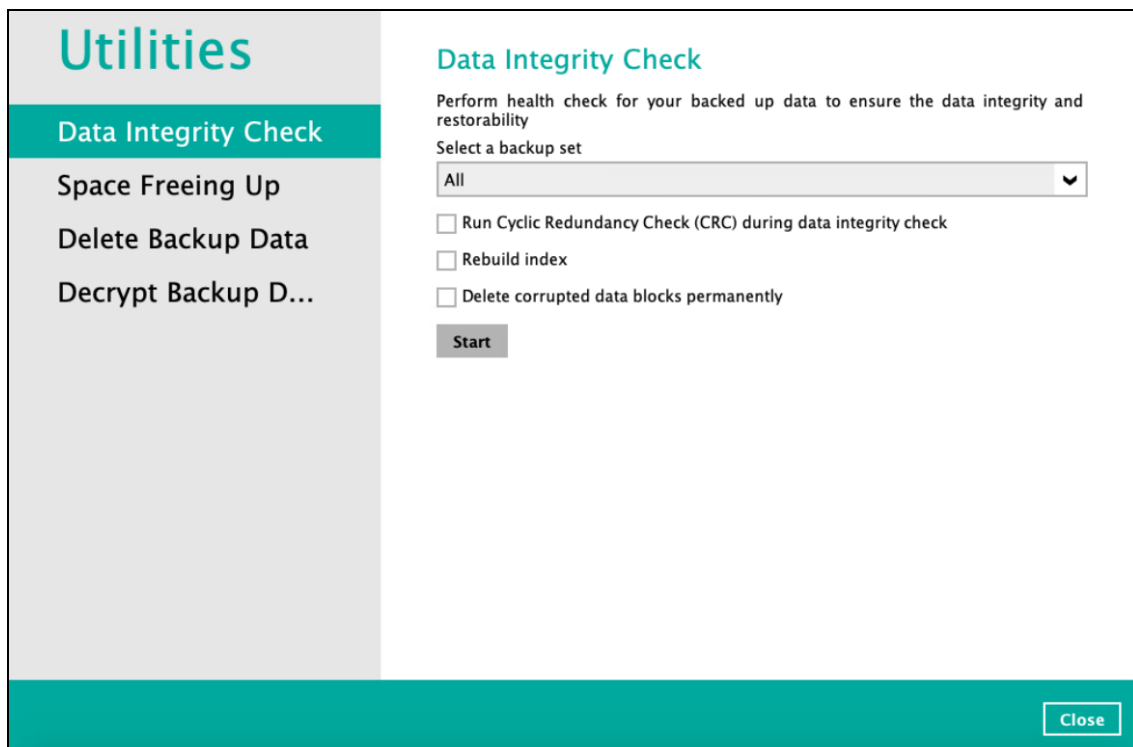
There are four (4) options available for this feature:

- [Data Integrity Check](#)
- [Space Freeing Up](#)
- [Delete Backup Data](#)
- [Decrypt Backup Data](#)

9.9.1 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).

The screenshot shows a web-based utility interface. On the left is a sidebar with a teal header "Utilities" and four menu items: "Data Integrity Check" (highlighted in teal), "Space Freeing Up", "Delete Backup Data", and "Decrypt Backup D...". The main content area is titled "Data Integrity Check" in teal. It contains the instruction "Perform health check for your backed up data to ensure the data integrity and restorability". Below this is a dropdown menu labeled "Select a backup set" with "All" selected. There are three checkboxes: "Run Cyclic Redundancy Check (CRC) during data integrity check", "Rebuild index", and "Delete corrupted data blocks permanently", all of which are currently unchecked. A grey "Start" button is positioned below the checkboxes. At the bottom right of the main area is a teal "Close" button.

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 that the data integrity check is completed with error(s) and had skipped a backup set with an active backup job.

Run Cyclic Redundancy Check (CRC)

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

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

Delete corrupted data blocks permanently

When this option is enabled, it overrides the Recycle Bin setting of the backup set. The DIC will delete corrupted data blocks permanently instead of moving it to the Recycle Bin.

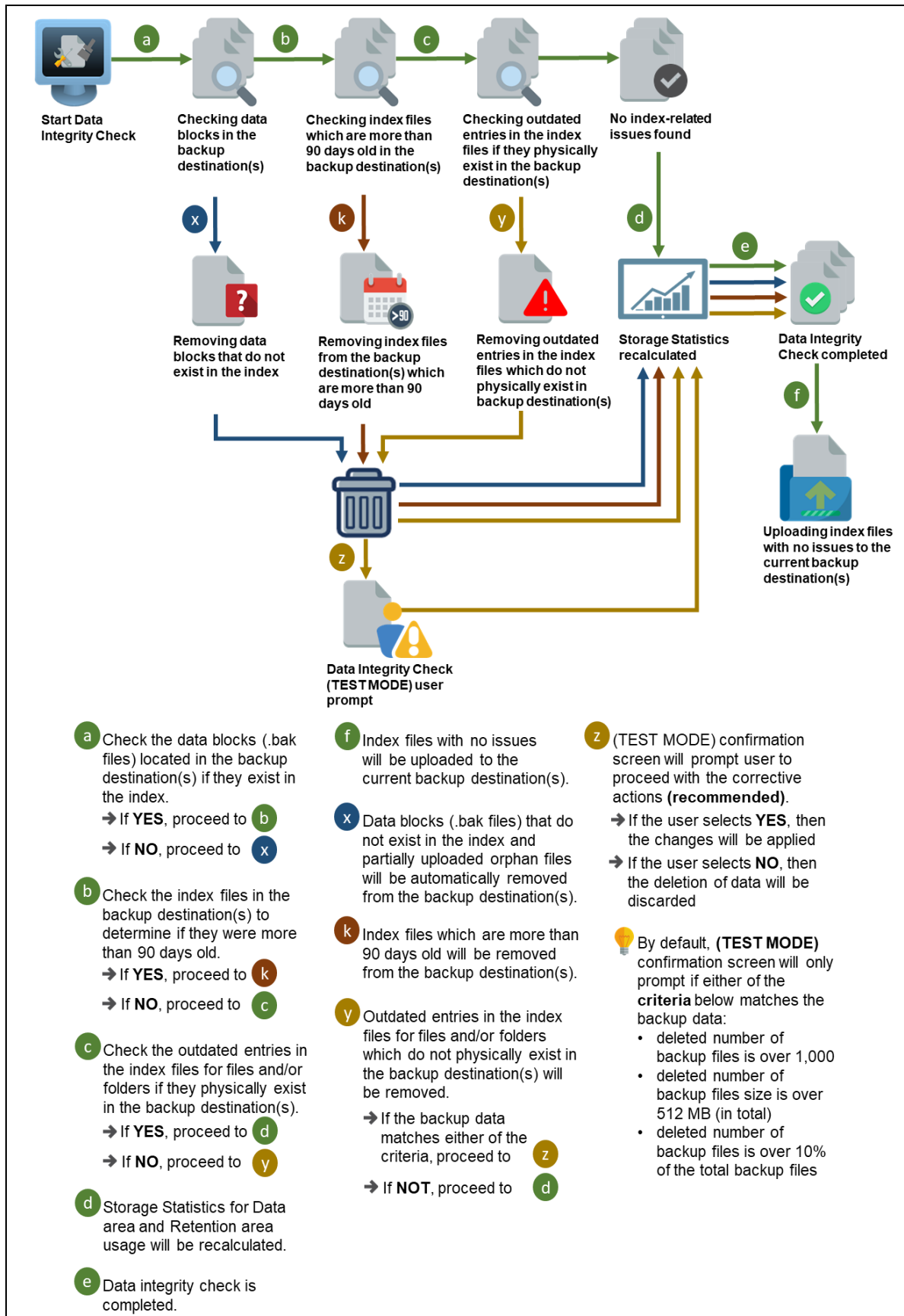
There are four (4) options in performing the Data Integrity Check:

| Settings | Function |
|--|--|
| Option 1 <input type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check <input type="checkbox"/> Rebuild index <input type="checkbox"/> Delete corrupted data blocks permanently <input type="button" value="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 <input type="checkbox"/> Delete corrupted data blocks permanently <input type="button" value="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 <input type="checkbox"/> Delete corrupted data blocks permanently <input type="button" value="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 <input type="checkbox"/> Delete corrupted data blocks permanently <input type="button" value="Start"/> | For checking of index, integrity of files against the checksum file generated at the time of the backup job and rebuilding of index. |

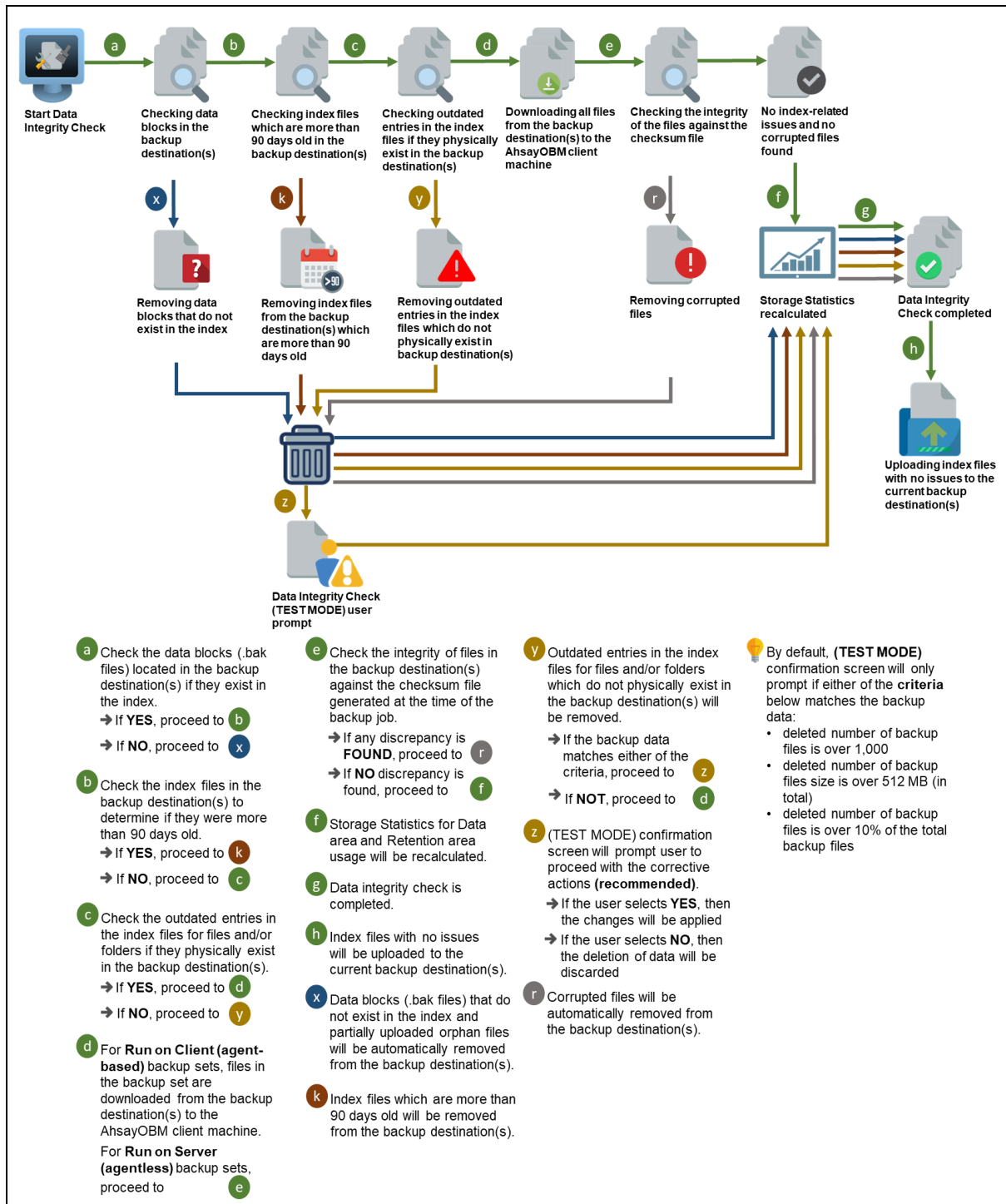
The following diagrams show the detailed process of the Data Integrity Check (DIC) in four (4) modes:

- [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

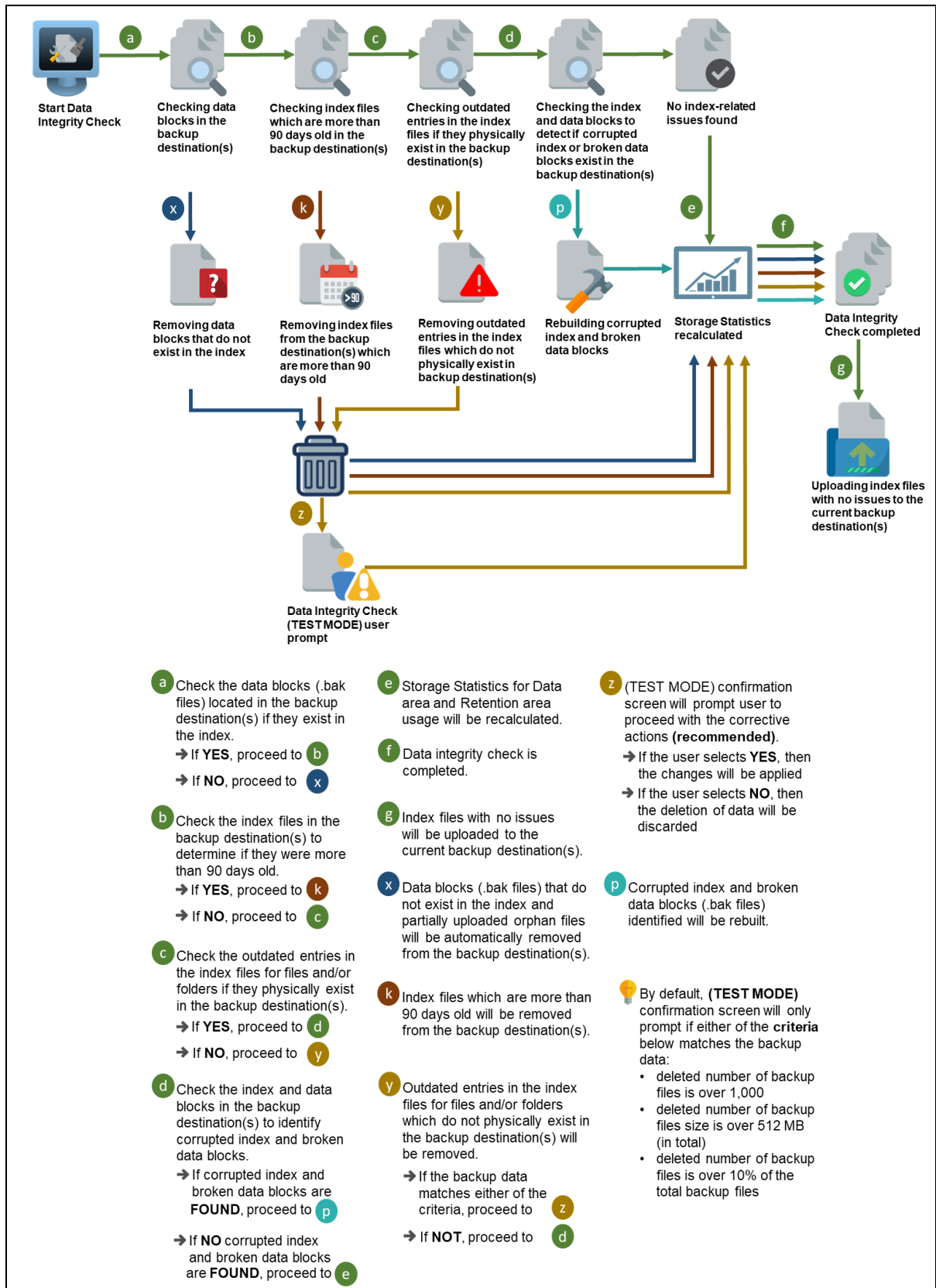
Option 1 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Rebuild index DISABLED (Default mode)



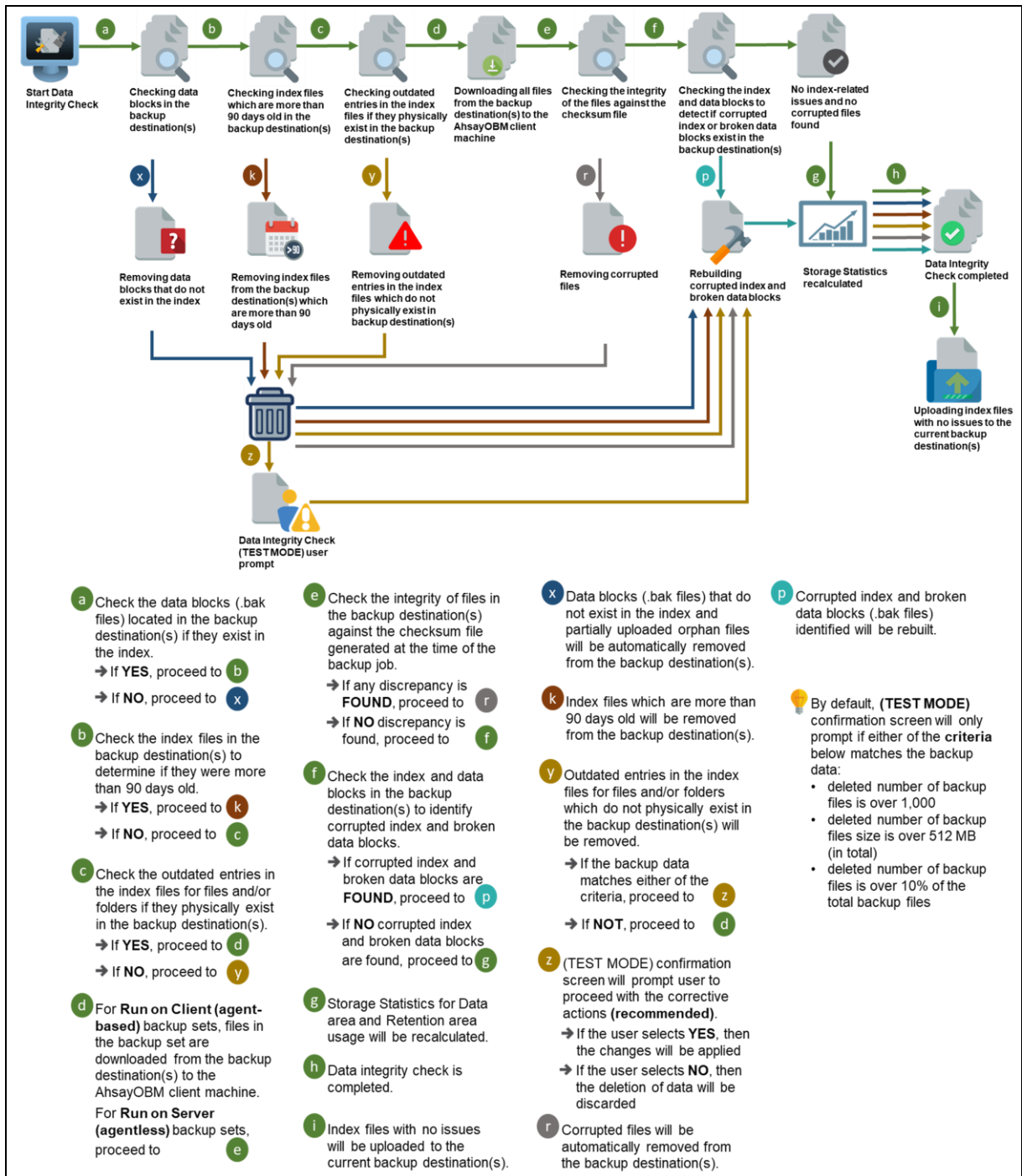
Option 2 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) **ENABLED** and Rebuild index **DISABLED**



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



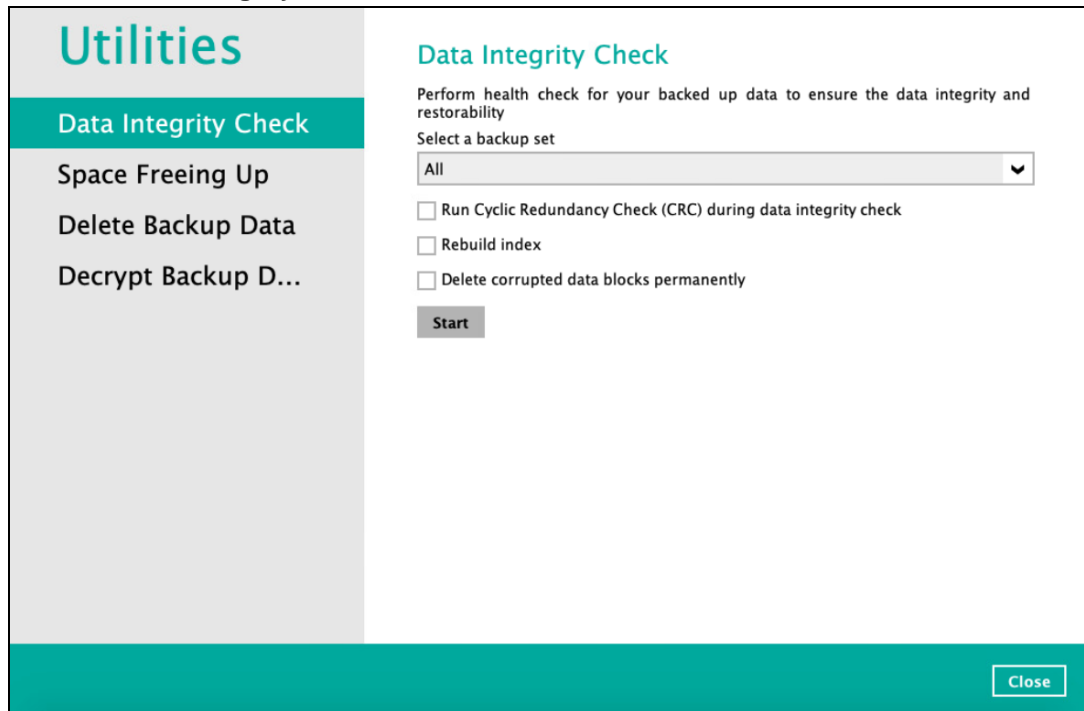
Option 4 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Rebuild index **ENABLED**



Perform a Data Integrity Check

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

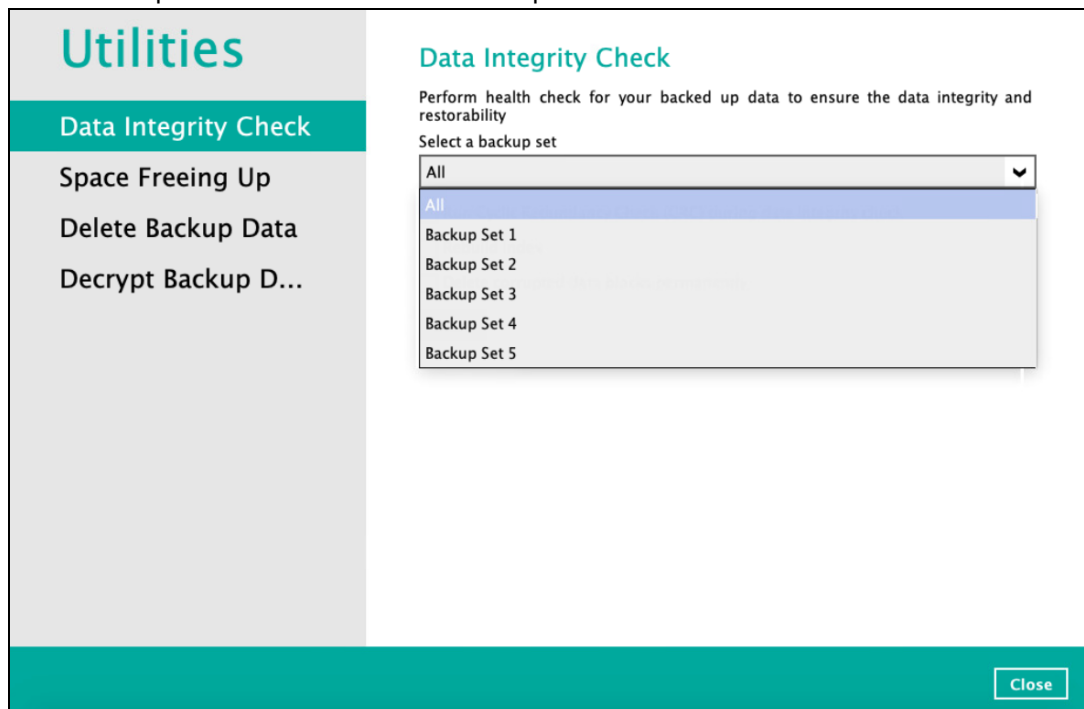
1. Go to the **Data Integrity Check** tab in the Utilities menu.



The screenshot shows the 'Utilities' menu on the left with 'Data Integrity Check' selected. The main panel is titled 'Data Integrity Check' and contains the following elements:

- Data Integrity Check** (Section Header)
- Perform health check for your backed up data to ensure the data integrity and restorability
- Select a backup set: A dropdown menu currently showing 'All'.
- ☐ Run Cyclic Redundancy Check (CRC) during data integrity check
- ☐ Rebuild index
- ☐ Delete corrupted data blocks permanently
- Start** button
- Close** button (bottom right)

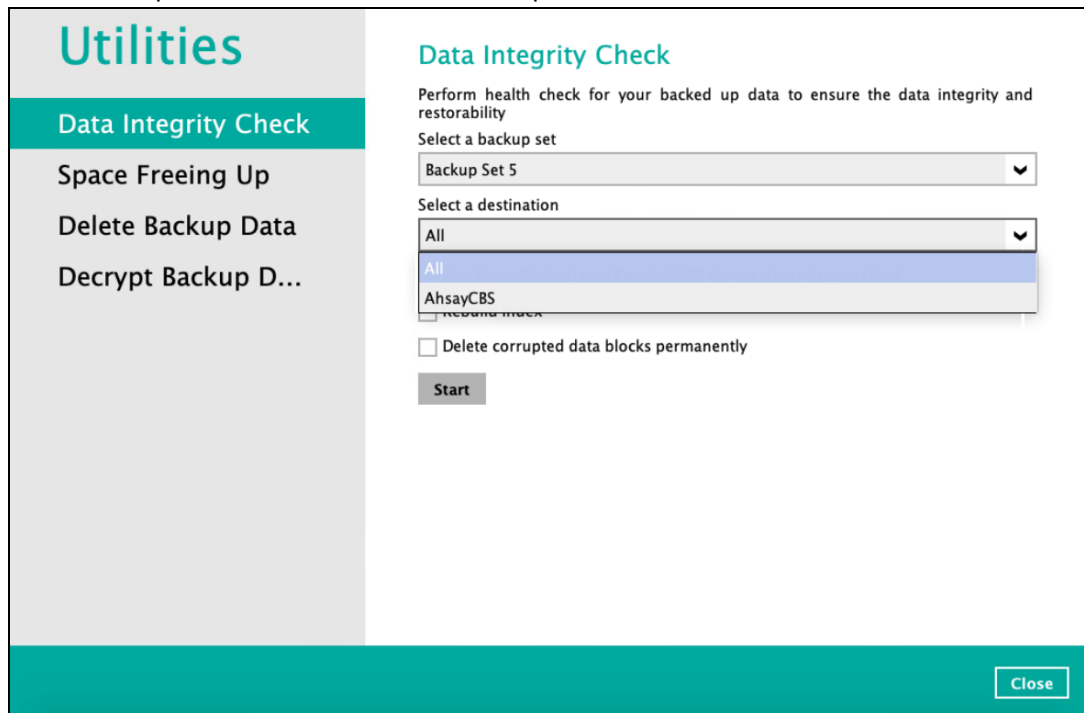
2. Click the drop-down button to select a backup set.



This screenshot is identical to the previous one, but the dropdown menu for 'Select a backup set' is open, displaying the following options:

- All (highlighted)
- Backup Set 1
- Backup Set 2
- Backup Set 3
- Backup Set 4
- Backup Set 5

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



Utilities

Data Integrity Check

Perform health check for your backed up data to ensure the data integrity and restorability

Select a backup set

Backup Set 5

Select a destination

All

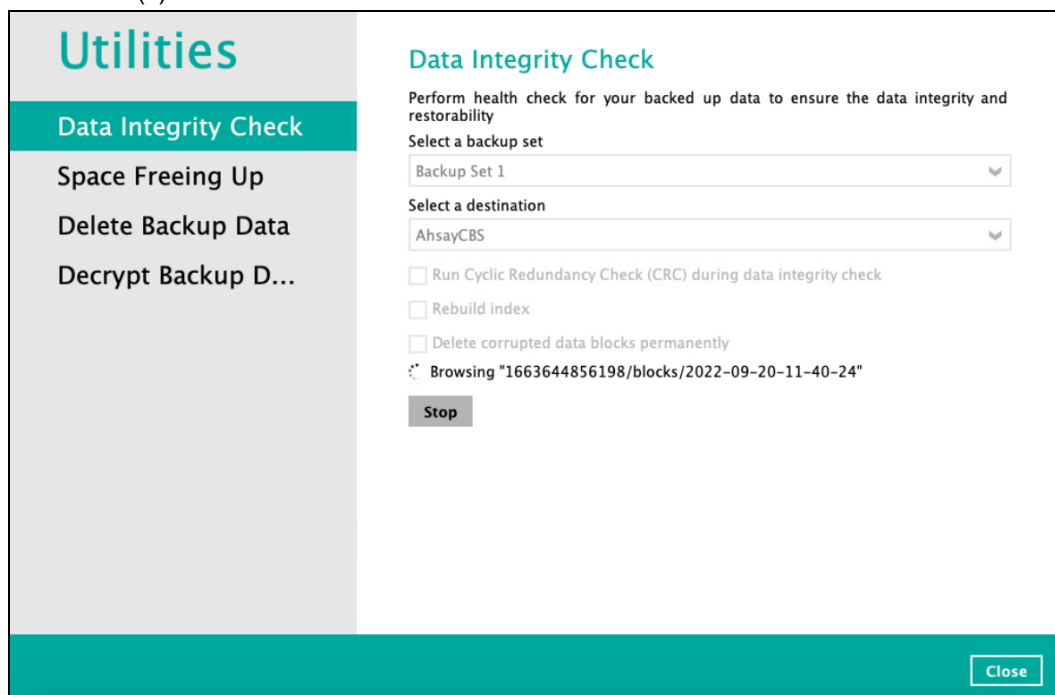
AhsayCBS

☐ Delete corrupted data blocks permanently

Start

Close

- Click the **Start** button to begin the Data Integrity Check.
- The Data Integrity Check will start running on the selected backup set(s) and backup destination(s).



Utilities

Data Integrity Check

Perform health check for your backed up data to ensure the data integrity and restorability

Select a backup set

Backup Set 1

Select a destination

AhsayCBS

☐ Run Cyclic Redundancy Check (CRC) during data integrity check

☐ Rebuild index

☐ Delete corrupted data blocks permanently

Browsing "1663644856198/blocks/2022-09-20-11-40-24"

Stop

Close

6. Once the DIC is completed, click the **View log** button to check the detailed process of the Data Integrity Check.

Utilities

Data Integrity Check

Space Freeing Up

Delete Backup Data

Decrypt Backup D...

Data Integrity Check

Perform health check for your backed up data to ensure the data integrity and restorability

Select a backup set

Backup Set 1

Select a destination

AhsayCBS

☐ Run Cyclic Redundancy Check (CRC) during data integrity check

☐ Rebuild index

☐ Delete corrupted data blocks permanently

✓ Data Integrity Check is completed successfully

View log

Close

The detailed log of Data Integrity Check process will be displayed.

Utilities

Data Integrity Check

Log 27/09/2022 14:34

Show All

| Type | Log | Time |
|------|--|---------------------|
| 1 | Start [AhsayOBM v9.4.2.0] | 27/09/2022 14:34:53 |
| 1 | Start data integrity check on backup set "Backup Set 1(1663644856198)", "AhsayCBS(1663644876782)", crc disabled, r... | 27/09/2022 14:34:53 |
| 1 | Start processing data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS" | 27/09/2022 14:34:59 |
| 1 | Download valid index files from backup job "2022-09-21-10-47-36" to "/Users/admin/C:/Users/Administrator/.obm\te... | 27/09/2022 14:35:00 |
| 1 | Vacuuming index | 27/09/2022 14:35:01 |
| 1 | Vacuuming index... Completed | 27/09/2022 14:35:01 |
| 1 | Existing statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Data ar... | 27/09/2022 14:35:01 |
| 1 | Recalculated statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Da... | 27/09/2022 14:35:01 |
| 1 | The statistics of backup set= "Backup Set 1" destination= "AhsayCBS" is incorrect. It is now to update the statistics. | 27/09/2022 14:35:01 |
| 1 | Deleting out of retention period recycled files... | 27/09/2022 14:35:02 |
| 1 | Delete out of retention period recycled files result - Size: 0 B, File Count: 0 | 27/09/2022 14:35:02 |
| 1 | Deleting out of retention period recycled files... Completed | 27/09/2022 14:35:02 |
| 1 | Saving encrypted backup file index to 1663644856198/blocks/2022-09-27-14-34-53 at destination AhsayCBS... | 27/09/2022 14:35:02 |
| 1 | Data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS" is completed | 27/09/2022 14:35:02 |
| 1 | Finished data integrity check on backup set "Backup Set 1(1663644856198)", "AhsayCBS(1663644876782)", crc disable... | 27/09/2022 14:35:02 |
| 1 | Completed data integrity check on backup set "Backup Set 1(1663644856198)", "AhsayCBS(1663644876782)", crc disa... | 27/09/2022 14:35:02 |

Logs per page 50

Page 1 / 1

Close

Close

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

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

Log: 27/09/2022 14:34

Show: All

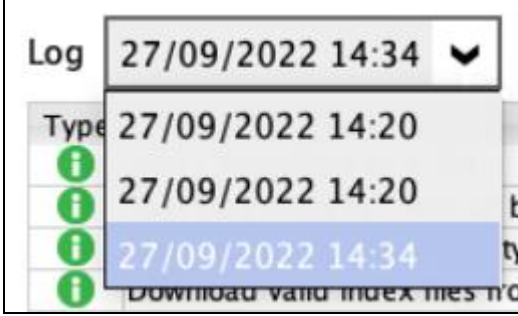
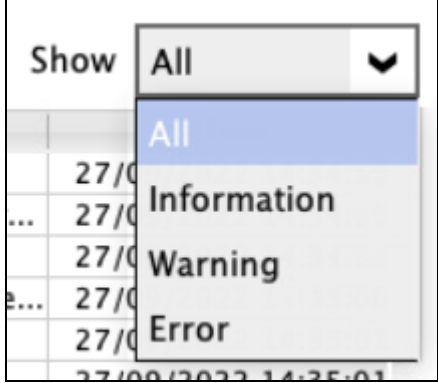
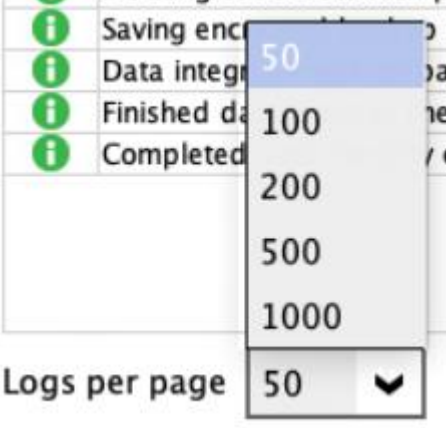
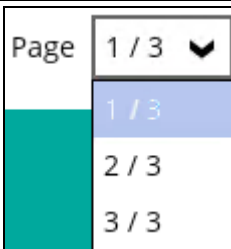
| Type | Log | Time |
|------|--|---------------------|
| 1 | Start [AhsayOBM v9.4.2.0] | 27/09/2022 14:34:53 |
| 1 | Start data integrity check on backup set "Backup Set 1(1663644856198)", "AhsayCBS(1663644876782)", crc disabled, r... | 27/09/2022 14:34:53 |
| 1 | Start processing data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS" | 27/09/2022 14:34:59 |
| 1 | Download valid index files from backup job "2022-09-21-10-47-36" to "/Users/admin/C:/Users/Administrator/.obm\te... | 27/09/2022 14:35:00 |
| 1 | Vacuuming index | 27/09/2022 14:35:01 |
| 1 | Vacuuming index... Completed | 27/09/2022 14:35:01 |
| 1 | Existing statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Data ar... | 27/09/2022 14:35:01 |
| 1 | Recalculated statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Da... | 27/09/2022 14:35:01 |
| 1 | The statistics of backup set= "Backup Set 1" destination= "AhsayCBS" is incorrect. It is now to update the statistics. | 27/09/2022 14:35:01 |
| 1 | Deleting out of retention period recycled files... | 27/09/2022 14:35:02 |
| 1 | Delete out of retention period recycled files result - Size: 0 B, File Count: 0 | 27/09/2022 14:35:02 |
| 1 | Deleting out of retention period recycled files... Completed | 27/09/2022 14:35:02 |
| 1 | Saving encrypted backup file index to 1663644856198/blocks/2022-09-27-14-34-53 at destination AhsayCBS... | 27/09/2022 14:35:02 |
| 1 | Data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS" is completed | 27/09/2022 14:35:02 |
| 1 | Finished data integrity check on backup set "Backup Set 1(1663644856198)", "AhsayCBS(1663644876782)", crc disable... | 27/09/2022 14:35:02 |
| 1 | Completed data integrity check on backup set "Backup Set 1(1663644856198)", "AhsayCBS(1663644876782)", crc disa... | 27/09/2022 14:35:02 |

Logs per page: 50

Page: 1 / 1

Close

Close

| Option | Screenshot | Function |
|---------------|--|--|
| Log Filter |  | This option is used to display the available logs of the Data Integrity Check jobs. |
| Show filter |  | This option is used to sort the Data Integrity Check log by its status (i.e., All, Information, Warning, and Error). |
| Logs per page |  | This option allows user to choose the displayed number of logs per page. |
| Page |  | This option allows user to navigate the logs to the next page(s). |

Data Integrity Check Completed with Errors

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

The screenshot shows the 'Data Integrity Check' utility window. On the left is a sidebar with 'Utilities' and a list of actions: 'Data Integrity Check' (highlighted), 'Space Freeing Up', 'Delete Backup Data', and 'Decrypt Backup D...'. The main area is titled 'Data Integrity Check' and contains the following options:

- Perform health check for your backed up data to ensure the data integrity and restorability
- Select a backup set: Backup Set 5
- Select a destination: All
- ☐ Run Cyclic Redundancy Check (CRC) during data integrity check
- ☐ Rebuild index
- ☐ Delete corrupted data blocks permanently
- ☒ Data Integrity Check is completed with error(s)
- [View log](#)

A 'Close' button is located at the bottom right of the window.

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

The screenshot shows the log details for the Data Integrity Check. At the top, there is a 'Log' dropdown set to '27/09/2022 14:20' and a 'Show' dropdown set to 'All'. Below this is a table with the following data:

| Type | Log | Time |
|---|-----|---------------------|
| Start [AhsayOBM v9.4.2.0] | | 27/09/2022 14:20:46 |
| Start data integrity check on backup set "Backup Set 5(1664259338415)" all destination, crc disabled, rebuild index disa... | | 27/09/2022 14:20:46 |
| Skipped Backup Set = "Backup Set 5". Reason = "Scheduled backup set "Backup Set 5" is still running." | | 27/09/2022 14:20:52 |
| Finished data integrity check with error on backup set "Backup Set 5(1664259338415)" all destination, crc disabled, rebu... | | 27/09/2022 14:20:52 |
| Completed data integrity check on backup set "Backup Set 5(1664259338415)" all destination, crc disabled, rebuild inde... | | 27/09/2022 14:20:52 |

At the bottom, there is a 'Logs per page' dropdown set to '50' and a 'Page' dropdown set to '1 / 1'. A 'Close' button is located at the bottom right of the window.

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.

The screenshot displays the 'Data Integrity Check' log window. At the top, there's a 'Log' dropdown set to '27/09/2022 14:34' and a 'Show' dropdown set to 'All'. Below this is a table with columns 'Type', 'Log', and 'Time'. The log entries show a successful check process, including starting the check, downloading index files, vacuuming the index, and recalculating statistics. The final entry states 'Completed data integrity check on backup set "Backup Set 1(1663644856198)", "AhsayCBS(1663644876782)", crc disable...'. At the bottom, there are 'Logs per page' (set to 50) and 'Page' (1 / 1) indicators, along with 'Close' buttons.

| Type | Log | Time |
|--|-----|---------------------|
| Start [AhsayOBM v9.4.2.0] | | 27/09/2022 14:34:53 |
| Start data integrity check on backup set= "Backup Set 1(1663644856198)", "AhsayCBS(1663644876782)", crc disabled, r... | | 27/09/2022 14:34:53 |
| Start processing data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS" | | 27/09/2022 14:34:59 |
| Download valid index files from backup job "2022-09-21-10-47-36" to "/Users/admin/C:/Users/Administrator/.obm\te... | | 27/09/2022 14:35:00 |
| Vacuuming index | | 27/09/2022 14:35:01 |
| Vacuuming index... Completed | | 27/09/2022 14:35:01 |
| Existing statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Data ar... | | 27/09/2022 14:35:01 |
| Recalculated statistics of backup set= "Backup Set 1" destination= "AhsayCBS": Data area compressed size: 15.64 MB, Da... | | 27/09/2022 14:35:01 |
| The statistics of backup set= "Backup Set 1" destination= "AhsayCBS" is incorrect. It is now to update the statistics. | | 27/09/2022 14:35:01 |
| Deleting out of retention period recycled files... | | 27/09/2022 14:35:02 |
| Delete out of retention period recycled files result - Size: 0 B, File Count: 0 | | 27/09/2022 14:35:02 |
| Deleting out of retention period recycled files... Completed | | 27/09/2022 14:35:02 |
| Saving encrypted backup file index to 1663644856198/blocks/2022-09-27-14-34-53 at destination AhsayCBS... | | 27/09/2022 14:35:02 |
| Data integrity check on backup set= "Backup Set 1" destination= "AhsayCBS" is completed | | 27/09/2022 14:35:02 |
| Finished data integrity check on backup set "Backup Set 1(1663644856198)", "AhsayCBS(1663644876782)", crc disable... | | 27/09/2022 14:35:02 |
| Completed data integrity check on backup set "Backup Set 1(1663644856198)", "AhsayCBS(1663644876782)", crc disa... | | 27/09/2022 14:35:02 |

If any index-related error(s) or data corrupted item(s) is found, the **(TEST MODE)** confirmation screen will be displayed.

The screenshot shows the 'Data Integrity Check' window in 'TEST MODE'. It features a yellow warning icon and a message: 'The result of data integrity check (TEST MODE) is as follow. No actions are performed yet. Data corrupted items, checksum incorrect items and index broken data blocks will be deleted. Are you sure you want to continue?'. Below this, it specifies 'Backup set: Sample Backup Set 01'. A table displays the results of the check:

| Destination | Items found in index | Data corrupted items | Index broken data blocks | Statistics |
|-------------|----------------------|----------------------|--------------------------|------------|
| AhsayCBS | 368 (130.4MB) | 181 (111.3MB) | 23 (490.1MB) | Incorrect |

* File count (File size)

At the bottom, there are 'Yes', 'No', and 'View log' buttons, along with a 'Close' button.

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)



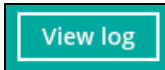
Test Mode Confirmation

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

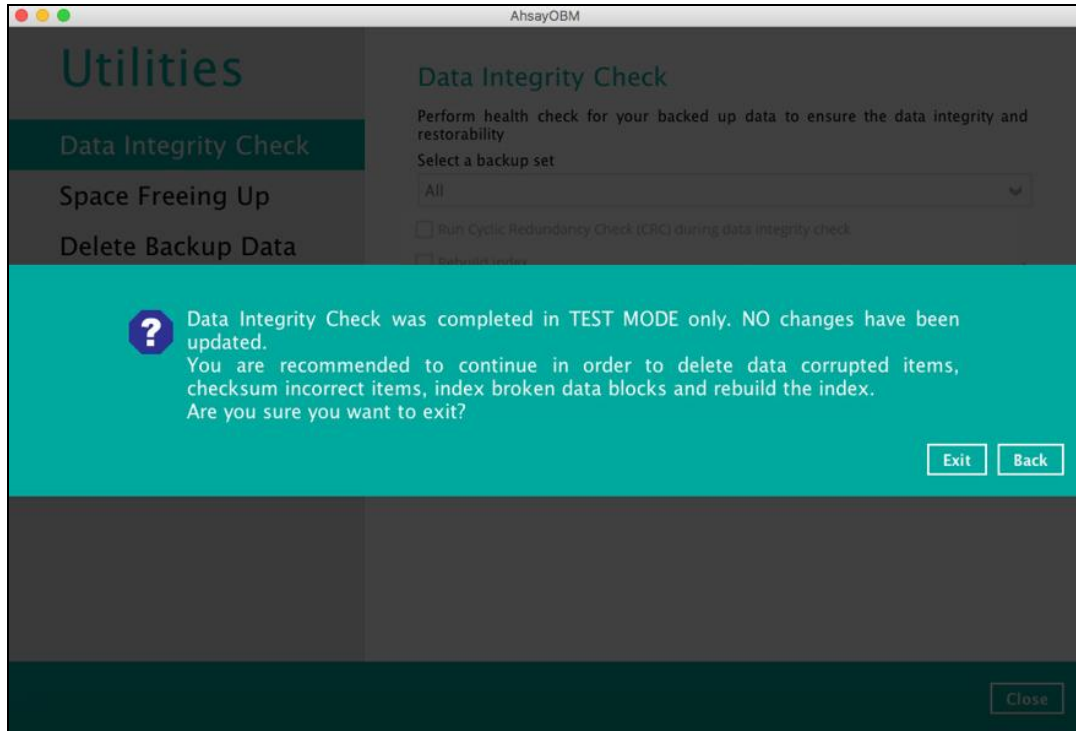
- deleted number of backup files is over 1,000
- deleted number of backup file size is over 512 MB (in total)
- deleted number of backup files is over 10% of the total backup files

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

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

| Option | Screenshot | Function |
|-----------------|---|---|
| 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.

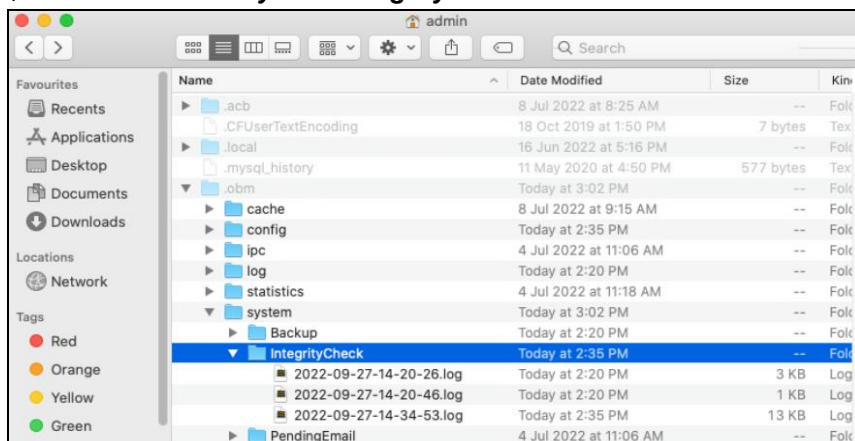
If the **Back** button is clicked, it will go back to the (TEST MODE) confirmation screen.

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/.obm/system/IntegrityCheck

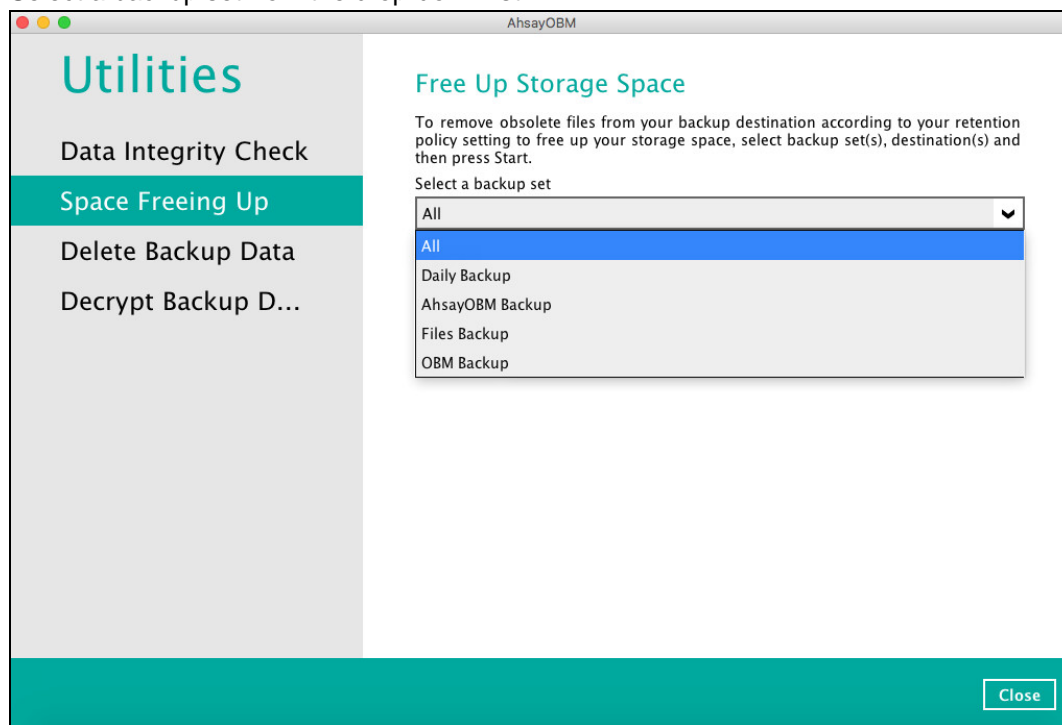


9.9.2 Space Freeing Up

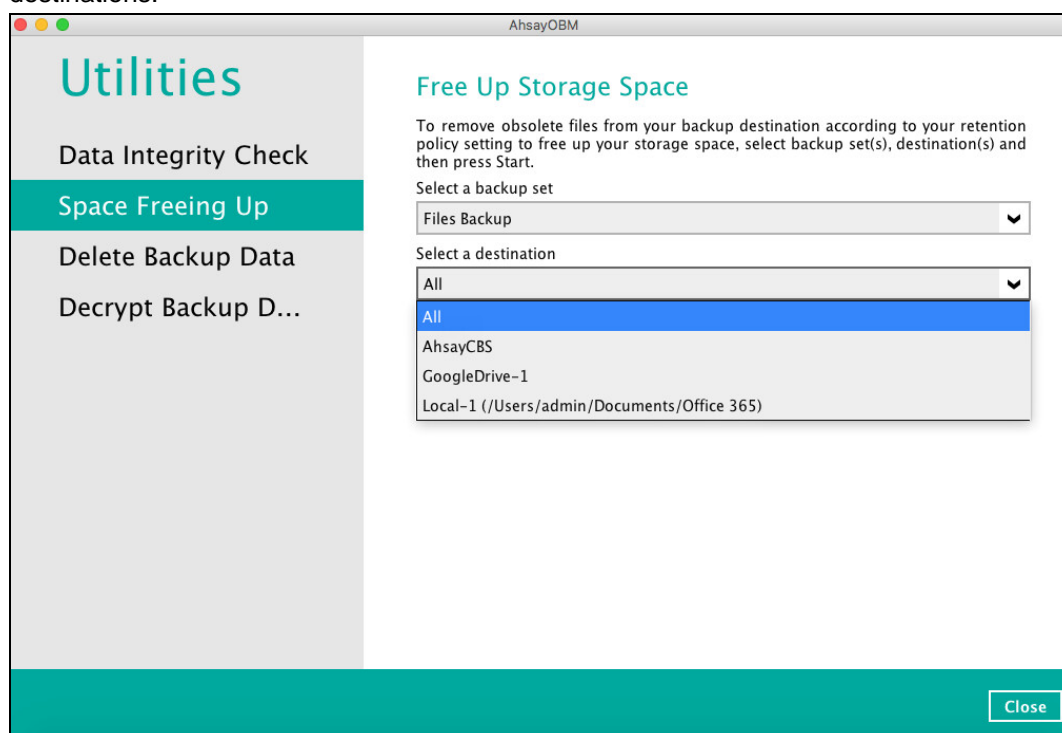
This feature is used to remove obsolete file(s) from your backup set and destination (manually start Retention Policy). After the Space Freeing Up job is completed, the storage statistics of the backup set(s) are updated.

To perform Space Freeing Up, follow the instructions below:

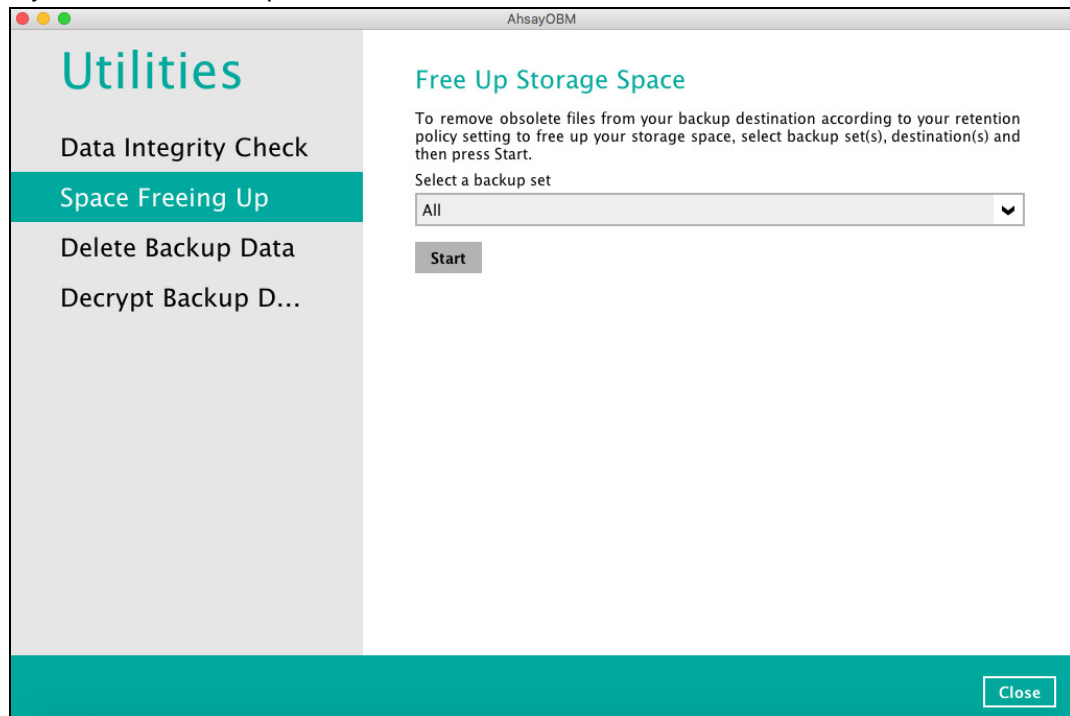
1. Select a backup set from the drop-down list.



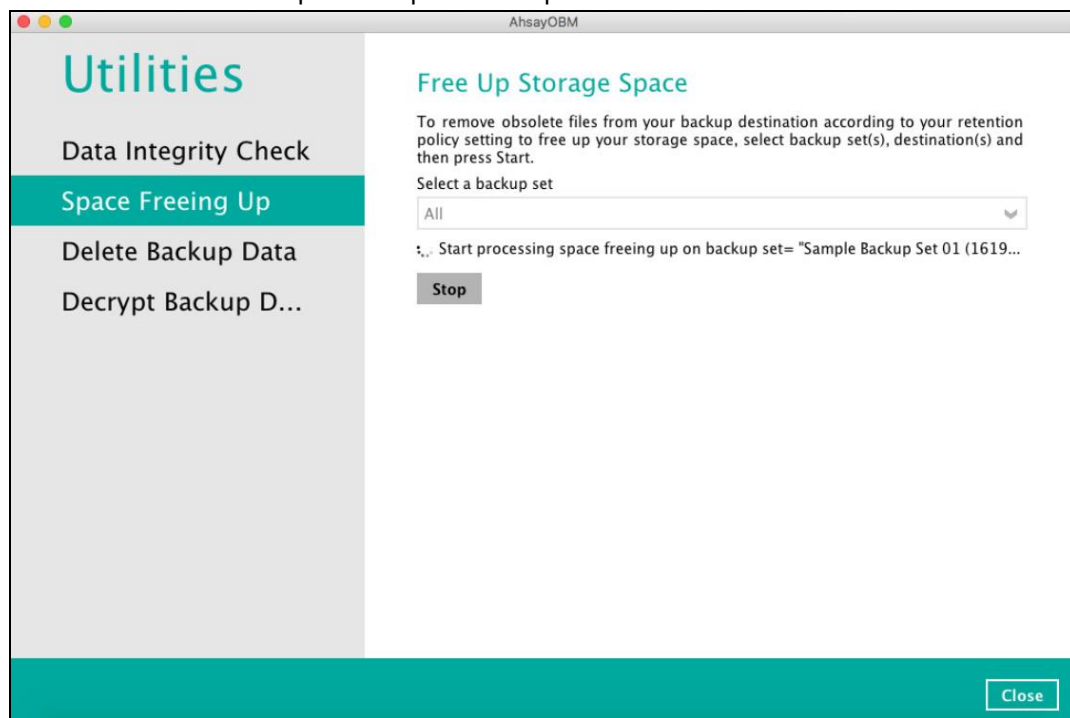
If you select a specific backup set, then you will also have to select a specific destination or all destinations.



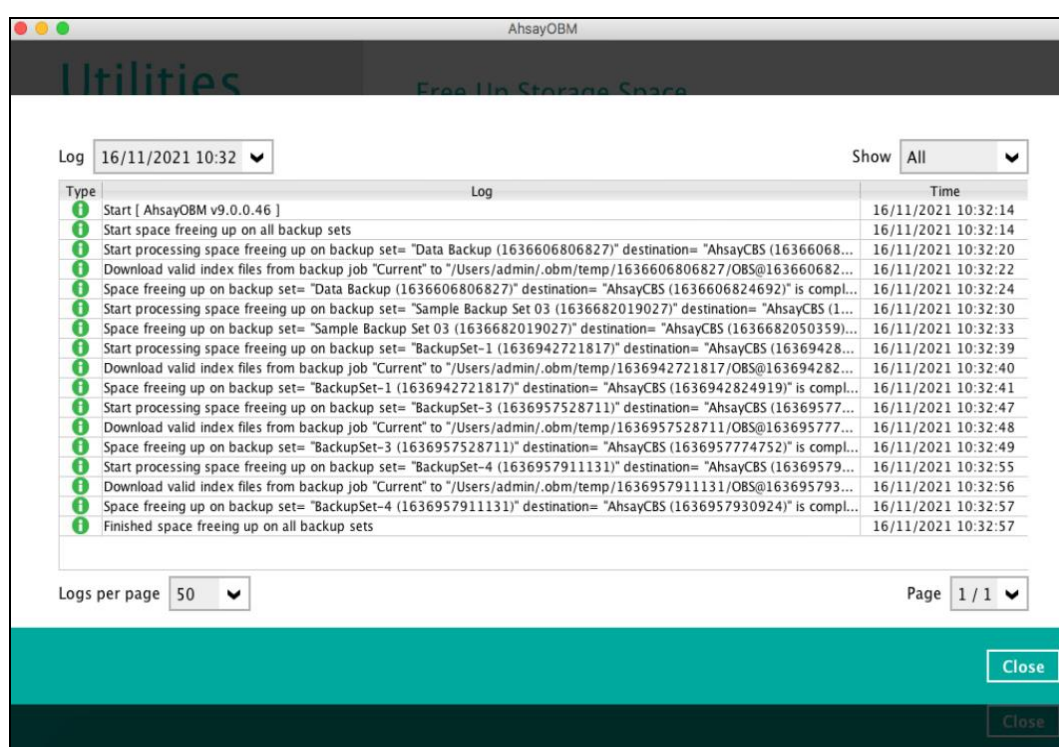
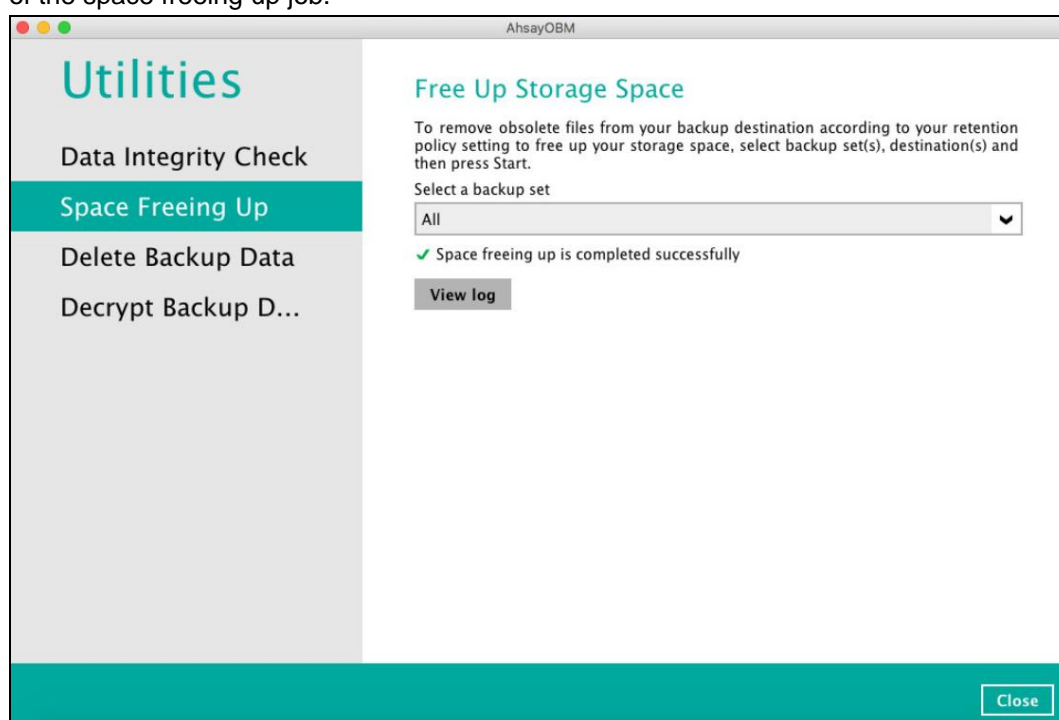
If you select All backup sets, then there is no need to select a destination.



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.

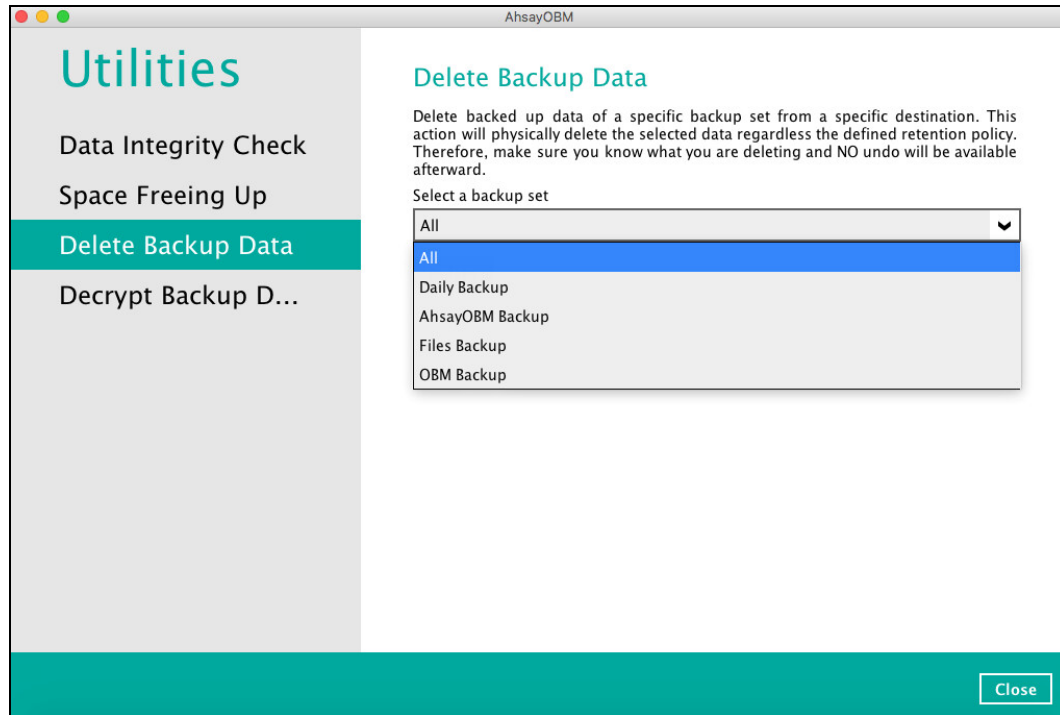


9.9.3 Delete Backup Data

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:

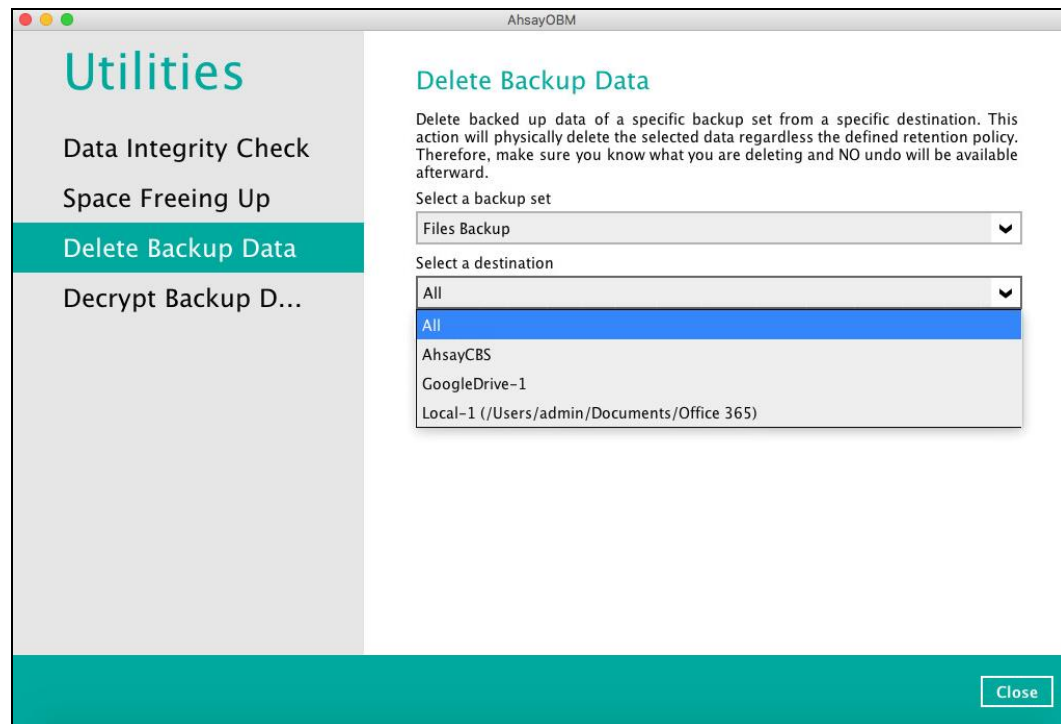
1. Select a backup set from the drop-down list.



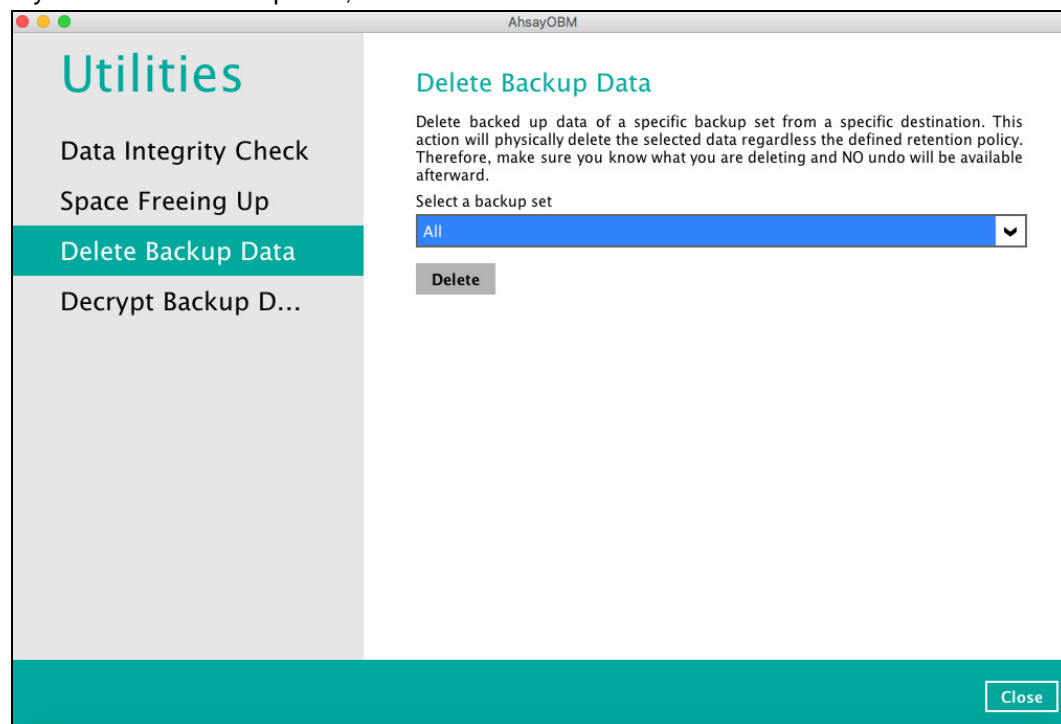
NOTE

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

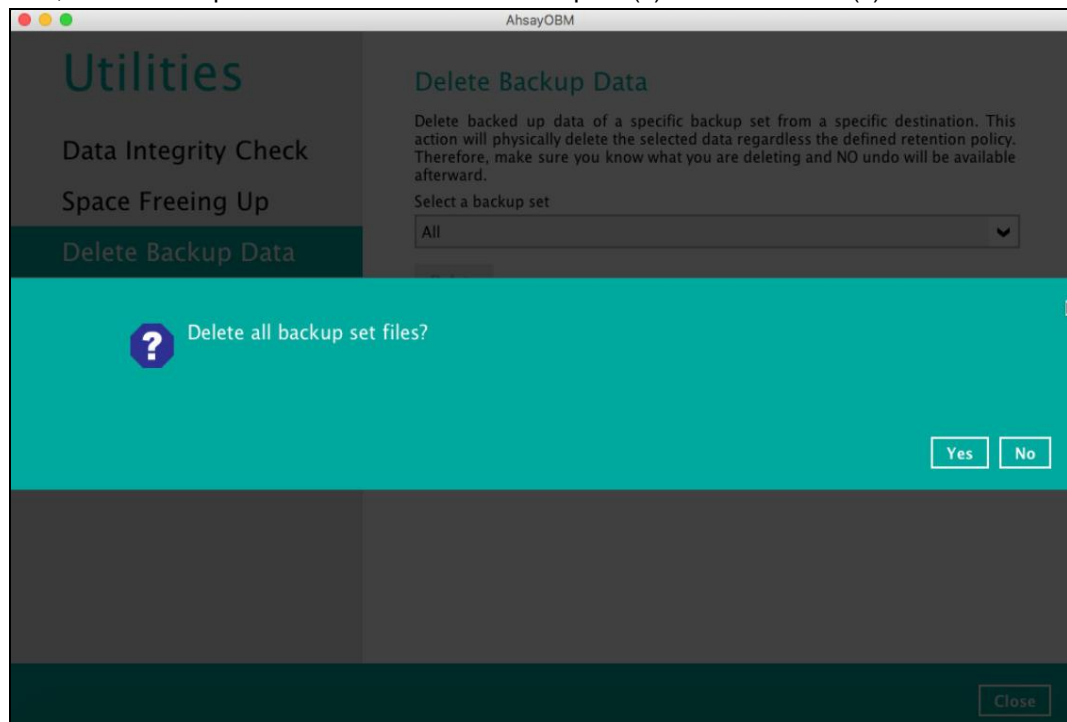
If you select a specific backup set, then you will also have to select a specific destination or all destinations.



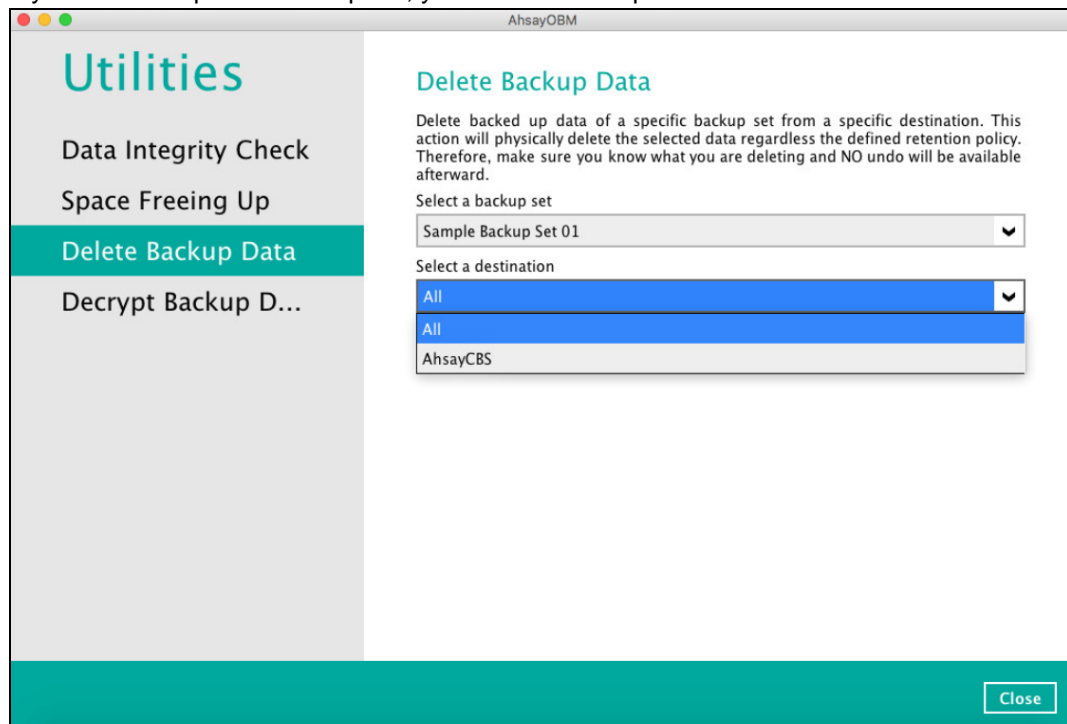
If you select **All** backup sets, then there is no need to select a destination.



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.

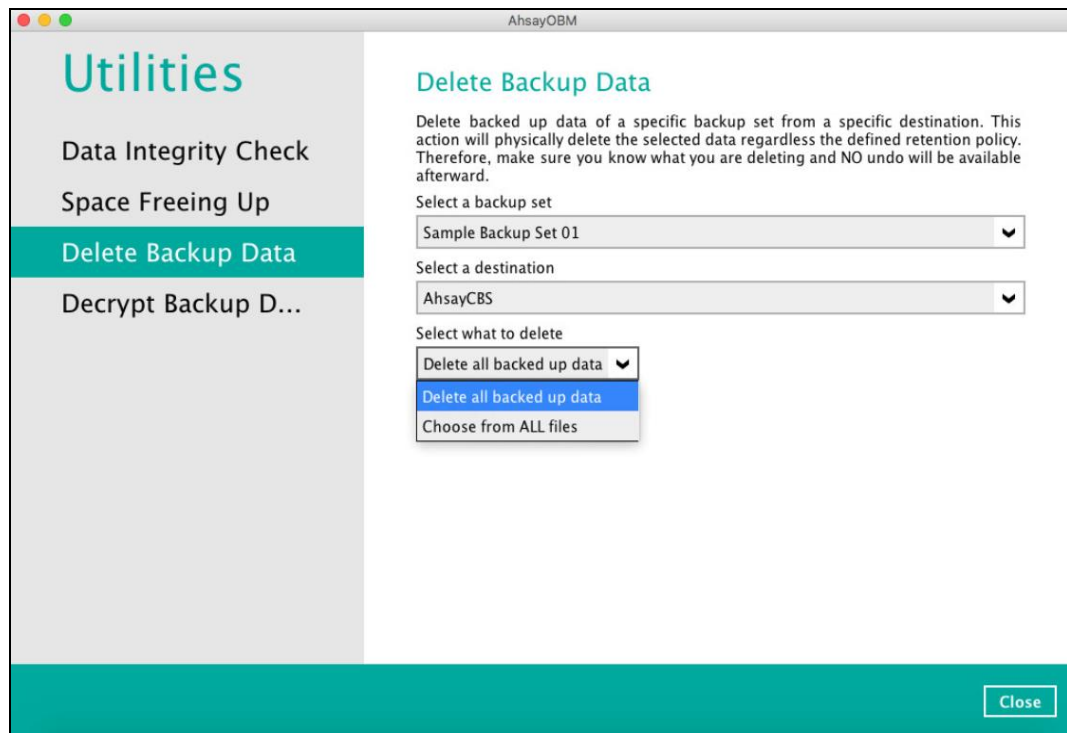


If you select a specific backup set, you will have an option to choose a destination.



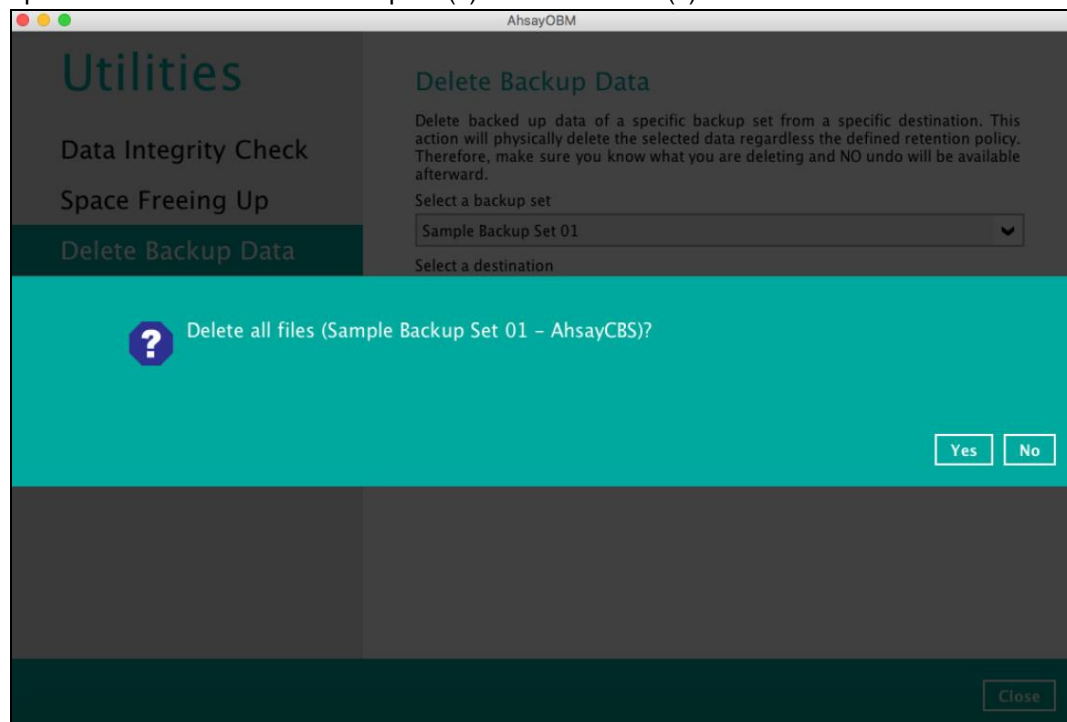
If you select a specific destination, there are two (2) available options for the type of files you wish to delete.

- Delete all backed up data
- Choose from ALL files



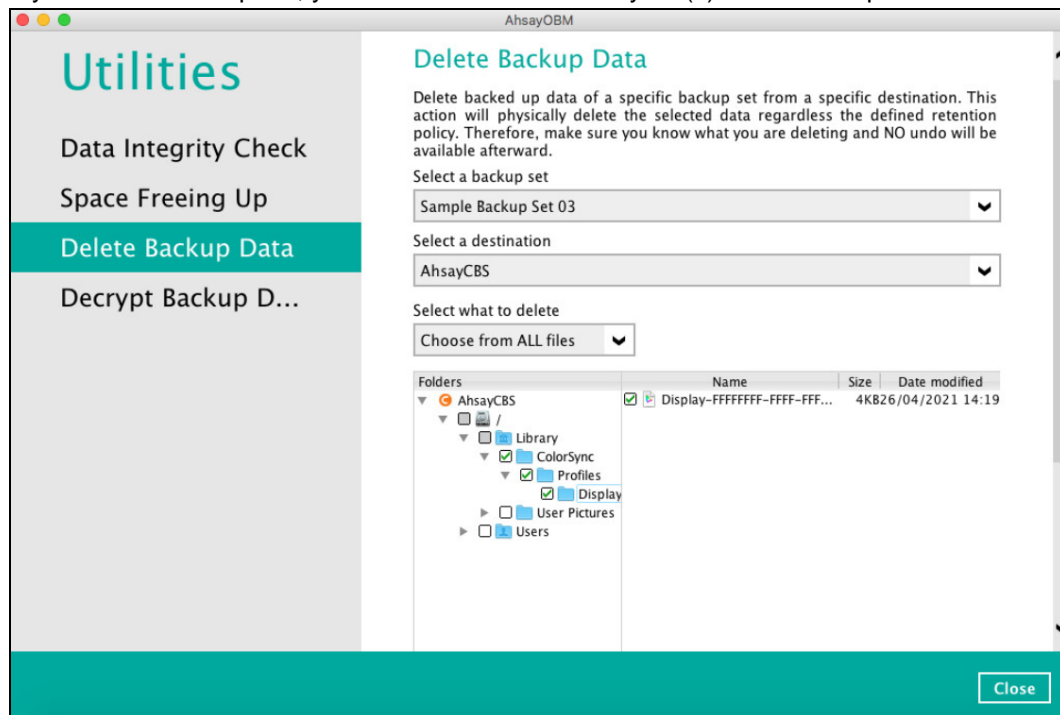
Delete all backed up data

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.

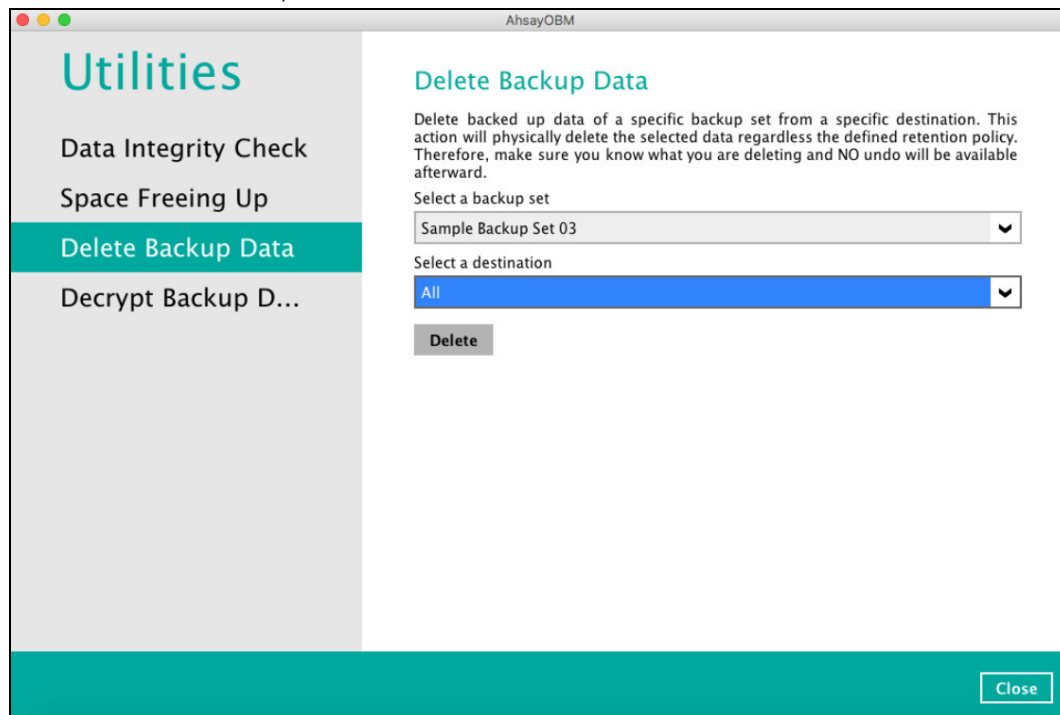


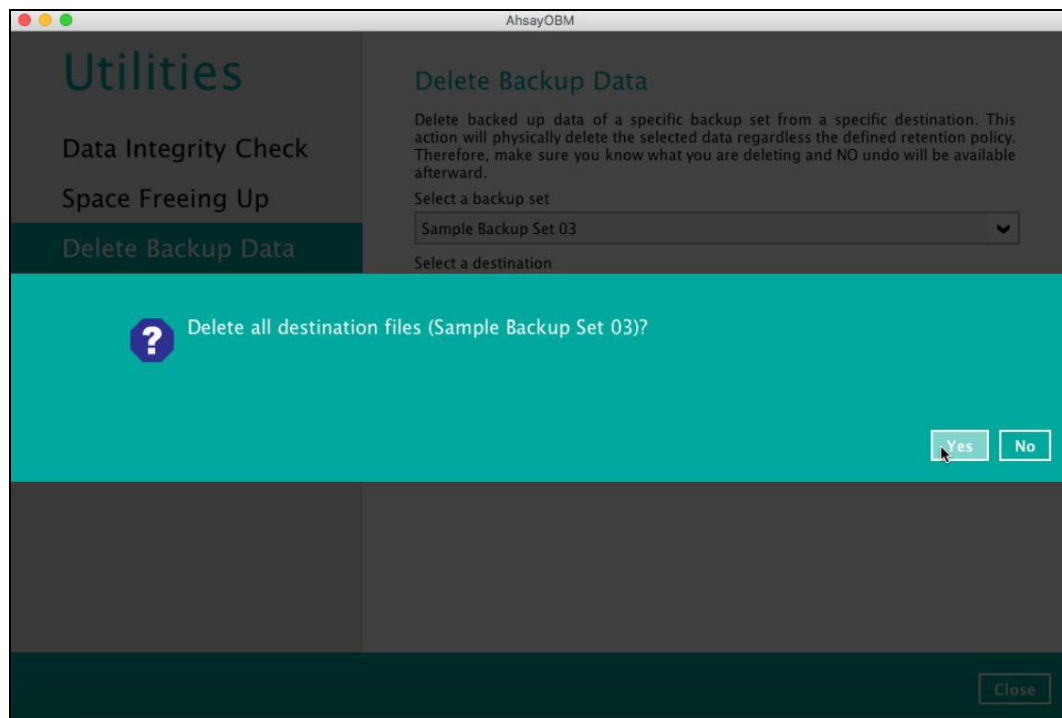
Choose from ALL files

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

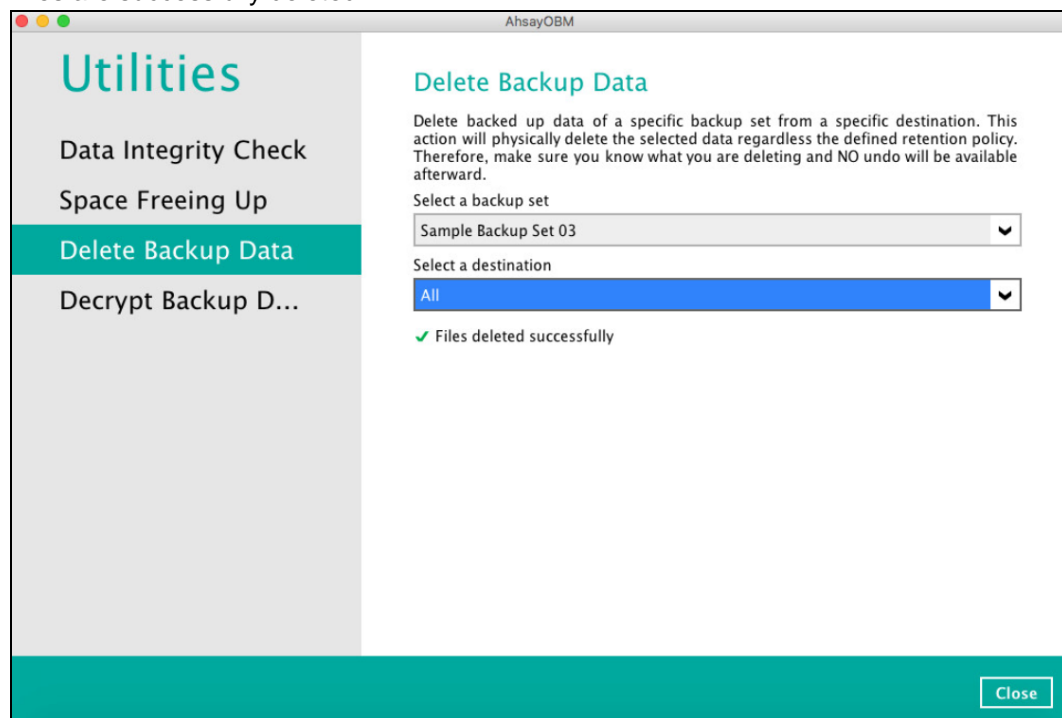


3. Click the **Delete** button, then click **Yes** to start the deletion of files.





4. Files are successfully deleted.

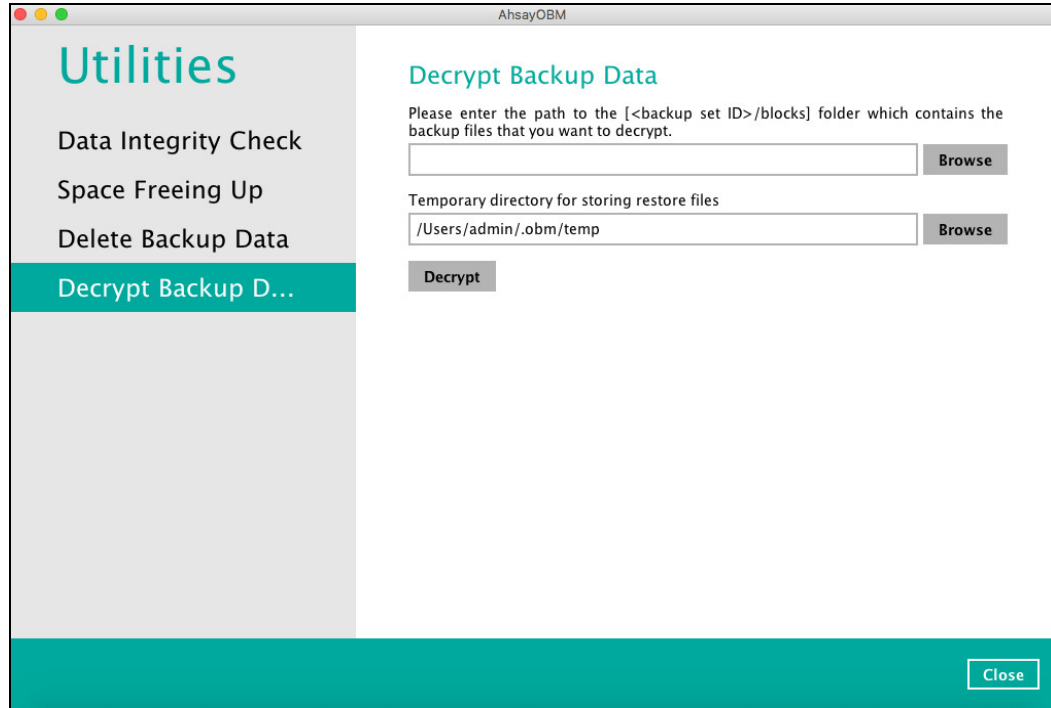


9.9.4 Decrypt Backup Data

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

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

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



AhsayOBM

Utilities

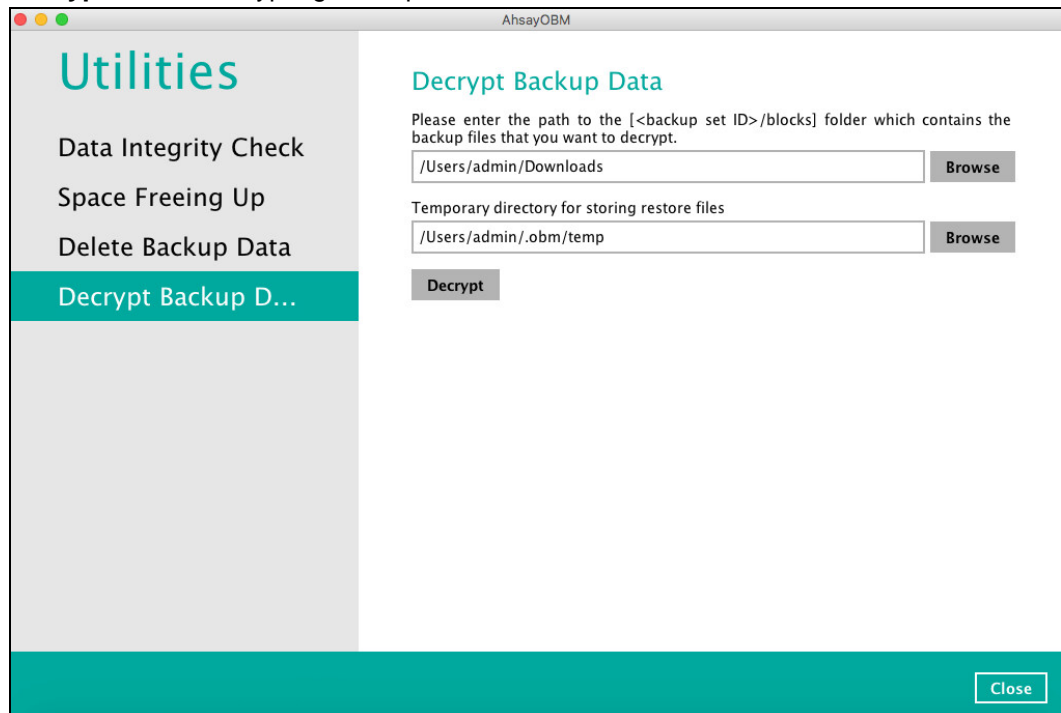
- Data Integrity Check
- Space Freeing Up
- Delete Backup Data
- Decrypt Backup D...**

Decrypt Backup Data

Please enter the path to the [<backup set ID>/blocks] folder which contains the backup files that you want to decrypt.

Temporary directory for storing restore files

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



AhsayOBM

Utilities

- Data Integrity Check
- Space Freeing Up
- Delete Backup Data
- Decrypt Backup D...**

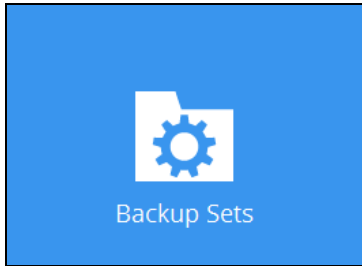
Decrypt Backup Data

Please enter the path to the [<backup set ID>/blocks] folder which contains the backup files that you want to decrypt.

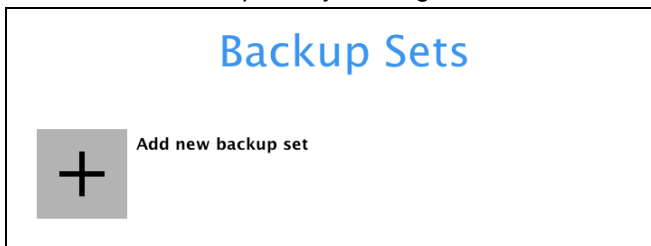
Temporary directory for storing restore files

10 Create a Backup Set

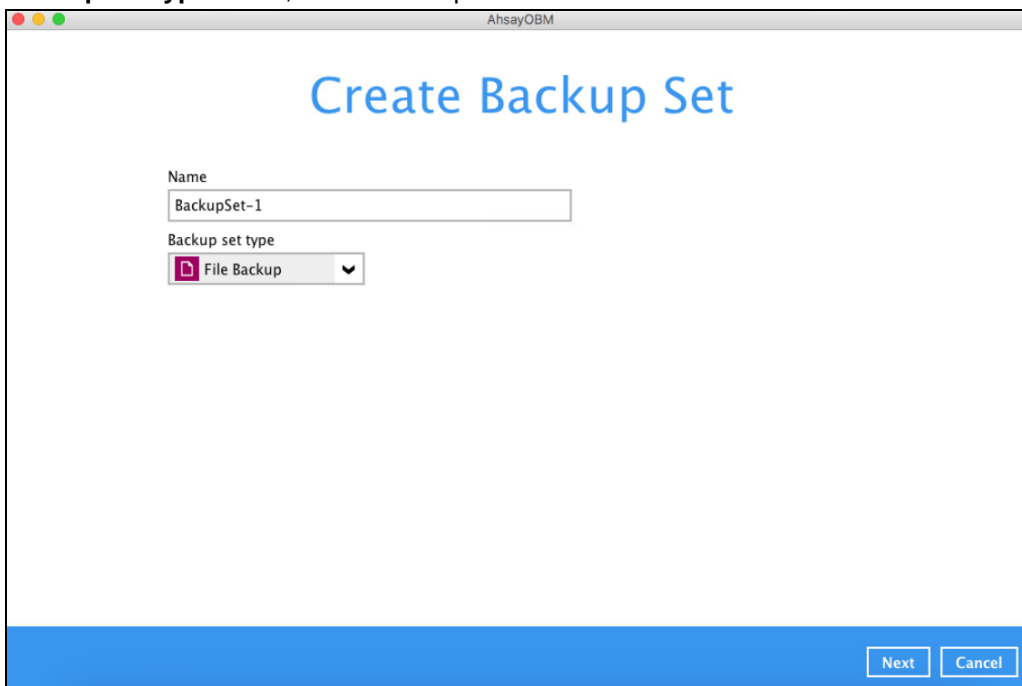
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.



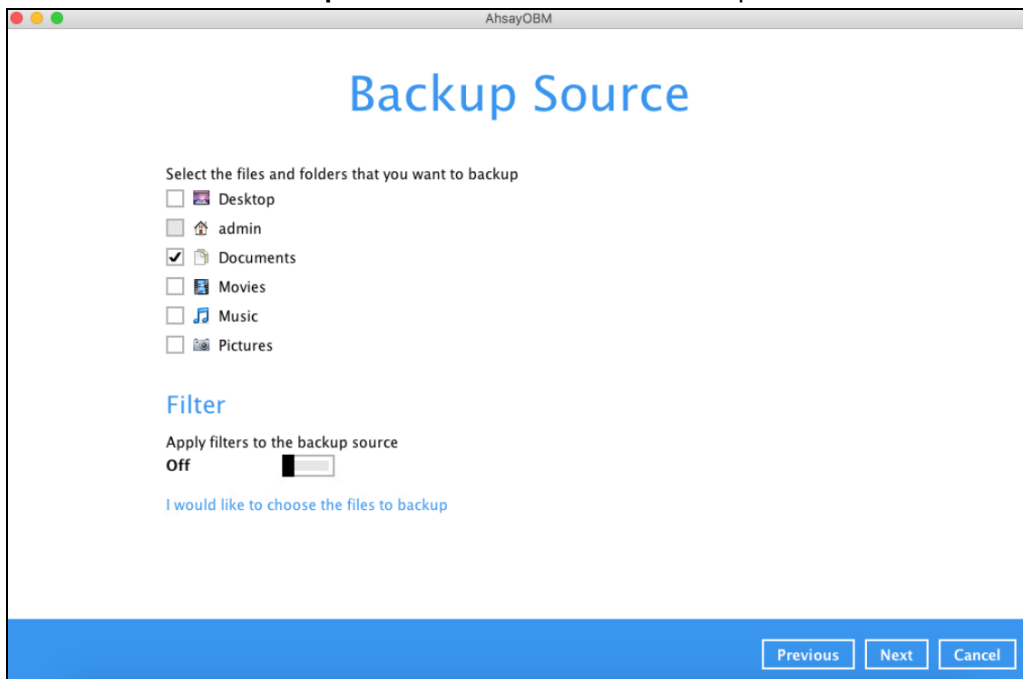
2. Create a new backup set by clicking  next to **Add new backup set**.



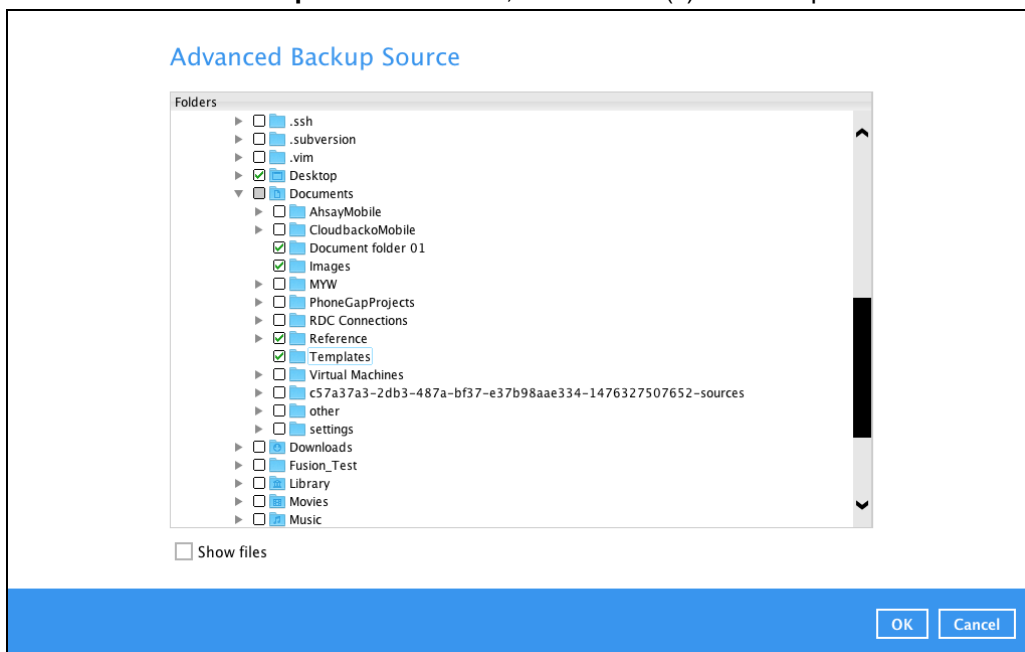
3. When the Create Backup Set window appears, name your new backup set, and select the **Backup set type**. Then, click **Next** to proceed.



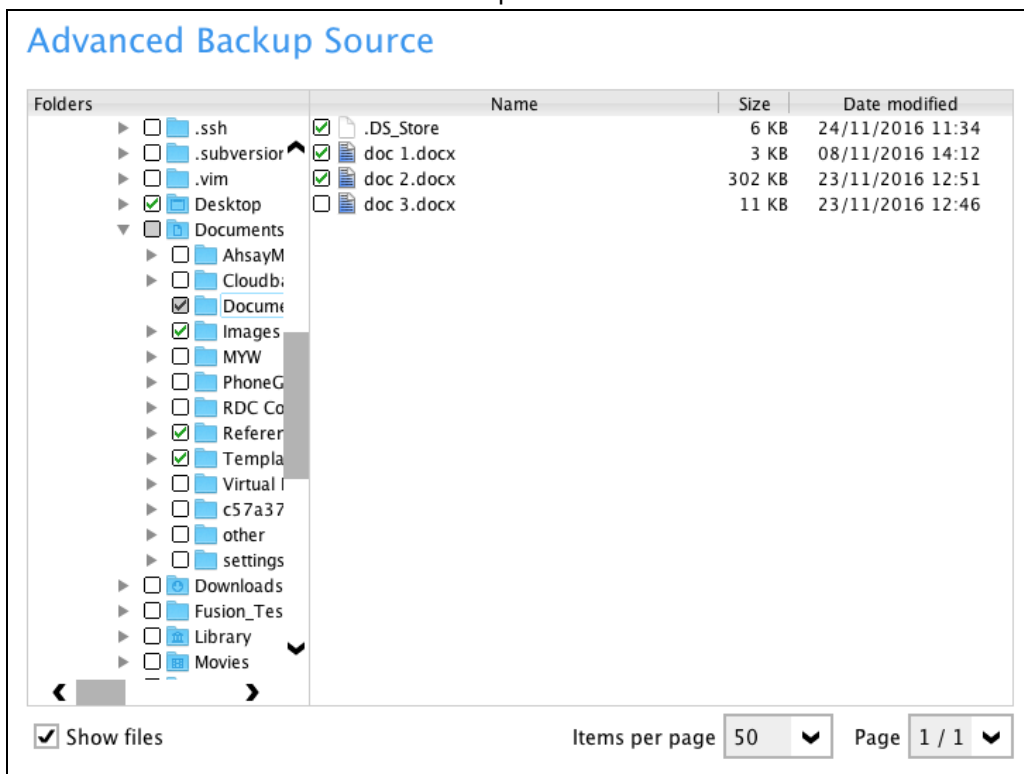
4. In the Backup Source window, select the source files and folders for backup. Click **I would like to choose the files to backup** to select individual files for backup.



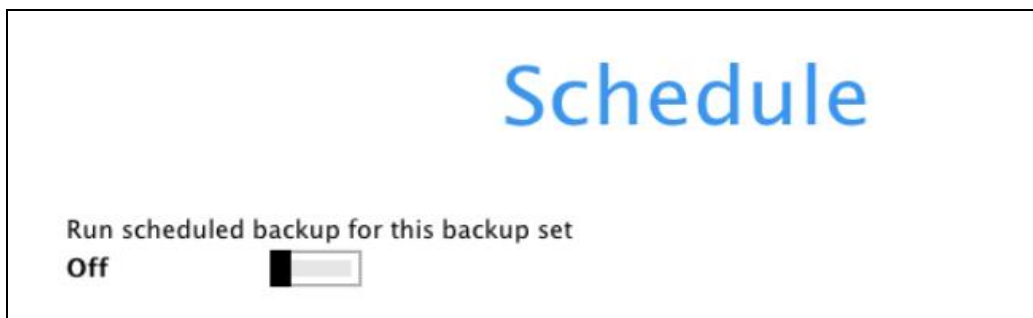
5. In the **Advanced Backup Source** window, select folder(s) to back up all files in the folder(s).




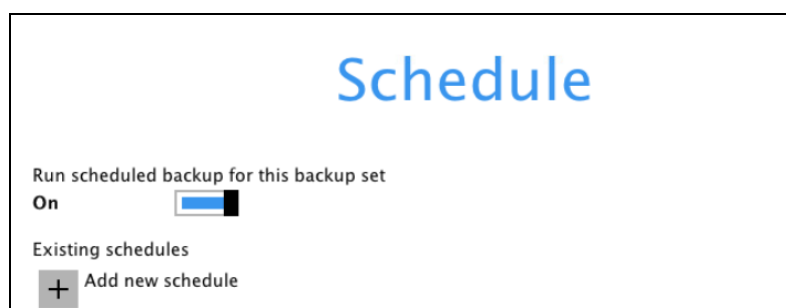
6. Alternatively, if you want to back up only specific files instead of all files in your selected folder(s), select the **Show files** checkbox at the bottom of the screen. A list of files will appear on the right-hand side. Select the checkbox(es) next to the file(s) to back up. Then, click **OK**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



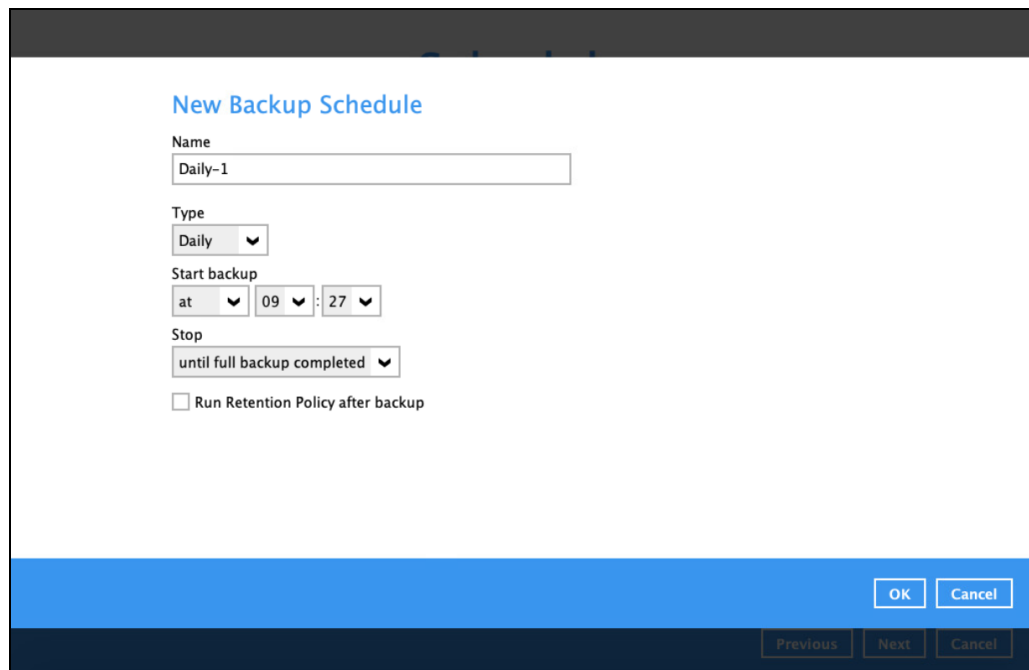
7. In the Backup Source window, click **Next** to proceed.
8. In the Schedule window, you can configure a backup schedule to automatically run a backup job at your specified time interval. In the Schedule window, the Run scheduled backup for this backup set is **Off** by default.



- 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.



New Backup Schedule

Name
Daily-1

Type
Daily

Start backup
at 09 : 27

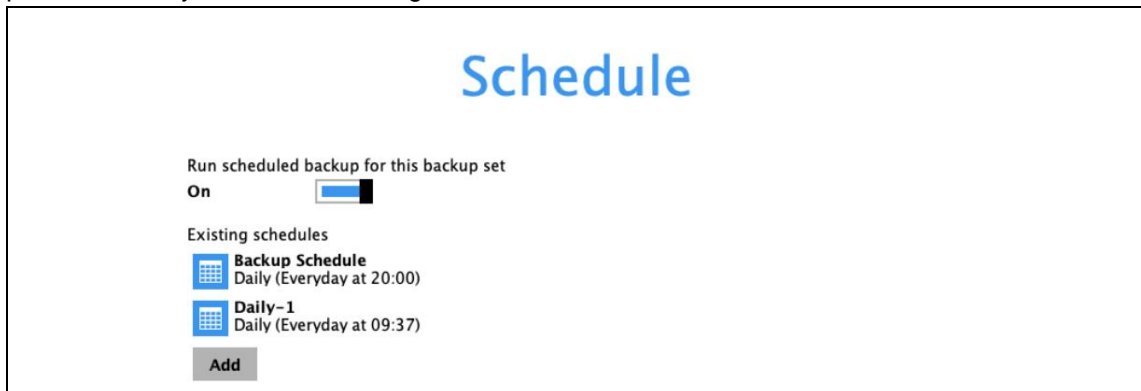
Stop
until full backup completed

☐ Run Retention Policy after backup

OK Cancel

Previous Next Cancel


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.




Schedule

Run scheduled backup for this backup set
On

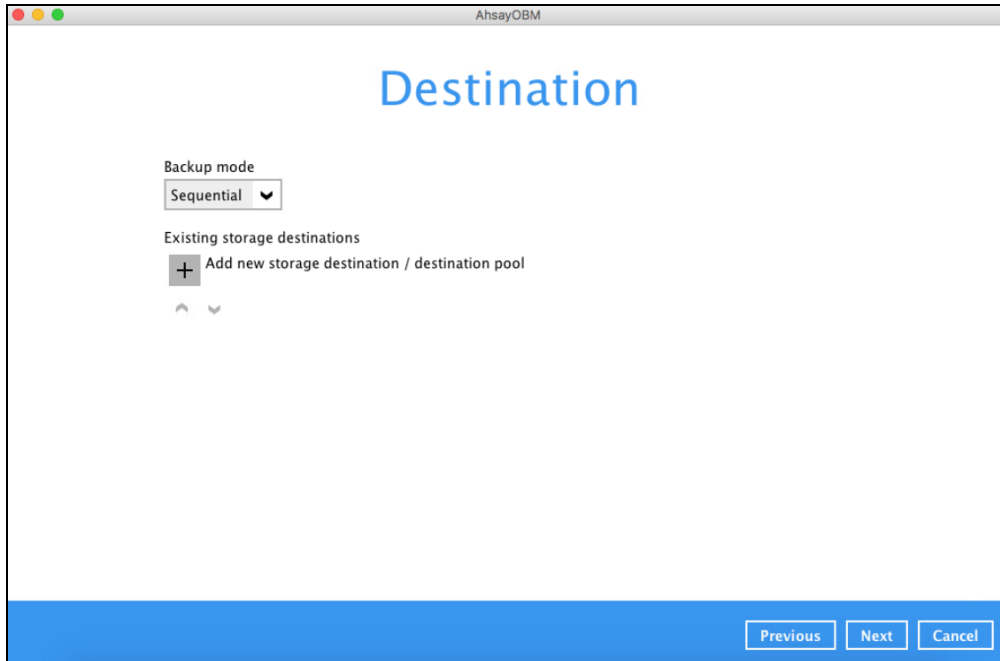
Existing schedules

 **Backup Schedule**
Daily (Everyday at 20:00)

 **Daily-1**
Daily (Everyday at 09:37)


Add

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

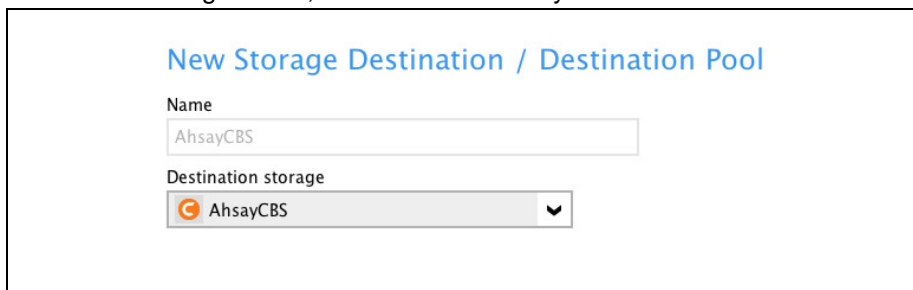


Select the appropriate option from the **Backup mode** dropdown menu.

- **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.

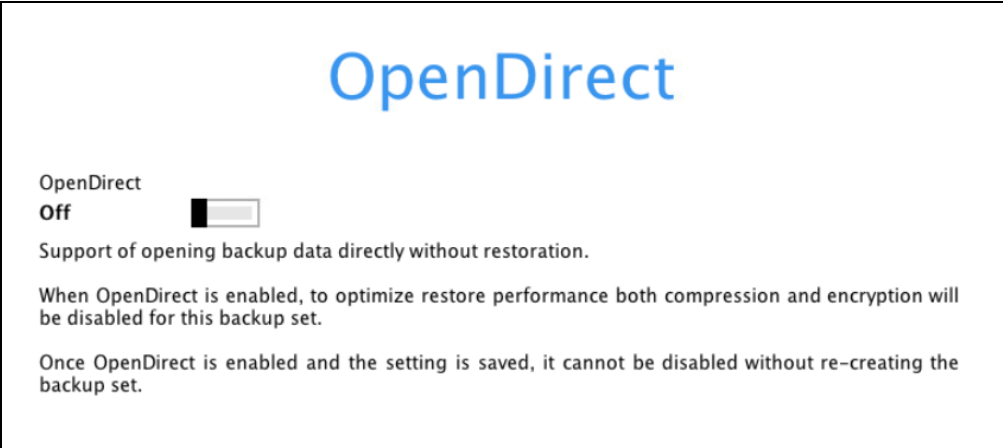


12. In the Destination window, your selected storage destination will be shown. Click **Next** to proceed.




The screenshot shows the 'Destination' window. At the top, the title 'Destination' is displayed in a large blue font. Below the title, there is a 'Backup mode' section with a dropdown menu currently set to 'Sequential'. Underneath, the 'Existing storage destinations' section lists one destination: 'AhsayCBS' with the host '10.3.121.17:80'. Below this list is a grey 'Add' button and two small navigation arrows (up and down) at the bottom left.

13. Keep the **OpenDirect** feature disabled as this feature is not supported on macOS platform. Click **Next** to proceed.



The screenshot shows the 'OpenDirect' window. The title 'OpenDirect' is at the top in a large blue font. Below the title, the 'OpenDirect' feature is shown as 'Off' with a toggle switch. A descriptive text states: '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.'

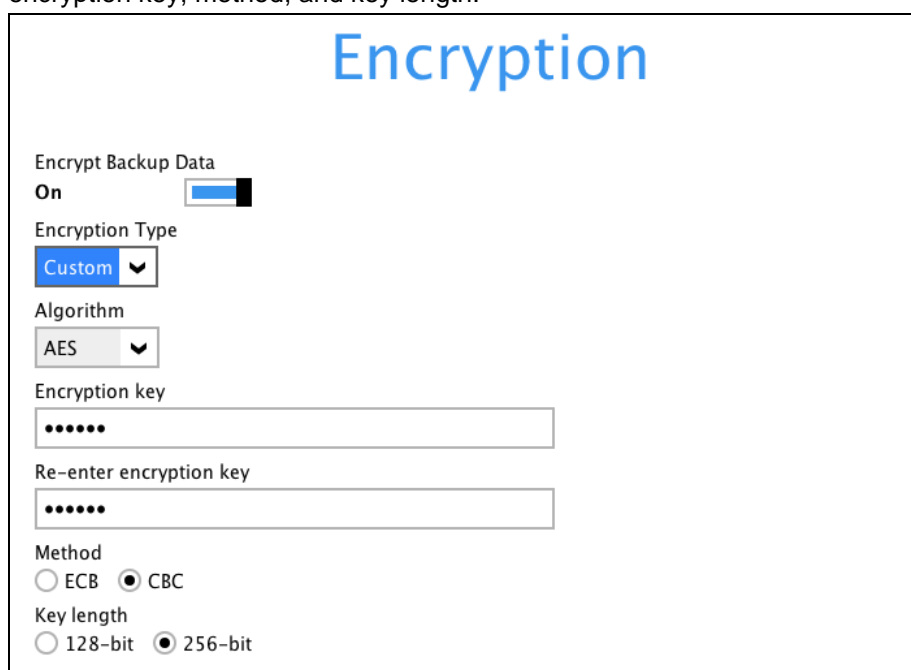
14. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



The screenshot shows the 'Encryption' window. The title 'Encryption' is at the top in a large blue font. Below the title, the 'Encrypt Backup Data' option is shown as 'On' with a toggle switch. Underneath, the 'Encryption Type' dropdown menu is open, showing four options: 'Default' (selected), 'Default', 'User password', and 'Custom'.

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

- **Default** – an encryption key with 44 alphanumeric 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.

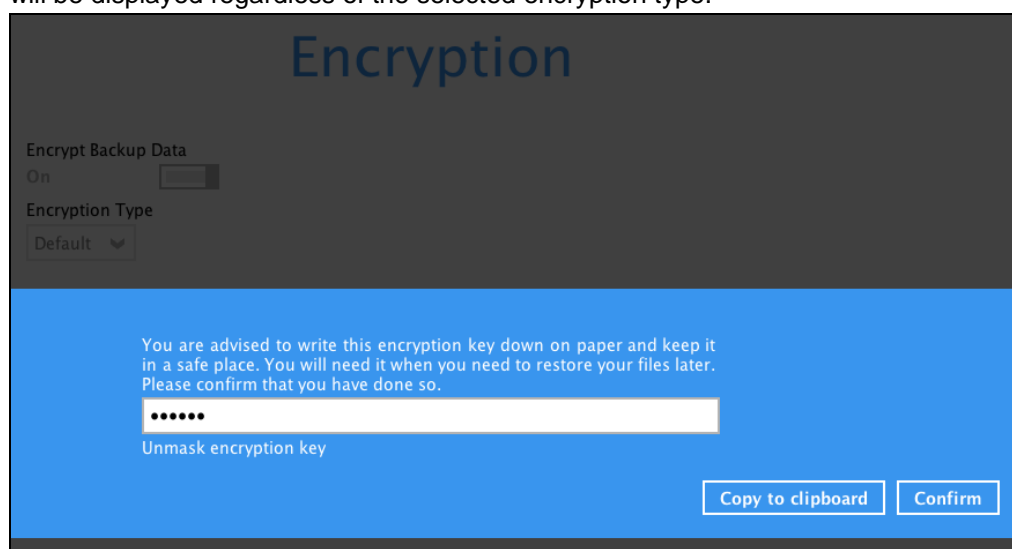


NOTE: For best practice on managing your encryption key, refer to the following KB article.

[FAQ: Best practices for managing encryption key on AhsayOBM or AhsayACB](#)

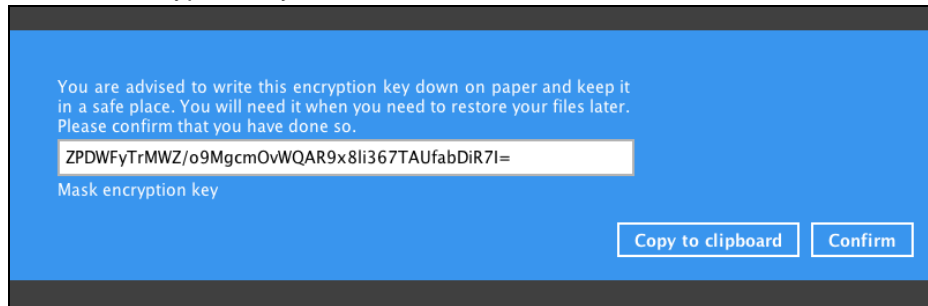
Click **Next** when you are done with the settings.

15. If you have enabled the Encryption Key feature in the previous step, the following pop-up window will be displayed regardless of the selected encryption type.



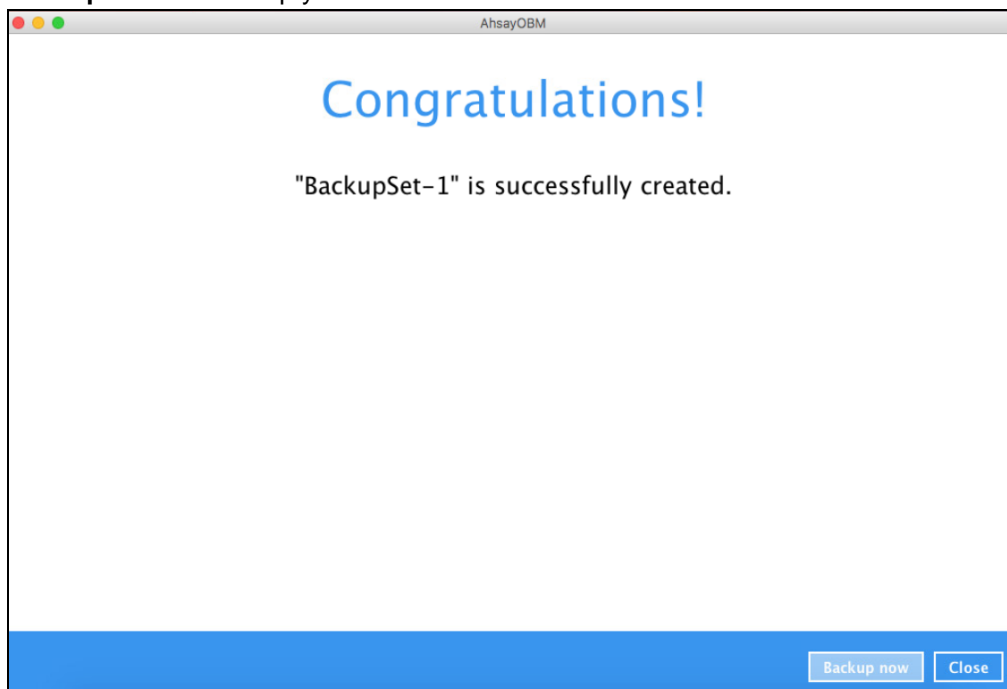
The pop-up window has the following three options to choose from:

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



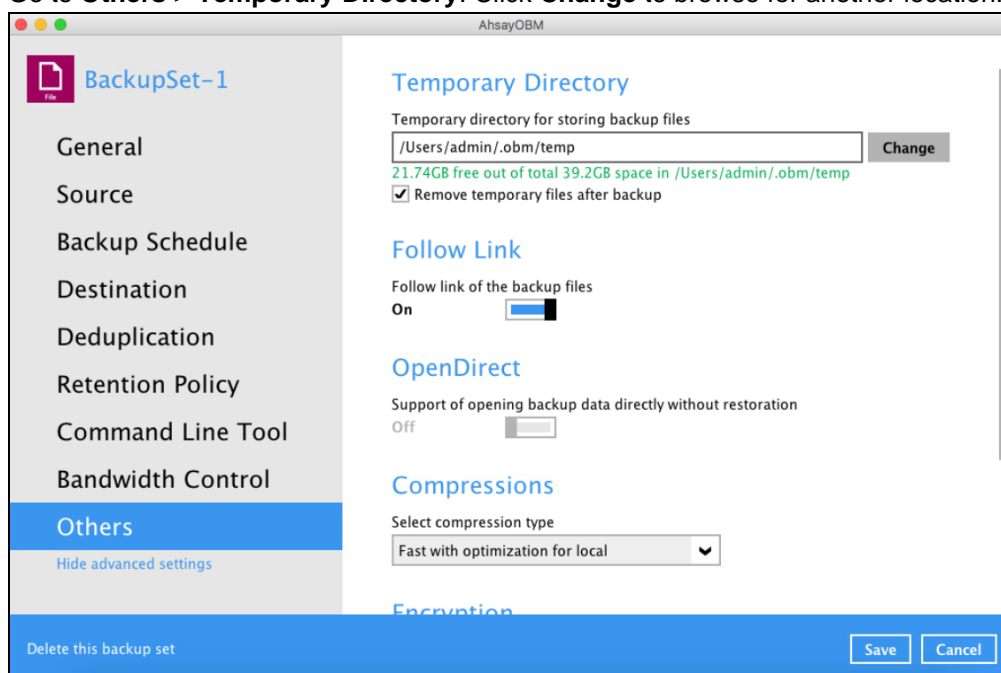
- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

16. 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.



17. It is highly recommended to change the Temporary Directory and select another location with sufficient free disk space other than /Users/admin/.obm/temp.

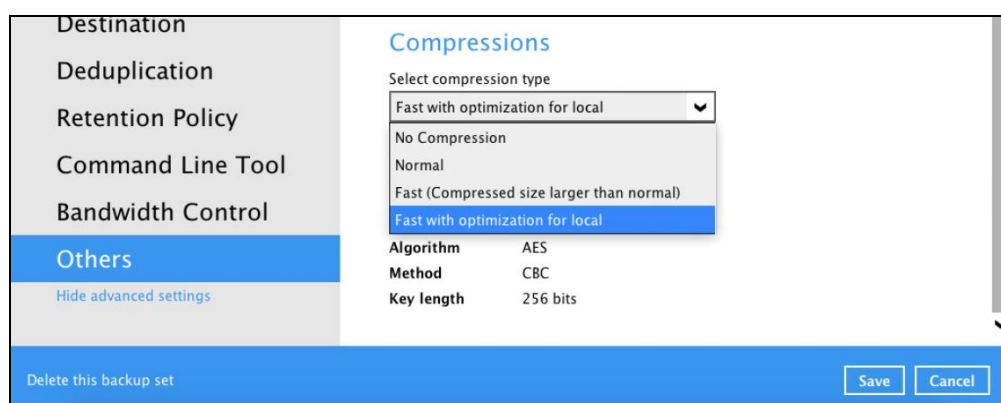
Go to **Others > Temporary Directory**. Click **Change** to browse for another location.



18. Optional: Select your preferred **Compression** type. For newly created backup set(s), “Fast with optimization for local” is selected by default.

Go to **Others > Compressions**. Click the drop-down button then select from the following list:

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



11 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 \(Step 10\)](#)



11.1 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: $1594627447932 \bmod 5 = 2$

| | |
|---|-----------|
| 2 | Wednesday |
|---|-----------|

In this example:

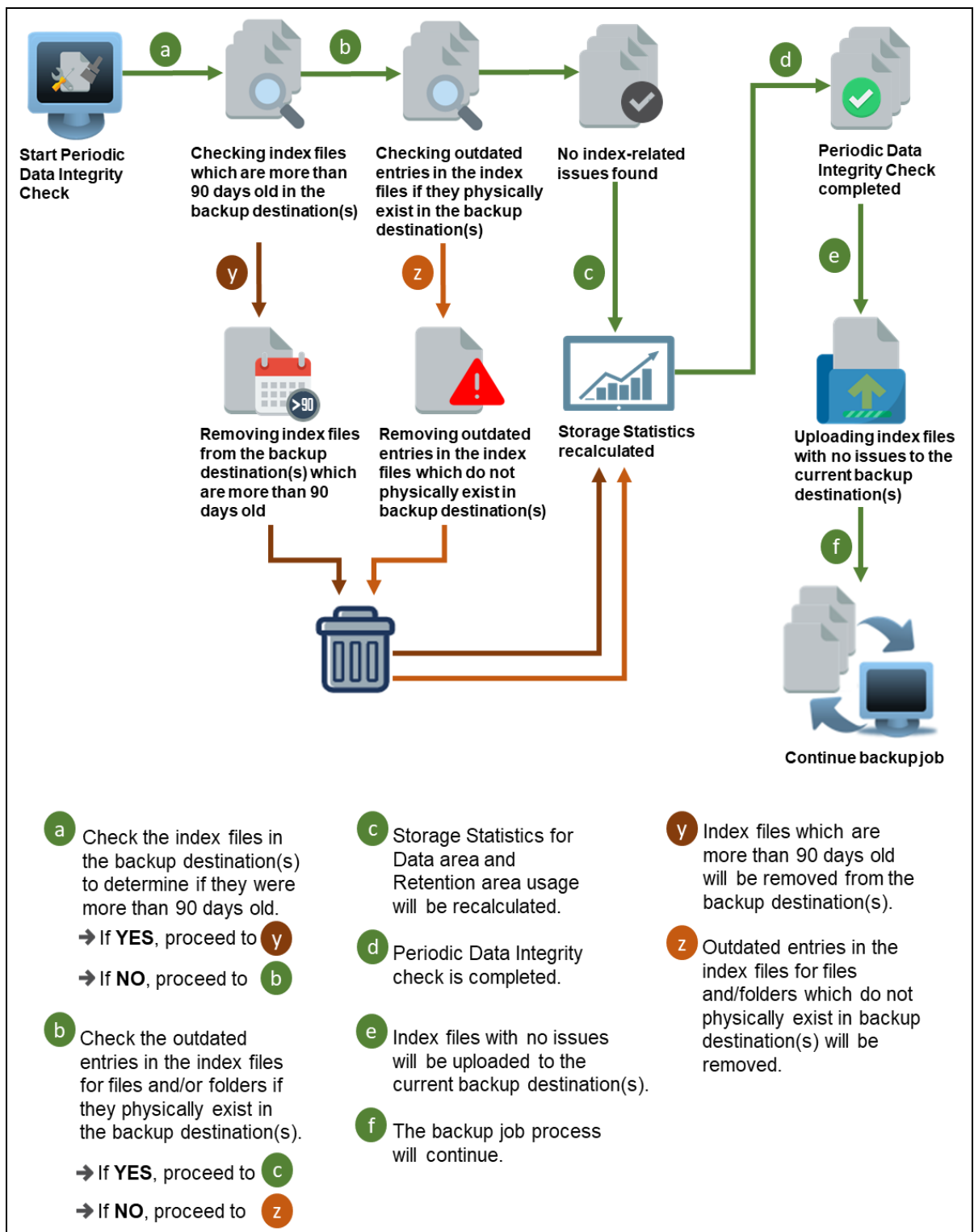
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

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:

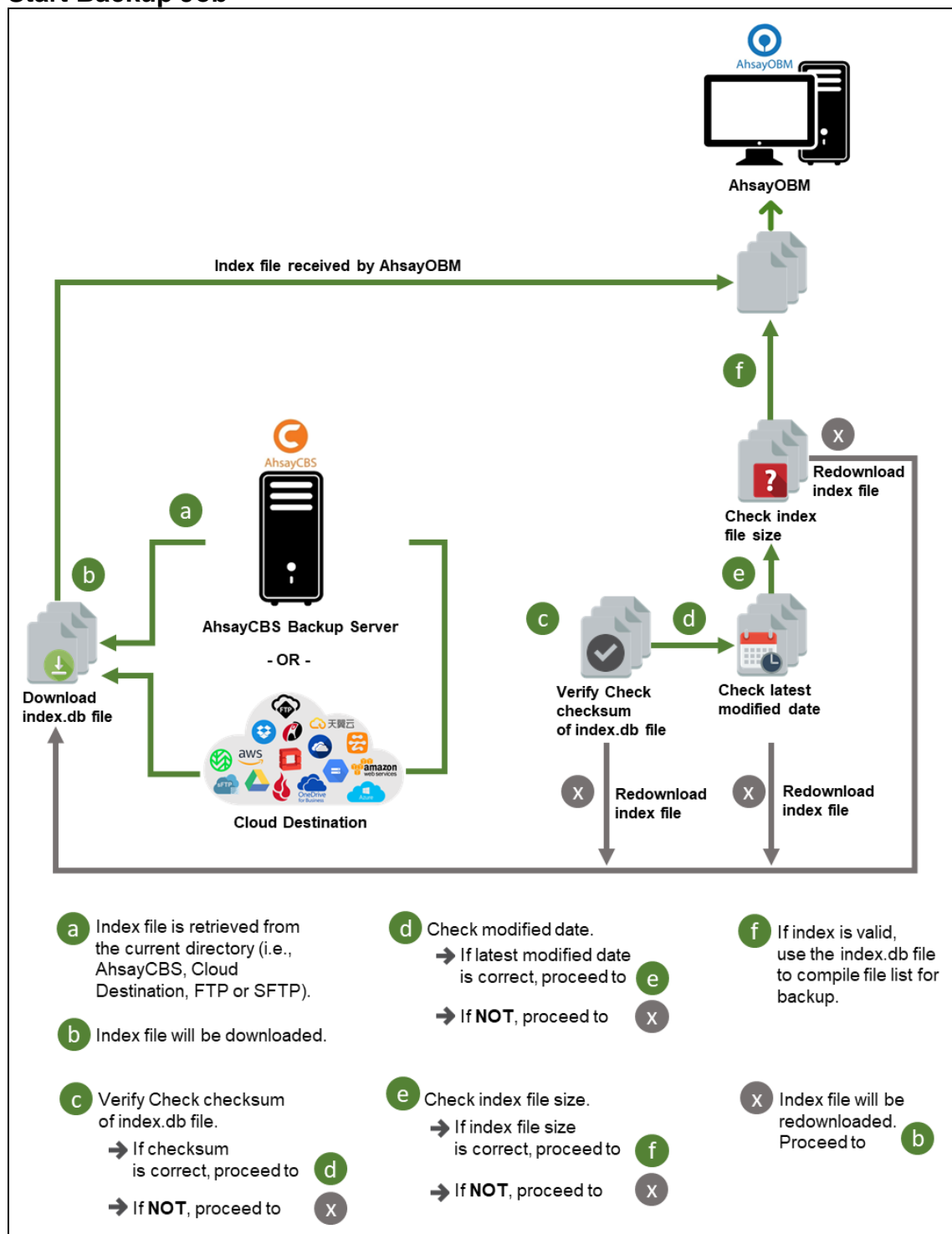
1. The PDIC job will run on the first backup job after upgrade to the latest client version from AhsayOBM v6, v7, or pre-8.3.6.0 version.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it 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 v9 block format.



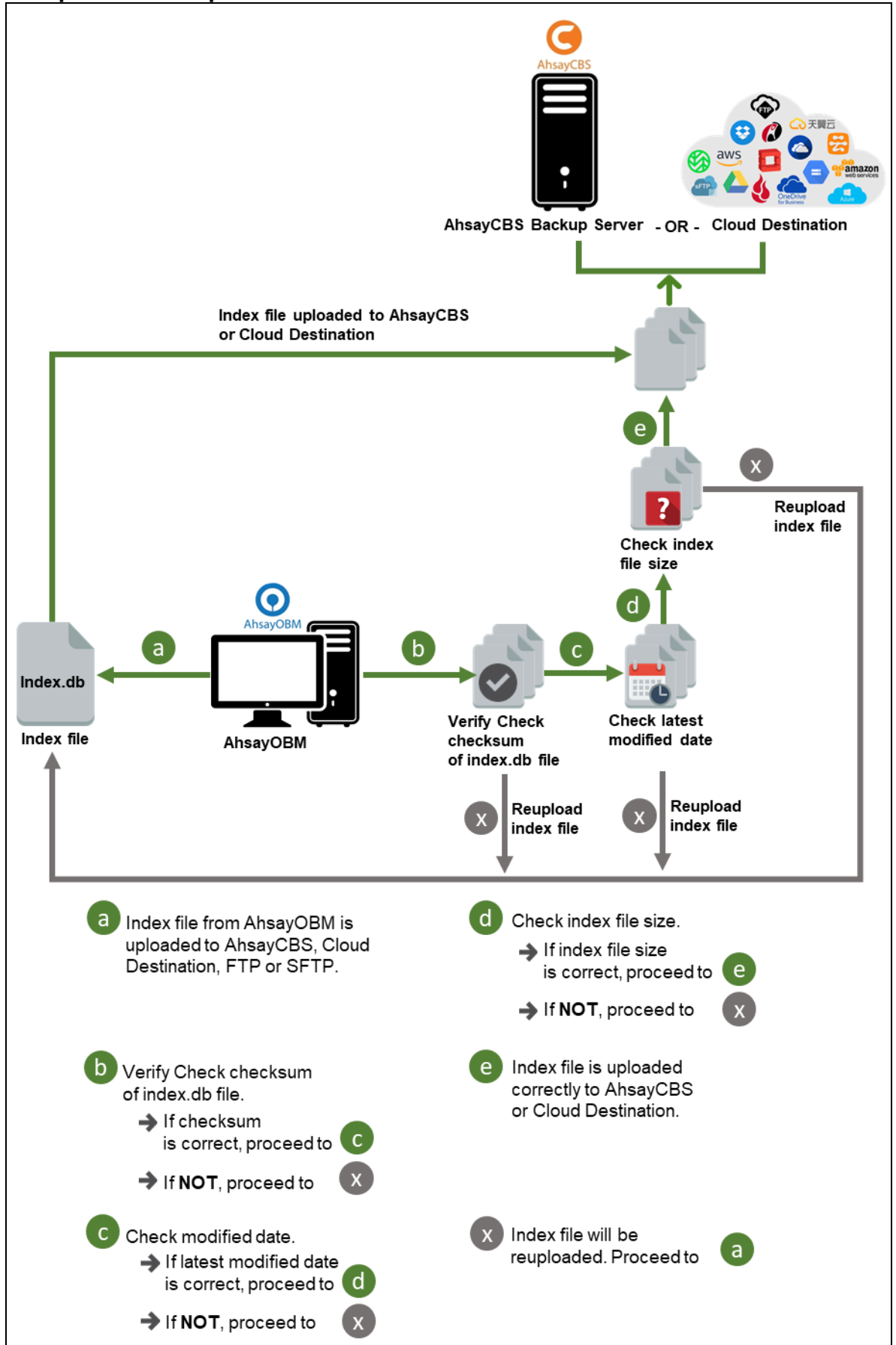
11.2 Backup Set Index Handling Process

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.

11.2.1 Start Backup Job

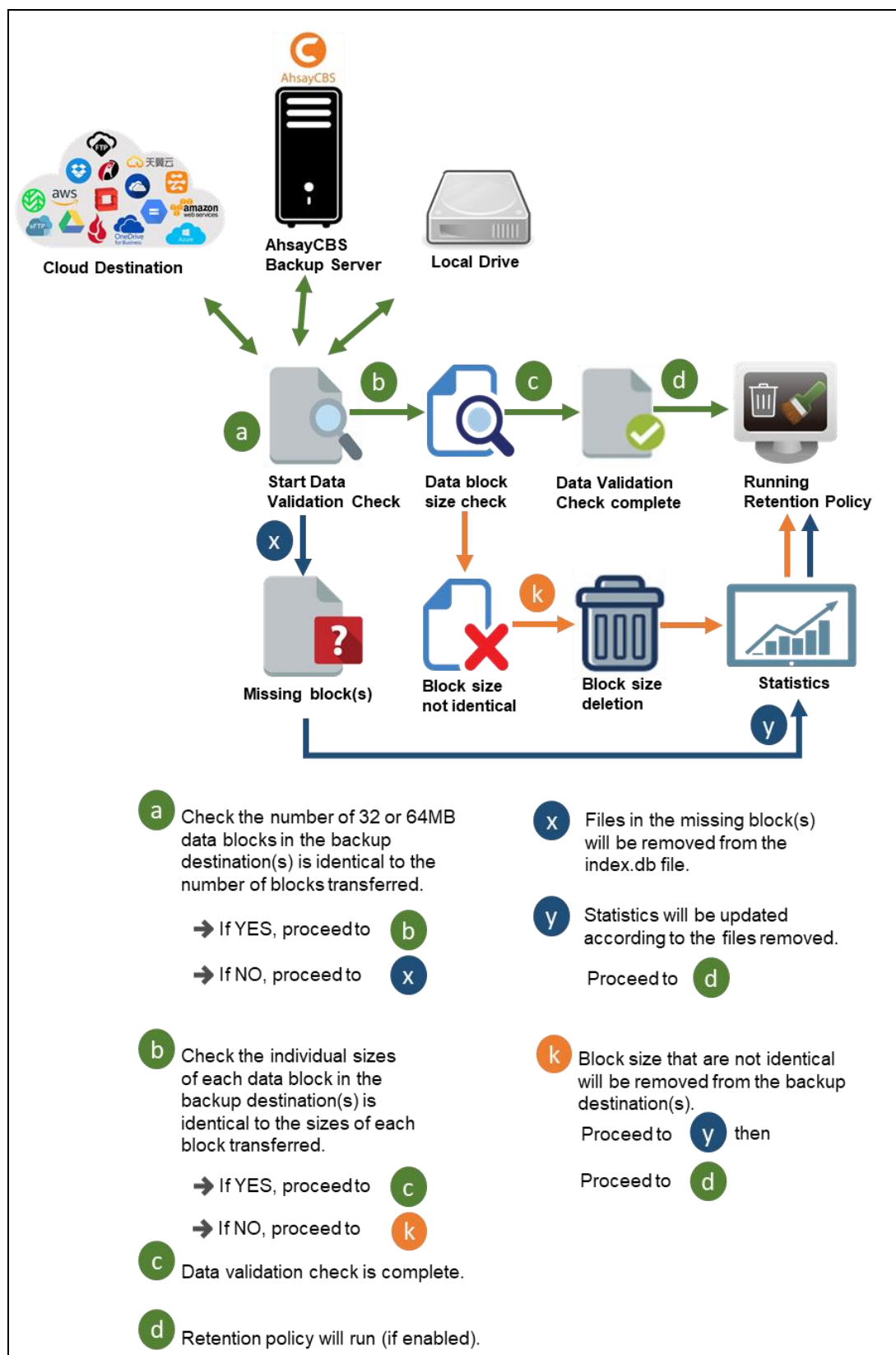


11.2.2 Completed Backup Job



11.3 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 32 or 64MB data block files and the size of each block file are checked again after the files are transferred.



12 Run Backup Jobs

12.1 Login to AhsayOBM

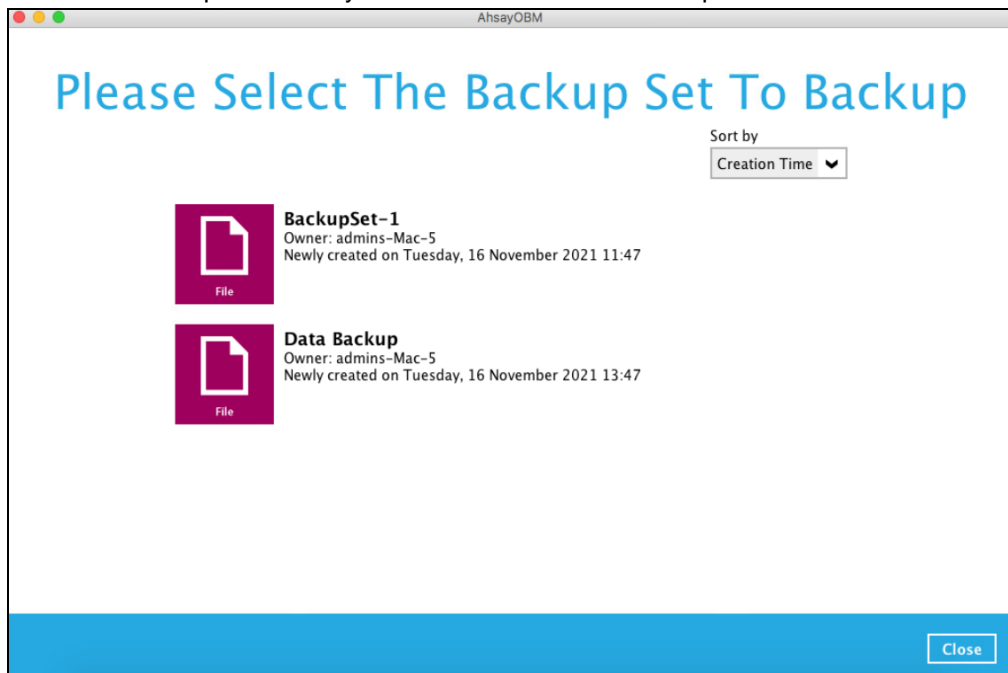
Login to the AhsayOBM application according to the instructions in [Chapter 7 Login to AhsayOBM](#).

12.2 Start a Manual Backup

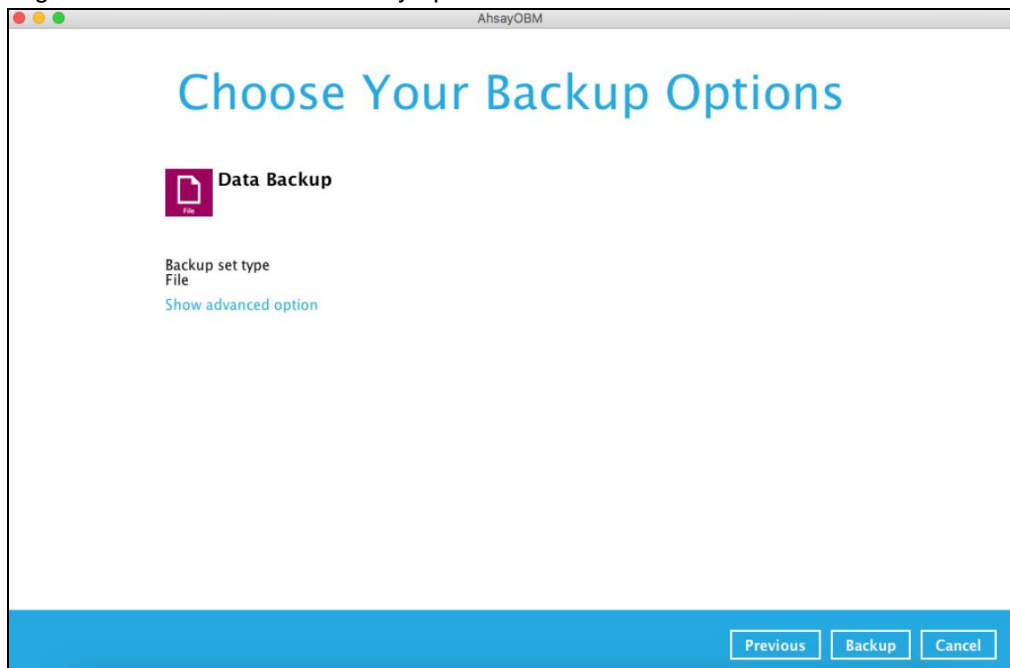
1. Click the **Backup** icon on the main interface of AhsayOBM.



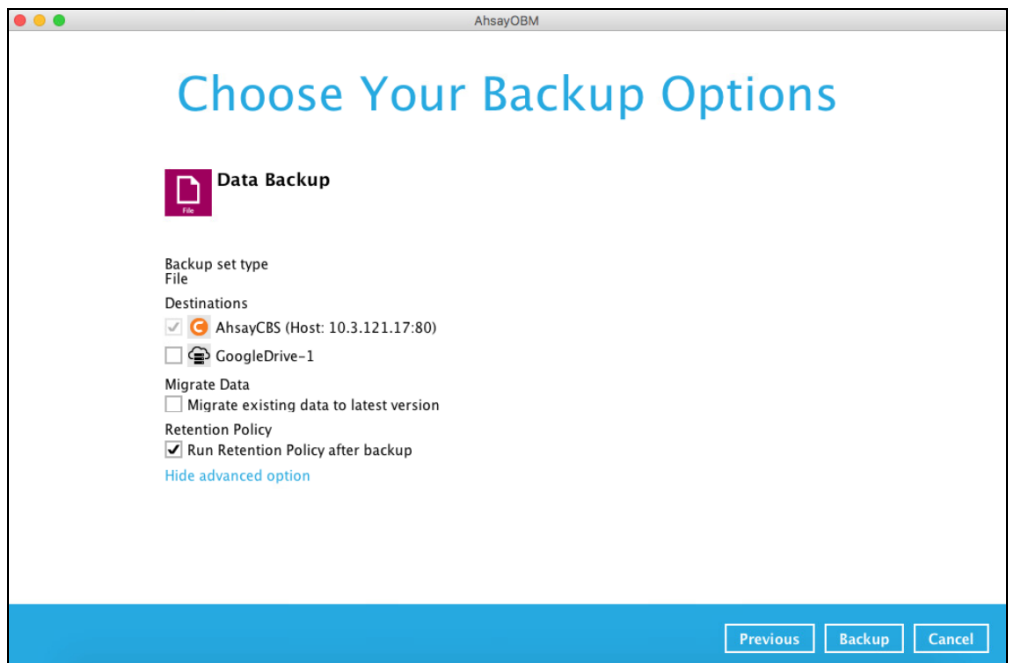
2. Select the backup set which you would like to start a backup for.



3. Click the **Show advanced option** in case you want to modify the Destinations, Migrate Data and Retention Policy options.



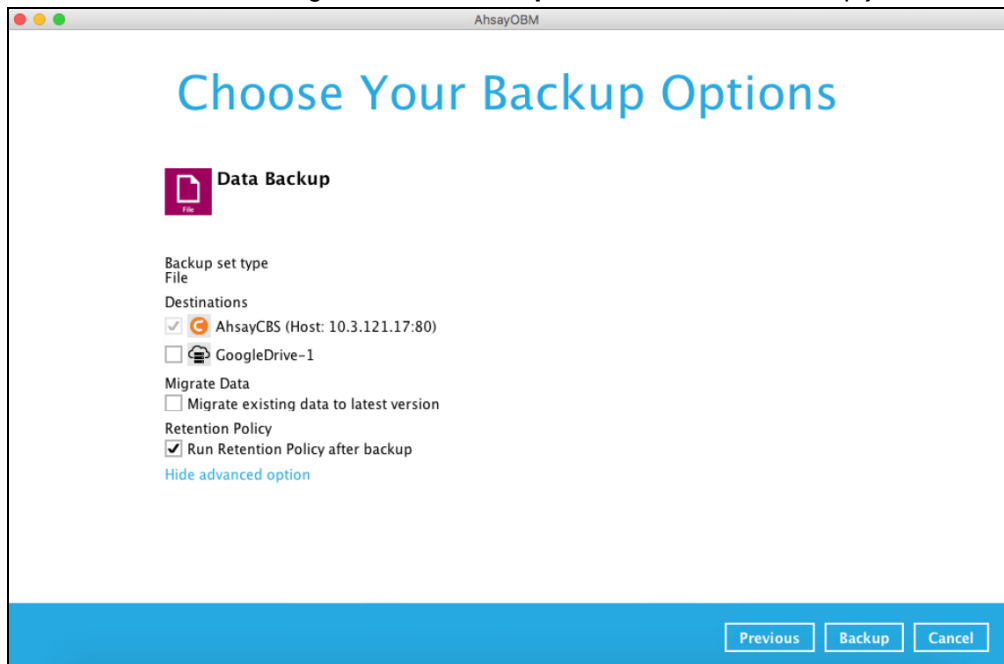
4. When the advanced options are shown, it is recommended to enable the **Run Retention Policy after backup**. This will help you save hard disk quota in the long run.




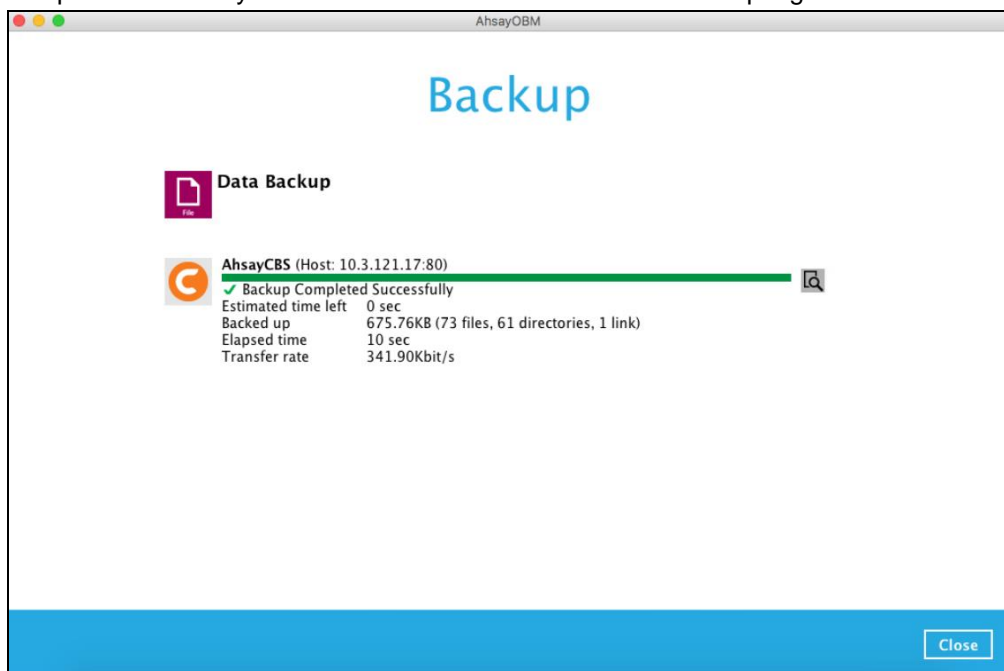
NOTE

The **Migrate Data** option will only be displayed if Deduplication is enabled for the backup set. When the Migrate Data option is enabled, the existing data will be migrated to the latest version during a backup job. Backup job(s) for backup sets with Migrate Data enabled may take longer to finish. For more information about this feature, refer to [AhsayCBS v9 New Features Supplemental document](#).

5. Once done with the settings, click the **Backup** button to start the backup job.



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



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

| Type | Log | Time |
|------|---|---------------------|
| i | Start [AhsayOBM v9.0.3.12] | 09/01/2022 14:20:24 |
| i | Saving encrypted backup set encryption keys to server... | 09/01/2022 14:20:24 |
| i | Start Backup ... [Deduplication: enabled, Deduplication scope: All files within the same backup set, Migrate Delta: disa... | 09/01/2022 14:20:25 |
| i | Using Temporary Directory /Users/admin/.obm/temp/1641707049259/OBS@1641707099728 | 09/01/2022 14:20:25 |
| i | Start running pre-commands | 09/01/2022 14:20:29 |
| i | Finished running pre-commands | 09/01/2022 14:20:29 |
| i | Downloading server file list... | 09/01/2022 14:20:29 |
| i | Download valid index files from backup job "null" to "/Users/admin/.obm/temp/1641707049259/OBS@1641707099... | 09/01/2022 14:20:29 |
| i | Downloading server file list... Completed | 09/01/2022 14:20:29 |
| i | Reading backup source from hard disk... | 09/01/2022 14:20:30 |
| i | Reading backup source from hard disk... Completed | 09/01/2022 14:20:30 |
| i | [New Directory]... / | 09/01/2022 14:20:31 |
| i | [New Directory]... /Users | 09/01/2022 14:20:31 |
| i | [New Directory]... /Users/admin | 09/01/2022 14:20:31 |
| i | [New Directory]... /Users/admin/Downloads | 09/01/2022 14:20:31 |
| i | [New Directory]... /Users/admin/Downloads/Test Files | 09/01/2022 14:20:31 |
| i | [New Directory]... /Users/admin/Downloads/Test Files/HTML files (Requirements) | 09/01/2022 14:20:31 |
| i | [New Directory]... /Users/admin/Downloads/Test Files/Latest version | 09/01/2022 14:20:31 |
| i | [New Directory]... /Users/admin/Downloads/Test Files/New updates | 09/01/2022 14:20:31 |
| i | [New File]... 22% of "/Users/admin/Downloads/Test Files/HTML files (Requirements)/BS_General_Oracle ---included.ht... | 09/01/2022 14:20:33 |
| i | [New File]... 44% of "/Users/admin/Downloads/Test Files/HTML files (Requirements)/BS_General_Oracle ---included.ht... | 09/01/2022 14:20:33 |
| i | [New File]... 67% of "/Users/admin/Downloads/Test Files/HTML files (Requirements)/BS_General_Oracle ---included.ht... | 09/01/2022 14:20:33 |

Logs per page 50 Page 1 / 4

Close

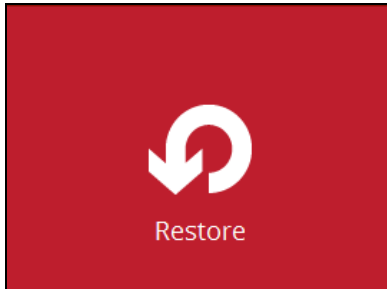
13 Restore Data

13.1 Login to AhsayOBM

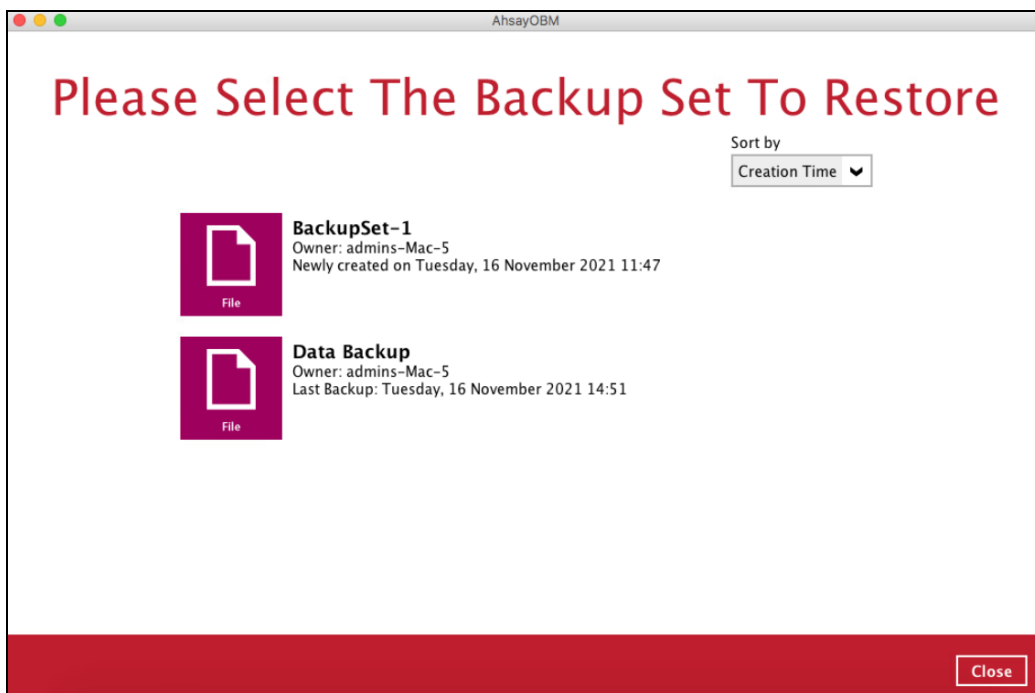
Login to the AhsayOBM application according to the instructions in [Chapter 7 Login to AhsayOBM](#).

13.2 Restore Data

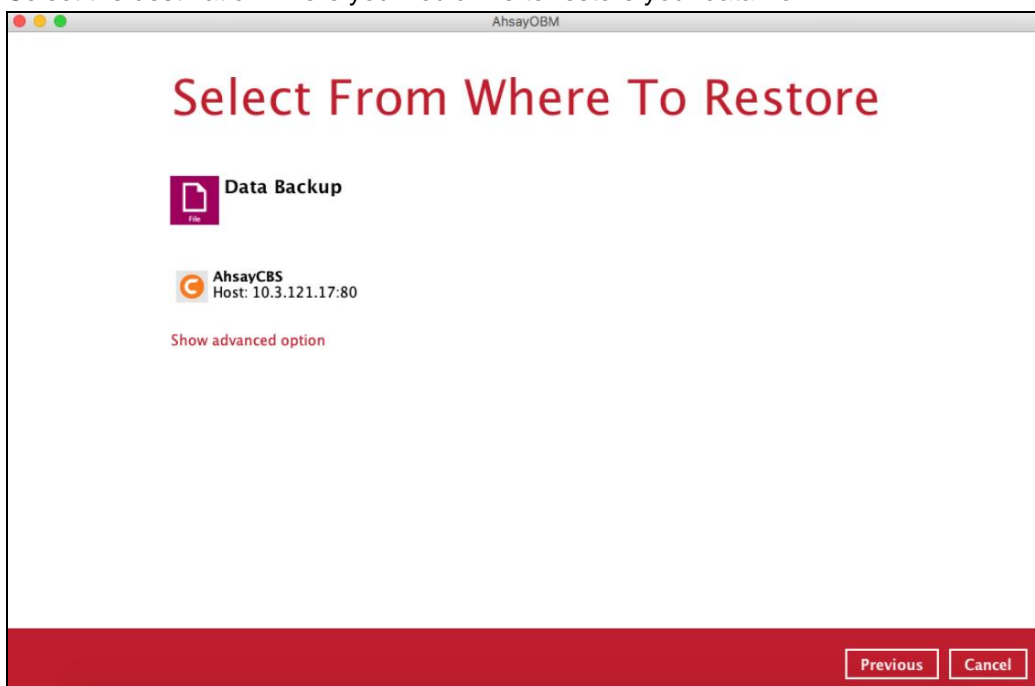
1. Click the **Restore** icon on the main interface of AhsayOBM.



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



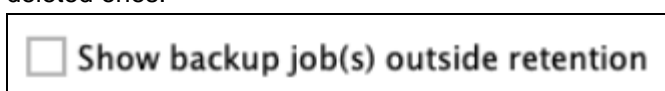
3. Select the destination where you would like to restore your data from.



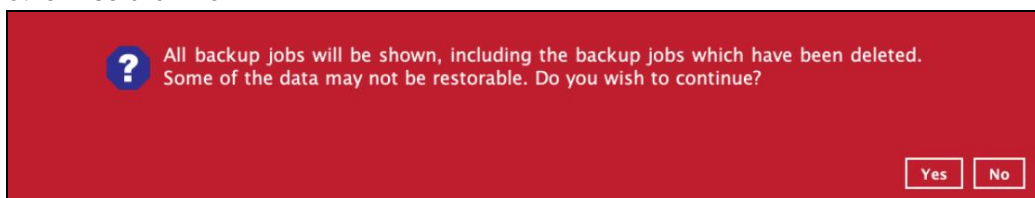
You may configure the **Temporary directory for storing restore files** by clicking **Show advanced** option. By default, the temporary files are stored under the temp directory of the user profile directory. In case the same directory path does not exist in the computer you are running AhsayOBM, you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



4. Tick **Show backup job(s) outside retention** if you want all backup jobs to be displayed, even the deleted ones.



Once ticked, this message will be displayed. Click **Yes** if you want all backup jobs to be displayed, otherwise click **No**.



- 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** drop-down menu:

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

| Name | Size |
|-------------|------|
| backup file | |

| Name | Size |
|-------------|------|
| backup file | |

| Name | Size |
|-------------|------|
| backup file | |

NOTE

Backup jobs that are outside the retention policy are greyed out.

- 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 |
|-----------|------------|----------|------------------|
| AhsayCBS | File 1.txt | 8.72 KB | 05/10/2022 13:52 |
| Users | File 1.txt | 9.54 KB | 05/10/2022 13:48 |
| admin | File 1.txt | 7.11 KB | 05/10/2022 13:34 |
| Documents | File 2.txt | 13.91 KB | 05/10/2022 13:53 |
| | File 2.txt | 12.93 KB | 05/10/2022 13:49 |
| | File 2.txt | 10.01 KB | 05/10/2022 13:42 |
| | File 3.txt | 17.27 KB | 05/10/2022 13:54 |
| | File 3.txt | 14.85 KB | 05/10/2022 13:51 |
| | File 3.txt | 10.96 KB | 05/10/2022 13:43 |

The following is an example showing all the available backup versions of the file **File1.txt**. 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.txt | 8.72 KB | 05/10/2022 13:52 |
| <input type="checkbox"/> File 1.txt | 9.54 KB | 05/10/2022 13:48 |
| <input type="checkbox"/> File 1.txt | 7.11 KB | 05/10/2022 13:34 |

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.

| Name | Date Modified | Size | Kind |
|-------------------------------|----------------|-------|------------|
| File1.txt | Today, 1:52 PM | 7 KB | Plain Text |
| File1_2022-10-05-13-51-34.txt | Today, 1:48 PM | 10 KB | Plain Text |
| File1_2022-10-05-13-46-05.txt | Today, 1:34 PM | 9 KB | Plain Text |

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

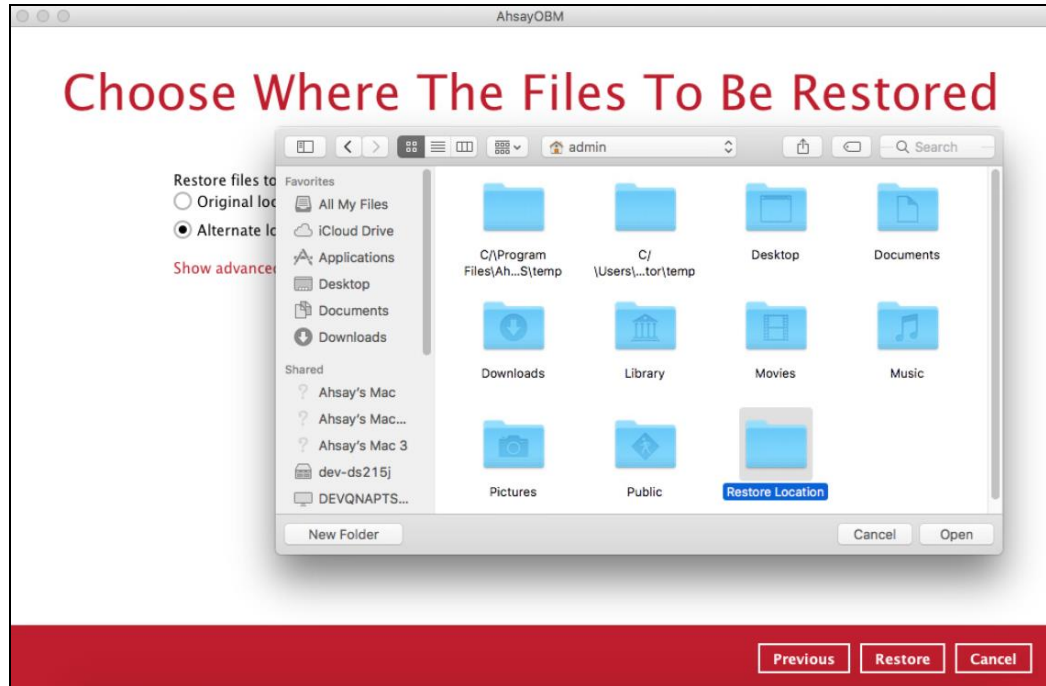
6. Select to restore the files to their **Original location**, or to an **Alternate location**. Then, click **Next** to proceed.

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

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

The screenshot shows a window titled "AhsayOBM" with the heading "Choose Where The Files To Be Restored" in red. Below the heading, there are two radio buttons: "Original location" (which is selected) and "Alternate location". To the right of the "Alternate location" radio button is a text input field and a "Browse" button. Below these options is a link that says "Show advanced option". At the bottom of the window, there is a red bar containing three buttons: "Previous", "Restore", and "Cancel".

- **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:

Restore files to
☒ Original location
☐ Alternate location

Show advanced option

☐ Delete unmatched data in restore location
☐ Verify checksum of in-file delta files during restore



Hide advanced option

Delete unmatched data in restore location

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

Example:

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

| Document folder 01 | |
|--|---------------------------|
| Name | |
|  doc 1.docx | } Files created initially |
|  doc 2.docx | |

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

| Document folder 01 | |
|--------------------|-----------------------------|
| Name | |
| doc 1.docx | Files created BEFORE backup |
| doc 2.docx | |
| doc 3.docx | Files created AFTER backup |
| doc 4.docx | |

- iv) A restore is performed for the **Document folder 01**, with **Delete unmatched data in restore location** 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.

| Document folder 01 | |
|--------------------|----------------------------|
| Name | |
| doc 1.docx | Files remain after restore |
| doc 2.docx | |

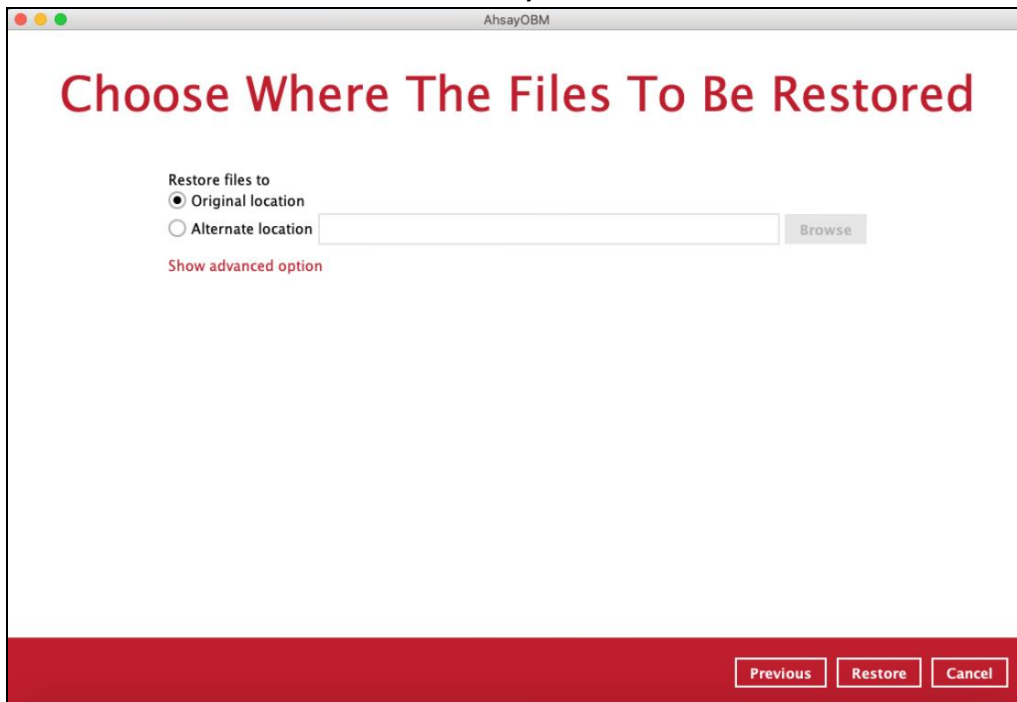
WARNING


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

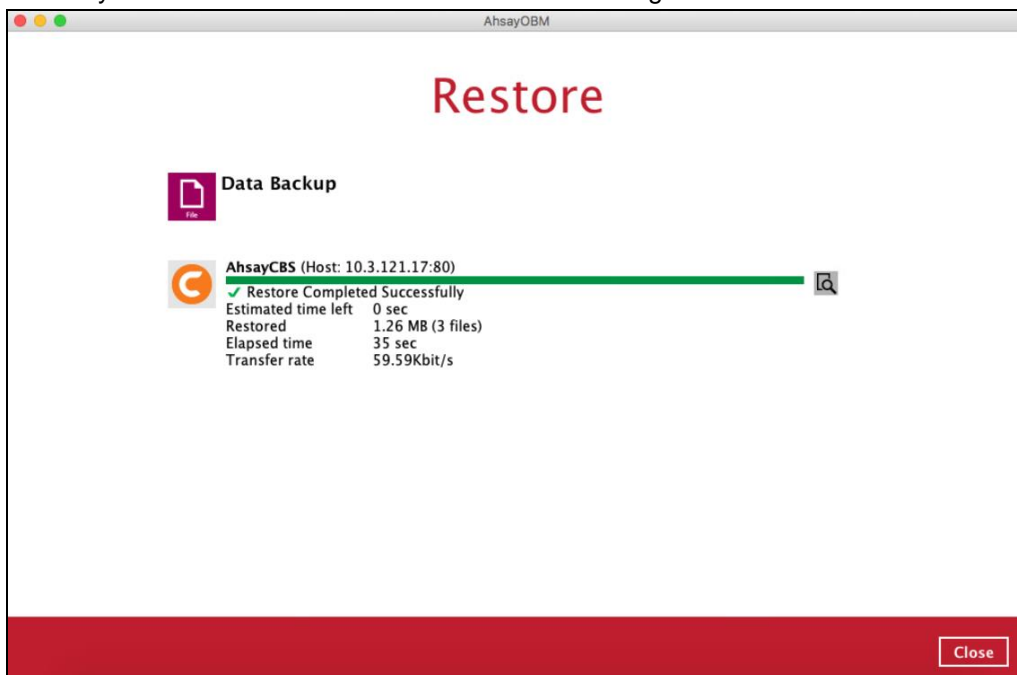
Verify checksum of in-file delta files during restore

Verify checksum of in-file delta files during restore is disabled by default. When you perform restore for non-RunDirect backup set, 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 if the merged file were correct.

8. Click the **Restore** button to start the restore job.



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



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

Window Title: AhsayOBM

Show: All

| Type | Log | Time |
|------|--|---------------------|
| i | Start [AhsayOBM v9.4.2.9] | 27/09/2022 16:40:45 |
| i | Downloading... "backup file/Archive/indexes_full_list_2020.txt" (Total 1.21 M bytes) | 27/09/2022 16:40:51 |
| i | Downloading... "backup file/Archive/indexes_full_list_2019.txt" (Total 1.21 M bytes) | 27/09/2022 16:40:54 |
| i | Downloading... "backup file/Archive/indexes_full_list_2018.txt" (Total 1.21 M bytes) | 27/09/2022 16:40:57 |
| i | Downloading... "backup file/Archive/asset_inventory_2020.xls" (Total 25 K bytes) | 27/09/2022 16:41:00 |
| i | Downloading... "backup file/Archive/asset_inventory_2018.xls" (Total 25 K bytes) | 27/09/2022 16:41:03 |
| i | Downloading... "backup file/Archive/asset_inventory_2018.xls" (Total 25 K bytes) | 27/09/2022 16:41:06 |
| i | Downloading... "backup file/Archive/Asset_inventory_2022.xls" (Total 25 K bytes) | 27/09/2022 16:41:09 |
| i | Downloading... "backup file/Archive/Asset_inventory_2021.xls" (Total 25 K bytes) | 27/09/2022 16:41:12 |
| i | Downloading... "backup file/Archive/indexes_full_list_2022.txt" (Total 2.43 M bytes) | 27/09/2022 16:41:15 |
| i | Downloading... "backup file/Archive/indexes_full_list_2021.txt" (Total 2.43 M bytes) | 27/09/2022 16:41:18 |
| i | Restore Completed Successfully | 27/09/2022 16:41:20 |

Logs per page: 50

Page: 1 / 1

Close

Close

13.3 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:

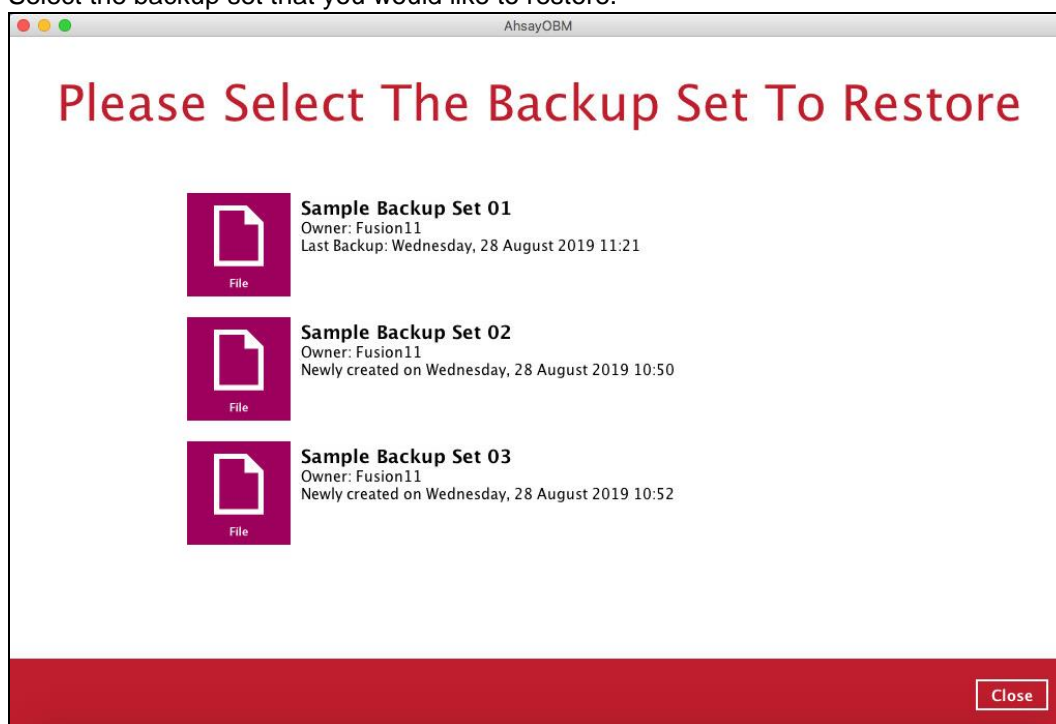
- **Contains**
These are Directories, Files, and Folders with the name **containing** the specific letter or word.
- **Exact**
These are Directories, Files, and Folders with the **exact** or **accurate** name.
- **Start With**
These are Directories, Files, and Folders with the name **starting** with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

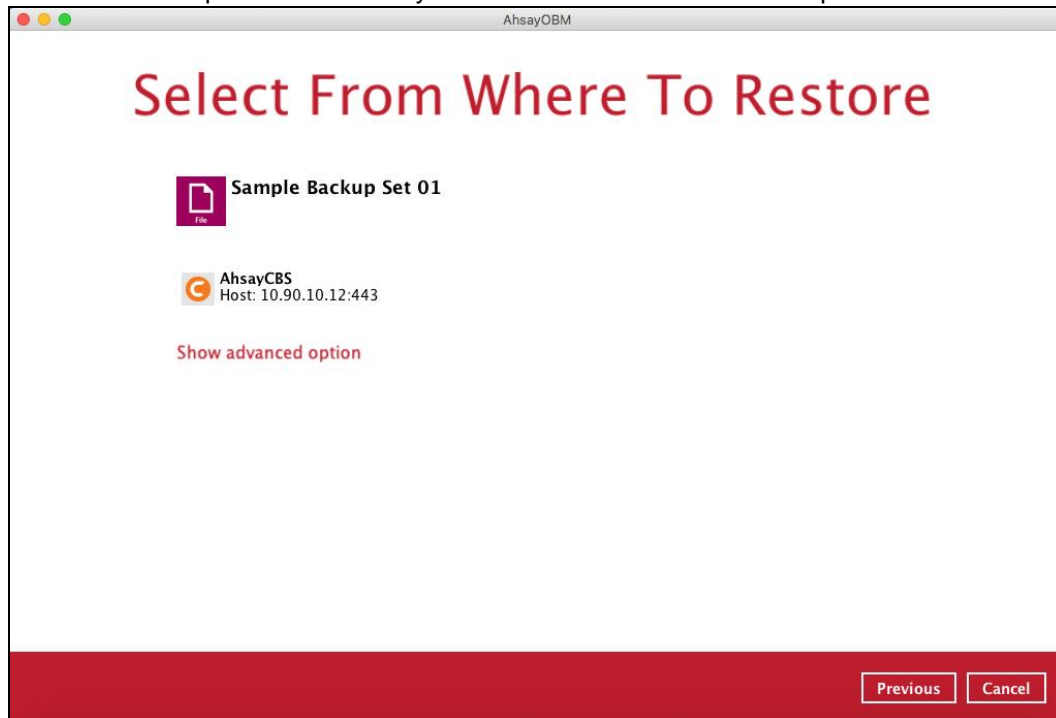
For more detailed examples using the restore filter on AhsayOBM, refer to [Appendix B: Example Scenarios for Restore Filter](#).

Follow the steps below to use the search feature:

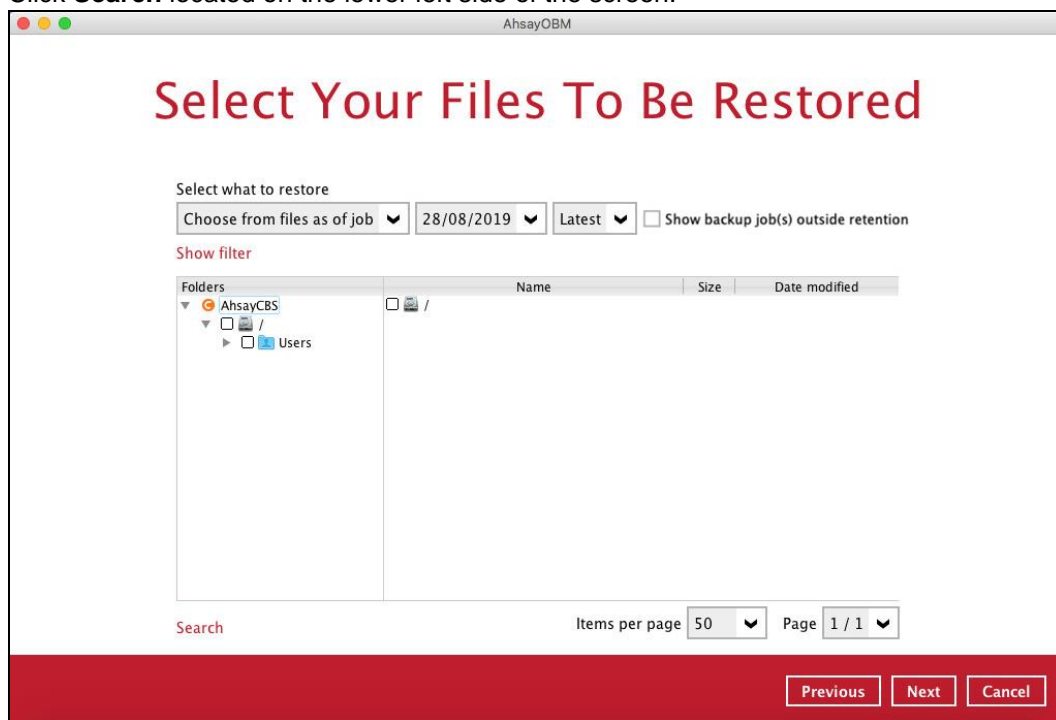
1. Login to AhsayOBM according to the instructions in [Chapter 7 Logging in to AhsayOBM](#).
2. Click the **Restore** icon on the main interface of AhsayOBM.
3. Select the backup set that you would like to restore.



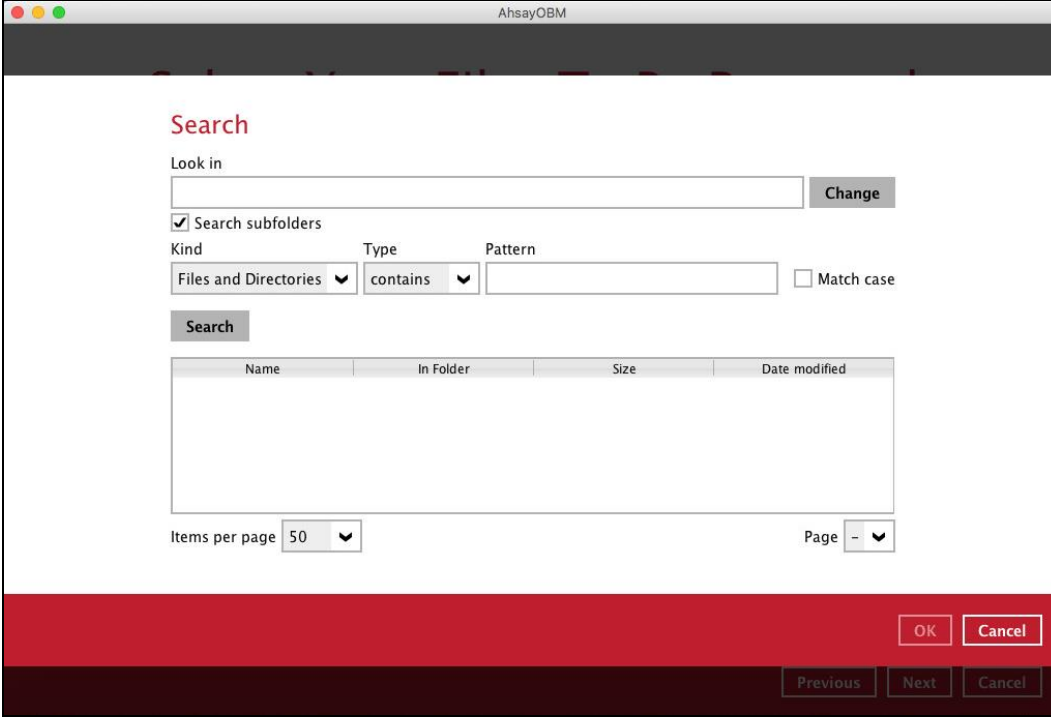
4. Select the backup destination that you would like to restore backed-up items to.



5. Click **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.



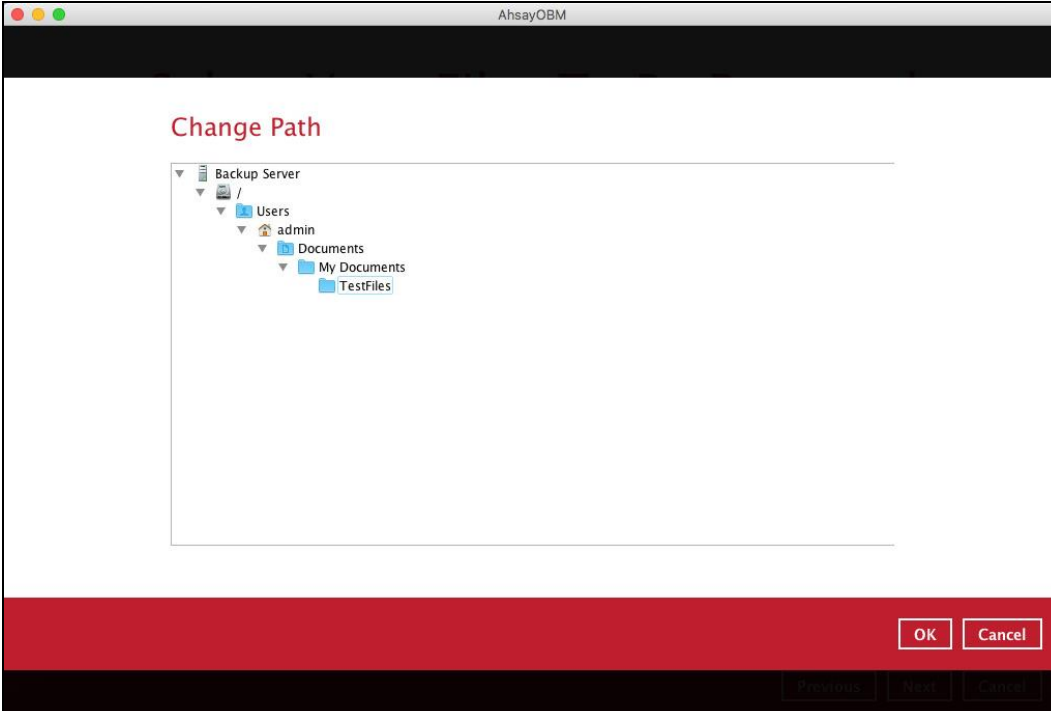
The screenshot shows the 'Search' dialog box in AhsayOBM. The title bar reads 'AhsayOBM'. The dialog has a 'Look in' text field with a 'Change' button to its right. Below this is a checked checkbox for 'Search subfolders'. There are three sections: 'Kind' with a dropdown set to 'Files and Directories', 'Type' with a dropdown set to 'contains', and 'Pattern' with an empty text field. A 'Match case' checkbox is to the right of the 'Pattern' field. A 'Search' button is below these fields. A table with four columns: 'Name', 'In Folder', 'Size', and 'Date modified' is present, but it is empty. At the bottom left, 'Items per page' is set to 50. At the bottom right, 'Page' is set to 1. A red bar at the bottom contains 'OK' and 'Cancel' buttons. Below the red bar are 'Previous', 'Next', and 'Cancel' buttons.

| Name | In Folder | Size | Date modified |
|------|-----------|------|---------------|
|------|-----------|------|---------------|

Items per page: 50 | Page: 1

OK Cancel

Previous Next Cancel



The screenshot shows the 'Change Path' dialog box in AhsayOBM. The title bar reads 'AhsayOBM'. The dialog displays a tree view of the file system. The root is 'Backup Server', which contains a folder 'Users'. 'Users' contains a folder 'admin'. 'admin' contains a folder 'Documents'. 'Documents' contains a folder 'My Documents'. 'My Documents' contains a folder 'TestFiles'. The 'TestFiles' folder is selected. A red bar at the bottom contains 'OK' and 'Cancel' buttons. Below the red bar are 'Previous', 'Next', and 'Cancel' buttons.

Backup Server

- Users
 - admin
 - Documents
 - My Documents
 - TestFiles

OK Cancel

Previous Next Cancel

Search

Look in
 Change

☐ Search subfolders

Kind Type Pattern

Files and Directories contains

☐ Match case

Search

| Name | In Folder | Size | Date modified |
|------|-----------|------|---------------|
|------|-----------|------|---------------|

Items per page 50 Page -

OK Cancel

Previous Next Cancel

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.

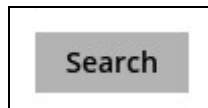
Pattern

☐ Match case

Pattern

☒ Match case

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



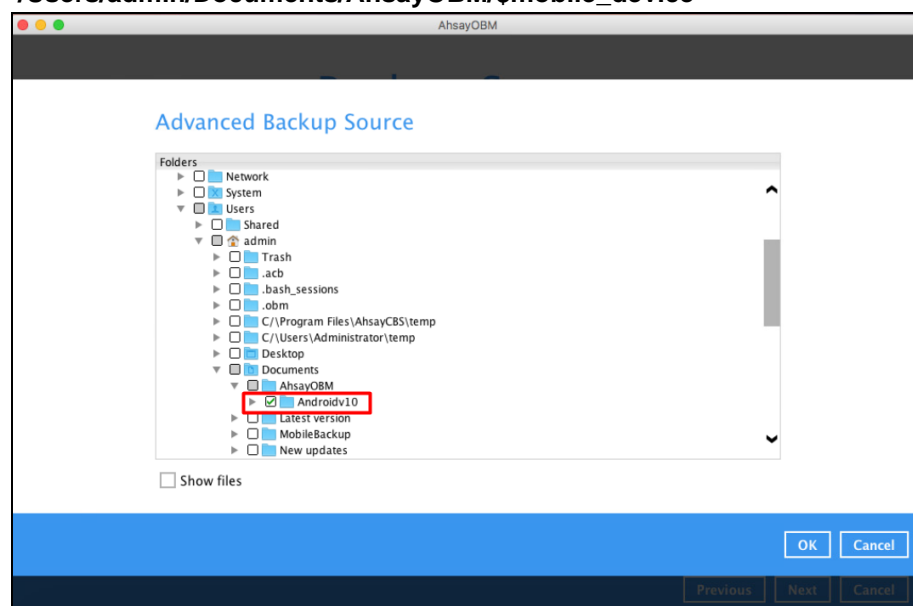
12. Check all the items or check a specific item, then click the **OK** button to proceed and return to the restore main screen.

14 Mobile Backup and Restore to AhsayCBS and Predefined Destination

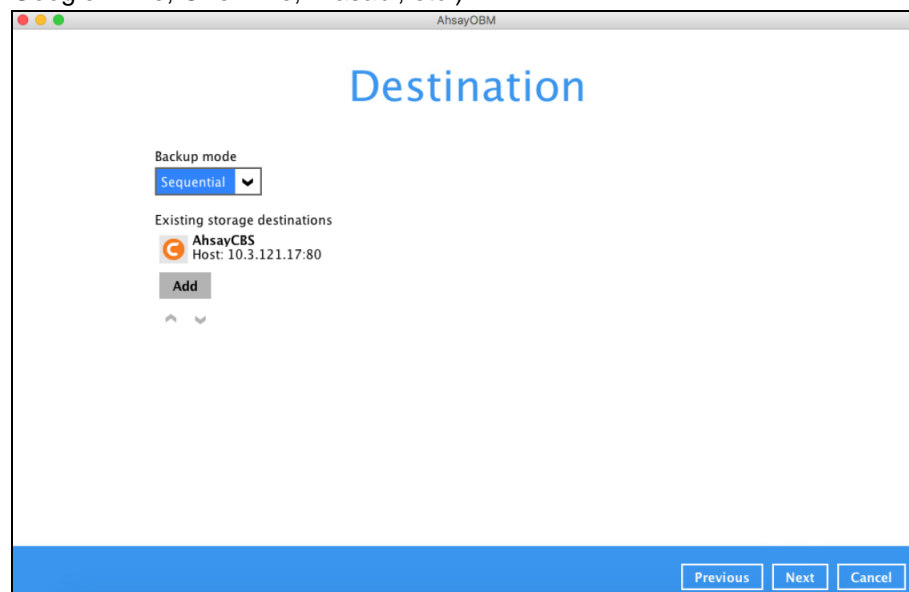
To perform a mobile backup and restore to AhsayCBS and/or Predefined Destination, follow the instructions below:

1. Back up photos, videos, documents and 2FA accounts from Ahsay Mobile app to AhsayOBM local destination. For more detailed information, refer to **Chapter 10** of the [Ahsay Mobile User Guide for Android and iOS](#).
2. Create a File backup set according to the instructions in [Chapter 10 Create Backup Set](#) with the following setup:
 - The backup source should be the photos, videos, documents and/or 2FA account(s) backed up in the AhsayOBM local destination. In this example, the backup source is located in:

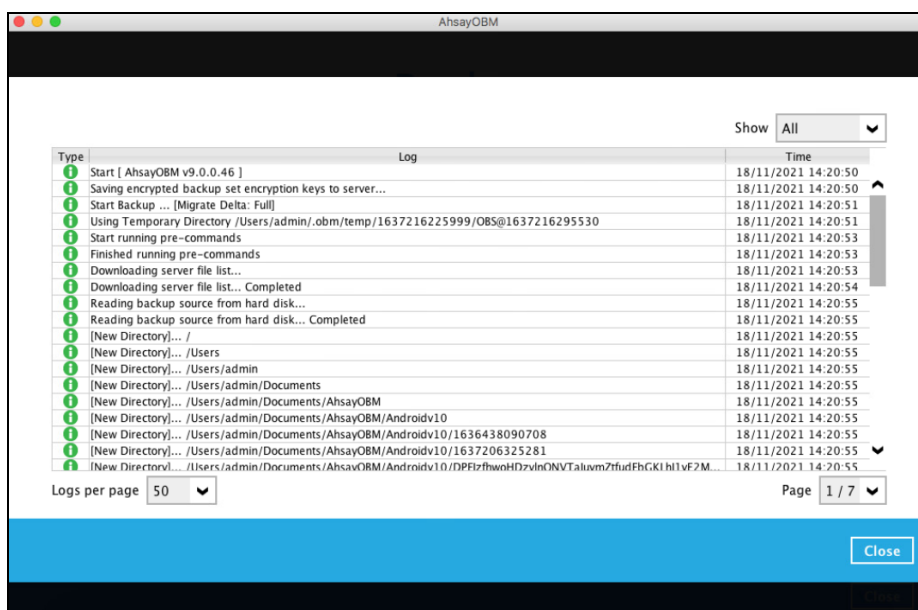
/Users/admin/Documents/AhsayOBM/\$mobile_device



- The backup destination must be AhsayCBS and/or Predefined Destination (i.e., Google Drive, OneDrive, Wasabi, etc.)



- After creating the backup set, run a backup job according to the instructions in [Chapter 12.2 Start Manual Backup](#). Below is an example of a backup report for mobile backup data.



| Type | Log | Time |
|--|---|---------------------|
| Start [AhsayOBM v9.0.0.46] | | 18/11/2021 14:20:50 |
| Saving encrypted backup set encryption keys to server... | | 18/11/2021 14:20:50 |
| Start Backup ... [Migrate Delta: Full] | | 18/11/2021 14:20:51 |
| Using Temporary Directory /Users/admin/.obm/temp/1637216225999/OBS@1637216295530 | | 18/11/2021 14:20:51 |
| Start running pre-commands | | 18/11/2021 14:20:53 |
| Finished running pre-commands | | 18/11/2021 14:20:53 |
| Downloading server file list... | | 18/11/2021 14:20:53 |
| Downloading server file list... Completed | | 18/11/2021 14:20:54 |
| Reading backup source from hard disk... | | 18/11/2021 14:20:55 |
| Reading backup source from hard disk... Completed | | 18/11/2021 14:20:55 |
| [New Directory]... | / | 18/11/2021 14:20:55 |
| [New Directory]... | /Users | 18/11/2021 14:20:55 |
| [New Directory]... | /Users/admin | 18/11/2021 14:20:55 |
| [New Directory]... | /Users/admin/Documents | 18/11/2021 14:20:55 |
| [New Directory]... | /Users/admin/Documents/AhsayOBM | 18/11/2021 14:20:55 |
| [New Directory]... | /Users/admin/Documents/AhsayOBM/Androidv10 | 18/11/2021 14:20:55 |
| [New Directory]... | /Users/admin/Documents/AhsayOBM/Androidv10/1636438090708 | 18/11/2021 14:20:55 |
| [New Directory]... | /Users/admin/Documents/AhsayOBM/Androidv10/1637206325281 | 18/11/2021 14:20:55 |
| [New Directory]... | /Users/admin/Documents/AhsayOBM/Androidv10/DPFzfrfwHdZvlnQNVtTaluvm7rfudFhGKIh11vE2M... | 18/11/2021 14:20:55 |

- Restore data according to the instructions in [Chapter 13.2 Restore Data](#).

There are two (2) options to restore data from AhsayCBS and/or 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.

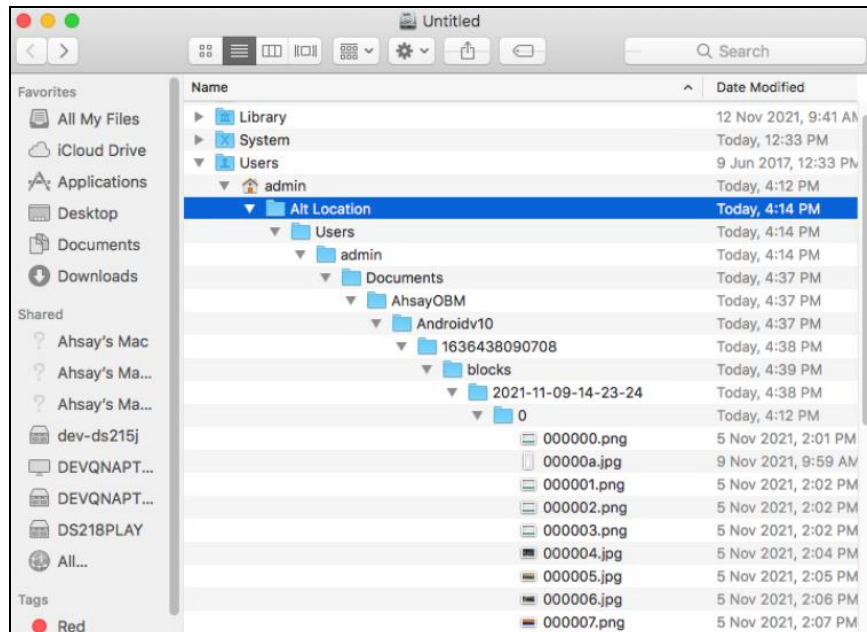
NOTE: Restore to alternate location is not supported on another AhsayOBM machine. Options 1 and 2 must be on the original machine where the backups were performed.

In case the original machine is no longer available, AhsayOBM will be able to restore the photos, videos and 2FA accounts 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, videos and 2FA accounts from the AhsayOBM.

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

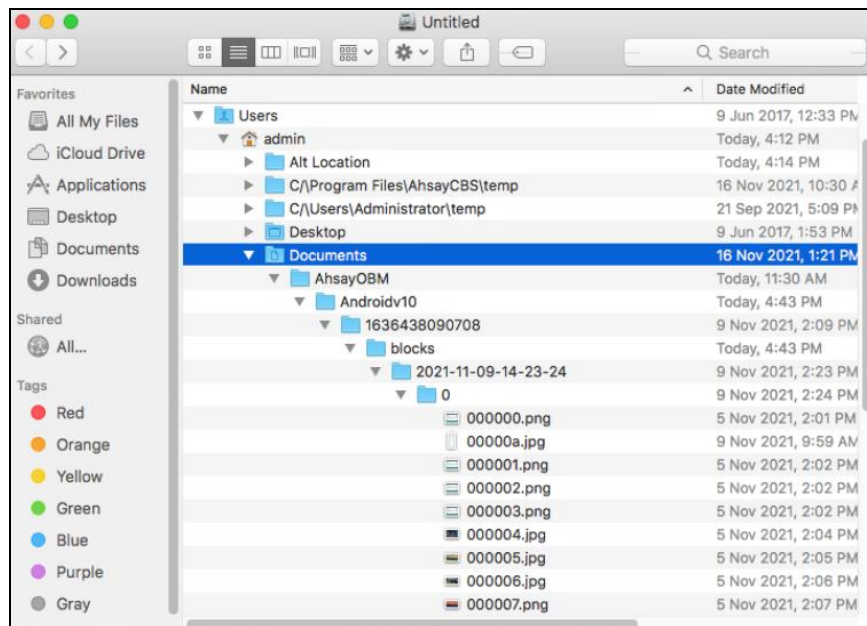
Example of the Alternate location:

/Users/admin/Alt Location



Example of the Original location:

/Users/admin/Documents



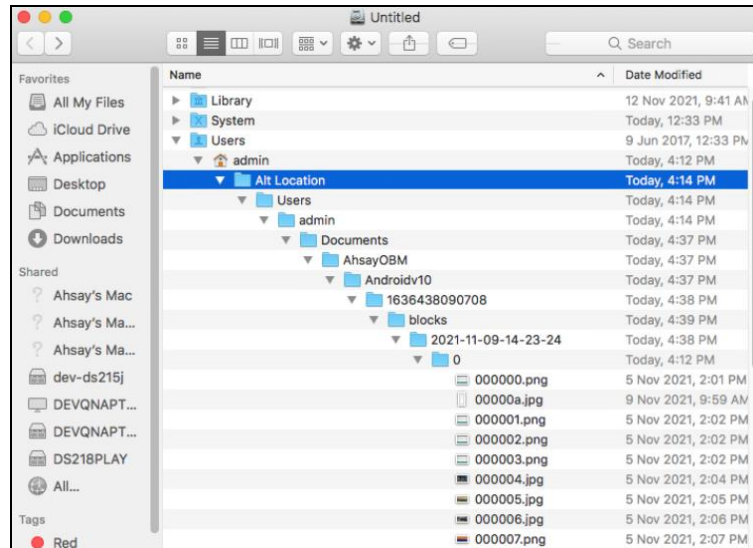
You can now use the Ahsay Mobile app to restore the photos, videos, documents and 2FA accounts back to your mobile device.

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

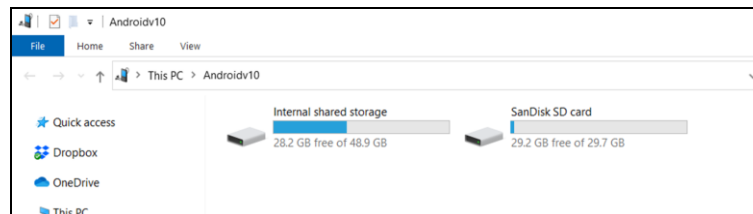
Instructions:

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

Example of the Alternate location: **/Users/admin/Alt Location**

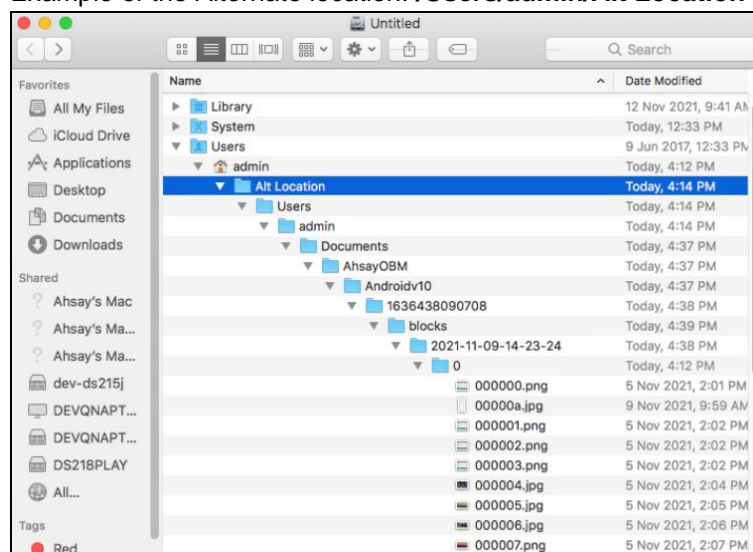


Mobile device storage: Android device Internal storage and SD card

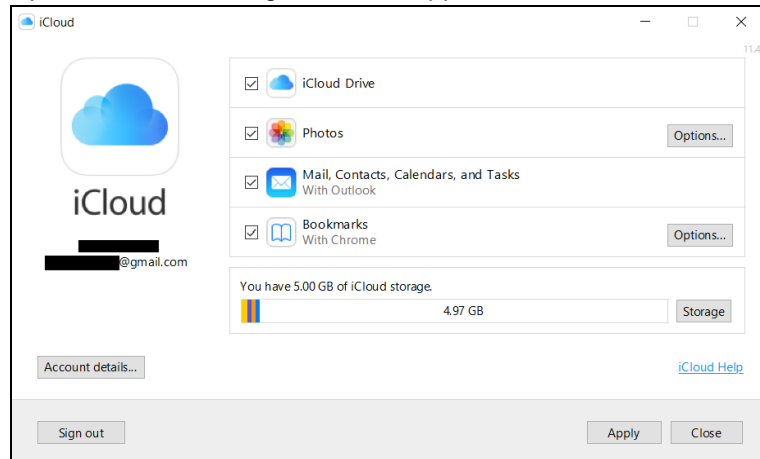


- For an iOS device, you need to transfer the restored data from the alternate location to iCloud.

Example of the Alternate location: **/Users/admin/Alt Location**



Upload to iCloud using the iCloud app



15 Contact Ahsay

15.1 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/>

15.2 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/downloads/ahsay-downloads_documentation_guides.jsp

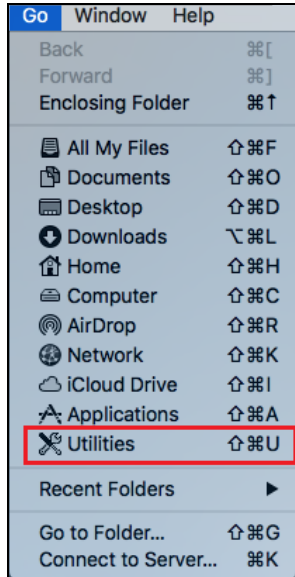
You can send us suggestions for improvements or report on issues in the documentation by contacting us at:
<https://www.ahsay.com/partners/>

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.



Terminal.app

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]$
```

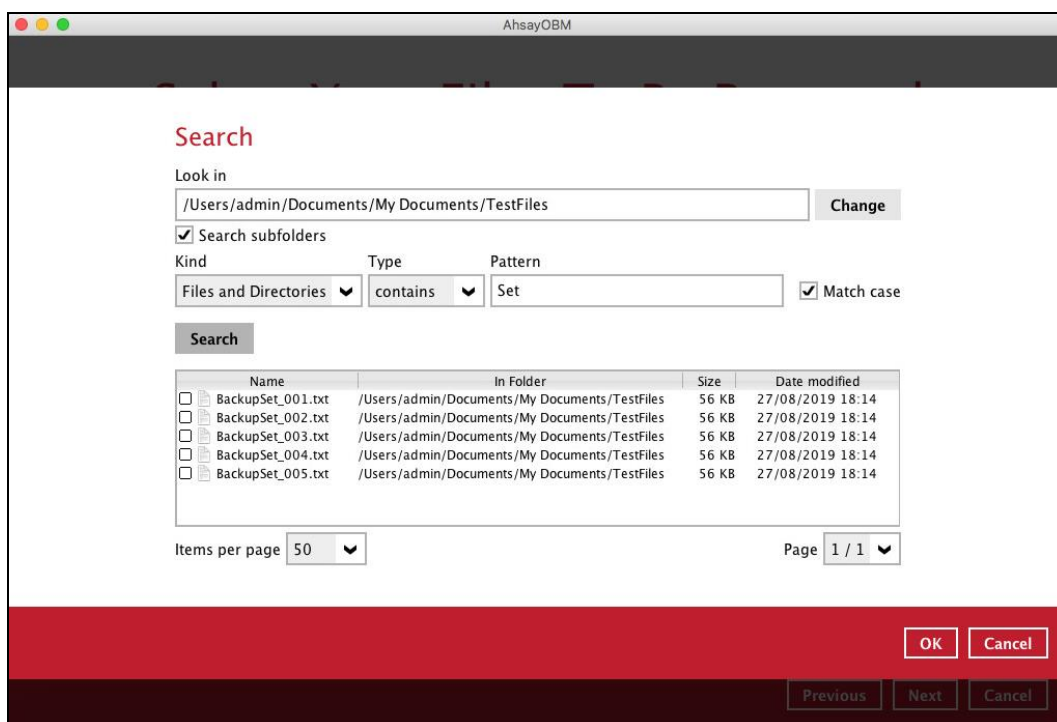
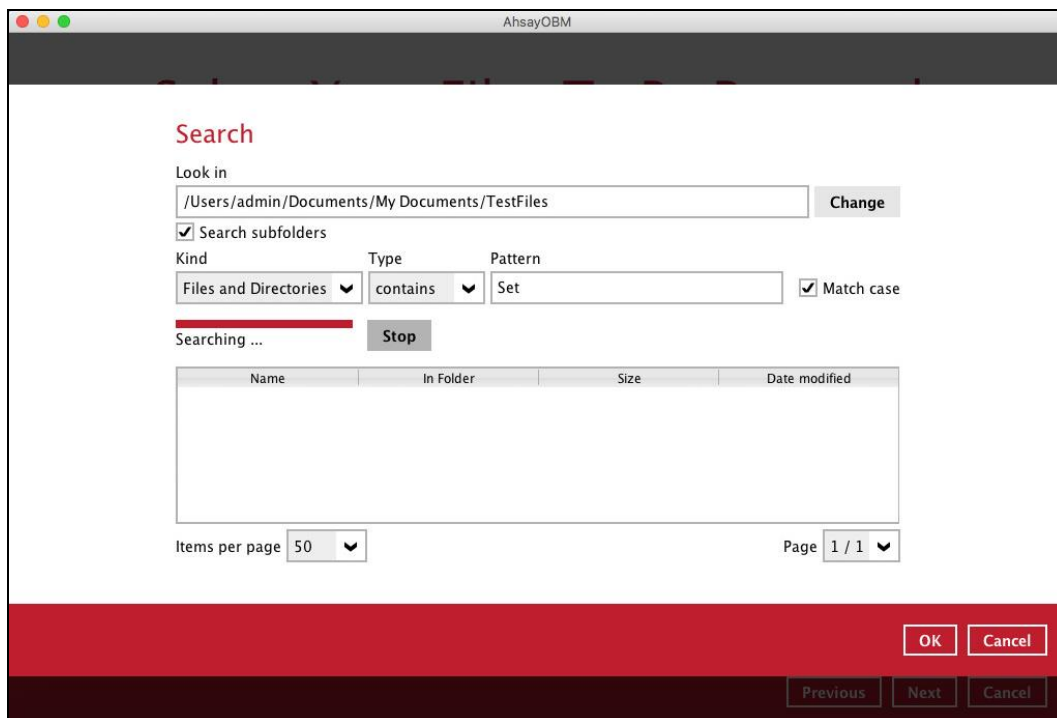
Appendix B: Example Scenarios for Restore Filter

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 area is titled 'Search' in red. Below the title, there is a 'Look in' text box containing the path '/Users/admin/Documents/My Documents/TestFiles' and a 'Change' button to its right. Below this is a checked checkbox labeled 'Search subfolders'. Further down are three labels: 'Kind', 'Type', and 'Pattern'. Under 'Kind' is a dropdown menu showing 'Files and Directories'. Under 'Type' is a dropdown menu showing 'contains'. Under 'Pattern' is a text box containing 'Set'. To the right of these is a checked checkbox labeled 'Match case'. Below these settings is a 'Search' button. Under the 'Search' button is a table with four columns: 'Name', 'In Folder', 'Size', and 'Date modified'. The table body is currently empty. At the bottom left of the table area is a label 'Items per page' followed by a dropdown menu showing '50'. At the bottom right is a label 'Page' followed by a dropdown menu showing '-'. At the very bottom of the dialog, there is a red bar containing 'OK' and 'Cancel' buttons. Below the red bar, there is a dark bar containing '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. This means that the filter will include all available subfolders in /TestFiles upon searching. And it will strictly search only the specified pattern and case which starts with 'Set'.

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

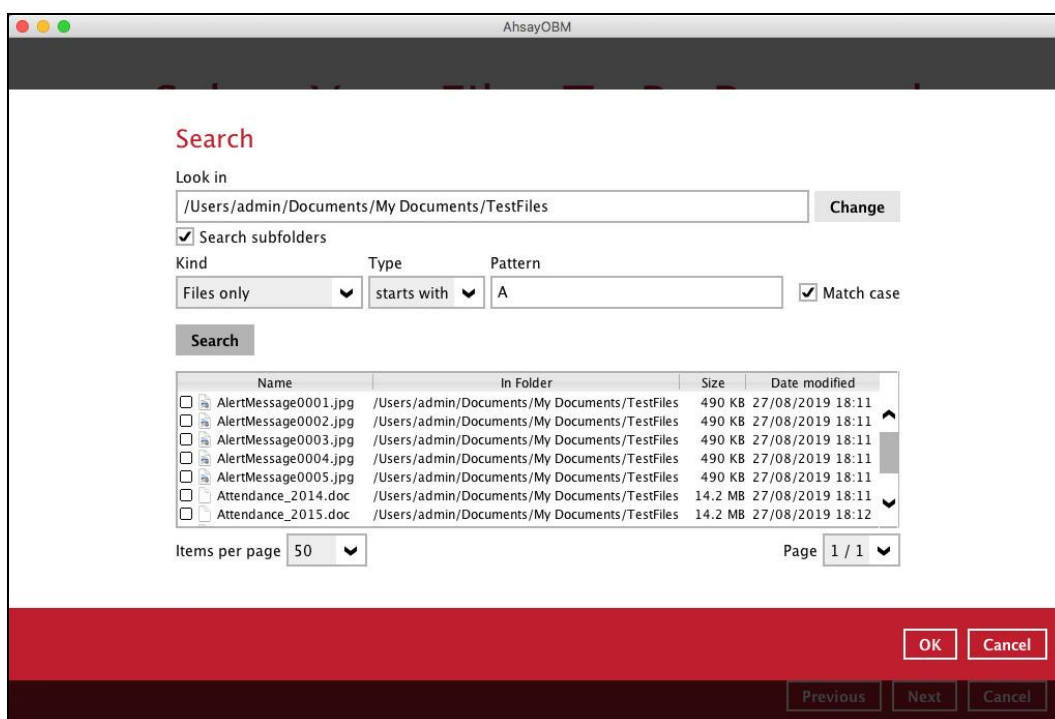
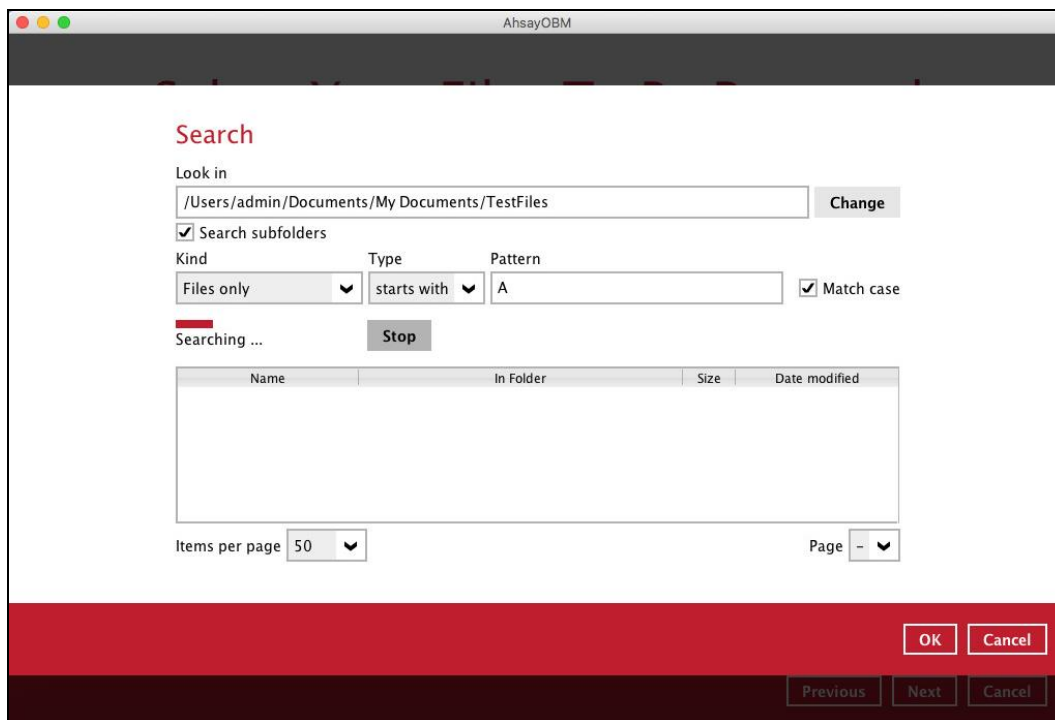
| | |
|--------------------|---|
| Location: | /Users/admin/Documents/My Documents/TestFiles |
| Search subfolders: | True |
| Kind: | Files |
| Type: | Starts With |
| Pattern: | A |
| Match Case: | True |

Follow the step-by-step procedure indicated on [Restore Filter](#).

The screenshot shows the AhsayOBM Search dialog box. The title bar reads 'AhsayOBM'. The main area is titled 'Search' in red. Below the title, there are several input fields and checkboxes:

- Look in:** A text field containing '/Users/admin/Documents/My Documents/TestFiles' with a 'Change' button to its right.
- Search subfolders:** A checked checkbox.
- Kind:** A dropdown menu set to 'Files only'.
- Type:** A dropdown menu set to 'starts with'.
- Pattern:** A text field containing 'A'.
- Match case:** A checked checkbox.

Below these settings is a 'Search' button. Underneath the button is a table with the following headers: 'Name', 'In Folder', 'Size', and 'Date modified'. The table body is currently empty. At the bottom left of the table area, there is a label 'Items per page' followed by a dropdown menu set to '50'. At the bottom right, there is a label 'Page' followed by a dropdown menu set to '-'. At the very bottom of the dialog, there is a red bar containing 'OK' and 'Cancel' buttons. Below this bar, there is a dark bar containing 'Previous', 'Next', and 'Cancel' buttons.



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. This means that the filter will include all available subfolders in `/TestFiles` upon searching. And it will strictly search only the specified pattern and case which starts with 'A'.

Example No.3: Restore filter setting from /Users/admin/Documents/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](#).

Search

Look in
/Users/admin/Documents/My Documents/TestFiles Change

☒ Search subfolders

Kind: Files and Directories ▼ Type: ends with ▼ Pattern: g ▼ ☒ Match case

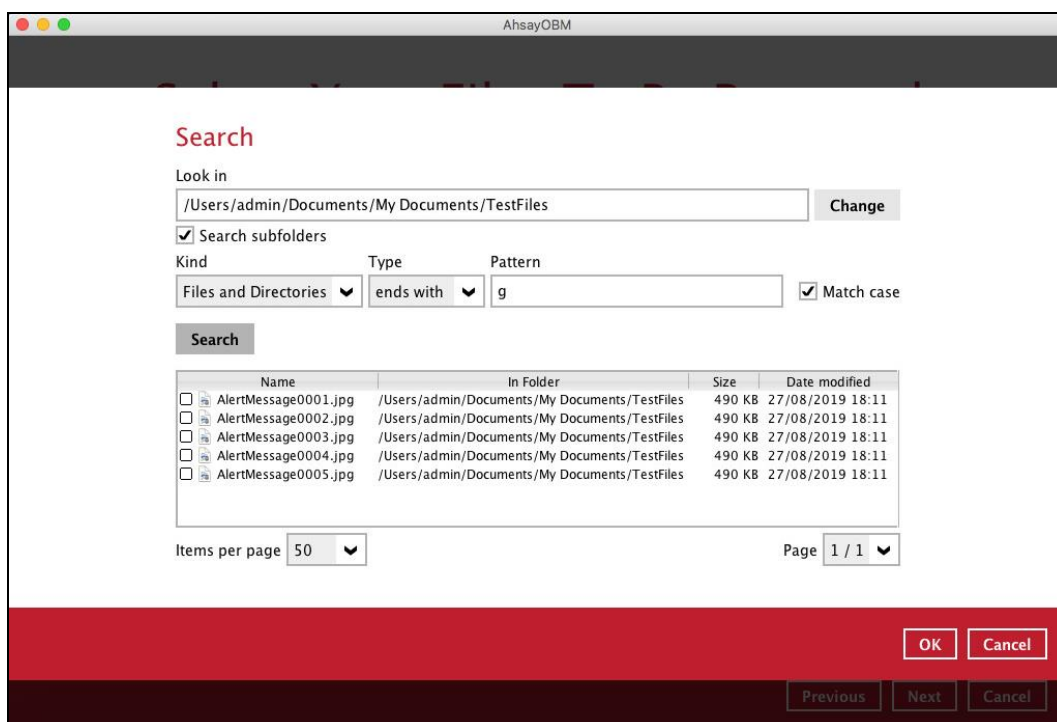
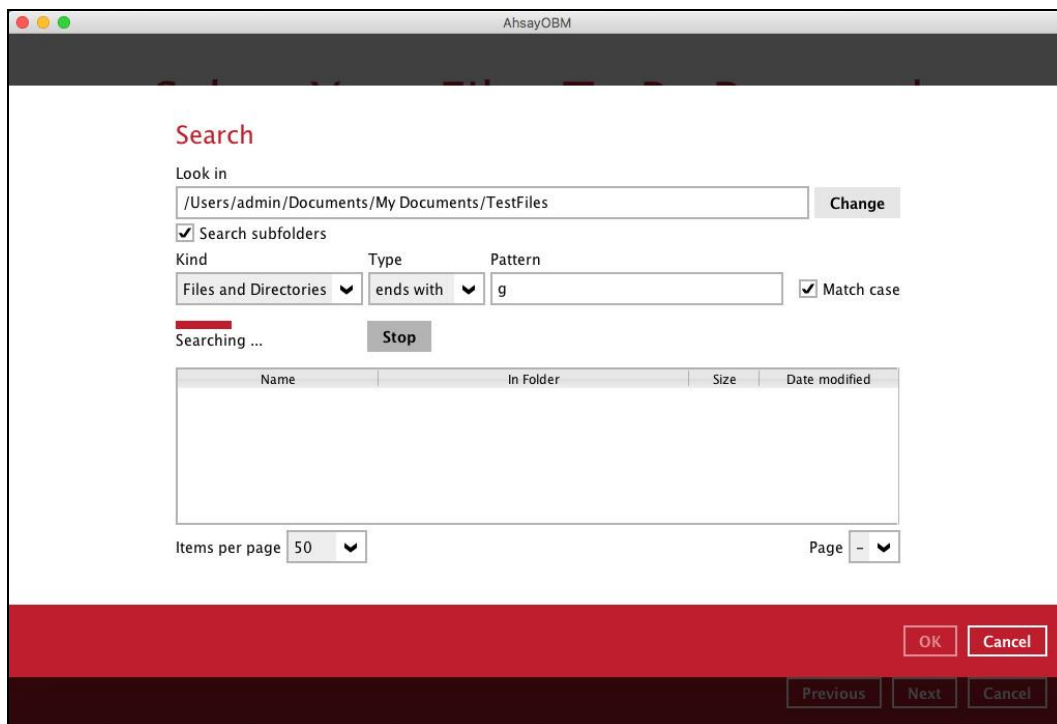
Search

| 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 ends with 'g' with match case set to true will be included upon performing search.

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

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

Example No.4: Restore filter setting from /Users/admin/Documents/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](#).

AhsayOBM

Search

Look in
 Change

☒ Search subfolders

Kind Type Pattern

☒ Match case

Search

| Name | In Folder | Size | Date modified |
|------|-----------|------|---------------|
|------|-----------|------|---------------|

Items per page Page

OK Cancel

Previous Next Cancel

Search

Look in: Change

☒ Search subfolders

Kind: Files and Directories Type: exact Pattern: ☒ Match case

Searching ... Stop

| Name | In Folder | Size | Date modified |
|------|-----------|------|---------------|
|------|-----------|------|---------------|

Items per page: 50 Page: -

OK Cancel

Previous Next Cancel

Search

Look in: Change

☒ Search subfolders

Kind: Files and Directories Type: exact Pattern: ☒ Match case

Search

| Name | In Folder | Size | Date modified |
|--|---|------|------------------|
| <input type="checkbox"/> SpreadSheet_05.xlsx | /Users/admin/Documents/My Documents/TestFiles | 8 KB | 27/08/2019 18:15 |

Items per page: 50 Page: 1 / 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.

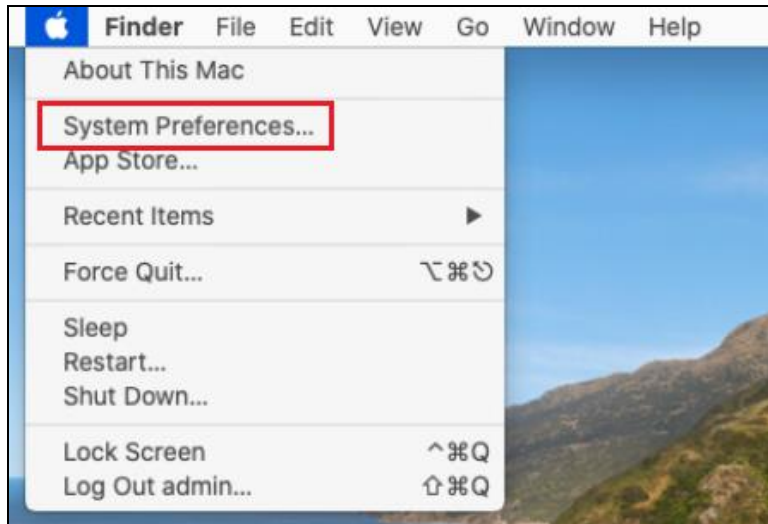
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in /TestFiles upon searching. And it will strictly search only the specified pattern and case which starts with 'SpreadSheet_05.xlsx'.

Appendix C: Setting up Full Disk Access Permission

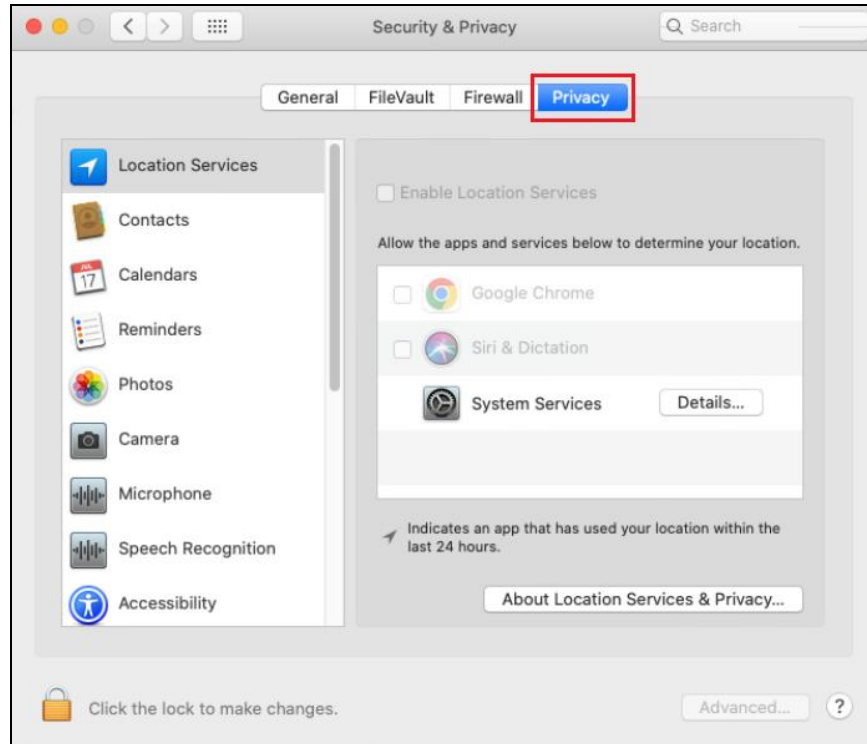
What is Full Disk Access? Full Disk Access is a new security feature in macOS 10.15 or higher that requires some applications to be given full permission to access your protected files and have certain administrative settings available.

Here are the steps on how to setup and grant AhsayOBM and java Full Disk Access:

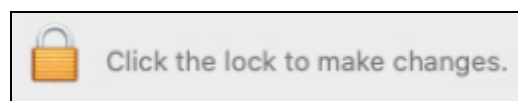
1. Open **System Preferences > Security & Privacy**.



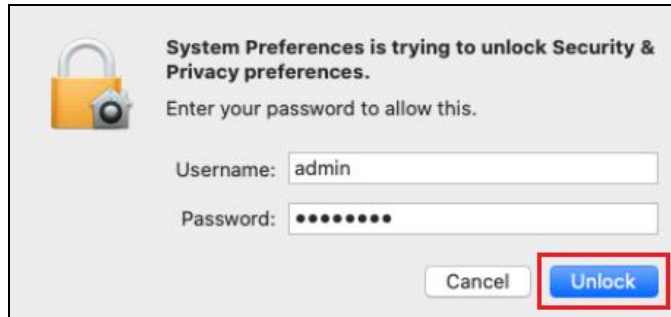
2. Select the **Privacy** tab.



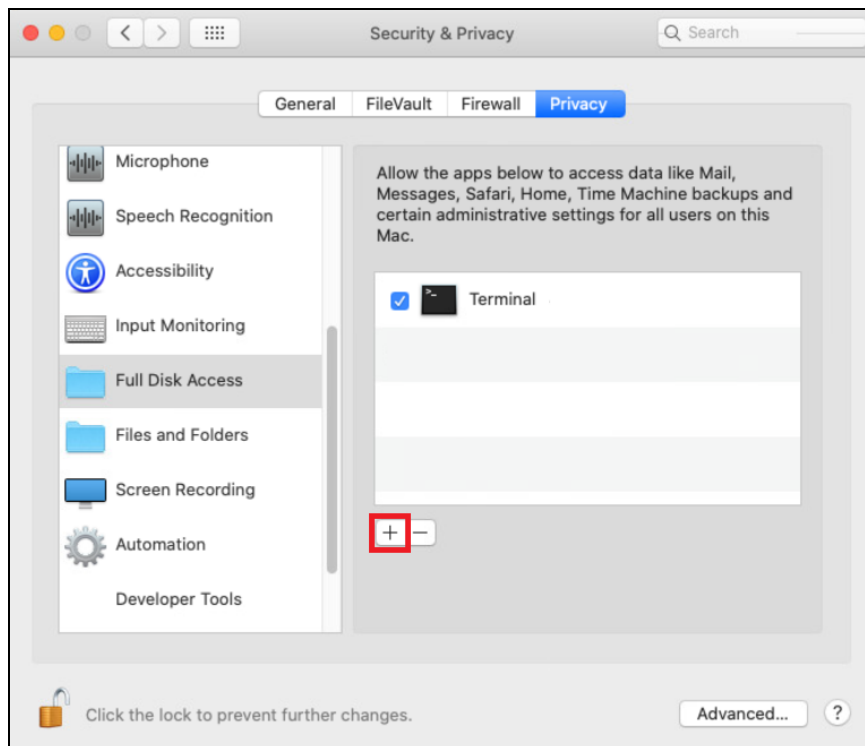
3. Select **Full Disk Access**, then click the lock icon.



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

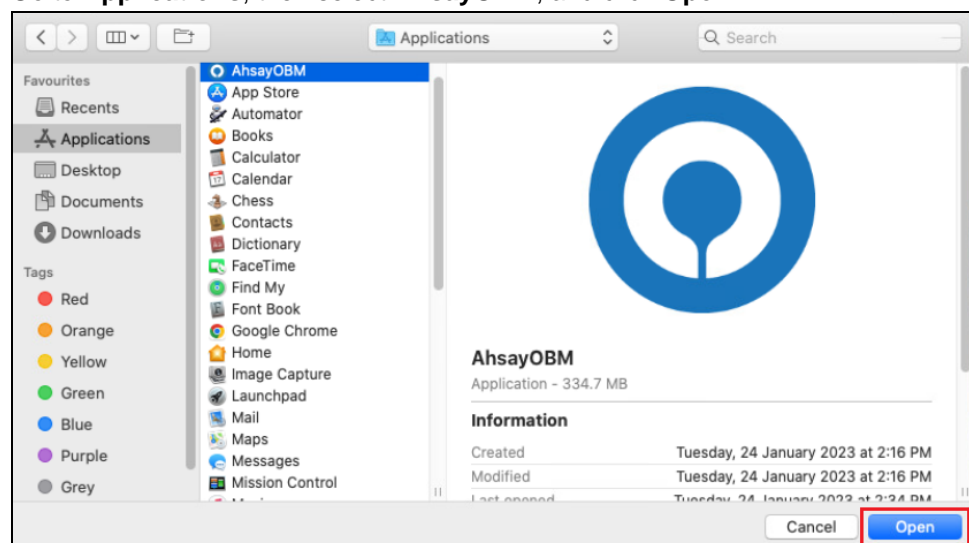


5. Click the **+** icon.

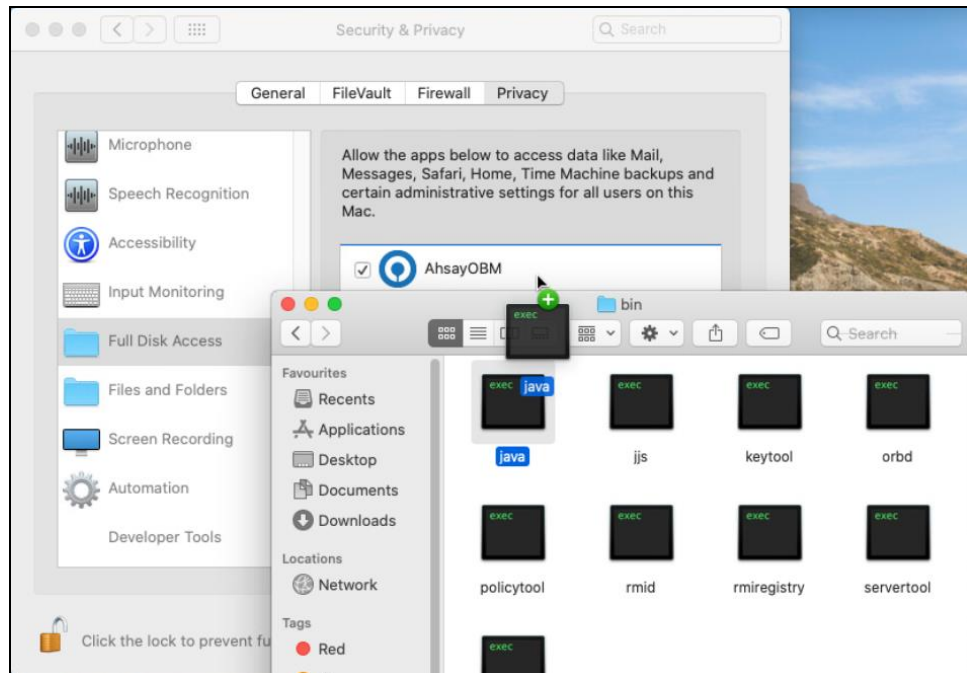


6. Add the following:

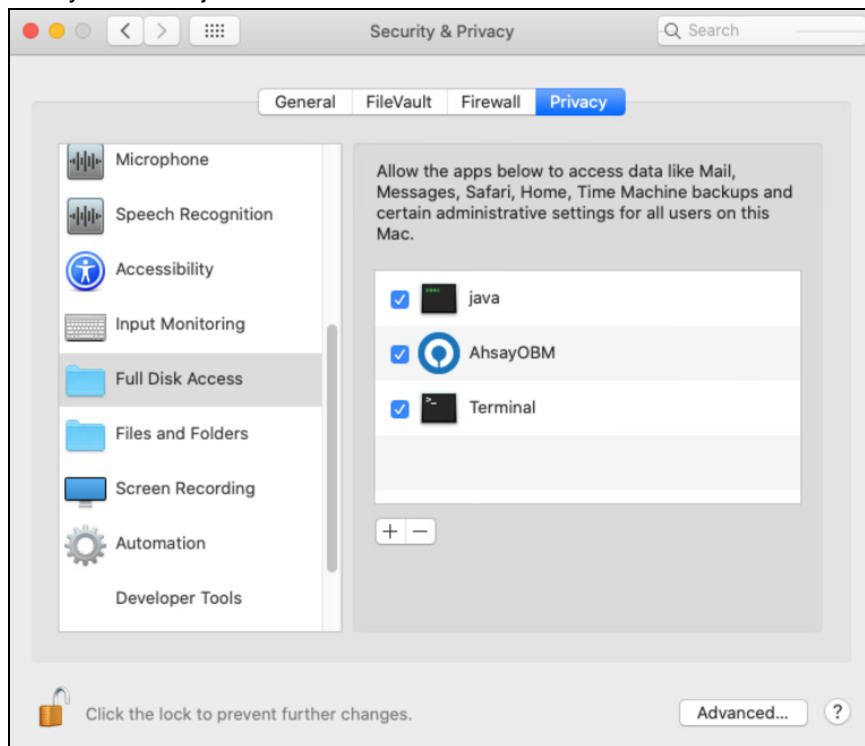
- Go to **Applications**, then select **AhsayOBM**, and click **Open**.



- To add java open **Applications > AhsayOBM > jvm > bin**, then drag **java** to the Full Disk Access window.



7. AhsayOBM and java now have Full Disk Access.



Appendix D: Create Free Trial Account in AhsayOBM

Users can create a free trial account when they login to AhsayOBM for the first time. Please ensure that the following requirements are met before creating your trial account:

- A valid email address which will be used for receiving notices. A welcome message will also be sent upon creation of the account which specifies the User Setting and Quota set for backup in AhsayCBS.

While here are the limitations of a trial account:

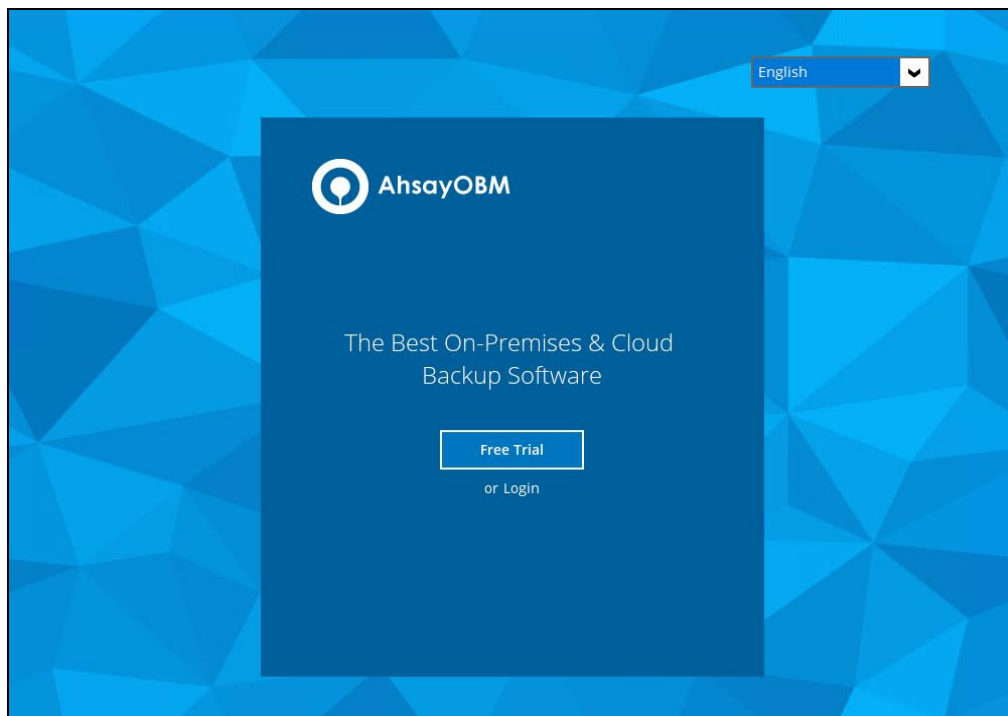
- The Free Trial button will only be displayed once when the user login for the first time. If you cannot create a free trial account kindly contact your backup service provider.
- Only alphanumeric characters and selected special characters, A to Z, 0 to 9, @, - and _, are allowed to be used for the Login name. While there may be some limitations on password complexity and age which is determined by the backup service provider. Please contact your backup service provider for further details.
- The add-on modules available and quota size are determined by your backup service provider.
- The trial account period is determined by your backup service provider. Please contact your backup service provider for details.

NOTE

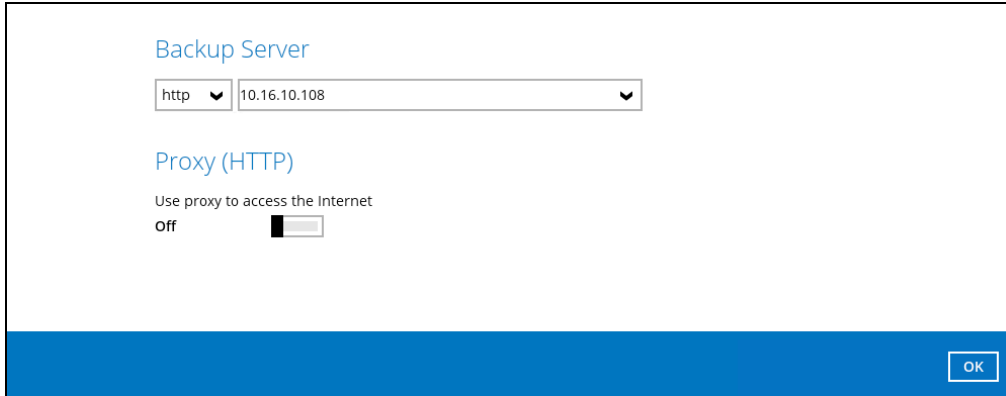
The Free Trial Registration option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

Follow the steps below to create a Free Trial backup account in AhsayOBM.

1. Click on **Free Trial**.

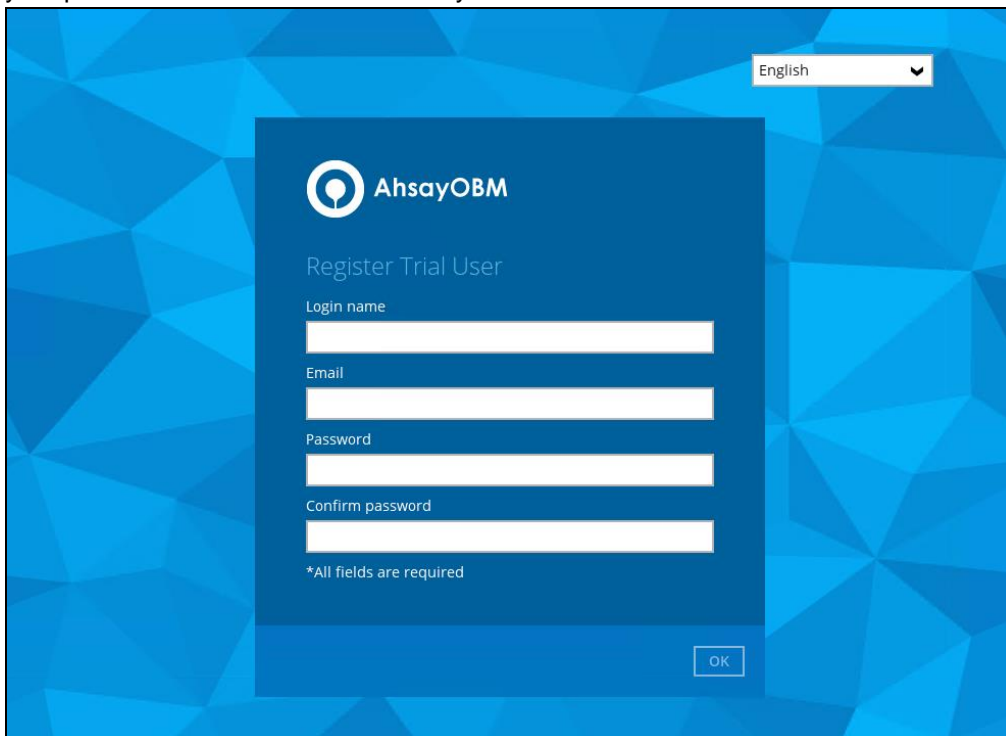


2. Configure your Backup Server settings.



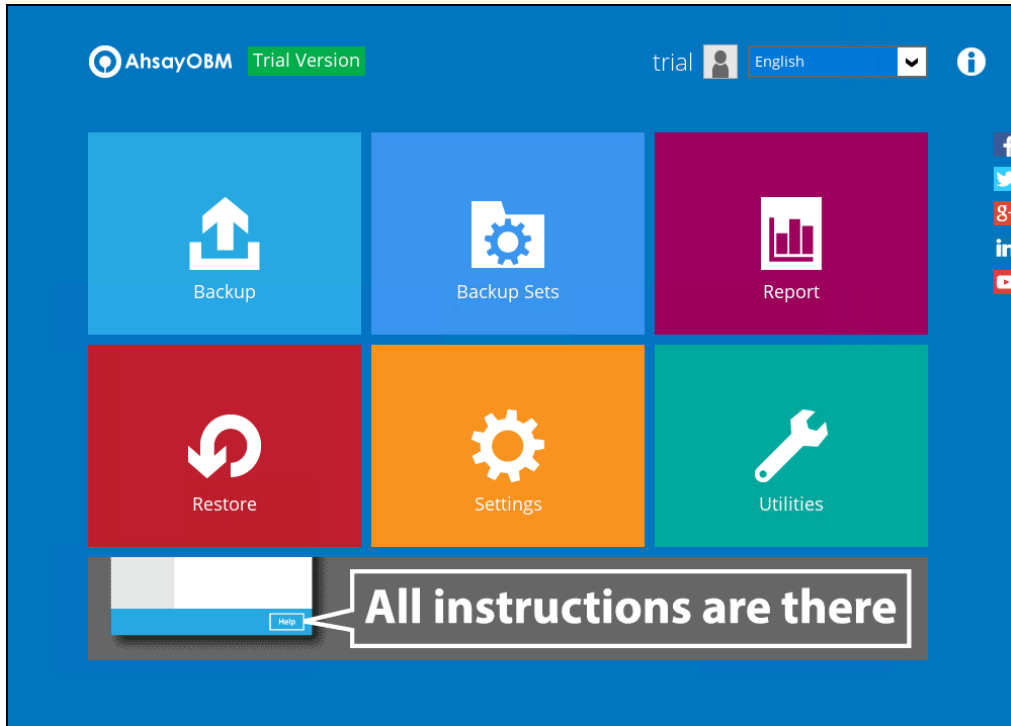
The screenshot shows a configuration window titled "Backup Server". It contains two dropdown menus: the first is set to "http" and the second is set to "10.16.10.108". Below these is a section titled "Proxy (HTTP)" with the text "Use proxy to access the Internet" and a toggle switch labeled "off". An "OK" button is located in the bottom right corner of the window.

3. Enter the Login name that you want. Also provide your email address and password. Confirm your password and click **OK** to create your trial account.



The screenshot shows the "Register Trial User" window in AhsayOBM. The window has a blue background with a geometric pattern. It features the AhsayOBM logo and the title "Register Trial User". There are four input fields labeled "Login name", "Email", "Password", and "Confirm password". Below the fields is a note that says "*All fields are required". An "OK" button is located in the bottom right corner of the window. A language dropdown menu in the top right corner is set to "English".

4. Once the trial account is created, this screen will be displayed.



5. If the user has input their email at **Step 3**, they will periodically receive an email notification(s) about the changes to their trial account such as backup report(s), or when the expiration date of their trial period is approaching in less than 10 days.

Below is an example of the trial expiration email.

