Ahsay Backup

Ahsay Online Backup Manager v8

Quick Start Guide for Windows

Ahsay Systems Corporation Limited

4 November 2021

A wholly owned subsidiary of
Ahsay Backup Software Development Company Limited
HKEx Stock Code: 8290

Copyright Notice

© 2021 Ahsay Systems Corporation Limited. All rights reserved.

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

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

Trademarks

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

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

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

Dropbox is a registered trademark of Dropbox Inc.

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

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

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

MariaDB is a registered trademark of MariaDB Corporation AB.

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

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

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

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

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

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

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

Ubuntu is a registered trademark of Canonical Ltd.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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

Disclaimer

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

Revision History

Date	Descriptions	Type of modification
7 April 2021	Updated Ch. 10; Added sub-chapters for the detailed process diagrams in Ch. 10.1, 10.2, 10.2.1, 10.2.2 and 10.3	New / Modifications
30 April 2021	Updated Ch. 8.6.3; Added new diagrams for the detailed process of Data Integrity Check (DIC) and updated screenshots for the Rebuild index option in Ch. 8.9.1; Updated description of Space Freeing Up in Ch. 8.9.2; Updated description of Delete Backup Data in Ch. 8.9.3; Added notes for Periodic Data Integrity Check (PDIC) in Ch. 10.1	New / Modifications
25 May 2021	Added requirements in Ch. 3.10; Updated Ch. 6.1, 6.2.1 and Ch. 6.2.2; Updated screenshots of the Profile menu in Ch. 8.1.1 to 8.1.7; added Mobile Backup in Ch. 8.8.3	New / Modifications
18 June 2021	Added notes on free trial registration and save password options in Ch. 7.1, 7.2, 7.3, 8.1.5, 8.1.6 and Appendix E	New
9 August 2021	Updated windows user authentication discussion in Ch. 8.5	Modification
4 November 2021	Added 2FA registration steps in Ch. 7; Modified login steps to AhsayOBM in Ch. 8; Added unable to login with 2FA scenario in Ch. 9; Modified screenshots and added Re-pair with authenticator feature in Ch. 10.1.6; Updated screenshots, added browse files and change location in Ch. 10.8.3	New / Modifications

Table of Contents

1 Overview 1

1.1 What is this software? 1

1.2 System Architecture 1

1.3 Mobile Backup Server 2

1.4 Two-Factor Authentication 5

2 Requirements for Ahsay Mobile app 7

2.1 Backup Software Version Requirement 7

2.2 Network Connection 7

2.3 Android and iOS Version Requirement 7

3 Requirements for AhsayOBM on Windows 8

3.1 Hardware Requirements 8

3.2 Software Requirements 8

3.3 Antivirus Exclusion Requirement 8

3.4 Upgrade VMware Tools Requirement 8

3.5 Temporary Directory Requirements 9

3.6 Network Drive Requirements 9

3.7 Firewall Settings 9

3.8 Two-Factor Authentication Requirements 9

3.9 Mobile Backup Requirements 9

3.10 Network Bandwidth 9

3.11 Limitations 9

Enhanced Network Drive Support 9

3.12 Best Practices and Recommendations 10

3.12.1 Periodic Backup Schedule 10

3.12.2 Set up of both Periodic and Continuous Backup Schedule 10

3.12.3 Periodic Backup Schedule vs. Continuous Backup Schedule 10

3.12.4 Temporary Directory Folder Location 11

4 Get Started with AhsayOBM 12

5 OpenDirect Restore 13

5.1 What is OpenDirect Restore? 13

5.2 How does OpenDirect Restore work? 14

5.3 Benefits of using OpenDirect Restore 15

5.4 Requirements 16

5.4.1 Supported Backup Modules 16

5.4.2 License Requirements 16
5.4.3 Backup Quota Storage 16
5.4.4 Windows Operating System 16
5.4.5 Available Spare Drive Letter 16
5.4.6 Network Requirements 16
5.4.7 Other Dependencies 17
5.4.8 Permissions 17
6 Download and Install AhsayOBM 18
6.1 Download AhsayOBM 19
6.2 Install AhsayOBM 20
6.2.1 Online Installation using EXE online installer 20
6.2.2 Offline Installation using ZIP offline installer 26
6.3 AhsayOBM Services 32
6.4 Mobile Backup Server (MBS) Status Check and Ahsay Mobile app Connection Check 34
7 Register device for 2FA in AhsayOBM 36
7.1 Using Ahsay Mobile Authenticator 36
7.1.1 Without Mobile Add-on Module 36
7.1.2 With Mobile Add-on Module 49
7.2 Using Microsoft Authenticator 55
7.3 Using Google Authenticator 63
8 Logging in to AhsayOBM 70
8.1 Login to AhsayOBM without 2FA 70
8.2 Login to AhsayOBM with 2FA using Ahsay Mobile Authenticator 71
8.3 Login to AhsayOBM with 2FA using Microsoft Authenticator 76
8.4 Login to AhsayOBM with 2FA using Google Authenticator 79
8.5 Login to AhsayOBM with 2FA using Twilio 81
9 Unable to log in to AhsayOBM with 2FA 84
10 AhsayOBM Overview 86
10.1 Profile 87
10.1.1 General 87
10.1.2 Contacts 89
10.1.3 Time Zone 91
10.1.4 Encryption Recovery 92
10.1.5 Password 92
10.1.6 Authentication 94
10.1.7 Security Settings 103

10.2 Language 104
10.3 Information 104
10.4 Backup 105
10.5 Backup Sets 105
Backup Set Settings 106
10.6 Report 160
10.6.1 Backup 160
10.6.2 Restore 164
10.6.3 Usage 168
10.7 Restore 170
10.8 Settings 170
10.8.1 Proxy 170
10.8.2 Windows Event Log 172
10.8.3 Mobile Backup 173
10.9 Utilities 183
10.9.1 Data Integrity Check 183
10.9.2 Space Freeing Up 200
10.9.3 Delete Backup Data 203
10.9.4 Decrypt Backup Data 209
10.10 Online Help 212
10.11 System Tray 213
11 Create a Backup Set 219
12 Overview on the Backup Process 230
12.1 Periodic Data Integrity Check (PDIC) Process 231
12.2 Backup Set Index Handling Process 233
12.2.1 Start Backup Job 233
12.2.2 Completed Backup Job 234
12.3 Data Validation Check Process 235
13 Run Backup Jobs 236
13.1 Login to AhsayOBM 236
13.2 Start a Manual Backup 236
14 Restore Data 239
14.1 Restore Method 239
14.1.1 Traditional Restore 239
14.1.2 OpenDirect Restore 247
14.2 Restore Filter 252
15 Mobile Backup and Restore to AhsayCBS and Predefined Destination ... 257

15.1 Create a File Backup Set 257
15.2 Run a Backup Job 267
15.3 Restore Data 270
15.3.1 Original Location 271
15.3.2 Alternate Location 278
16 Contact Ahsay 286
16.1 Technical Assistance 286
16.2 Documentation 286
Appendix 287
Appendix A: Uninstall AhsayOBM 287
Appendix B: Example Scenarios for Restore Filter 290
Appendix C: Batch Files 299
RunCB.bat 299
RunConfigurator.bat 305
ListBackupSet.bat 309
RunBackupSet.bat 310
ListBackupJob.bat 316
Restore.bat 319
Decrypt.bat 325
RunDataIntegrityCheck.bat 331
Appendix D: Example Scenarios for the Reminder 336
Windows Log Off 336
Windows Restart 337
Windows Shutdown 338
Scenario 1 (Windows Log Off + Enabled Locking Workstation) 339
Scenario 2 (Windows Log Off + Unselected Locking Workstation) 340
Scenario 3 (Windows Restart + Enabled Locking Workstation) 341
Scenario 4 (Windows Restart + Unselected Locking Workstation) 342
Scenario 5 (Windows Shutdown + Enabled Locking Workstation) 343
Scenario 6 (Windows Shutdown + Unselected Locking Workstation) 344
Appendix E: Create Free Trial Account in AhsayOBM 345
Appendix F: How to Manage Network Drives which are not set in Windows 349

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.

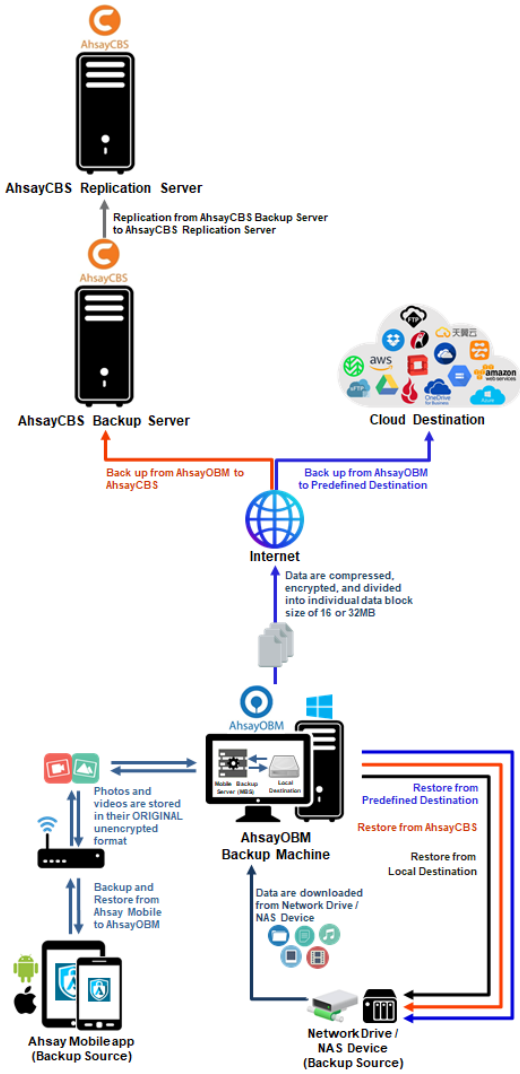
1.2 System Architecture

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.

NOTE

The first mobile backup may take up a few hours to back up all the photos and videos from your device. Subsequent backups will take less time. Please do the following for the first mobile backup to prevent any interruption during backup process:

- For Android, disable screen lock or timeout
- For iOS, disable auto-lock
- Turn off all power saving modes
- Connect to power source



1.3 Mobile Backup Server

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

System Diagram

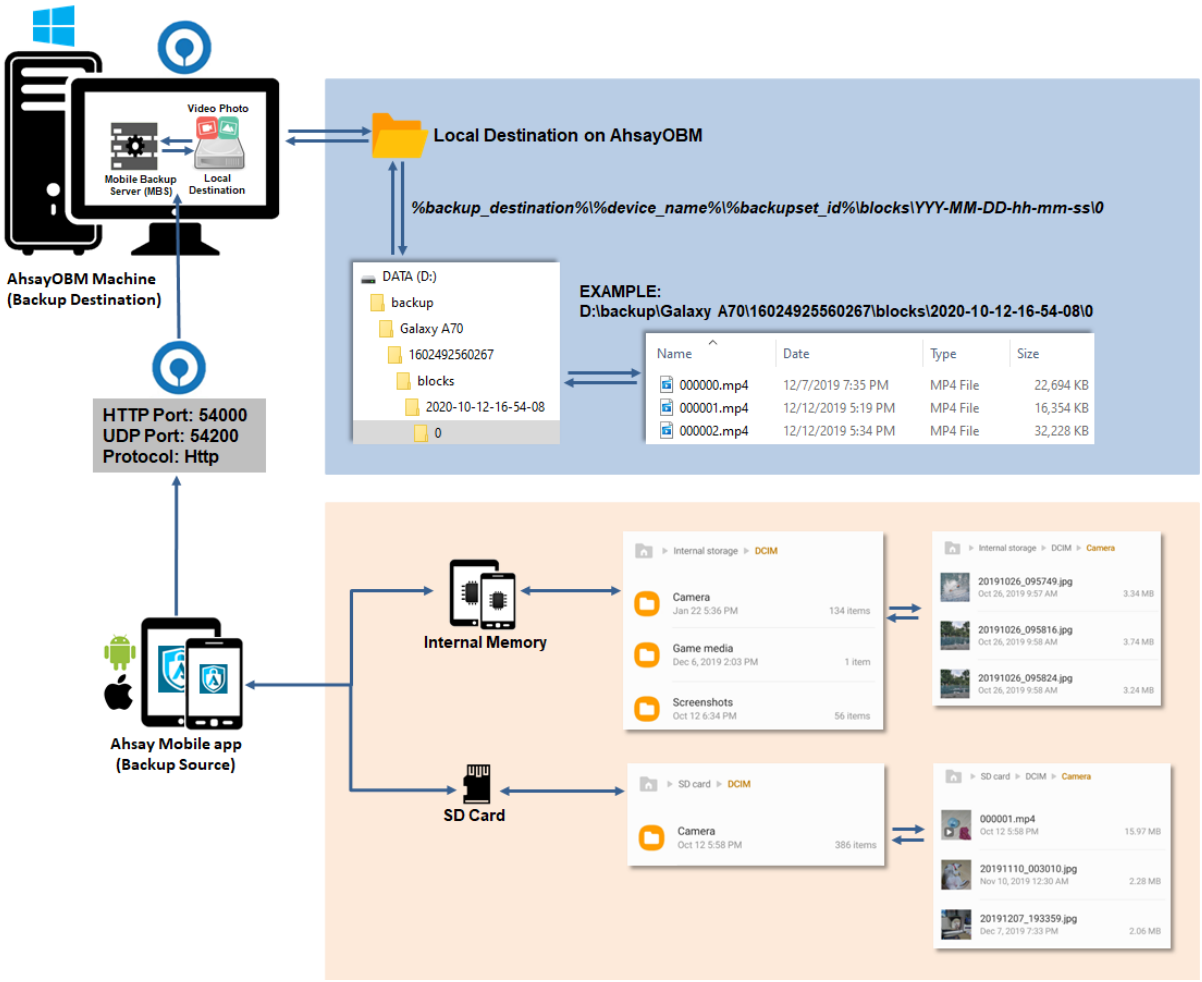
The Mobile Backup Server (MBS) will be activated automatically when a mobile device installed with the Ahsay Mobile app is successfully registered for mobile backup with AhsayOBM. Afterwards, it will be automatically restarted whenever the AhsayOBM services is restarted or when the AhsayOBM machine is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

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

The default TCP and UDP ports are **54000** and **54200**, if these ports are already in use by other applications or services, then the MBS will automatically acquire another port.

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

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

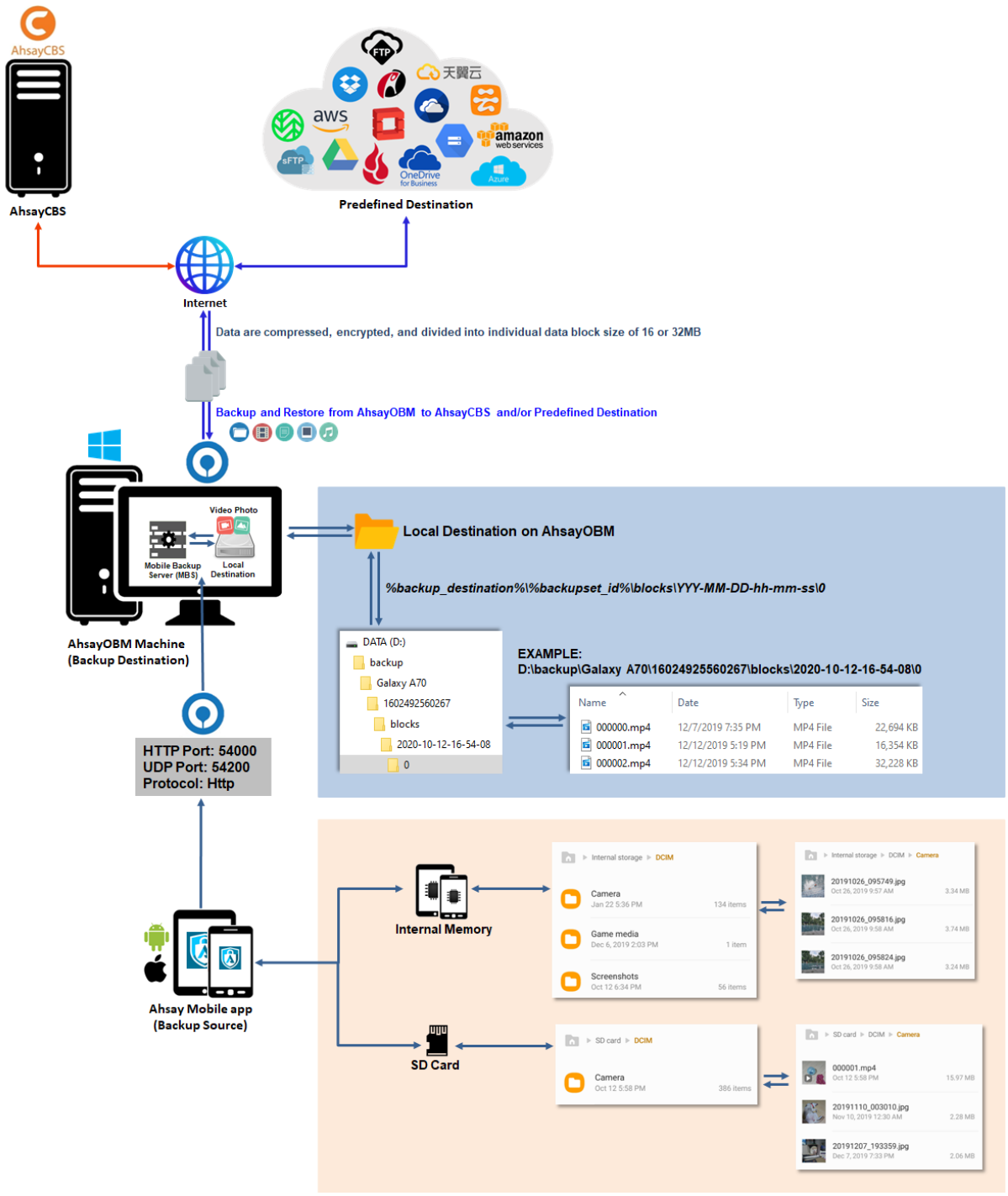


If storage of photos and videos to a predefined destination is required, then this can be done using AhsayOBM to perform a secondary backup and restore of the photos and videos on the local drive to the predefined destination.

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

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

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

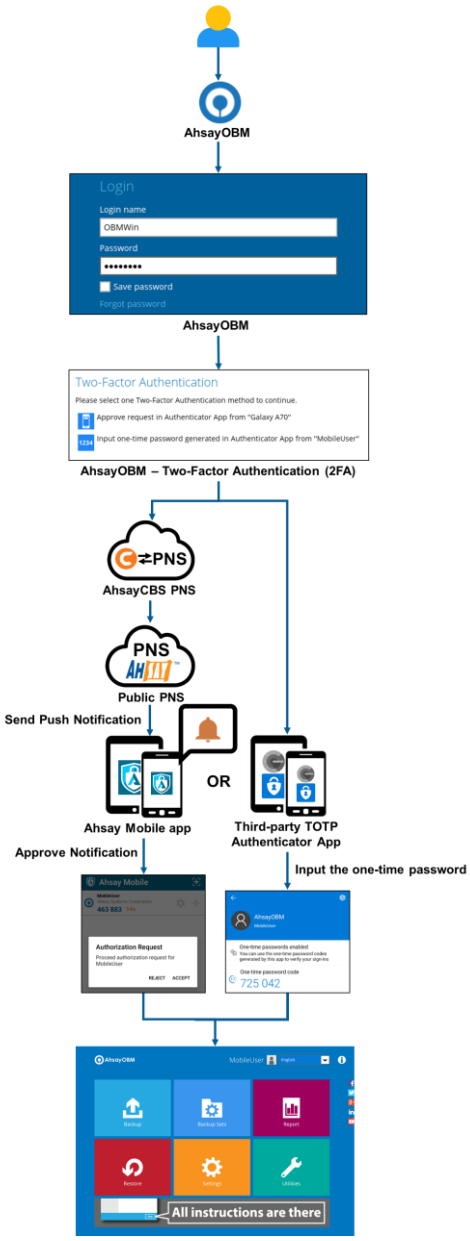


1.4 Two-Factor Authentication

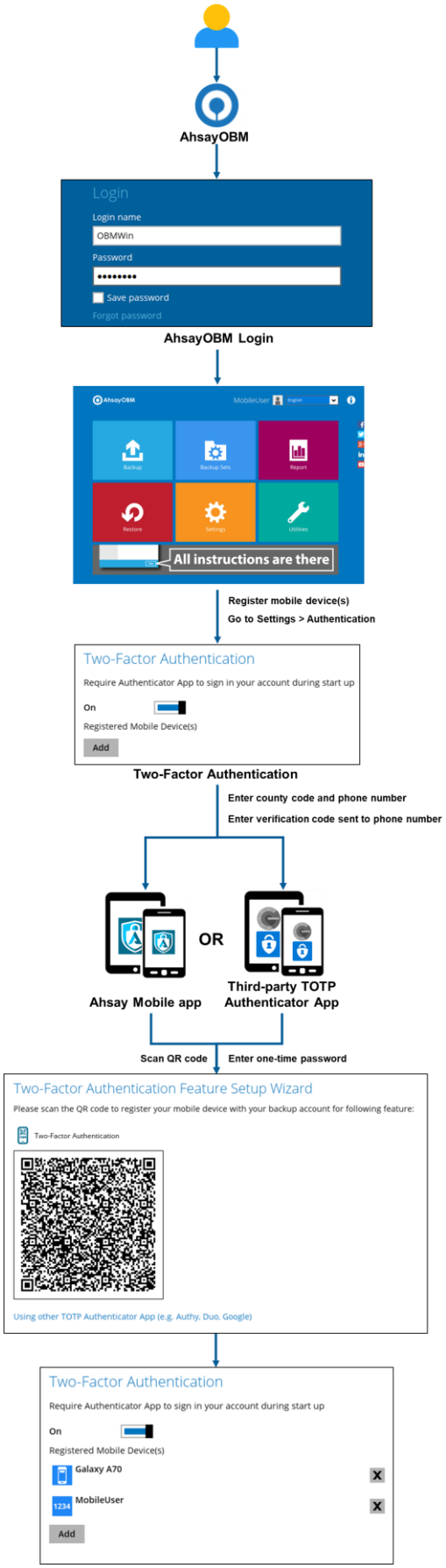
New two-factor authentication implemented on AhsayOBM v8.5.0.0 onwards, to include support for TOTP (Time-based One-time Password) and Push notification authentication using the Ahsay Mobile app to provide additional security for the user login process. Since aside from logging in with just a username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

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

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



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



2 Requirements for Ahsay Mobile app

2.1 Backup Software Version Requirement

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

2.2 Network Connection

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

2.3 Android and iOS Version Requirement

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

3 Requirements for AhsayOBM on Windows

3.1 Hardware Requirements

Refer to the link below for details of the minimum and recommended requirements for installing AhsayOBM:
FAQ: Ahsay Hardware Requirement List (HRL) for version 8.1 or above

3.2 Software Requirements

Refer to the following article for the list of compatible operating systems and Hyper-V platforms:
FAQ: Ahsay Software Compatibility List (SCL) for version 8.1 or above

Refer to the following article for the list of compatible operating system for OpenDirect and Granular Restore:
FAQ: Ahsay Software Compatibility List (SCL) for Granular and OpenDirect Restore

3.3 Antivirus Exclusion Requirement

To optimize performance of AhsayOBM on Windows, and to avoid conflict with your antivirus software, refer to the following wiki article the list of processes and directory paths that should be added to all antivirus software white-list / exclusion list:
https://wiki.ahsay.com/doku.php?id=public:8014_suggestion_on_antivirus_exclusions

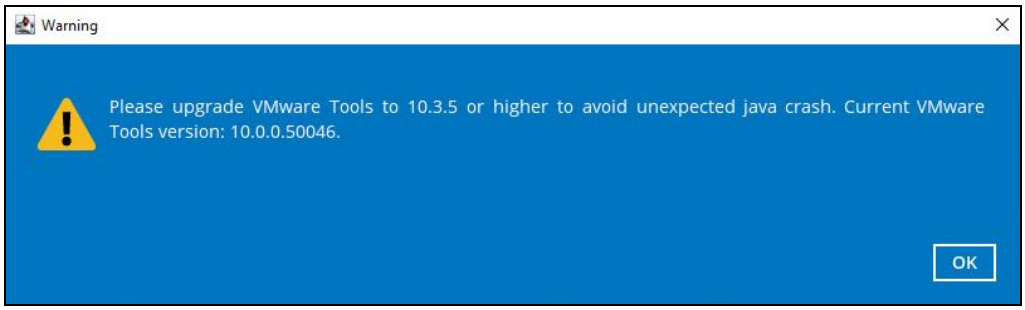
NOTE
The bJW.exe process is automatically added to Windows Defender exclusion list for Windows 10 and 2016 / 2019, during installation / upgrade via installer or upgrade via AUA.

For mobile backups, the mobile backup destination must also be added to all antivirus software white-list / exclusion list.

3.4 Upgrade VMware Tools Requirement

To avoid unexpected java crash, if the Windows machine is a guest VM hosted on a VMware Host then it is highly recommended that the VMware tools version installed on the guest VM must be 10.0.5 or above.

Below is the warning message that will be displayed if the version of the VMware Tools is less than 10.0.5.



NOTE
For more information about the upgrade of VMware Tools, refer to this article https://wiki.ahsay.com/doku.php?id=public:5288_ahsayobc_crash_on_vm_with_vmware_tools_pre-10.0.5.

3.5 Temporary Directory Requirements

The temporary directory is used for various purposes, such as storage of temporary spooled file (for database specific backup type in AhsayOBM), remote file list, local file list, temporary delta file and other files of temporary nature.

It is strongly recommended to use a local drive instead of a network drive to ensure optimal backup/restore performance.

3.6 Network Drive Requirements

The login accounts for network drives must have read and write access permission to ensure that backup and restore would be successful.

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 Two-Factor Authentication Requirements

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

3.9 Mobile Backup Requirements

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

3.10 Network Bandwidth

10 Mbps or above connection speed.

3.11 Limitations

Enhanced Network Drive Support

- For network drives which have not been already setup or mapped in Windows.
- Temporary folder location is not supported with individual login credentials but can still be setup separately using existing Windows User Authentication login.
- It also does not support Pre-Backup and Post-Backup Commands.
- Not supported on “Restore Raw file” and “Restore to local computer” options.
- Not supported for mobile backup destinations.

3.12 Best Practices and Recommendations

3.12.1 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 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 backup.

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.

3.12.2 Set up of both Periodic and Continuous Backup Schedule

On a Windows platform, although it is possible to setup both Periodic backup schedule and Continuous backup schedules on a File backup sets, it is recommended to only use one schedule as only one schedule backup job can run at any one time.

For example, a backup job is started by the Periodic backup schedule and is running, if a Continuous backup is scheduled to run, the backup job will be skipped and vice versa.

3.12.3 Periodic Backup Schedule vs. Continuous Backup Schedule

The following table shows the comparison between a periodic and continuous backup schedule.

Features	Periodic Backup Schedule	Continuous Backup Schedule
Will run whether or not a change on the backup source is made		
Run Retention Policy after backup		
Exclude system files from the backup		

Only apply to files smaller than (MB) size		
Exclude Filter		
Supported on all operating systems (i.e. Windows, MacOS, Linux, FreeBSD, QNAP, and Synology)		Only supported on Windows operating system
Supports all backup set types		Only supports File Backup Sets

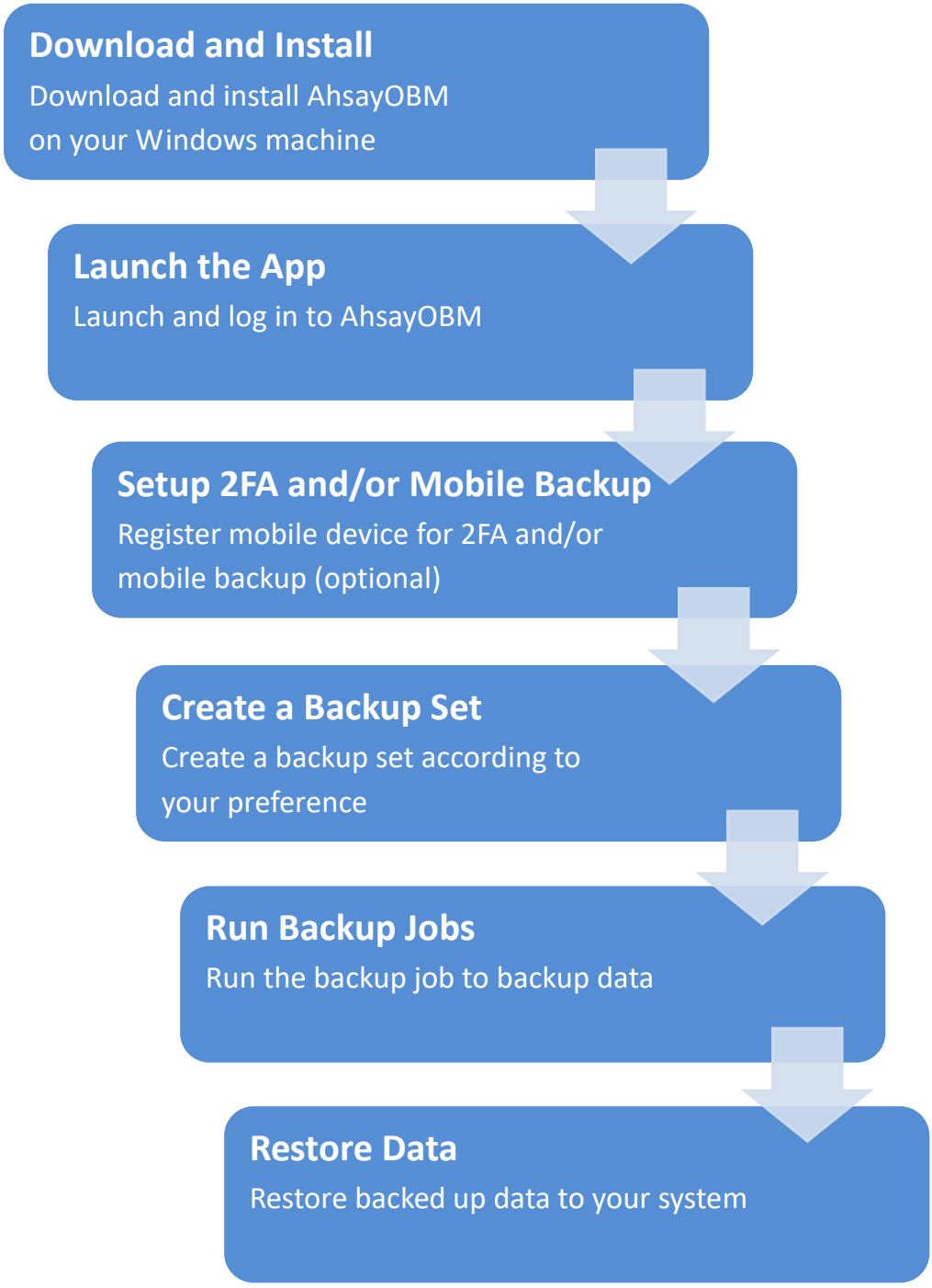
3.12.4 Temporary Directory Folder Location

Temporary directory folder is used by AhsayOBM for storing backup set index files and any incremental or differential backup files generated during a backup job.

To ensure optimal backup/restoration performance, it is recommended that the temporary directory folder is set to a local drive with sufficient free disk space.

4 Get Started with AhsayOBM

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



5 OpenDirect Restore

5.1 What is OpenDirect Restore?

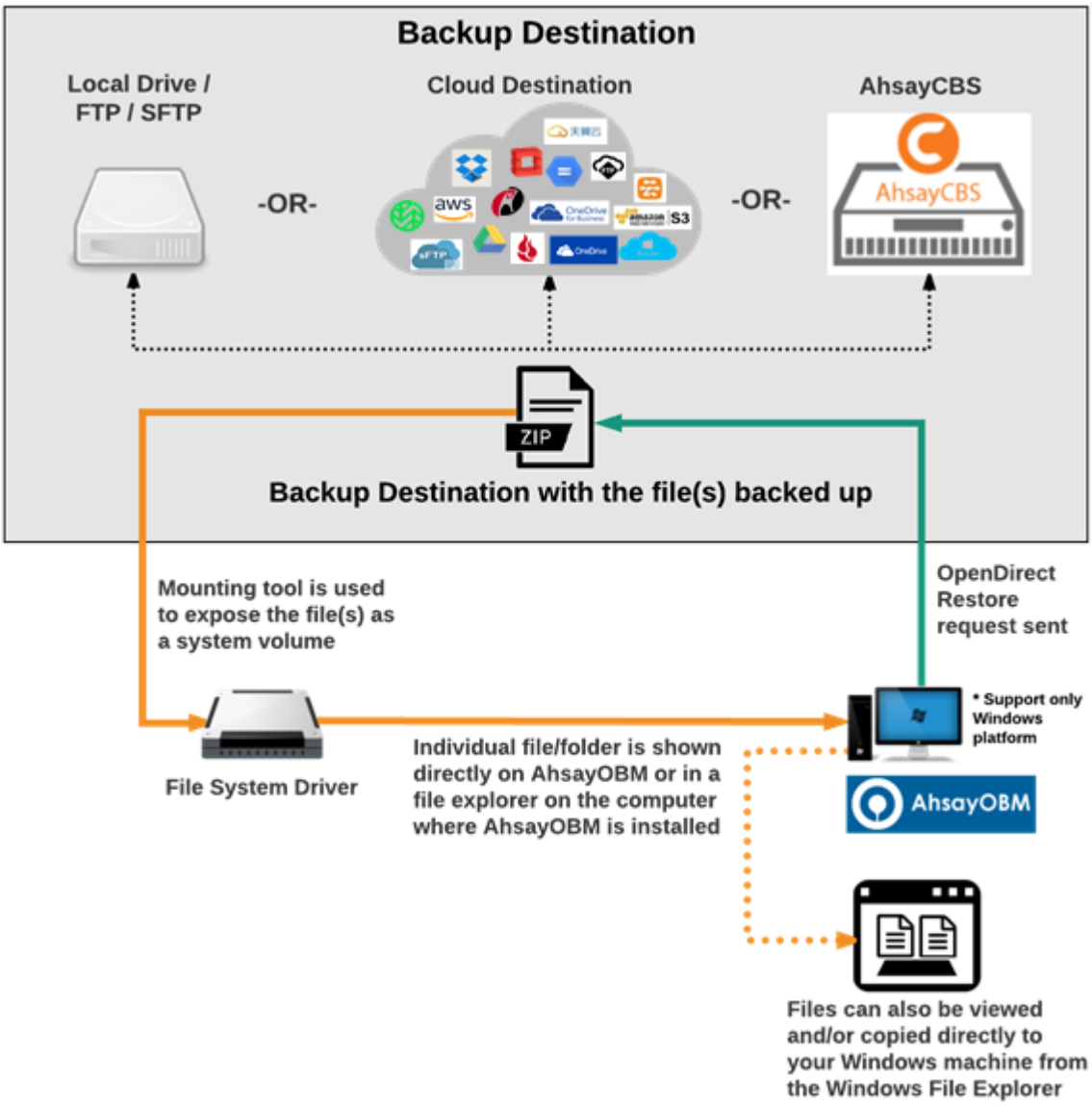
OpenDirect restore is an additional restore options for restoring files from a Windows File backup set. The OpenDirect restore method makes use of the granular restore technology to make selective restore of individual files from a large compressed or image file, for example zip, RAR, ISO files, without the need to restore the compressed or image file first, to give you a fast and convenient file restore solution.

During the OpenDirect restore process, the files/folder can be viewed and/or copied from the Windows File Explorer on the Windows machine you are performing the restore. OpenDirect restore is only supported on File backup sets created and backed up using AhsayOBM on Windows platform with OpenDirect restore feature enabled.

IMPORTANT

OpenDirect restore requires an additional OpenDirect / Granular Restore add-on module license to work. Contact your backup service provider for further details.

5.2 How does OpenDirect Restore work?



5.3 Benefits of using OpenDirect Restore

Comparison between OpenDirect File Restore and Traditional File Restore

OpenDirect Restore	
Introduction	
OpenDirect restore allows you to quickly access individual files from a large compressed or image file by viewing and/or copying files from the file explorer on the Windows you are performing the restore, without having to fully restore the whole compressed or image file first.	
Pros	
Restore of Entire Compressed File Not Required	As opposed to the traditional restore where you have to restore the entire compressed or image file first before you can access any individual file in it, OpenDirect restore allows you to view and download individual files from a compressed or image file, without having to restore compressed file or image file first.
Ability to Restore Selected Files	When restoring a large compressed or image file, sometimes, you may only need to restore individual file(s) out of the entire file, therefore, OpenDirect restore gives you the flexibility to restore selective file(s) quickly, so it saves you time and effort to achieve your restore goal.
Cons	
No Encryption and Compression	To ensure optimal restore performance, the backup of the files in an OpenDirect file backup set will **NOT** be encrypted and compressed, therefore, you may have to take these factors in consideration when selecting this restore option.

Traditional Restore	
Introduction	
The traditional restore method restores the entire compressed file or image file. Backed up data can only be accessed when complete restore is performed.	
Pros	
Backup with Compression and Encryption	Backup file(s) are compressed, therefore in smaller file size, and encrypted before being uploaded to the backup destination.
Cons	
Slower Recovery	As the entire compressed or image file must be restored before you can access any individual files, restore time could be long if the file size is large

5.4 Requirements

5.4.1 Supported Backup Modules

OpenDirect restore is only supported on File backup sets created and backed up using AhsayOBM on Windows platform with OpenDirect restore feature enabled

5.4.2 License Requirements

An OpenDirect / Granular restore add-on module license is required per backup set for this feature to work. Contact your backup service provider for more details

5.4.3 Backup Quota Storage

As compression is not enabled for OpenDirect file backup sets, to optimize restore performance the storage quota required will be higher than non-OpenDirect file backup sets. Contact your backup service provider for details

5.4.4 Windows Operating System

AhsayOBM must be installed on a 32 bit or 64-bit Windows Operating System as libraries for OpenDirect only supports Windows platform.

Windows 2008 R2 SP1 or above	Windows 2012	Windows 2012 R2
Windows 2016	Windows 7 SP1 or above	Windows 8
Windows 8.1	Windows 10	Windows 2019

5.4.5 Available Spare Drive Letter

One spare drive letter must be available on the Windows machine for the OpenDirect restore process, as the compressed file or image is mounted on Windows as a logical drive. AhsayOBM will automatically take the next available drive letter in alphabetical order for the compressed or image file.

NOTES

1. The Windows drive letters A, B, and C are not used by OpenDirect restore.
2. The OpenDirect restore assigned drive letter(s) will be released once you exit from AhsayOBM UI.

5.4.6 Network Requirements

Recommended minimum network speed is **at least 100Mbps download speed**.

The network bandwidth requirements will increase in proportion to the size of the compressed file/image and or the incremental delta chain length to ensure optimal performance. Working with limited network bandwidth may severely affect the granular restore performance.

You can use an online network speed test website (e.g., www.speedtest.net) to get an idea of the actual bandwidth of the machine

5.4.7 Other Dependencies

The following dependencies are restore-related. Therefore, they will be checked by AhsayOBM only when an OpenDirect restore is performed. Absence of these elements will not affect the backup job but would cause the restore to fail.

- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
  https://www.microsoft.com/en-us/download/details.aspx?id=48145
- Update for Universal C Runtime in Windows
  https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows
- **For Windows 7 and Windows Server 2008 R2 only**

  Microsoft Security Advisory 3033929
  https://technet.microsoft.com/en-us/library/security/3033929.aspx

5.4.8 Permissions

The Windows login account used for installation and operation of the AhsayOBM client machine requires Administrator privileges.

6 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.

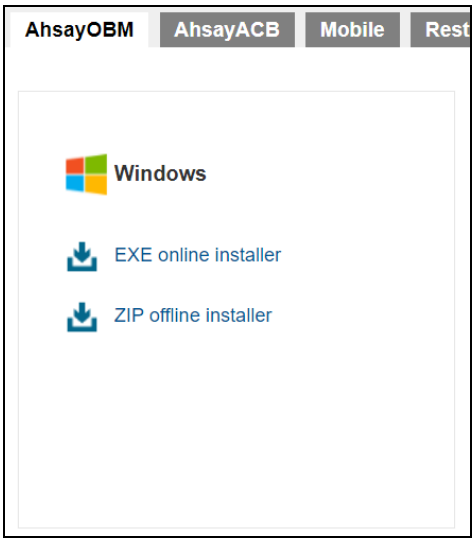
	Online Installation	Offline Installation
Installation Time	➢ Takes more time as it needs to download the binary and component files (80MB to 132MB depending on operating system) each time the installation is run. ➢ Online installer size is 6KB to 3.5MB depending on operating system as it contains only the initial installation package files.	➢ 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	➢ 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.	➢ 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.

6.1 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 **Windows** section under the **AhsayOBM** tab of the download page, you can choose between two installation methods:

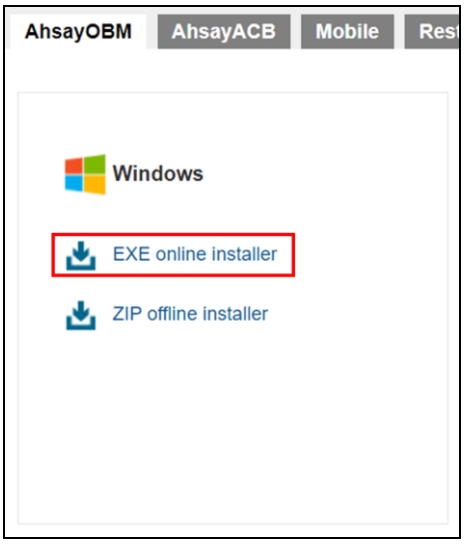
   - Online installation using EXE online installer
   - Offline installation using ZIP offline installer



6.2 Install AhsayOBM

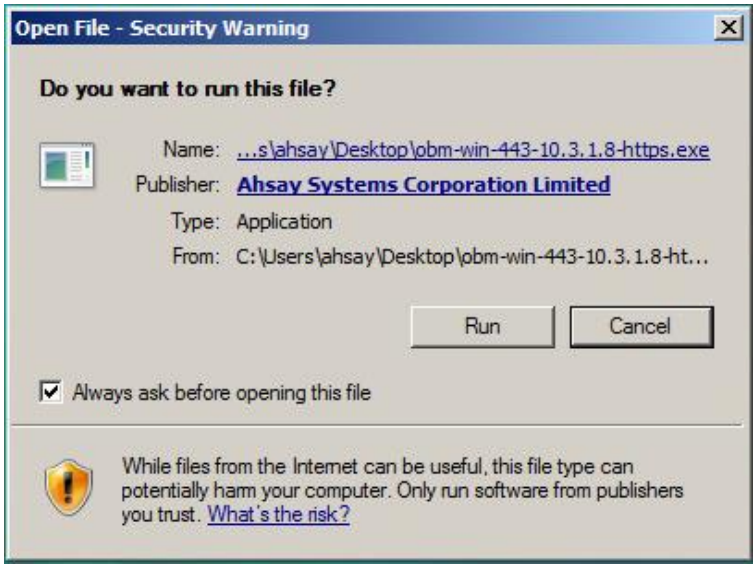
6.2.1 Online Installation using EXE online installer

1. Go to the download page of your backup service provider's website and download the AhsayOBM **EXE online installer**.

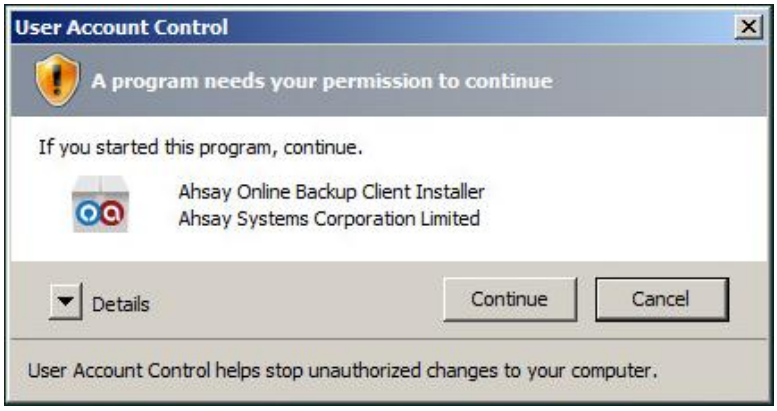


2. Double-click the icon of the AhsayOBM installation package **.exe** file you have downloaded.

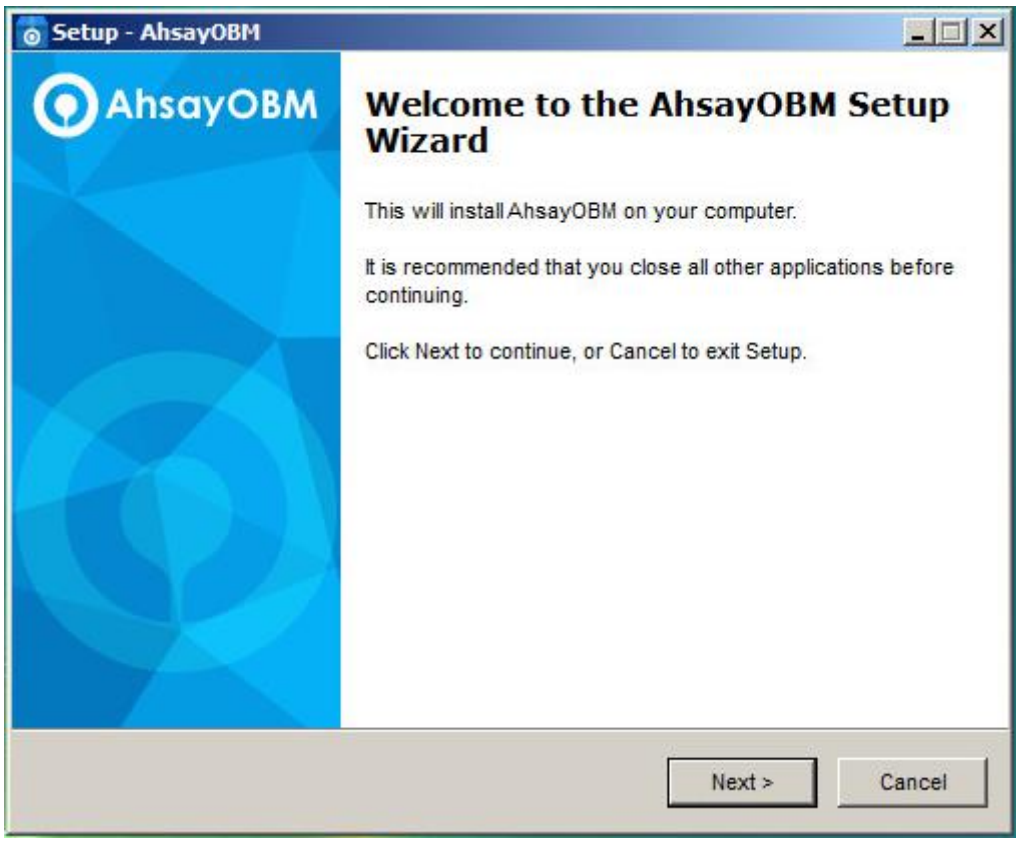
3. Click **Run** once you see the following message.



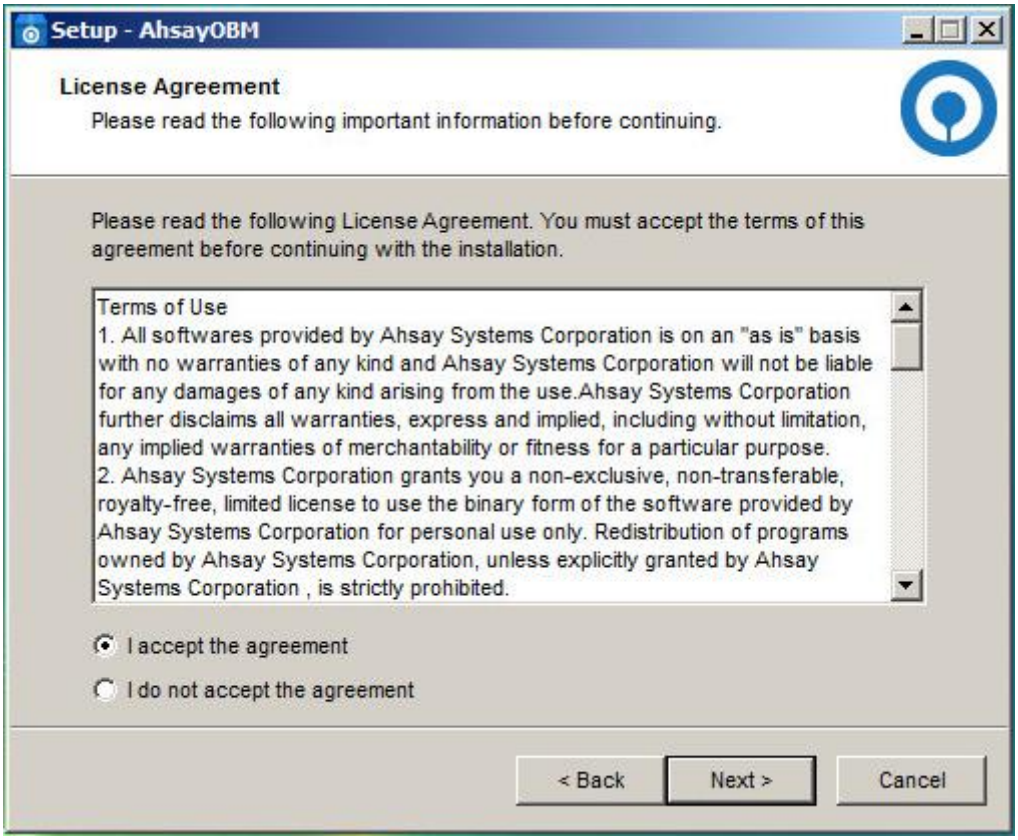
4. The following dialog box will appear only if User Account Control is enabled. Click **Continue** to start the installation.



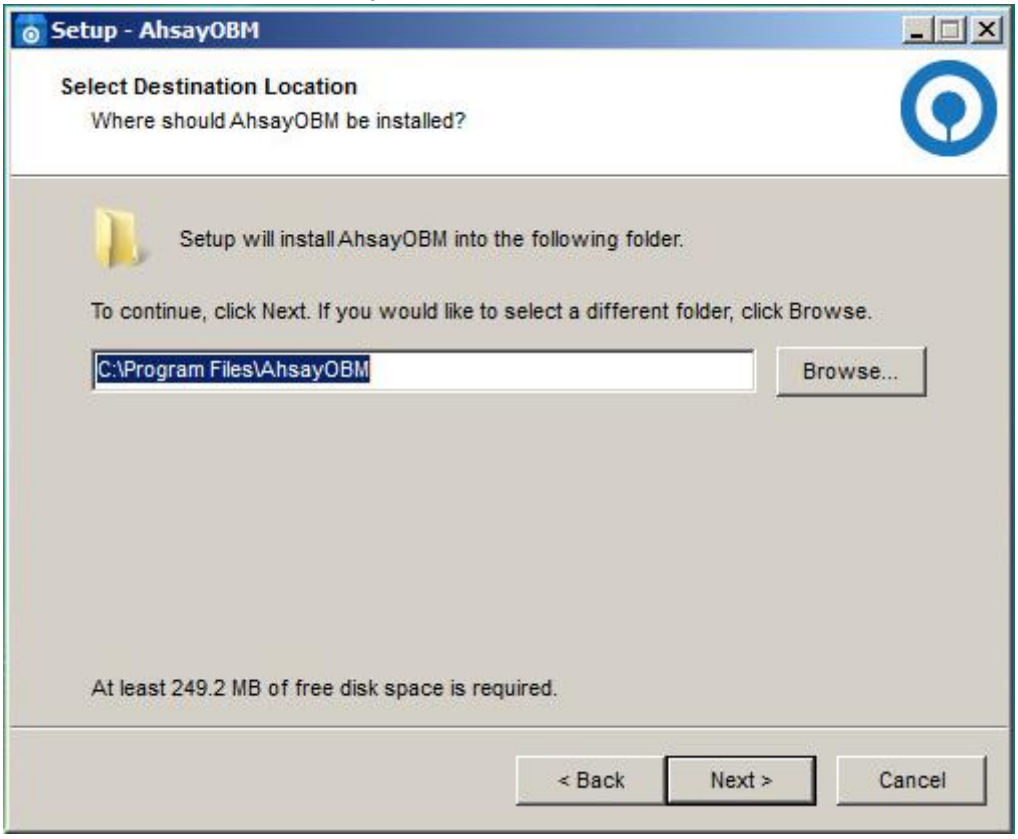
5. Click **Next** to continue.



6. Select **I accept the agreement** after reading the license agreement, then click **Next** to proceed.



7. Choose the installation directory. Then, click **Next** to continue.



8. Select the program group to which the software will be installed. The default setting is “Anyone who uses this computer”. The following are the difference between the two settings:

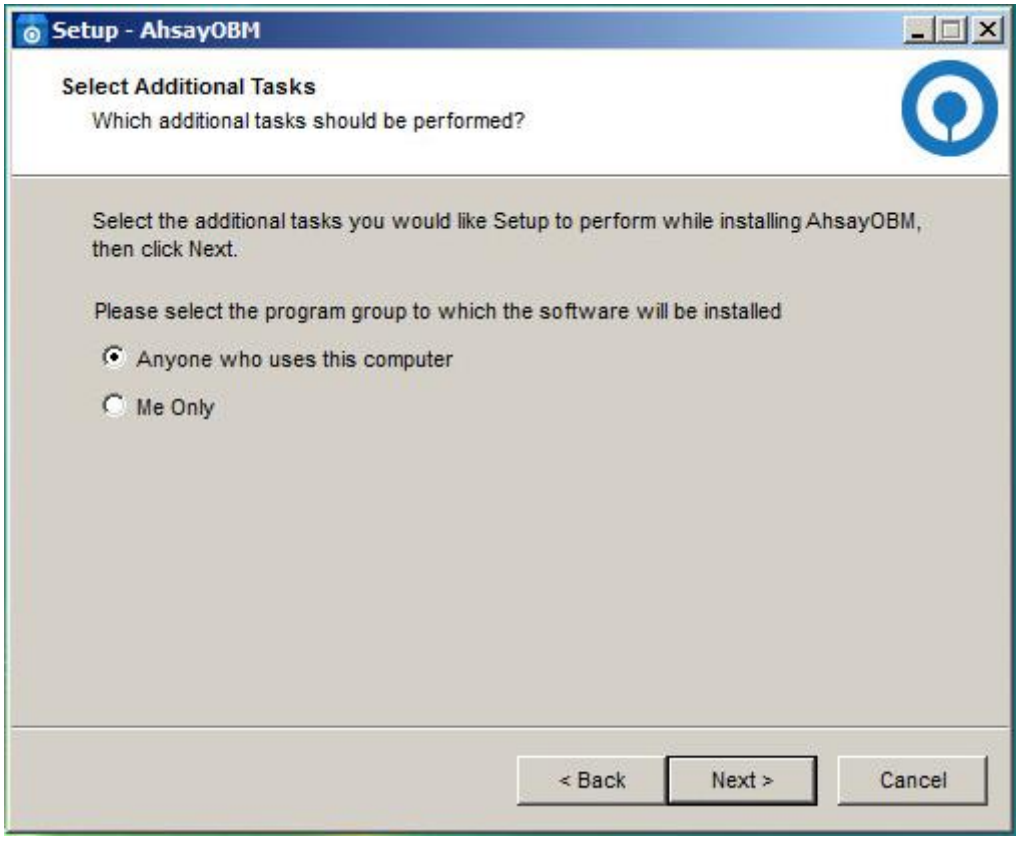
    - Anyone who uses this computer – the AhsayOBM System Tray icon will be available to all Windows users and backup notifications will be displayed on the Windows System Tray. For more information, please refer to Chapter 10.11 System Tray.

    - Me Only – the AhsayOBM System Tray icon will not be available and backup notifications will not be displayed on the Windows System Tray.

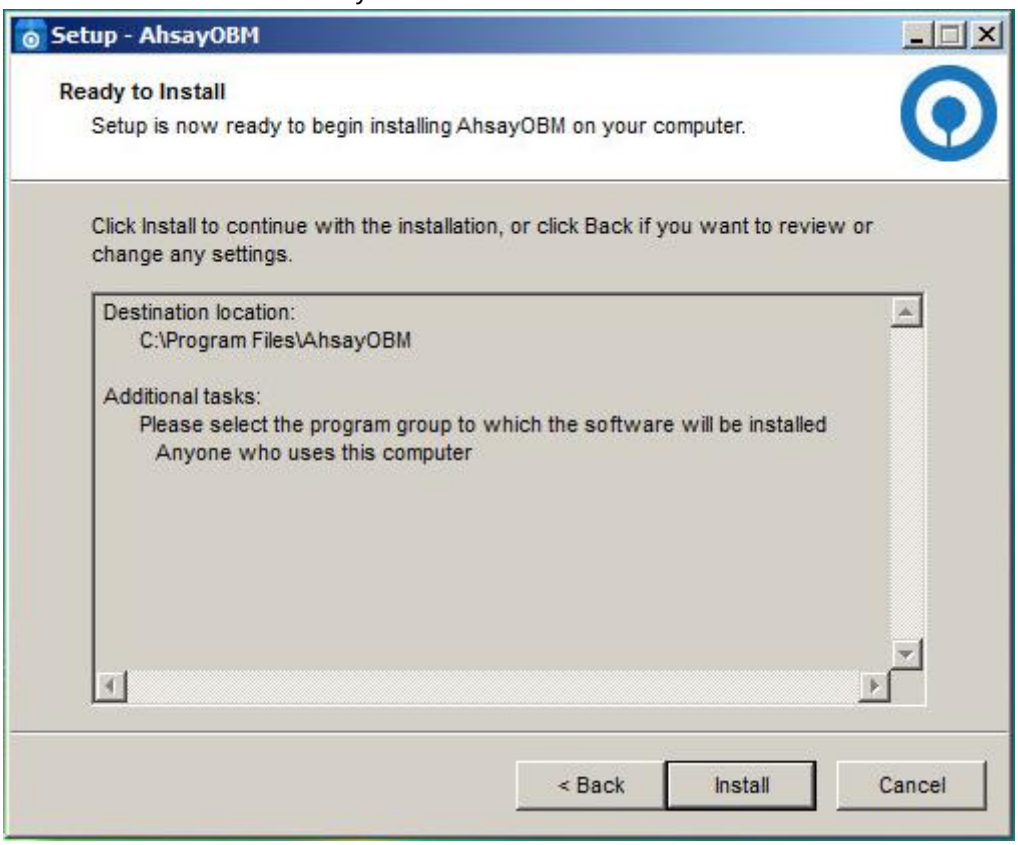
    NOTE

    Once the program group setting has been chosen and the installation completed; if you need to change the setting, this will require an uninstallation and re-installation of the application.

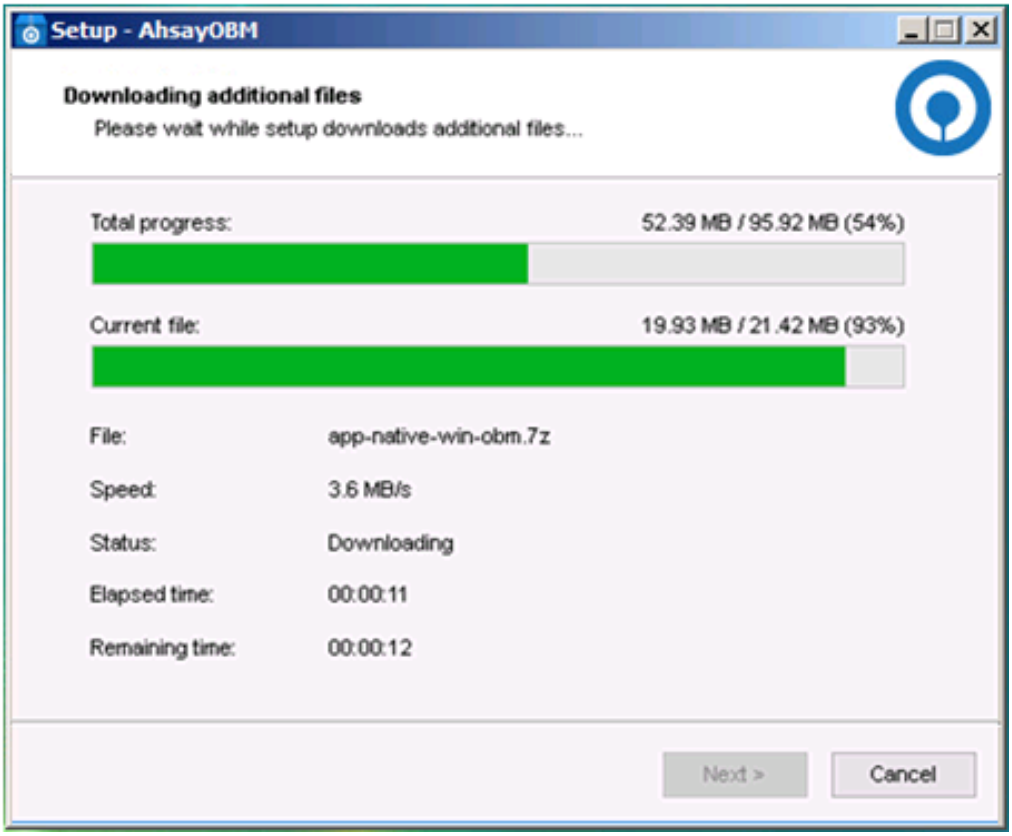
    Click **Next** to proceed.



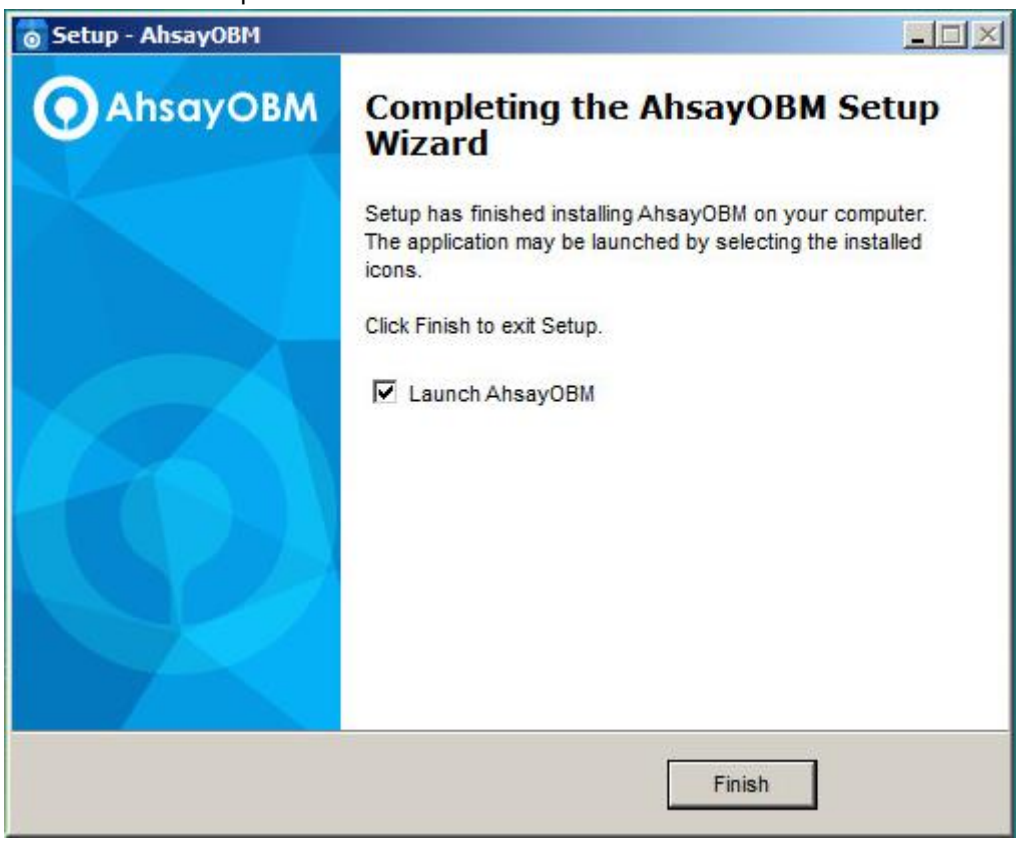
9. The installation will start after you click **Install**.



10. The component files will be downloaded first during installation.

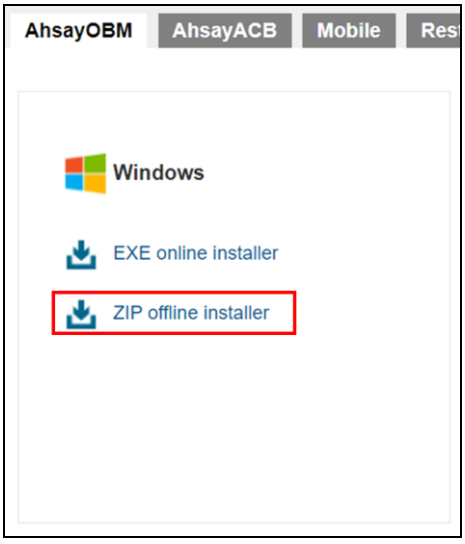


11. Click **Finish** to complete the installation.

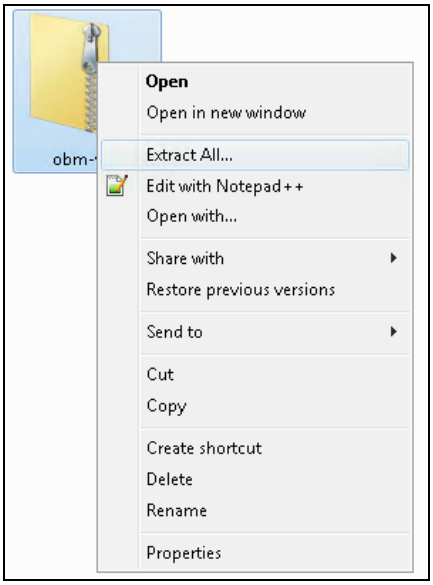


6.2.2 Offline Installation using ZIP offline installer

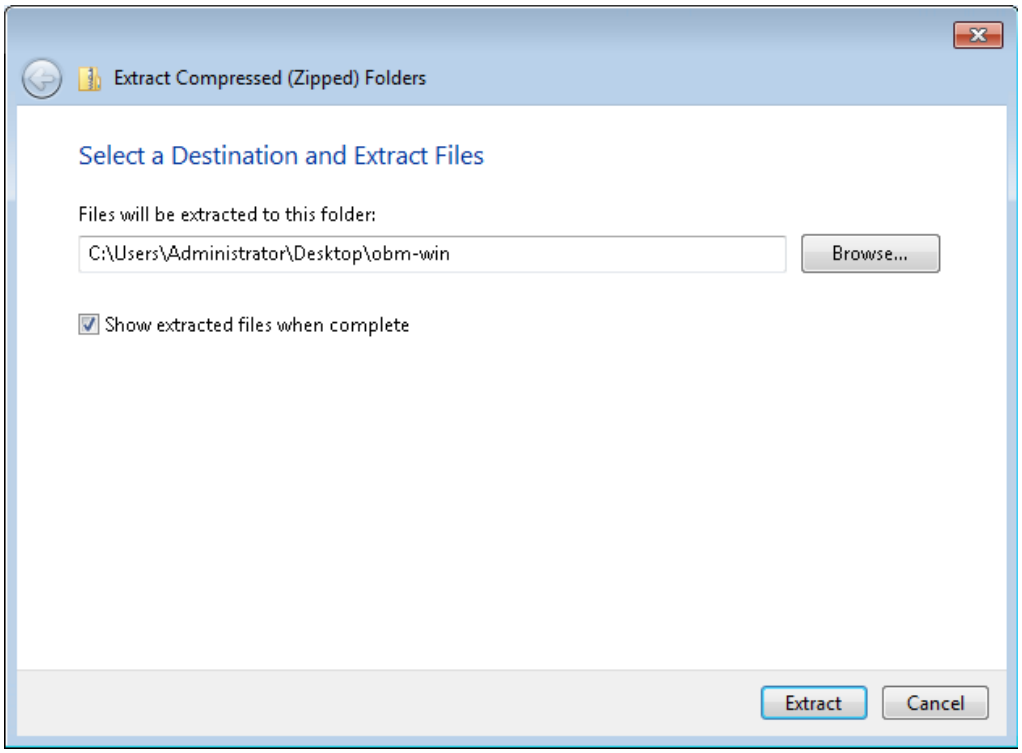
1. Go to the download page of your backup service provider's website and download the AhsayOBM **ZIP offline installer**.



2. Extract the offline installation package file (**obm-win.zip**) you have downloaded.

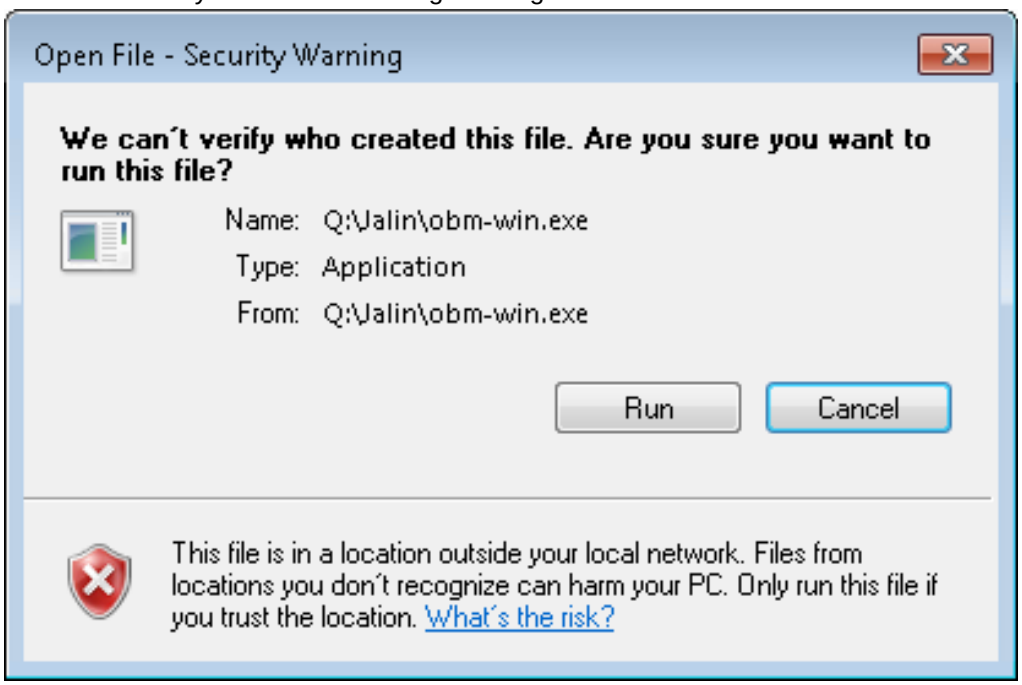


3. Select a destination and extract files.

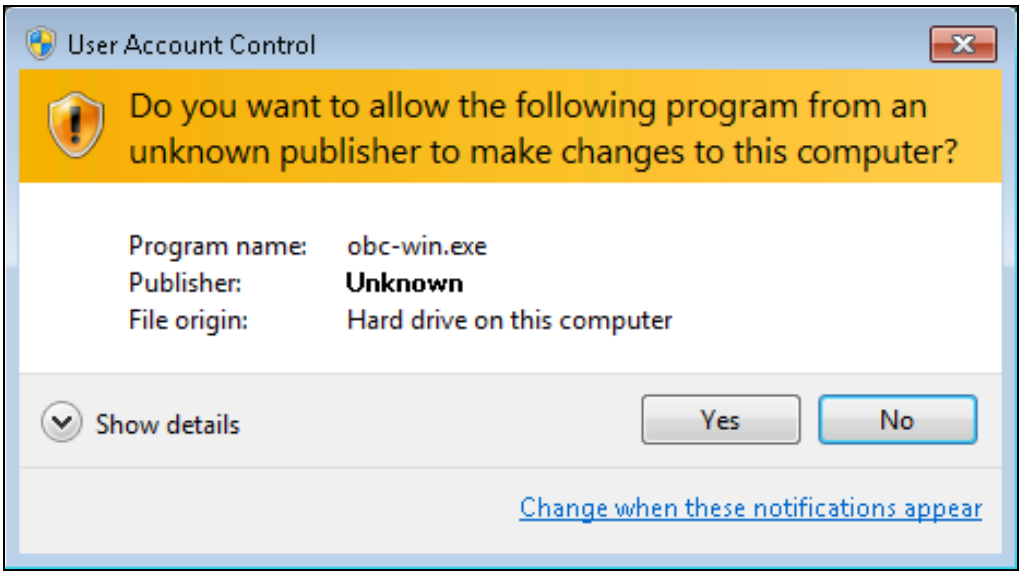


4. Launch the installer named **obm-win** you have extracted from the zip format file.

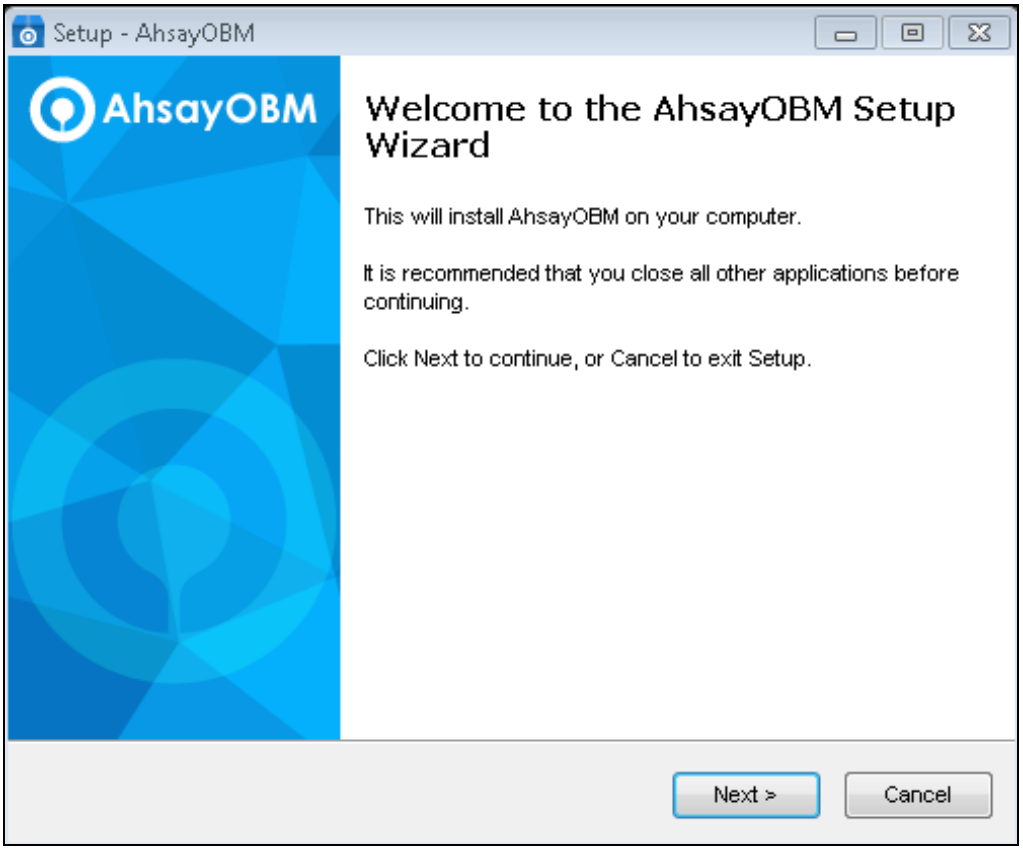
5. Click **Run** once you see the following message.



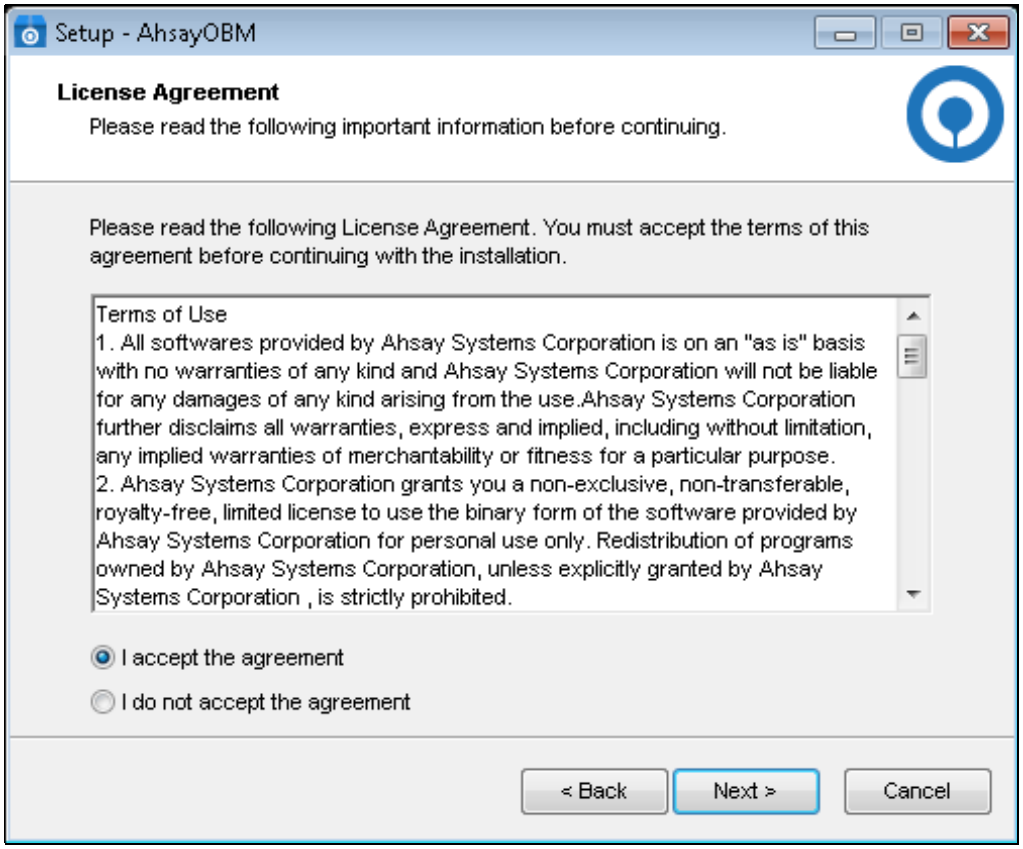
6. The following dialog box will appear only if User Account Control is enabled. Click **Yes** to start the installation.



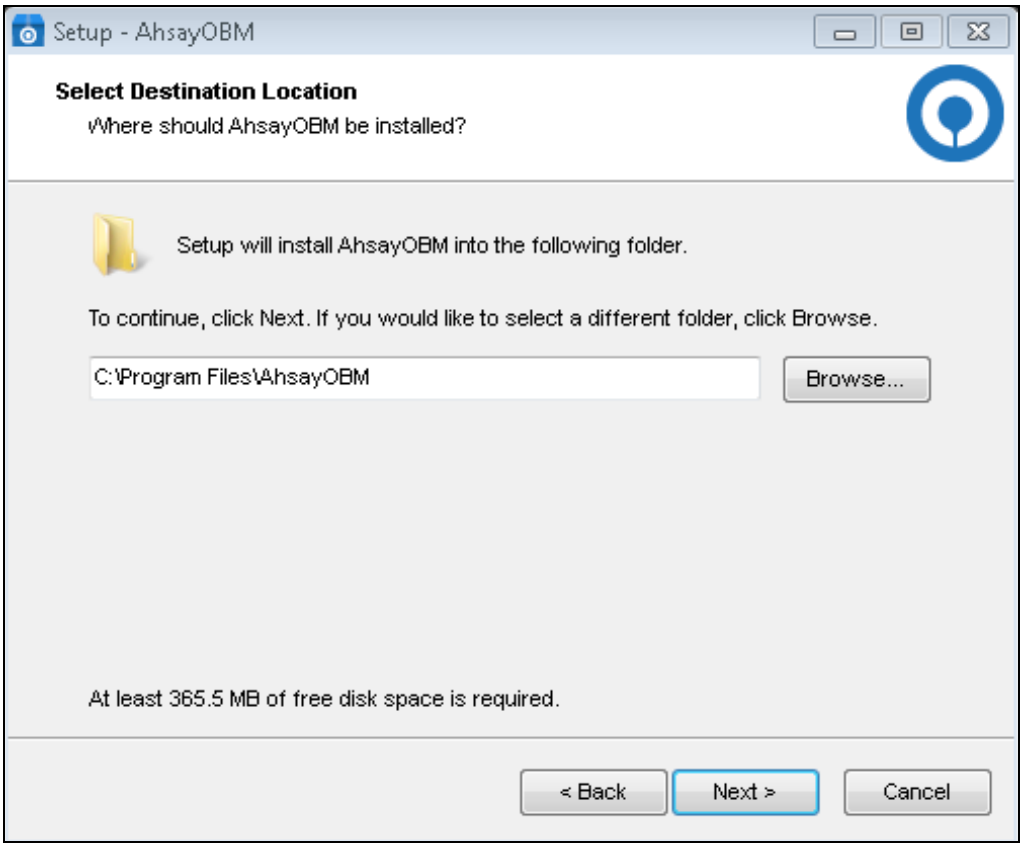
7. Click **Next** to continue.



8. Select **I accept the agreement** after reading the license agreement. Then, click **Next** to proceed.



9. Choose the installation directory. Then, click **Next** to continue.



10. Select the program group to which the software will be installed. The default setting is “Anyone who uses this computer”. The following are the difference between the two settings:

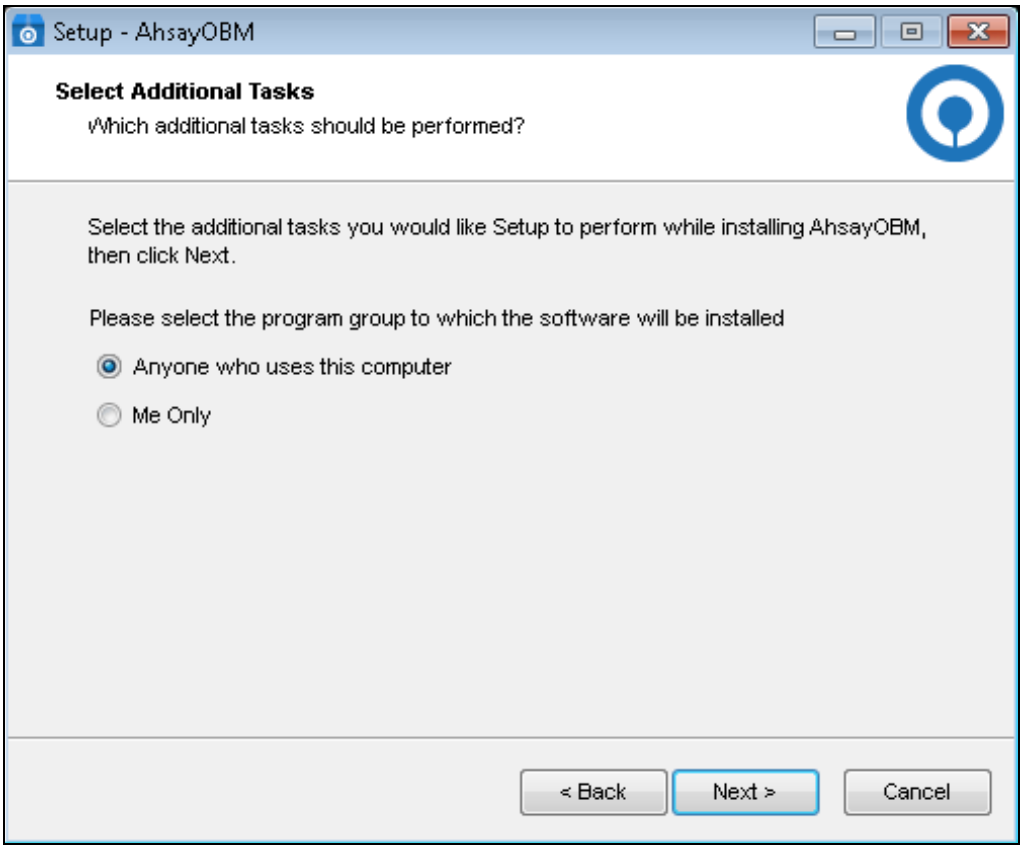
    - Anyone who uses this computer – the AhsayOBM System Tray icon will be available to all Windows users and backup notifications will be displayed on the Windows System Tray. For more information, please refer to Chapter 10.11 System Tray.

    - Me Only – the AhsayOBM System Tray icon will not be available and backup notifications will not be displayed on the Windows System Tray.

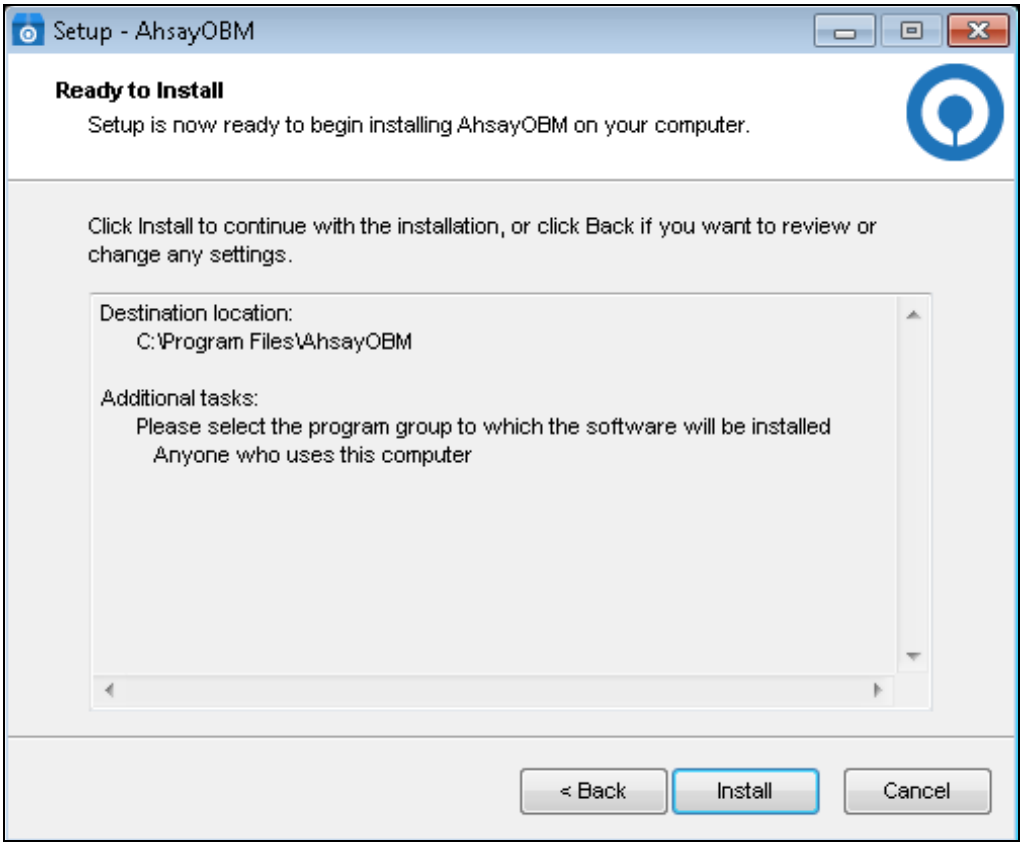
    NOTE

    Once the program group setting has been chosen and the installation completed; if you need to change the setting, this will require an uninstallation and re-installation of the application.

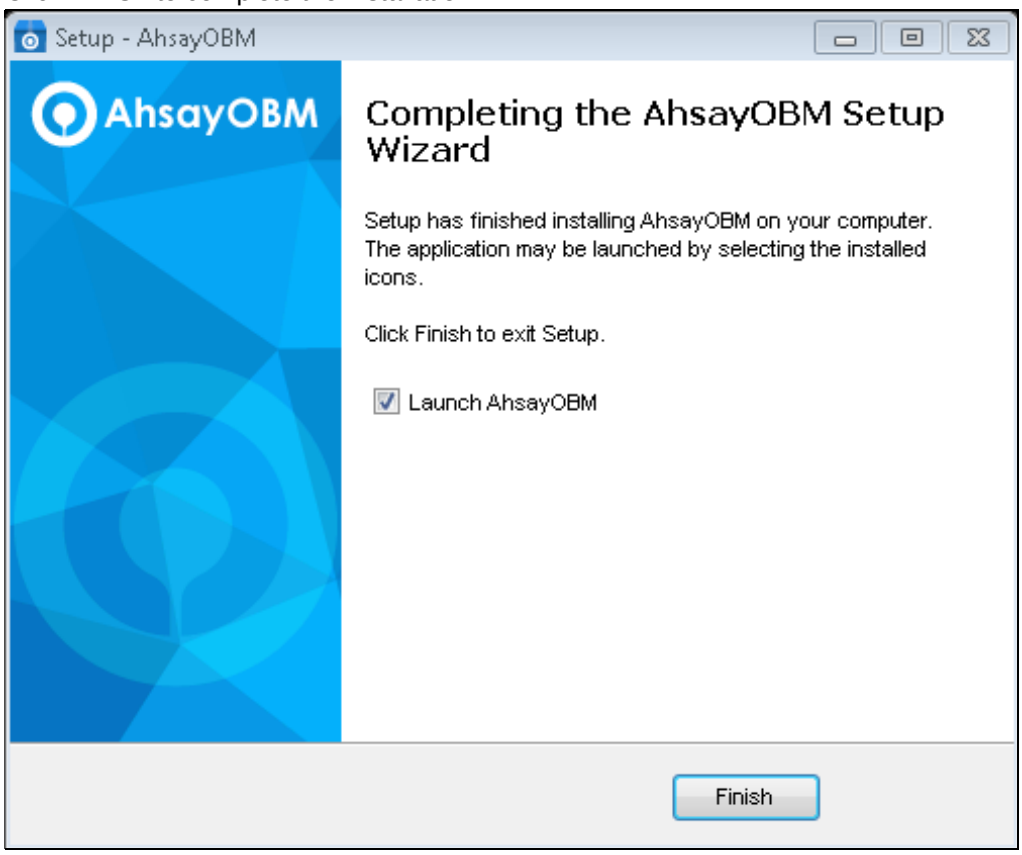
    Click **Next** to proceed.



11. The installation will start after you click **Install**.



12. Click **Finish** to complete the installation.



6.3 AhsayOBM Services

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

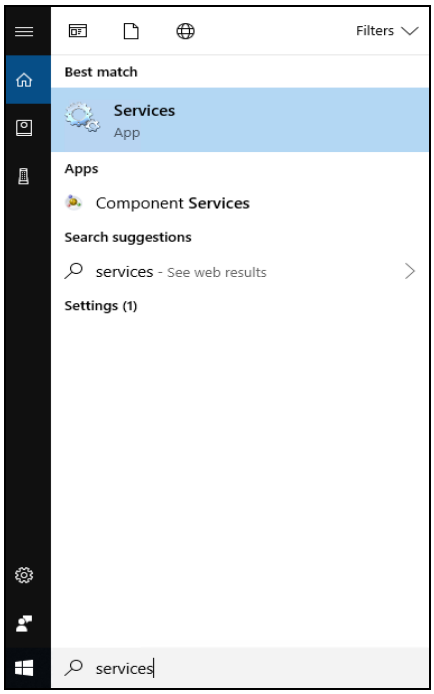
Function	Description
Scheduled Backups	Ensures that backup jobs which are setup to run at a certain date and/or time are started.
Continuous Backups (Windows platform only)	Ensures that Continuous backups are run according to the backup interval.
Mobile Backup Server (MBS)	Ensures that registered mobile devices can perform backups to AhsayOBM. The MBS will be activated when a mobile device is registered for mobile backup on AhsayOBM. The MBS will be deactivated when all mobile devices have been deregistered from the mobile backup settings and the AhsayOBM services is restarted.

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

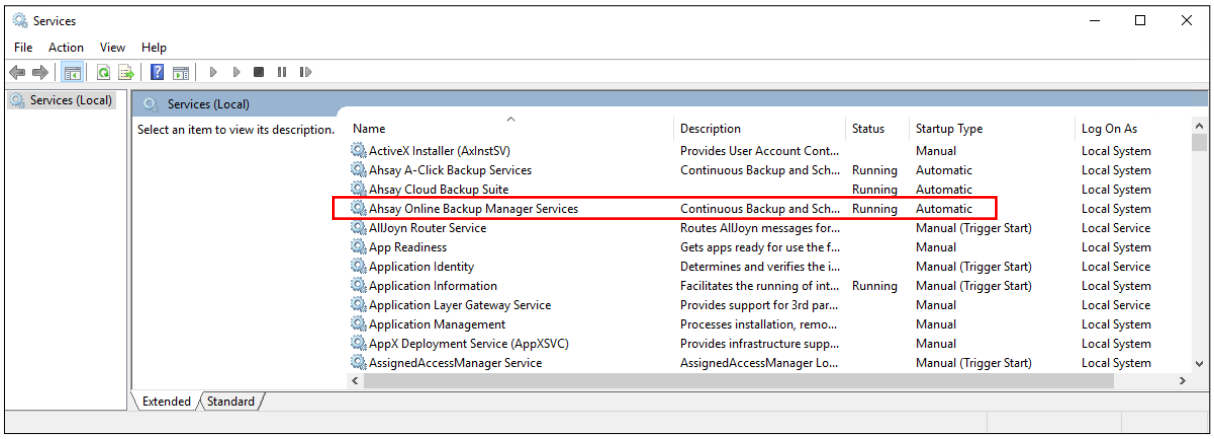
- a new AhsayOBM installation
- an AhsayOBM software update
- the machine was rebooted
- the machine is powered on
- the machine wakes up from hibernation or standby mode

Otherwise, all of the functions above will stop working.

To check if the AhsayOBM Scheduler Service is running properly on the local machine, go to start menu and search for **Services**.



Look for the **Ahsay Online Backup Manager Services** on the list. The **status** should be "Running", and the **Startup Type** should be "Automatic".

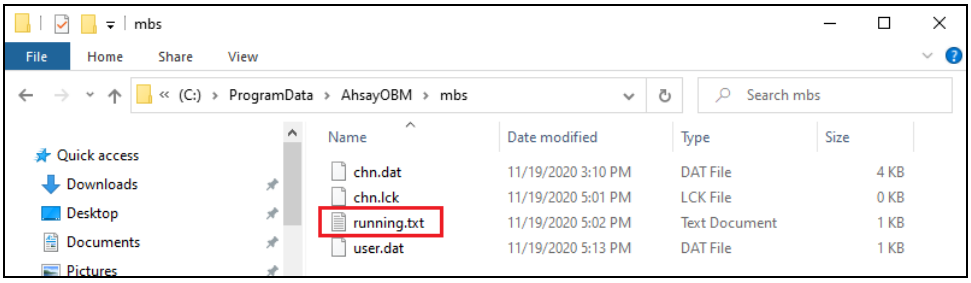


6.4 Mobile Backup Server (MBS) Status Check and Ahsay Mobile app Connection Check

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 \Program Data\AhsayOBM\mbs.

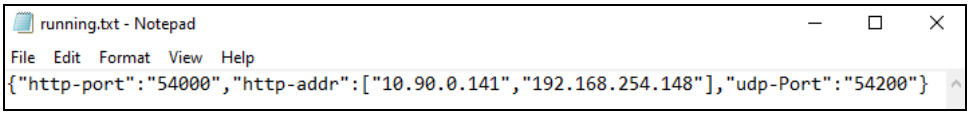
   Example: C:\ProgramData\AhsayOBM\mbs



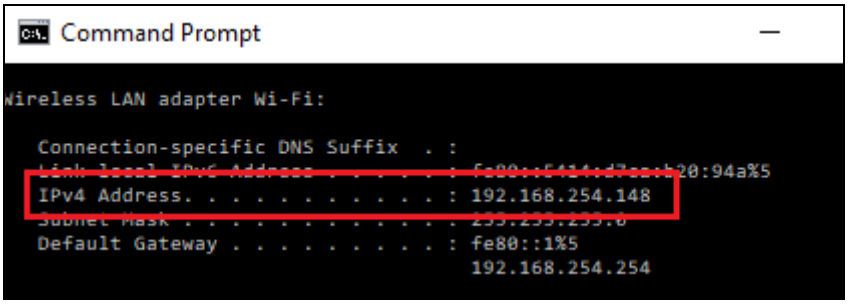
NOTE

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

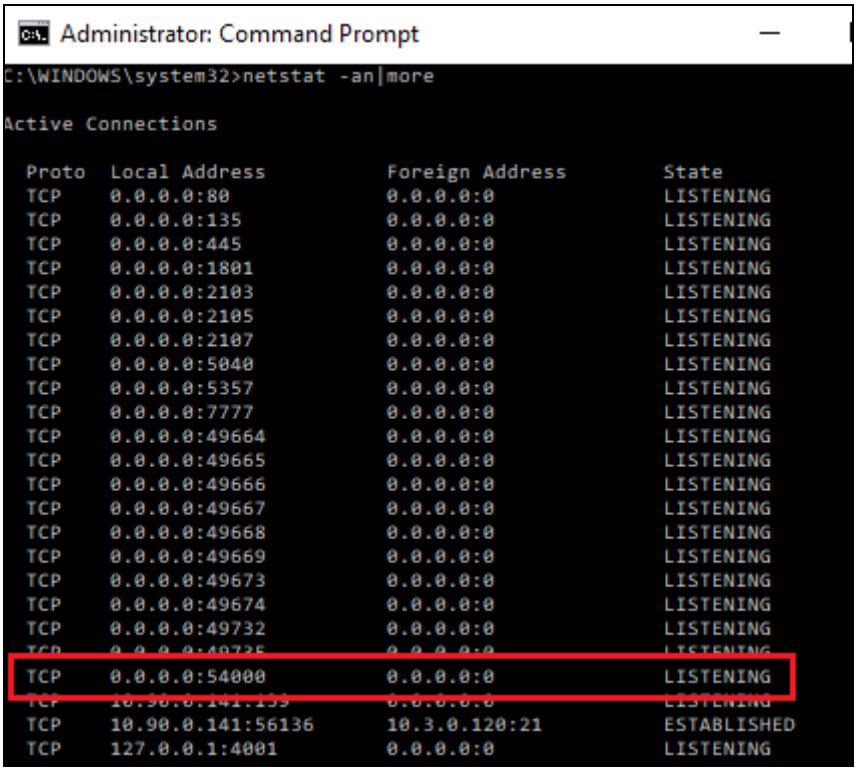
   After opening the file it will show the HTTP port, IP address and UDP port which are in actual use by the MBS.



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



3. To verify the actual HTTP port used by MBS, type the command `netstat -an|more`.

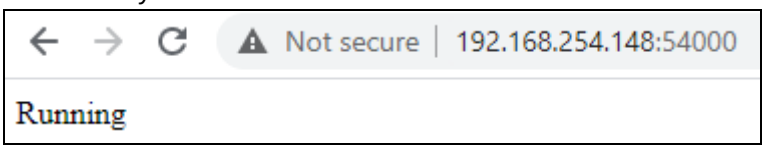


4. Make sure that your firewall setting allows network traffic through the following HTTP and UDP ports to ensure that the communication between your machine and mobile device is successful: HTTP Port: 54000 to 54099 and UDP Port: 54200 to 54299. Otherwise, mobile backup and restore will not work.

5. 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://192.168.254.148:54000, you should get the following result which shows “Running” status. This means the MBS is running.

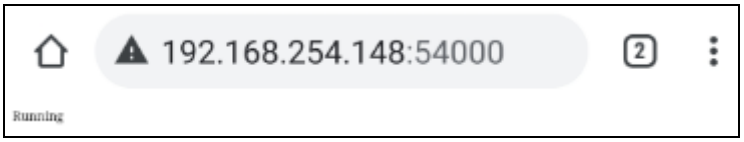
   In the AhsayOBM machine



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 55000, http://192.168.254.148:54000, 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



7 Register device for 2FA in AhsayOBM

Starting with AhsayOBM v8.5.0.0, you will find two new features introduced with this latest version which are the Mobile Backup and Two-Factor Authentication.

There are two types of Authenticator that can be used to register a device for 2FA in AhsayOBM such as Ahsay Mobile Authenticator and Third-party TOTP Authenticator (e.g., Microsoft Authenticator, Google Authenticator, Authy, Duo, and LastPass Authenticator, etc.).

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**

7.1 Using Ahsay Mobile Authenticator

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

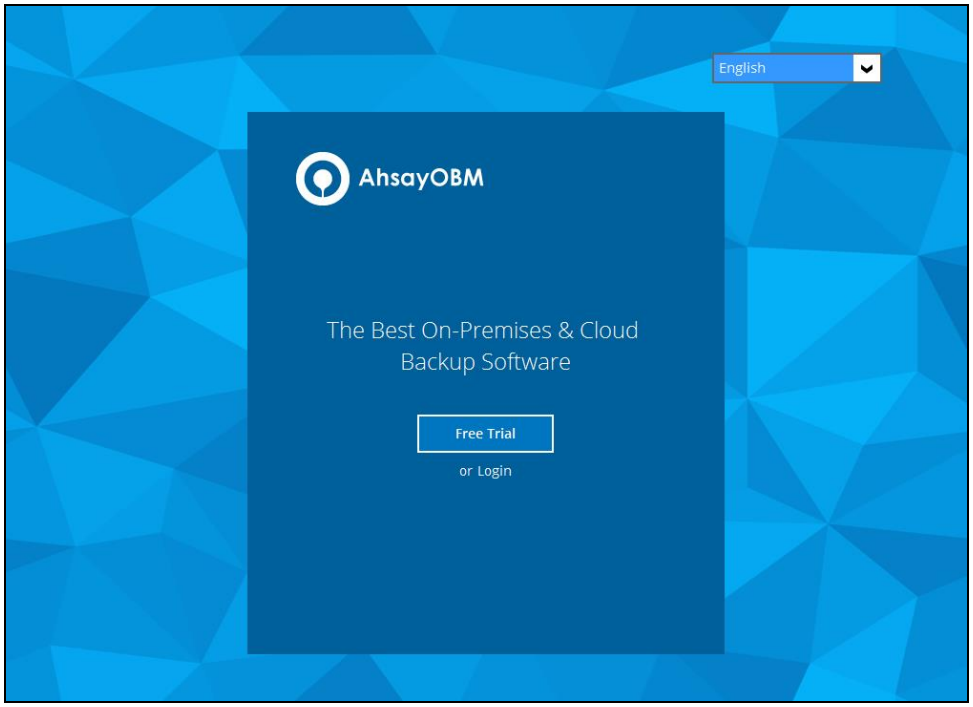
- Without Mobile Add-on Module
- With Mobile Add-on Module

7.1.1 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.

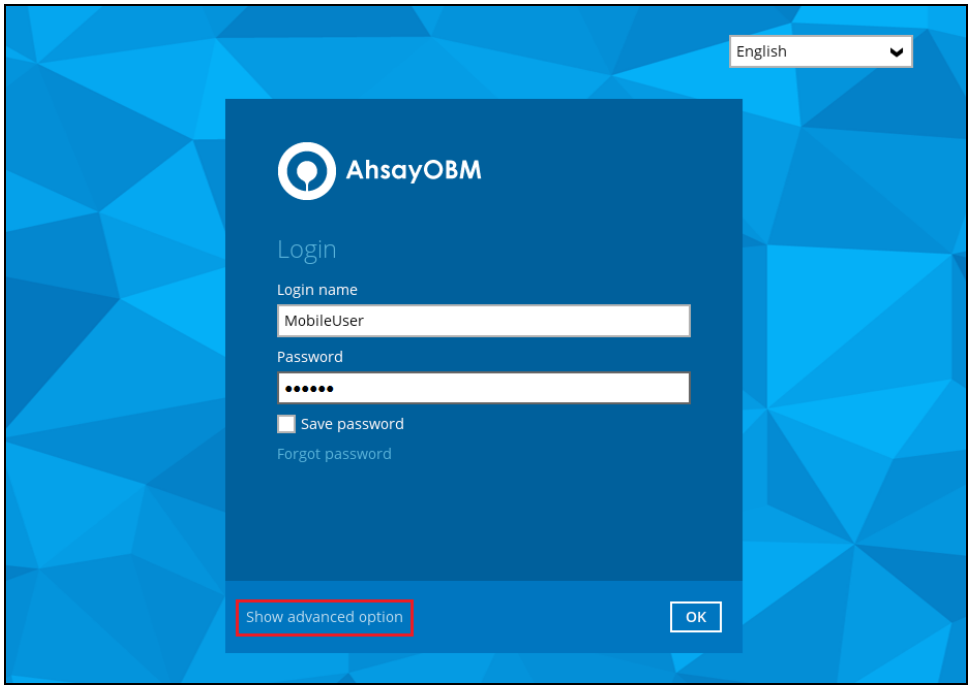
2. The Free Trial Registration option may be displayed when you login for the first time. If you want to create a free trial account please proceed to Appendix E. Otherwise, click **Login** if you already have an AhsayOBM account.



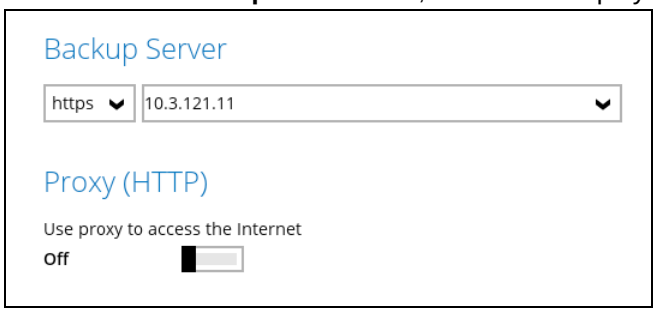
NOTE

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.

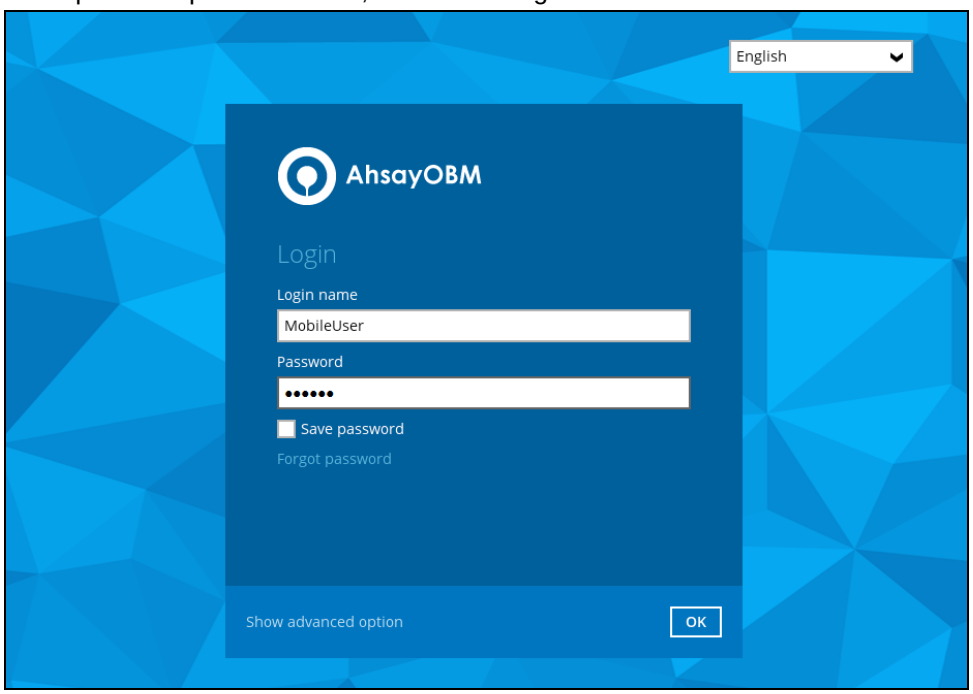
3. The **Show advanced option** may not be available if the backup server settings are already setup by your backup service provider. Please contact your backup service provider for more information.



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



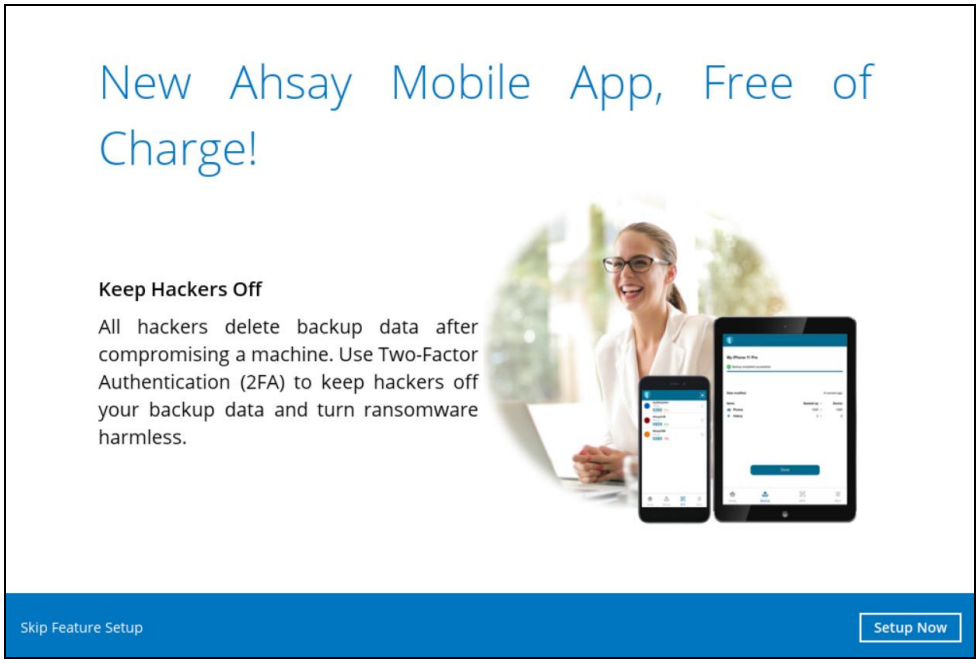
4. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.



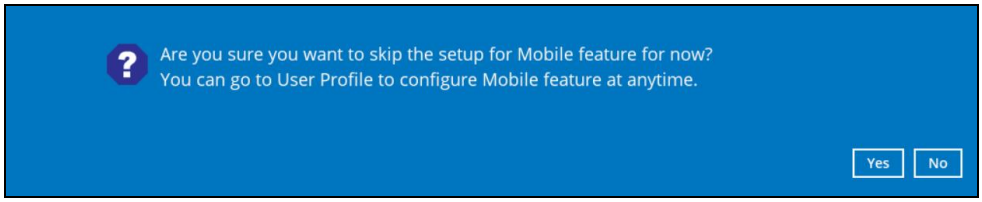
NOTE

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.

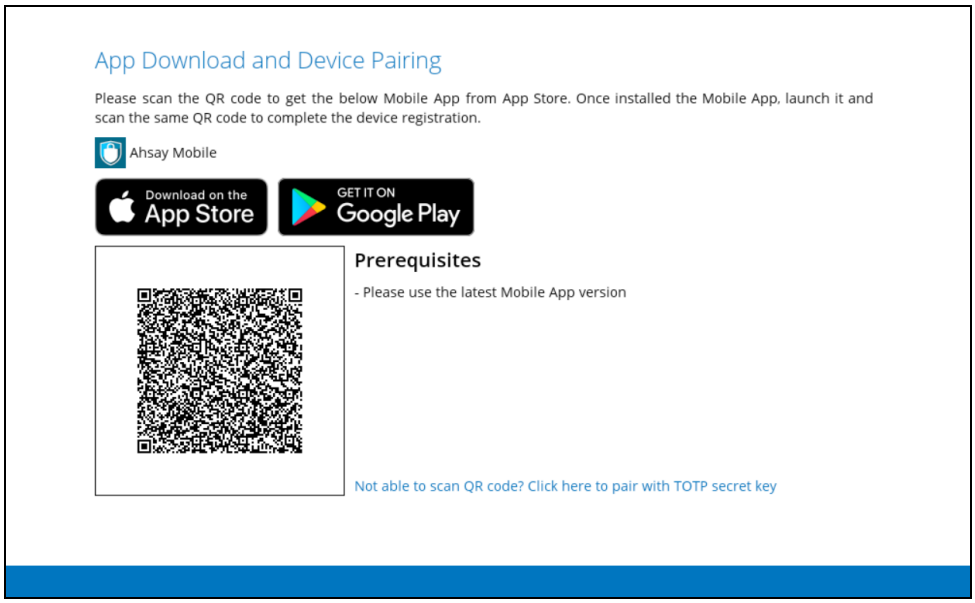
5. You will have the option to set up your 2FA. Click **Setup Now**.



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.



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



7. Ahsay Mobile supports two types of authentication method:

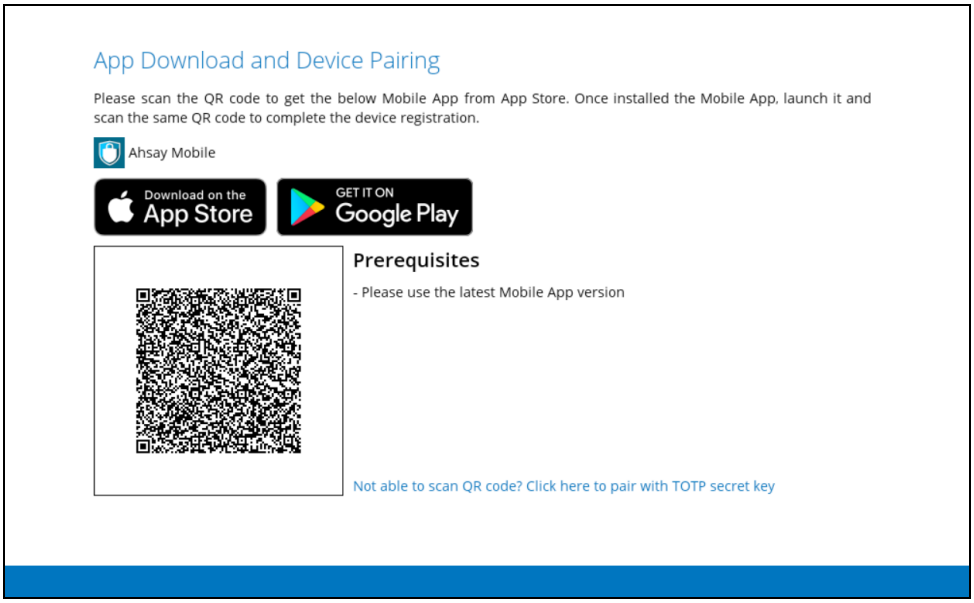
   - Push Notification
   - TOTP

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

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

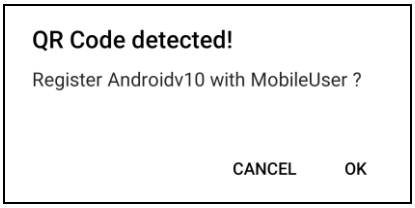
   Push Notification and TOTP (default mode)

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

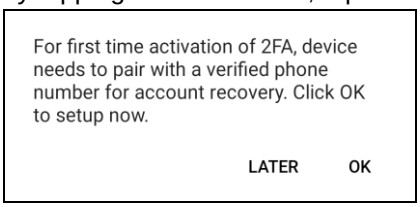


   ii. In this example, the Ahsay Mobile app is installed on a mobile device named “Androidv10”.

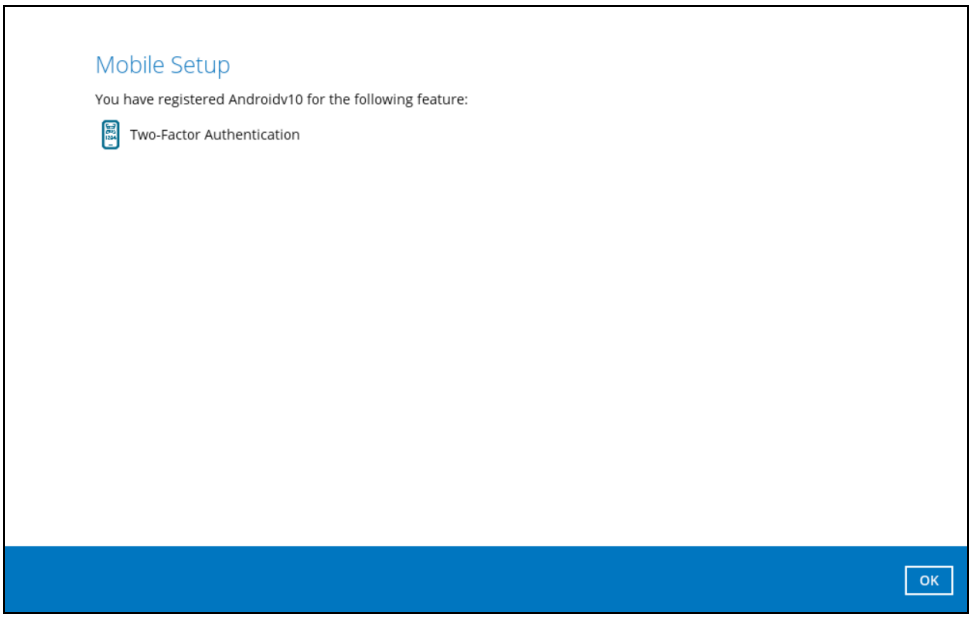
Tap **OK** to continue.



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.

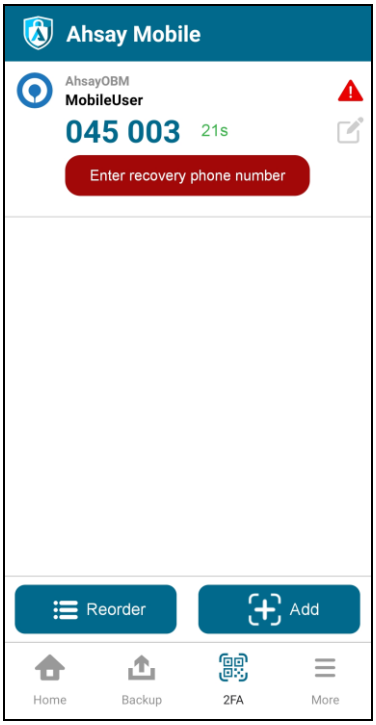


Phone number verification for account recovery

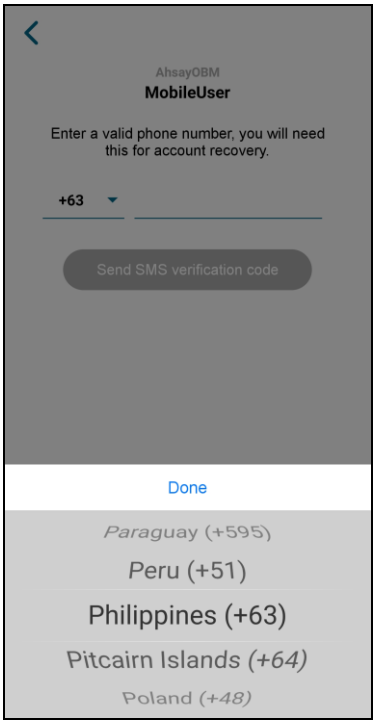
iv. In the Ahsay Mobile app, go to 2FA then enter the phone number for account recovery. Tap **Enter recovery phone number**.

NOTE

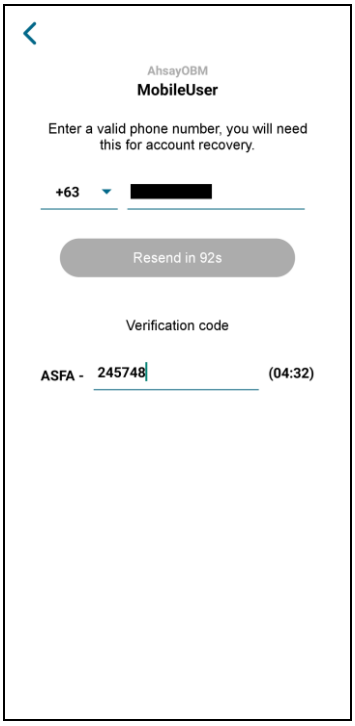
Although push notification and TOTP will still work if the recovery phone number registration is not completed, it is still strongly recommended to complete **step iv** as you will not be able to access the AhsayOBM if you lose your mobile device which also means loss of access to backup data.

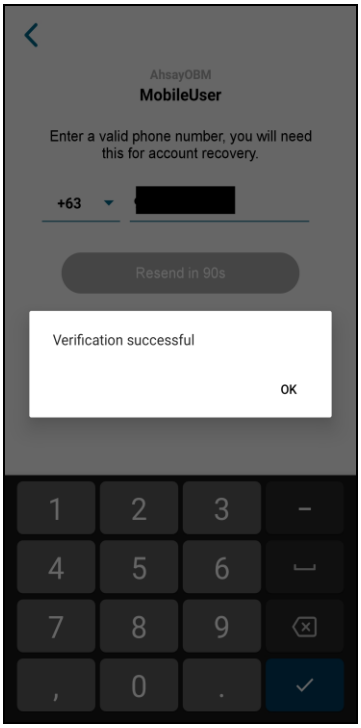


Select your country code and enter your phone number. Tap **Send SMS verification code**.



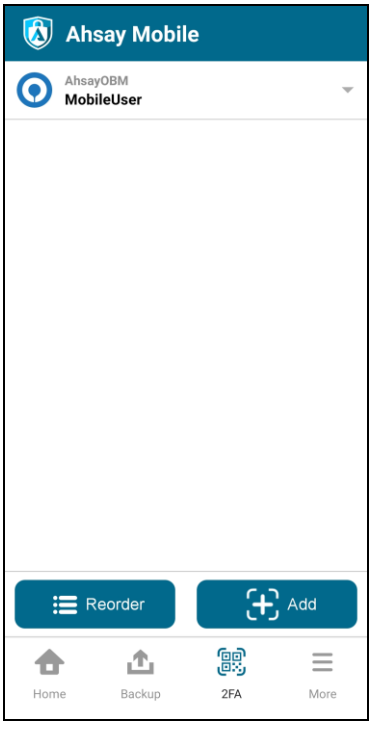
Enter the verification code sent to your mobile device.

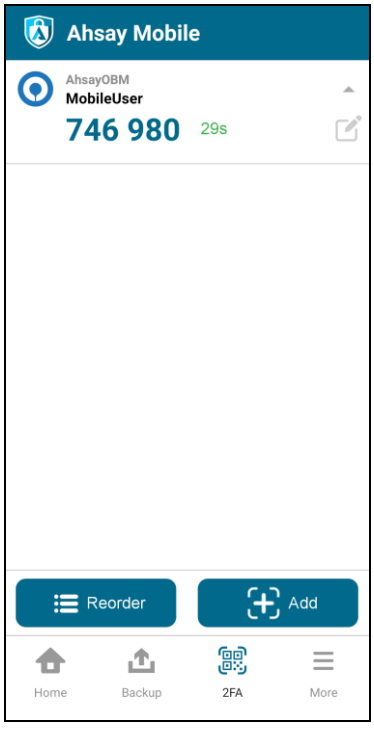




Example of verification code:

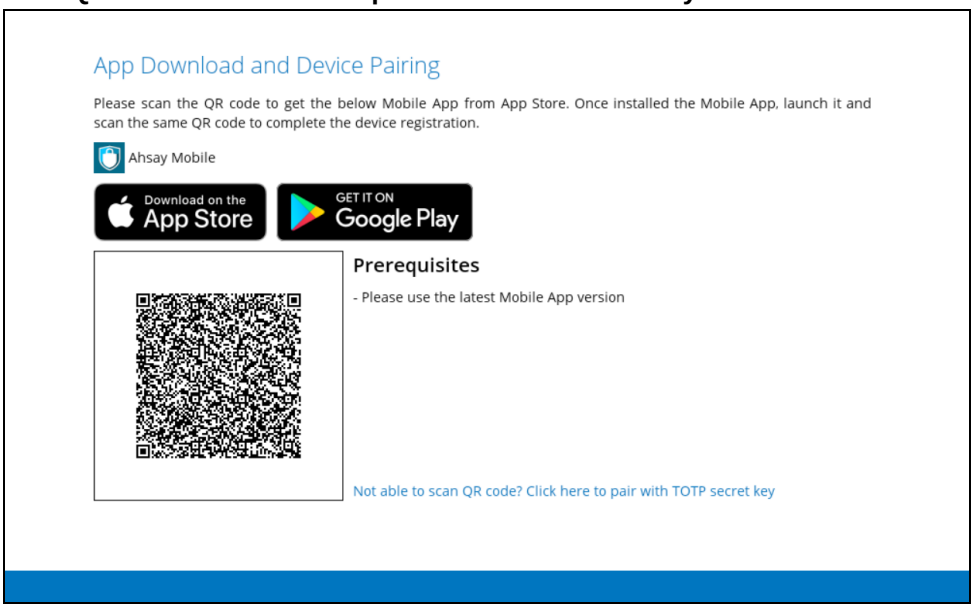
Your phone number for account recovery is successfully verified.



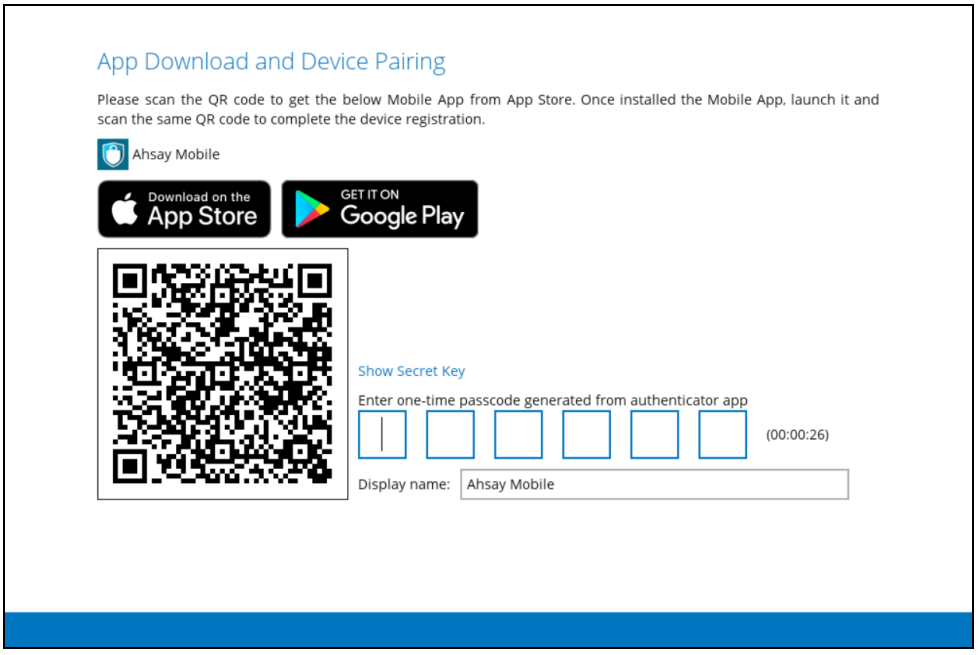


TOTP only

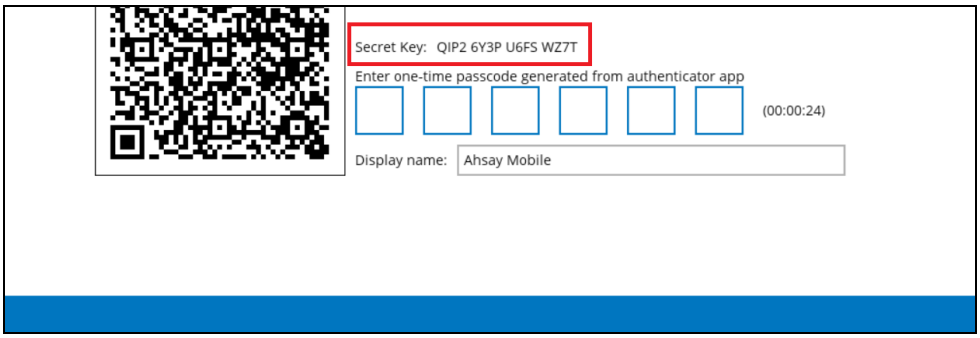
i. To configure a TOTP only 2FA with Ahsay Mobile, click the **"Not able to scan QR code? Click here to pair with TOTP secret key"** link.



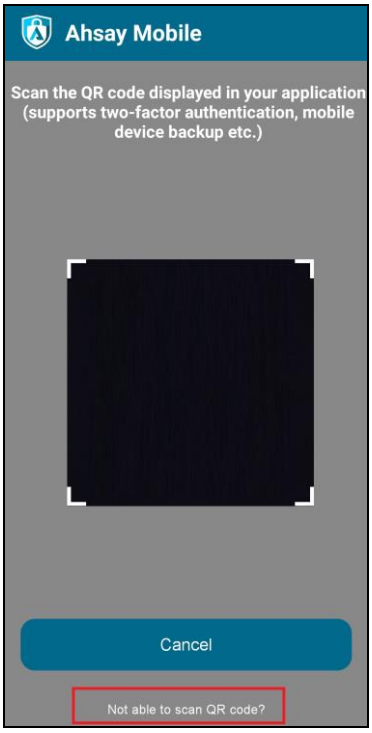
ii. After clicking the **"Not able to scan QR code? Click here to pair with TOTP secret key"** link, the QR code for the TOTP only authenticator will be displayed.

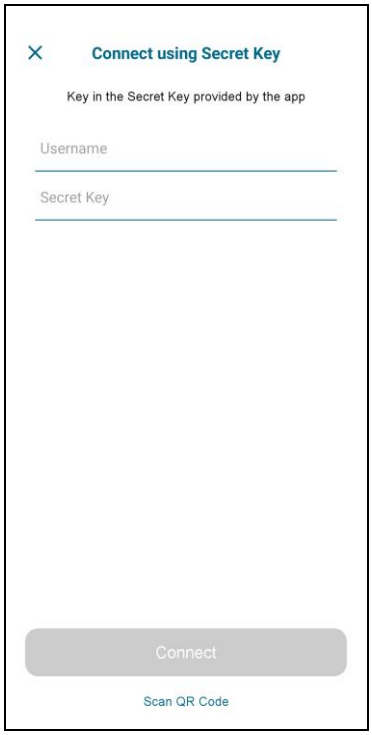


To show the secret key, click the **Show Secret Key** link to display the 16-character alphanumeric secret key. The display name will be “Ahsay Mobile” by default.

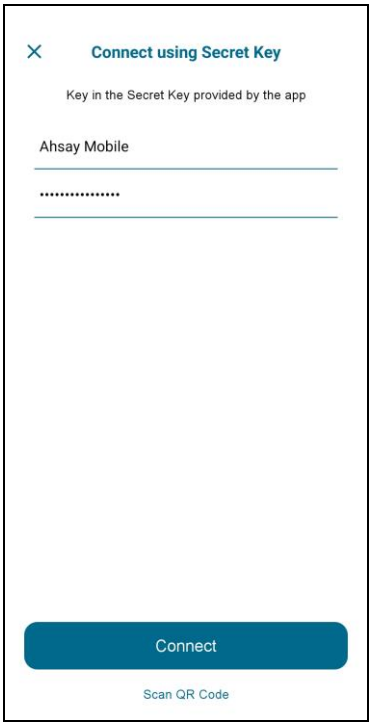


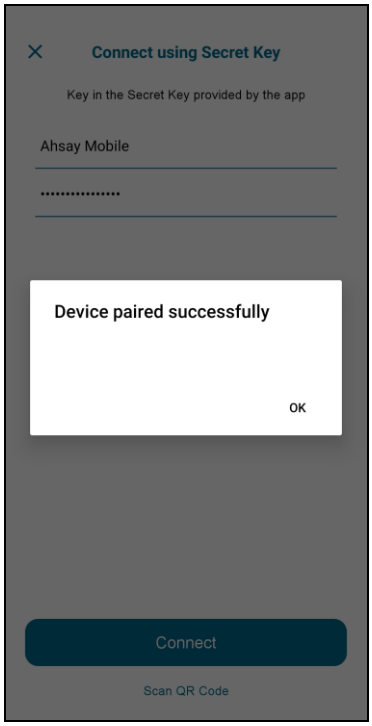
iii. In the Ahsay Mobile app, go to **2FA**. Tap the **Not able to scan QR code?** link.



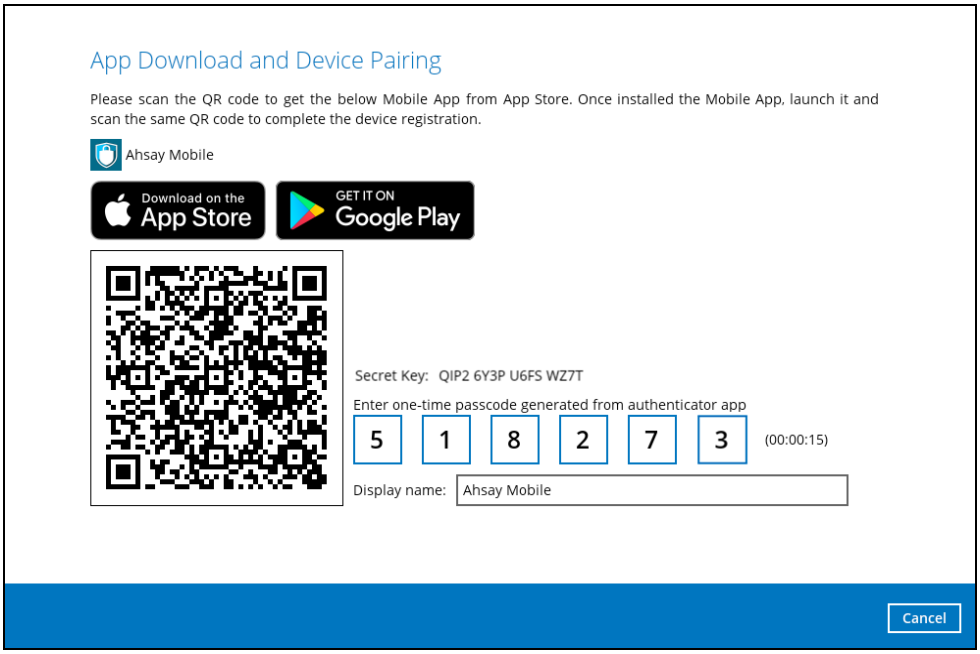


iv. Enter the Username and Secret Key shown in the AhsayOBM then tap **Connect**. Once the device is paired successfully, tap **OK** to continue.

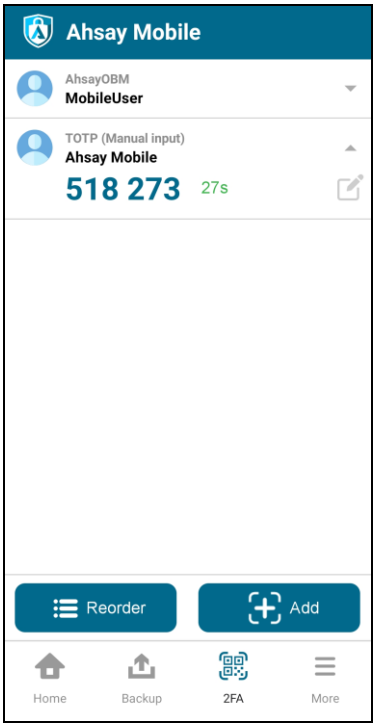




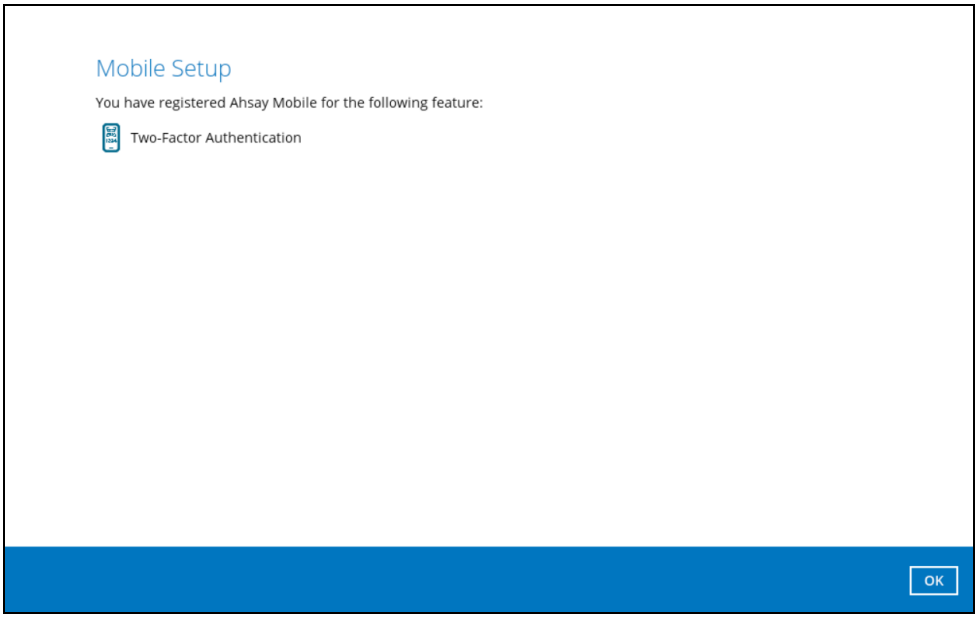
v. Enter the one-time passcode from the Ahsay Mobile app.



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

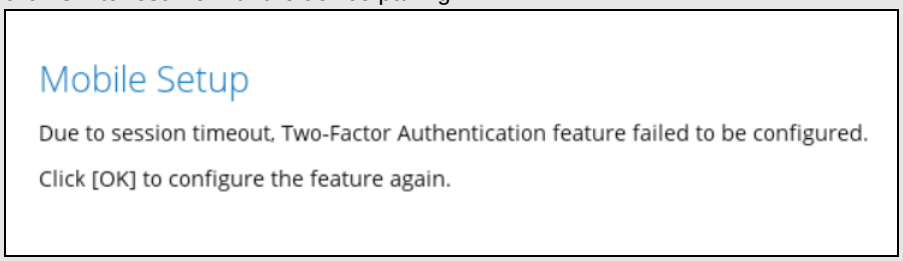


vi. Once the registration is successful, the following screen will be displayed. You have now registered Ahsay Mobile for TOTP only 2FA.

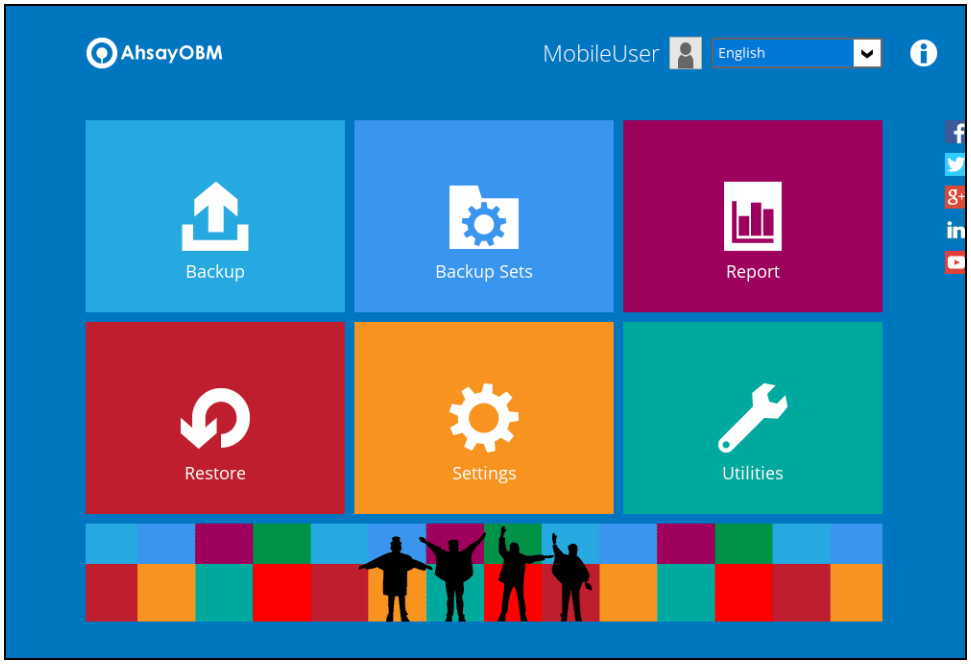


NOTE

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



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

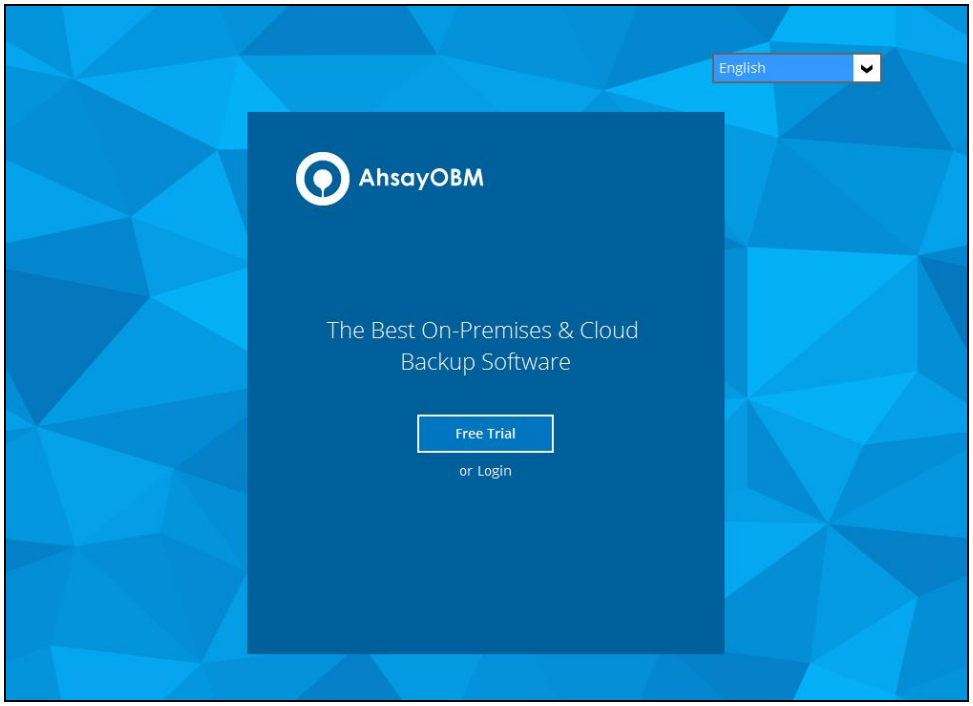


7.1.2 With Mobile Add-on Module

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.

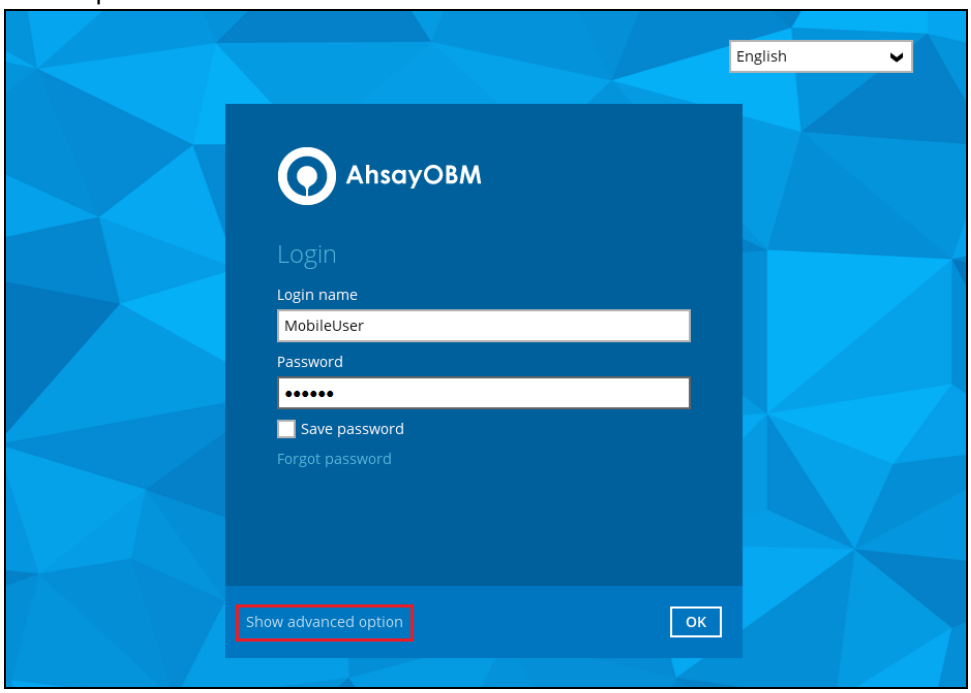
2. The Free Trial Registration option may be displayed when you login for the first time. If you want to create a free trial account please proceed to Appendix E. Otherwise, click **Login** if you already have an AhsayOBM account.



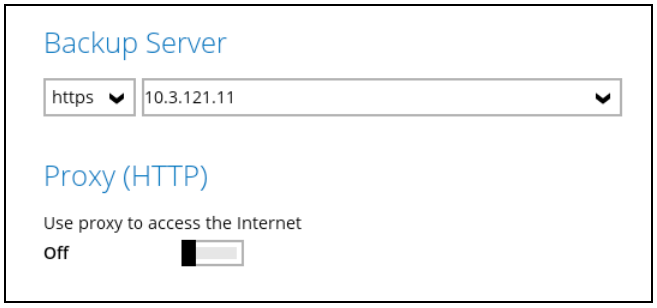
NOTE

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.

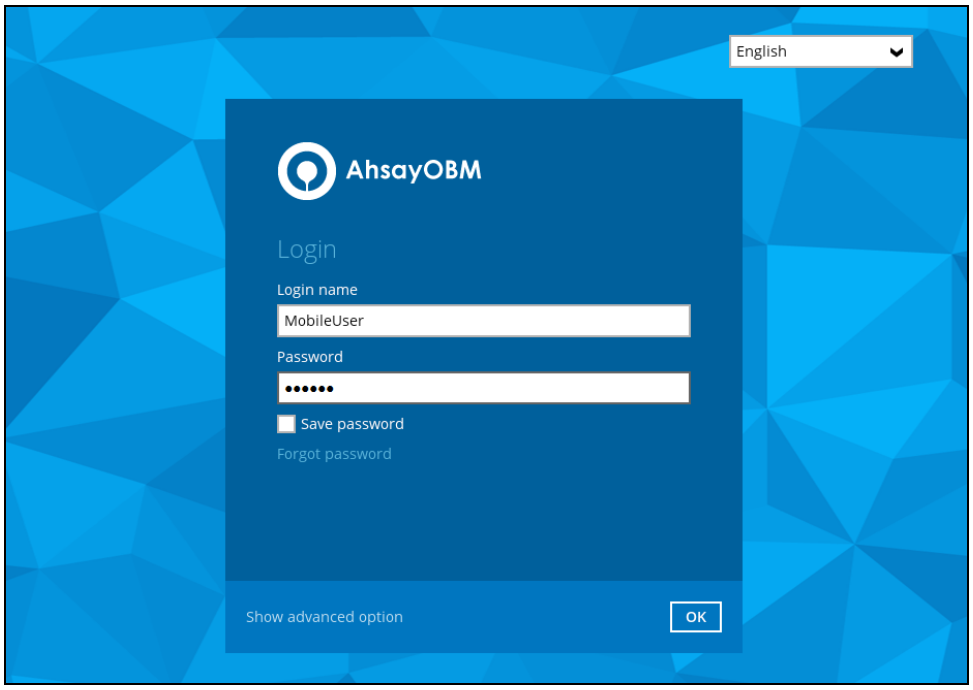
3. The **Show advanced option** may not be available if the backup server settings are already setup by your backup service provider. Please contact your backup service provider for more information.



If **Show advanced option** is clicke, this will be displayed



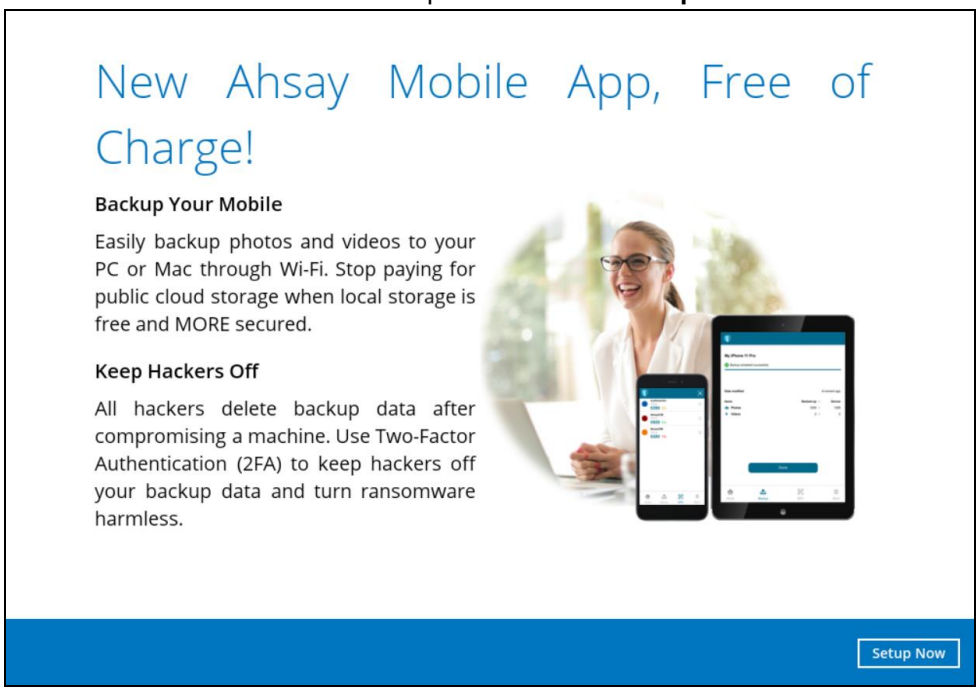
4. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.



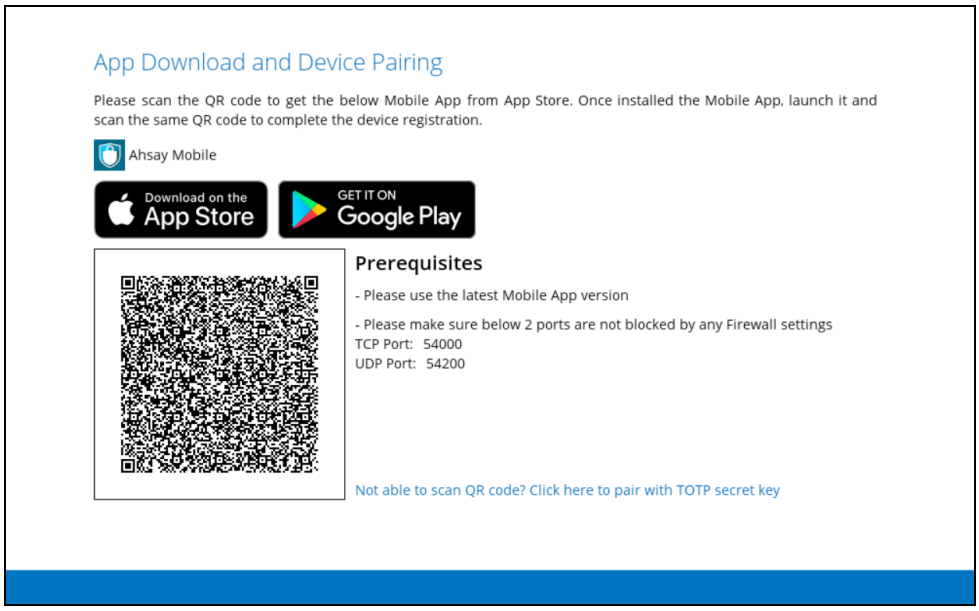
NOTE

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.

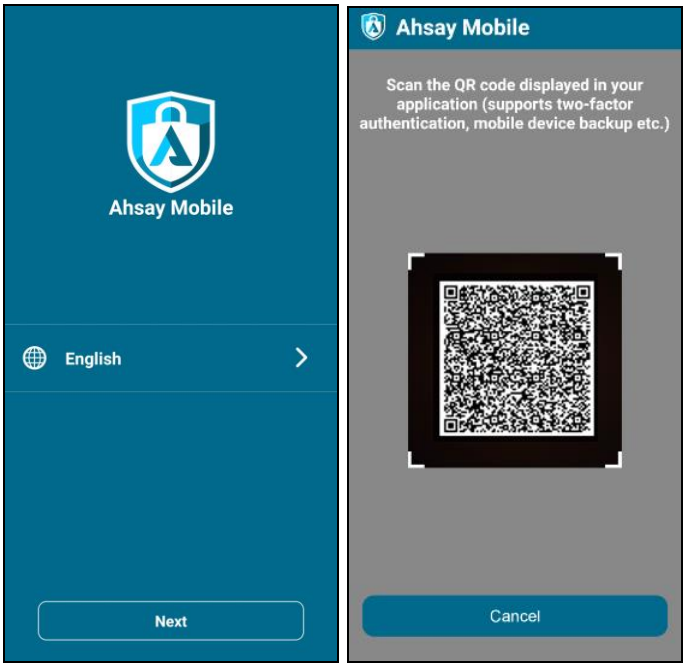
5. You will have the option to set up your 2FA and mobile backup if the **Mobile Add-on Module is enabled** in the backup account. Click **Setup Now**.



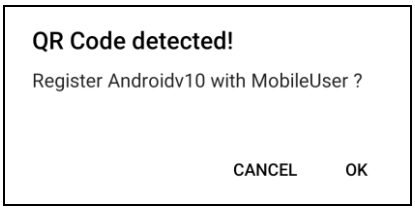
6. Download the Ahsay Mobile app from the App Store / Google Play Store. Ensure that the displayed Prerequisites are met.



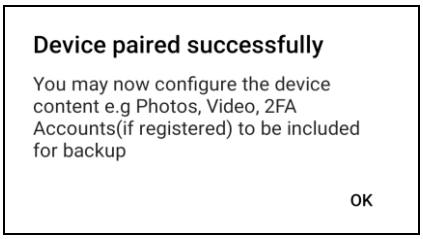
7. By using the Ahsay Mobile app, tap **Next** and scan the QR code displayed in AhsayOBM.



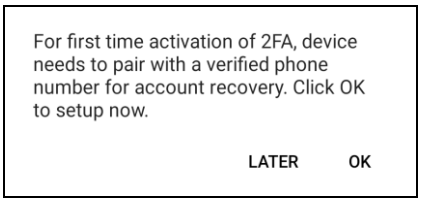
Tap **OK** to continue.



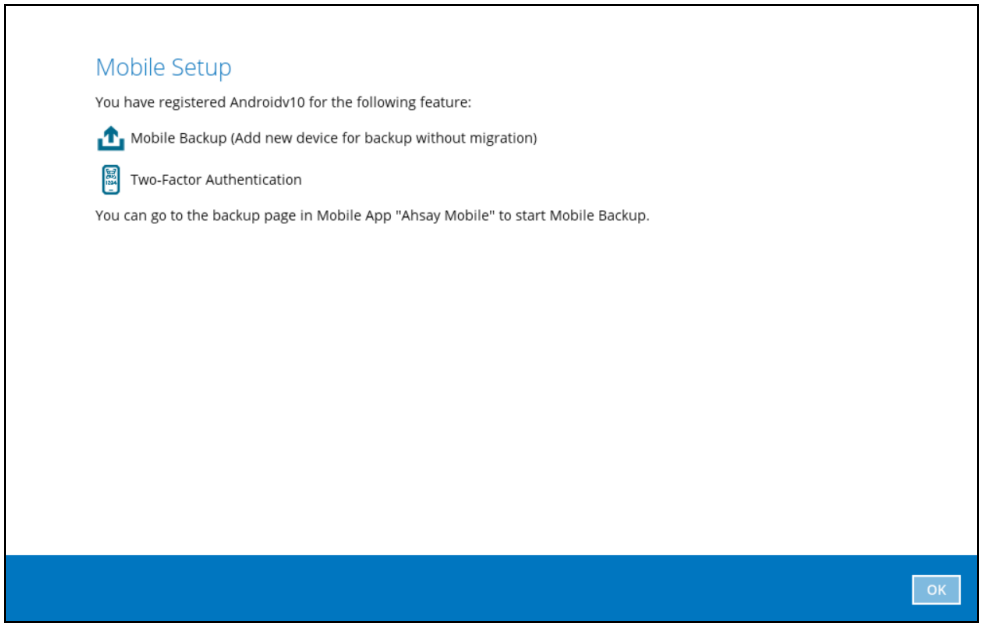
Once the device is successfully paired, the following message will be displayed in the Ahsay Mobile app. Click **OK** to continue.



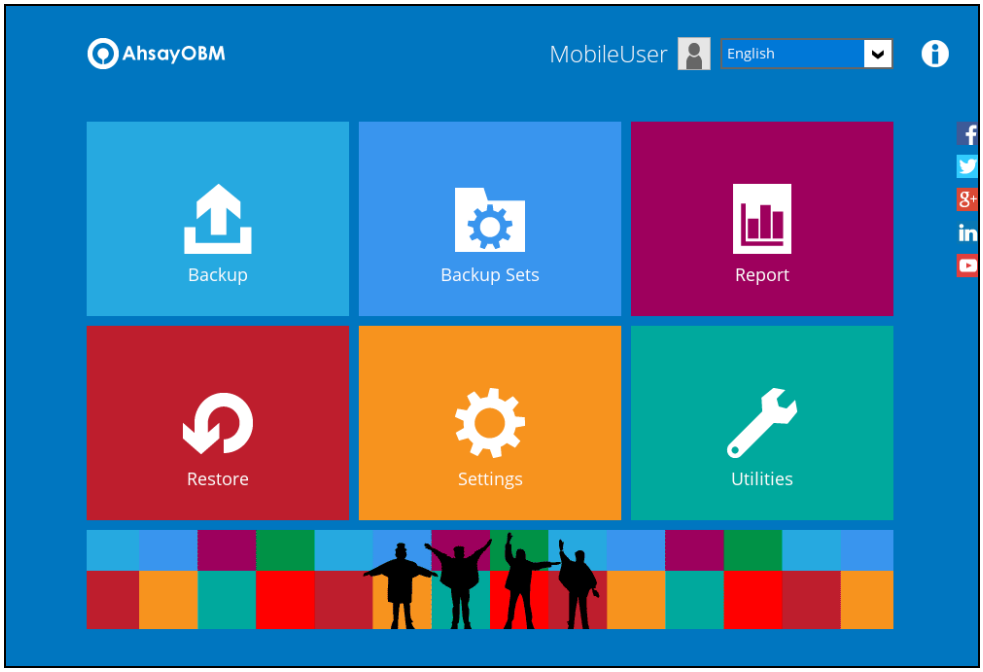
Once the device is successfully paired, the following message will be displayed in the Ahsay Mobile app. You can set up a recovery number here that will be used in case of the "Authentication Recovery" procedure by tapping **OK**. You may refer to Phone number verification for account recovery in **Chapter 7.1.1** 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.



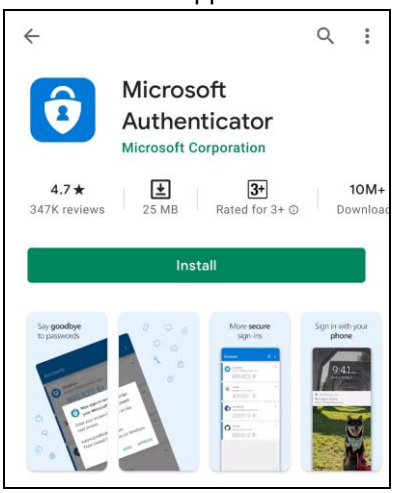
9. After successful pairing, the following screen will appear.



7.2 Using Microsoft Authenticator

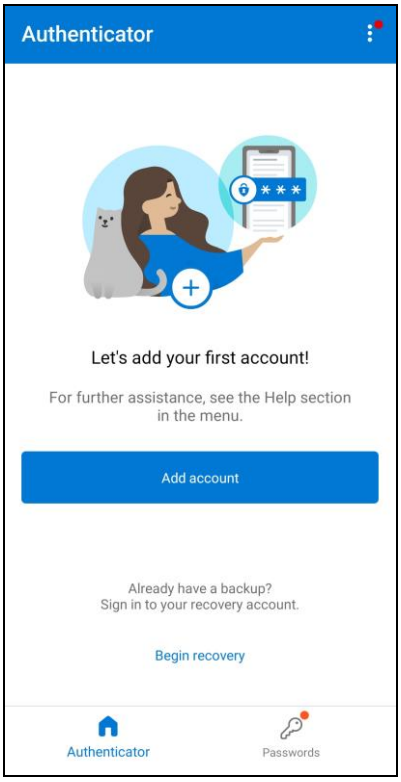
To register a device for TOTP 2FA in AhsayOBM using Microsoft Authenticator, please follow the steps below:

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

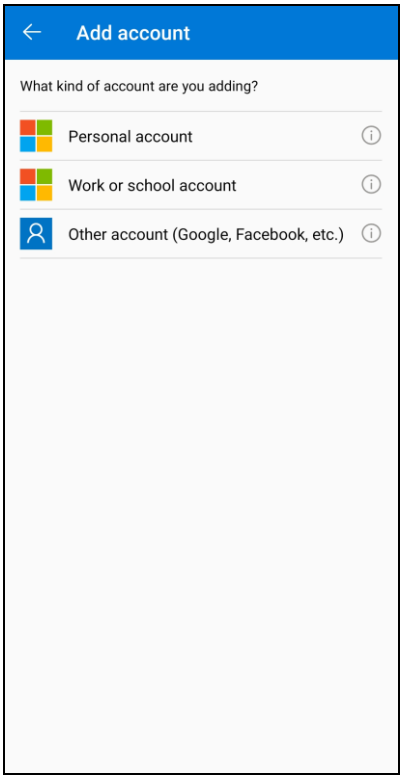


2. Launch the Microsoft Authenticator app.

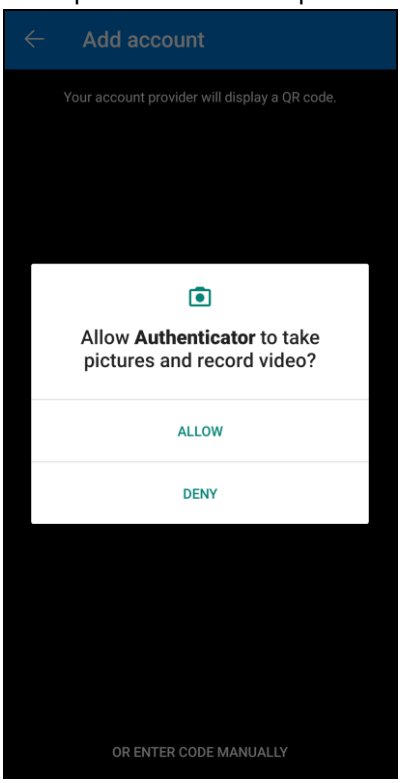
3. Tap **Add account**.



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



5. Allow permission to take pictures and record video.

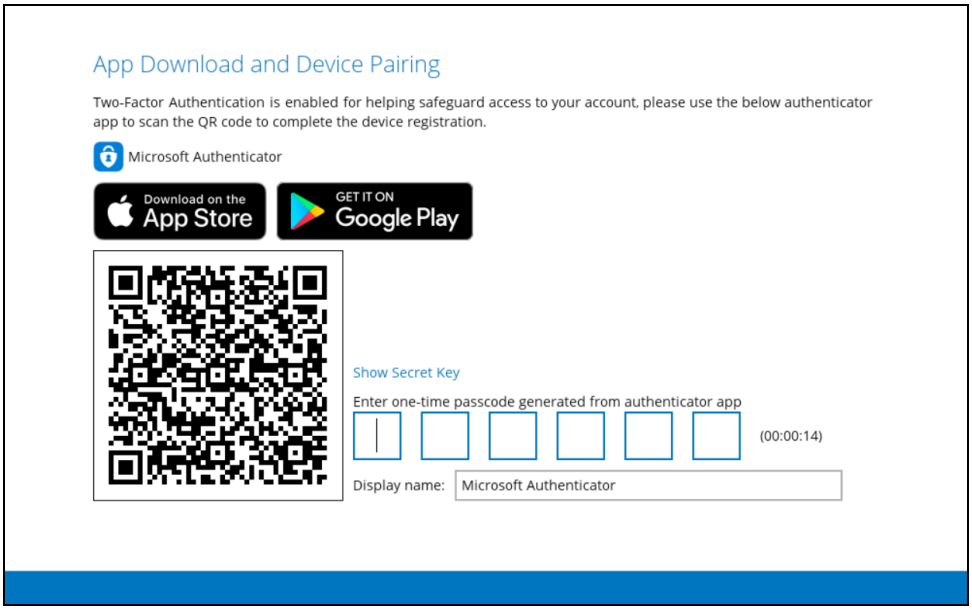


6. Set up the account by selecting from the following methods: Scan the QR code or Enter code manually.

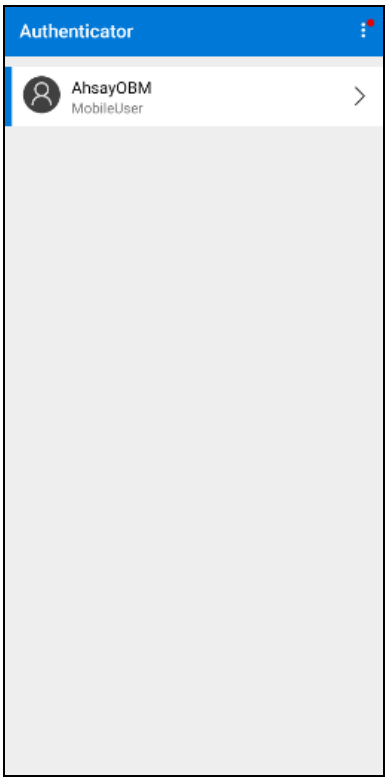
   Method 1: Scan the QR code

   i. Scan the QR code on AhsayOBM.

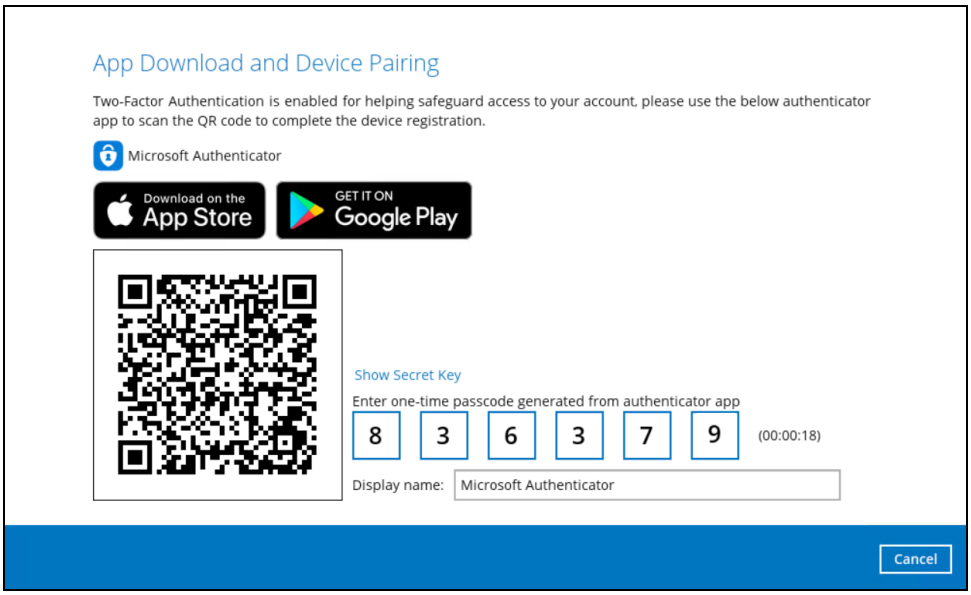
Example of the displayed QR code:



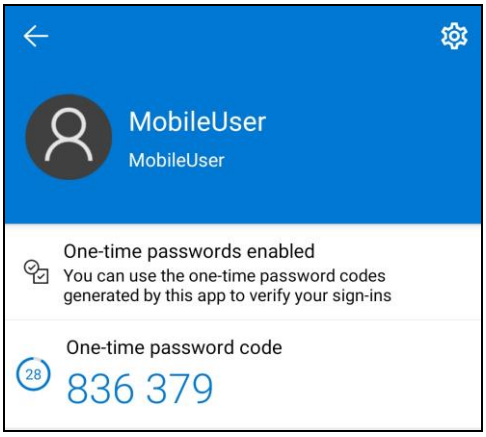
ii. The AhsayOBM account is successfully added to Microsoft Authenticator and the mobile device is registered in AhsayOBM.



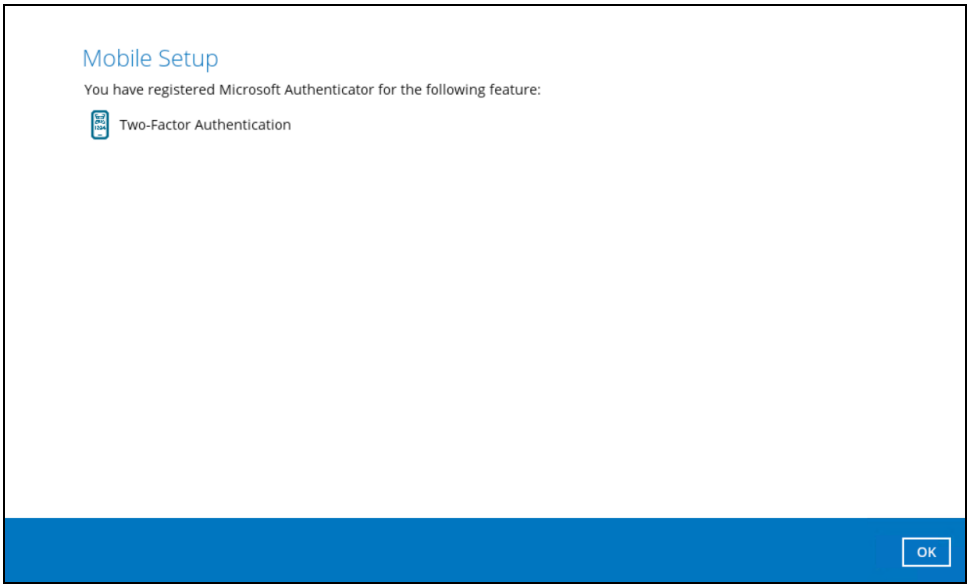
iii. Once the account is added to Microsoft Authenticator, enter the one-time passcode generated from the authenticator app to AhsayOBM.



Example of the one-time passcode generated:



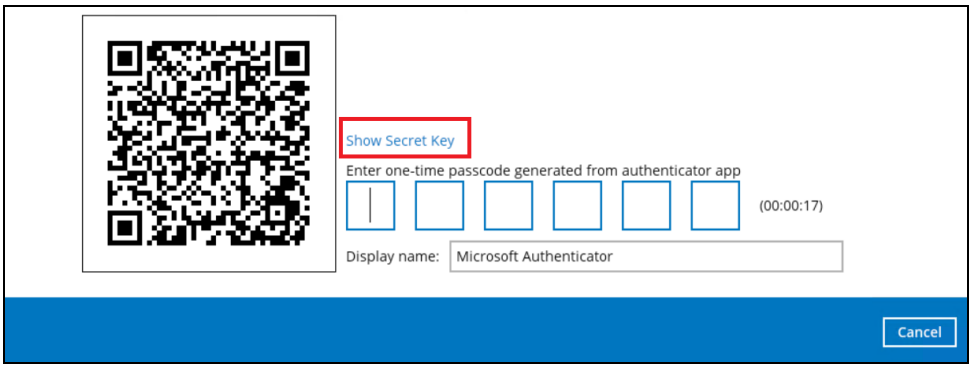
iv. The device is successfully registered for TOTP 2FA in AhsayOBM using Microsoft Authenticator. Click **OK** to continue.

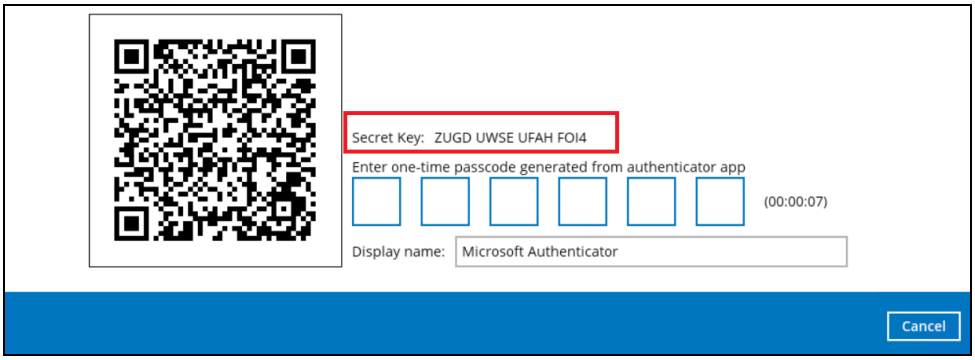


Method 2: Enter Code Manually

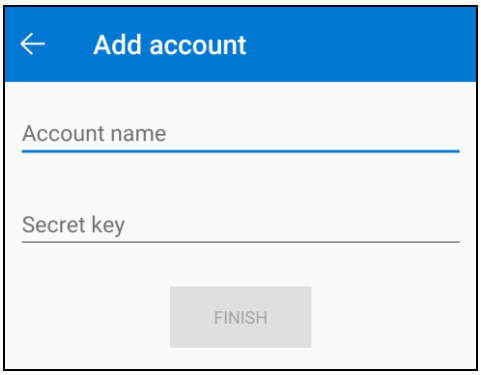
i. Tap **OR ENTER CODE MANUALLY**.

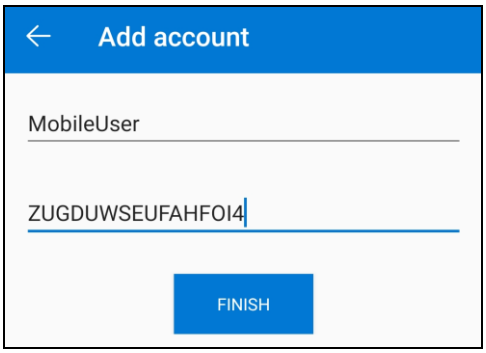
ii. Click the **Show Secret Key** link in the AhsayOBM to display the Secret Key which must be entered manually in the Microsoft Authenticator.



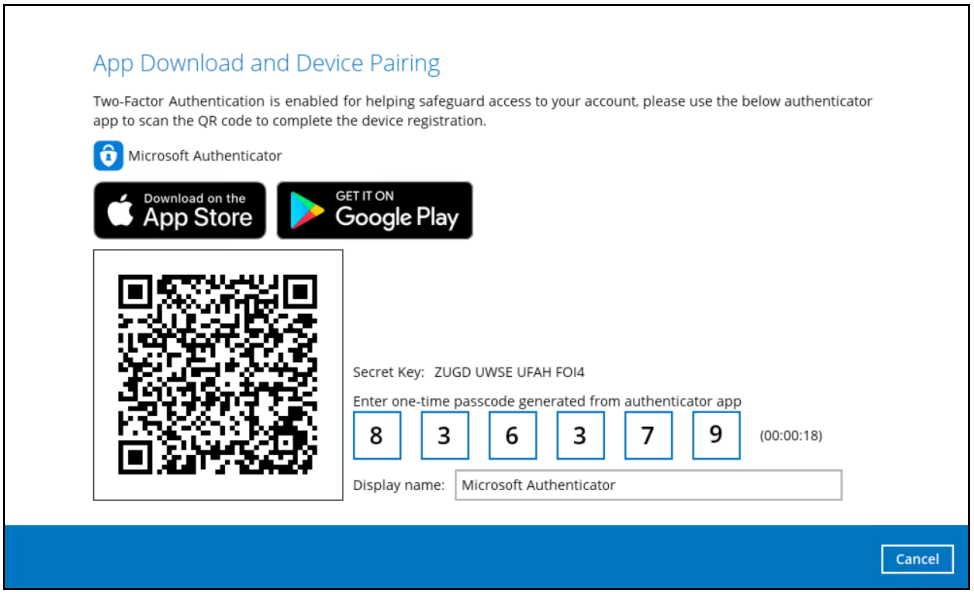


iii. On the Microsoft Authenticator app, input an account name, then enter the displayed Secret Key in the AhsayOBM. Tap **FINISH** to proceed.

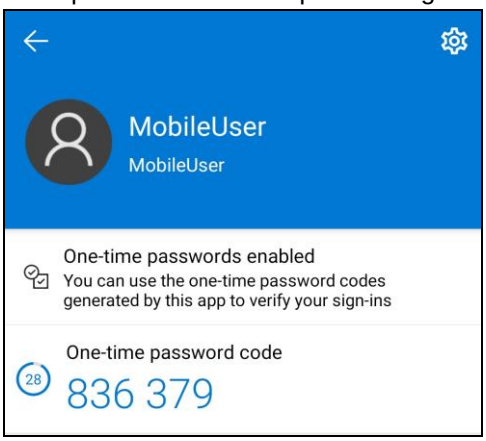




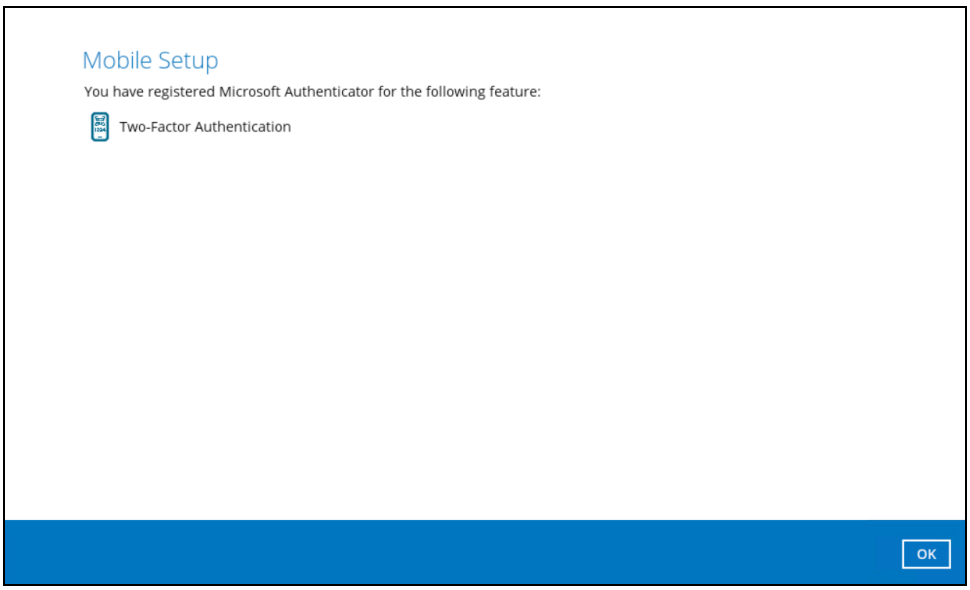
iv. Once the account is added to Microsoft Authenticator, enter the one-time passcode generated from the authenticator app to AhsayOBM.



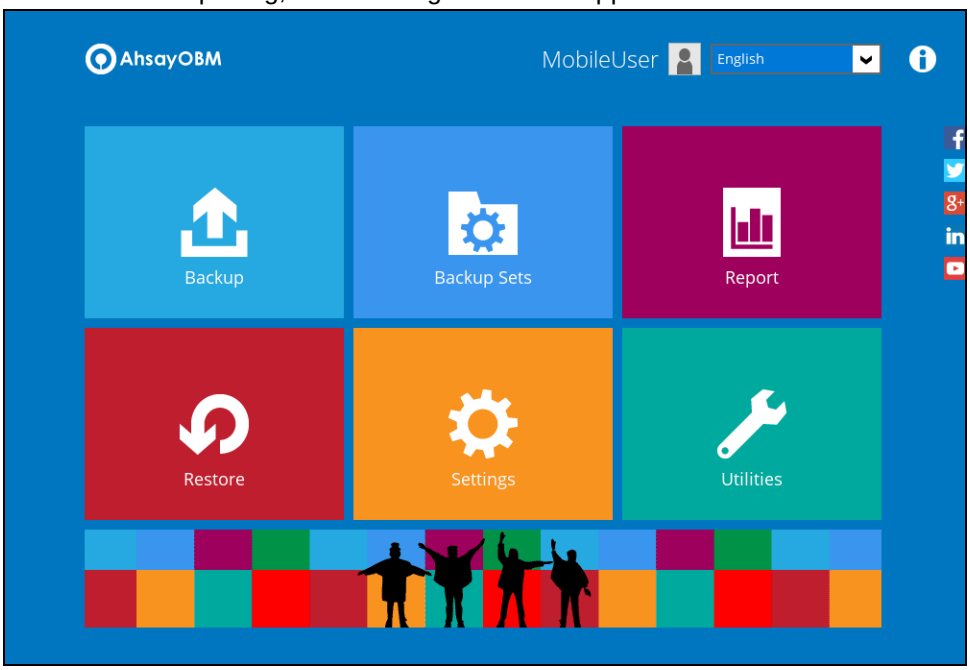
Example of the one-time passcode generated:



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



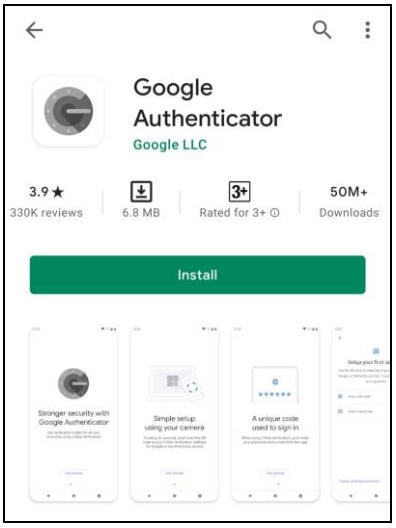
7. After successful pairing, the following screen will appear.



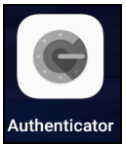
7.3 Using Google Authenticator

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.



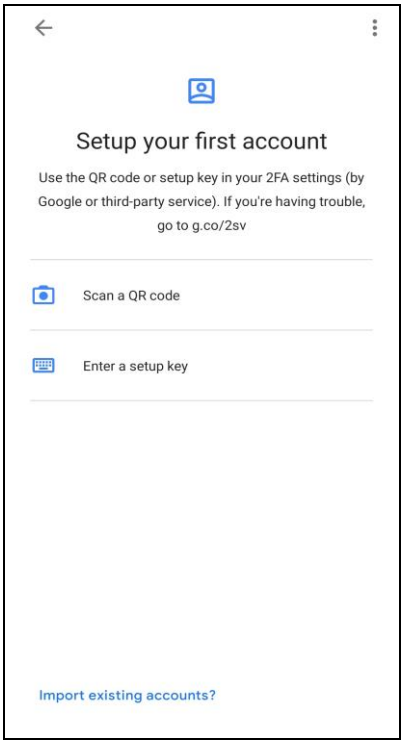
2. Launch the Google Authenticator app.



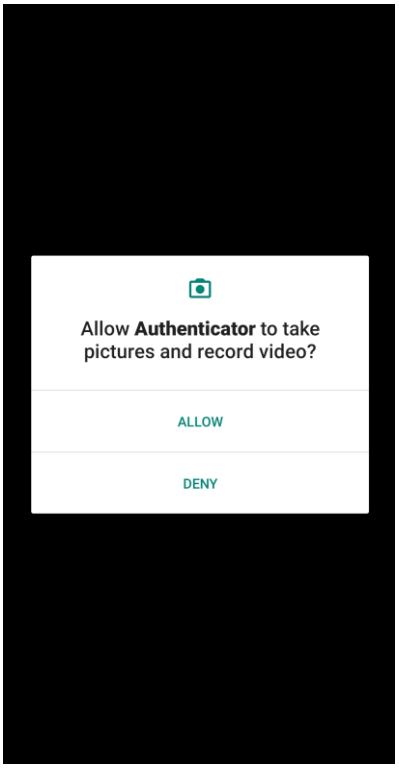
3. Set up the account by selecting from the following methods: Scan the QR code or Enter a setup key manually.

Method 1: Scan the QR code

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

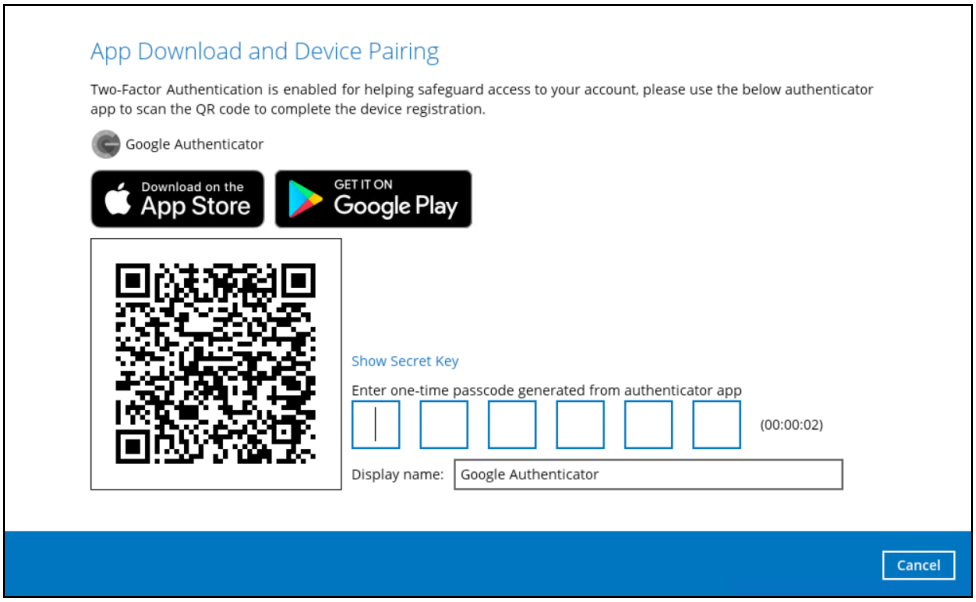


ii. Allow permission to take pictures and record video.

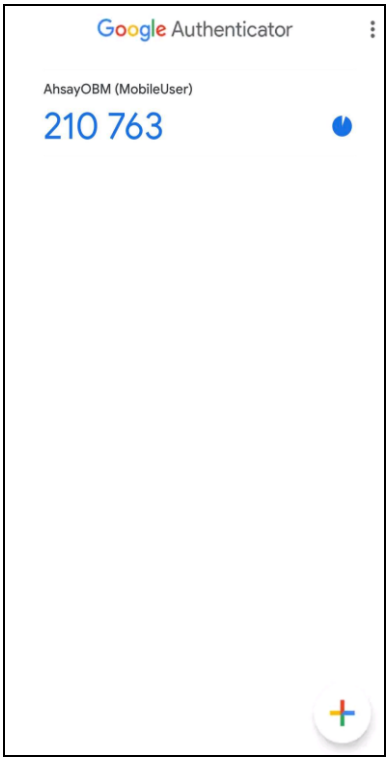


iii. Scan the QR code on AhsayOBM.

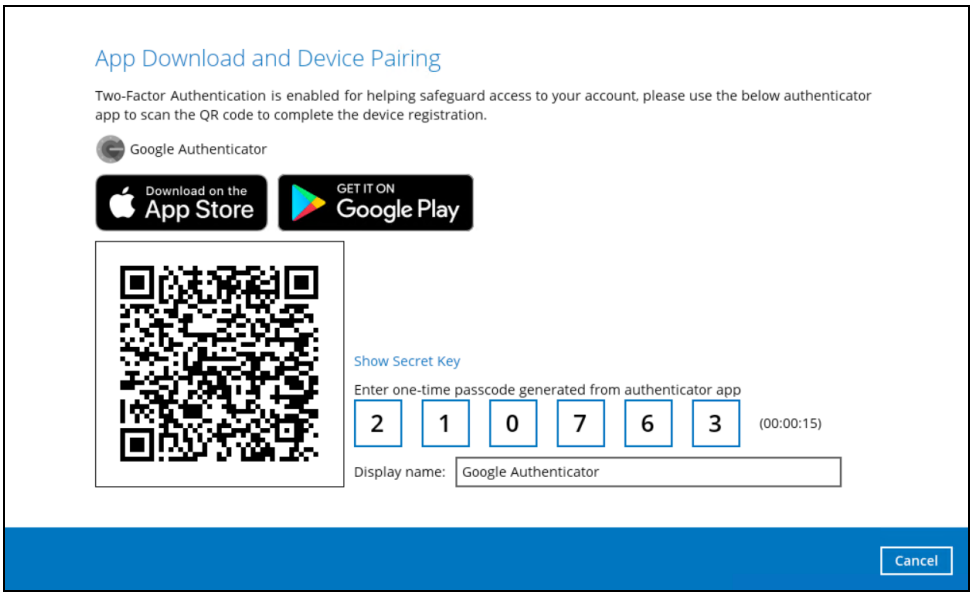
Example of the displayed QR code:



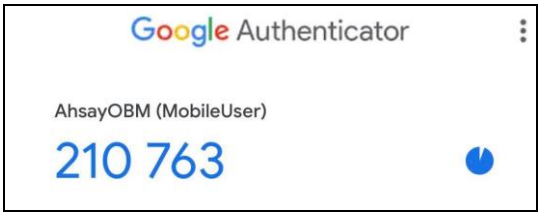
iv. The AhsayOBM account is successfully added to Google Authenticator and the mobile device is registered in AhsayOBM.



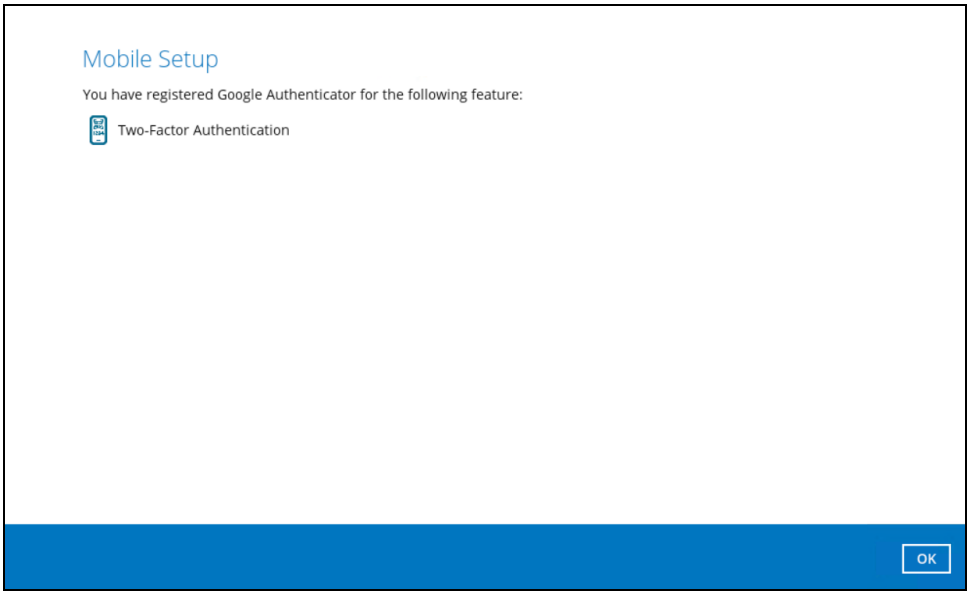
v. Once the account is added to Google Authenticator, enter the one-time passcode generated from the authenticator app to AhsayOBM.



Example of the one-time passcode generated:

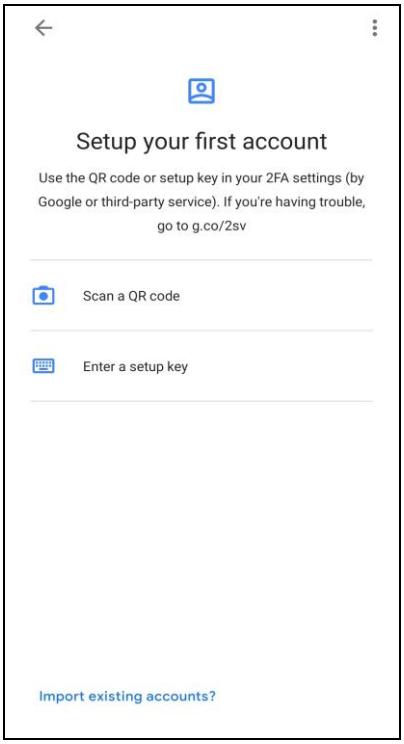


vi. The device is successfully registered for TOTP 2FA in AhsayOBM using Google Authenticator. Click **OK** to continue.

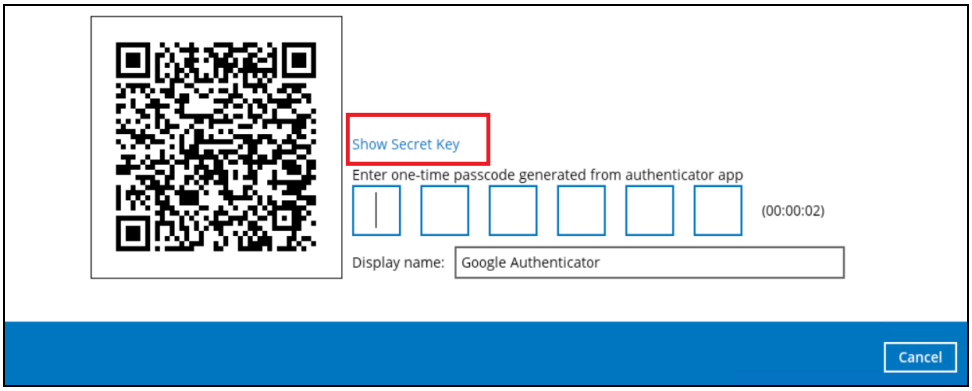


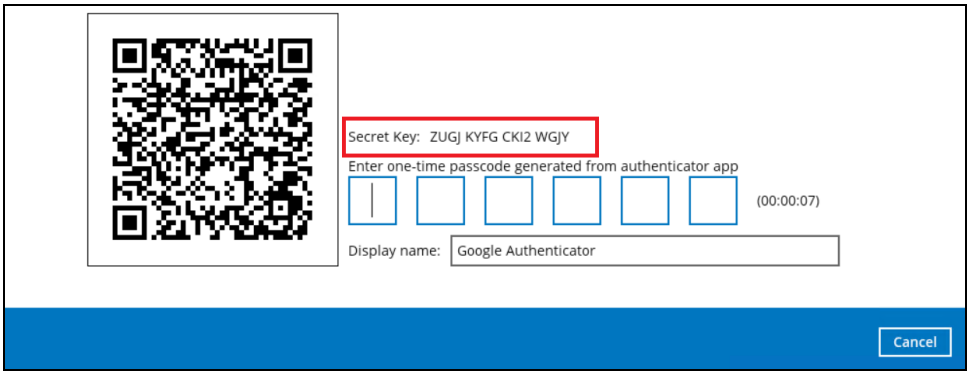
Method 2: Enter a setup key manually

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

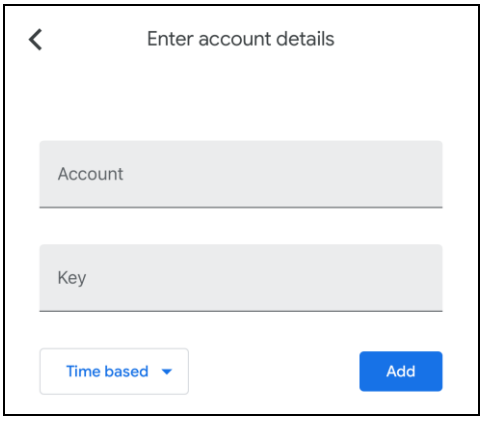


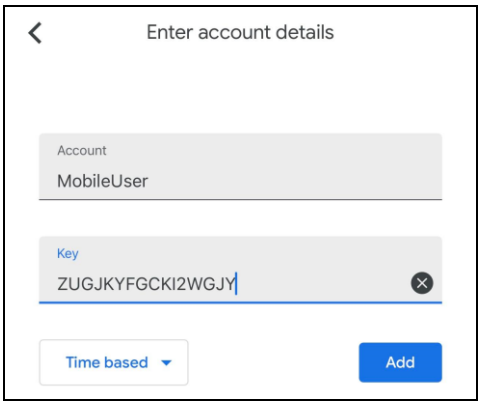
ii. Click the **Show Secret Key** link in the AhsayOBM to display the Secret Key which must be entered manually on the Google Authenticator.



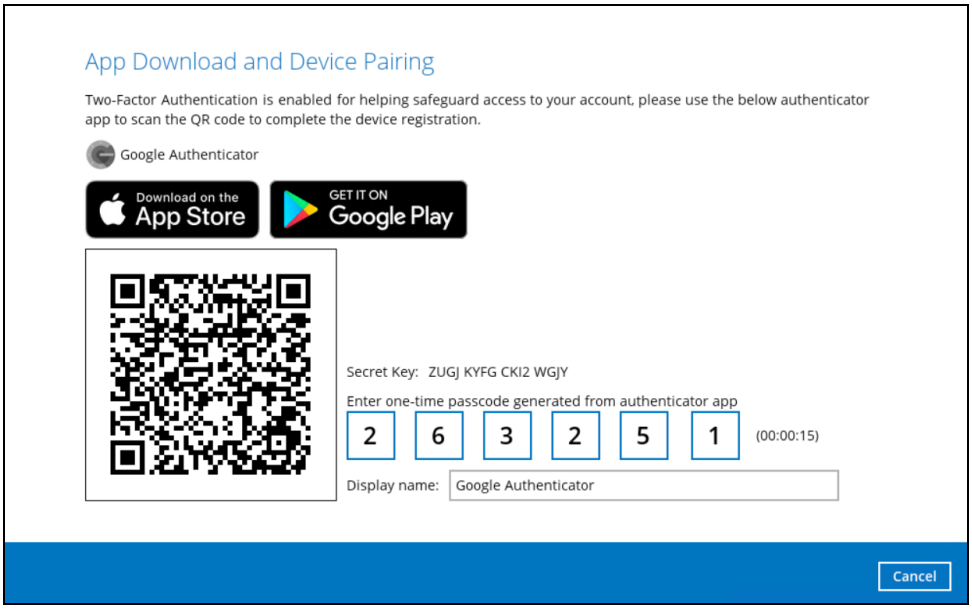


iii. On the Google Authenticator app, input an account name, then enter the displayed Secret Key in the AhsayOBM. Tap **Add** to proceed.

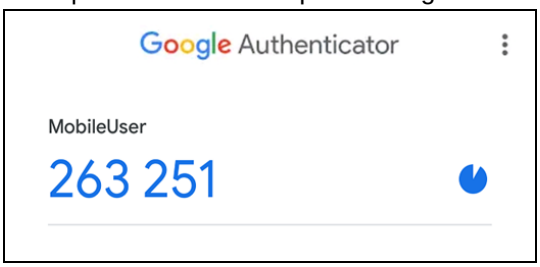




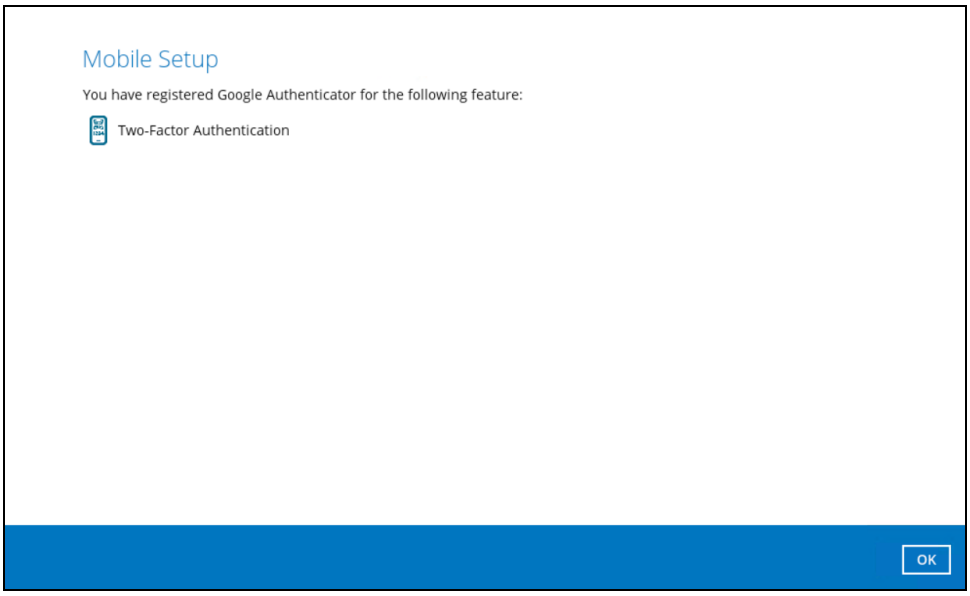
iv. Once the account is added to Google Authenticator, enter the one-time passcode generated from the authenticator app to AhsayOBM.



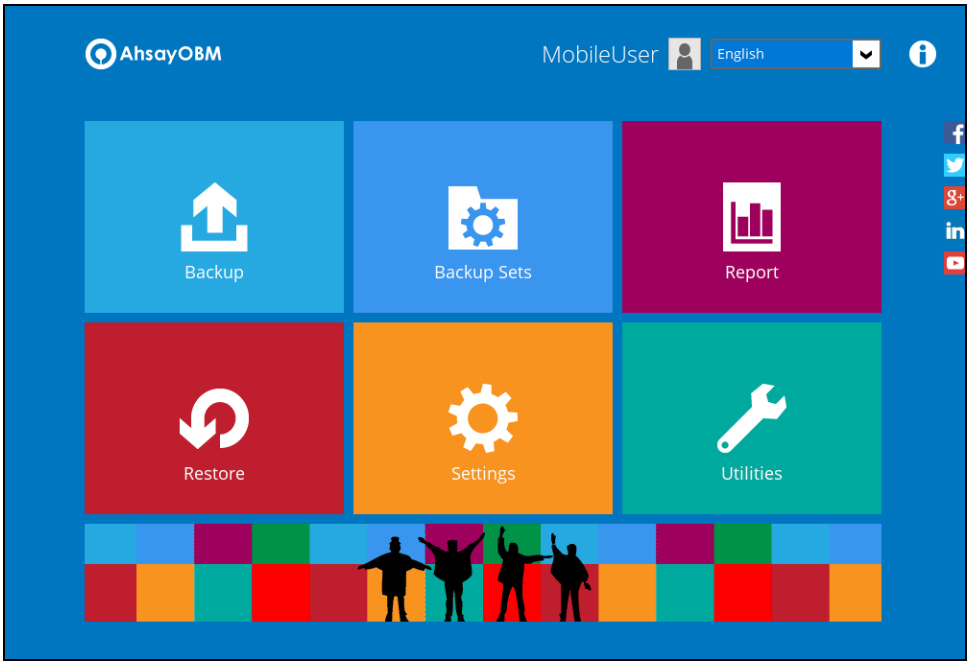
Example of the one-time passcode generated:



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.



8 Logging in to AhsayOBM

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

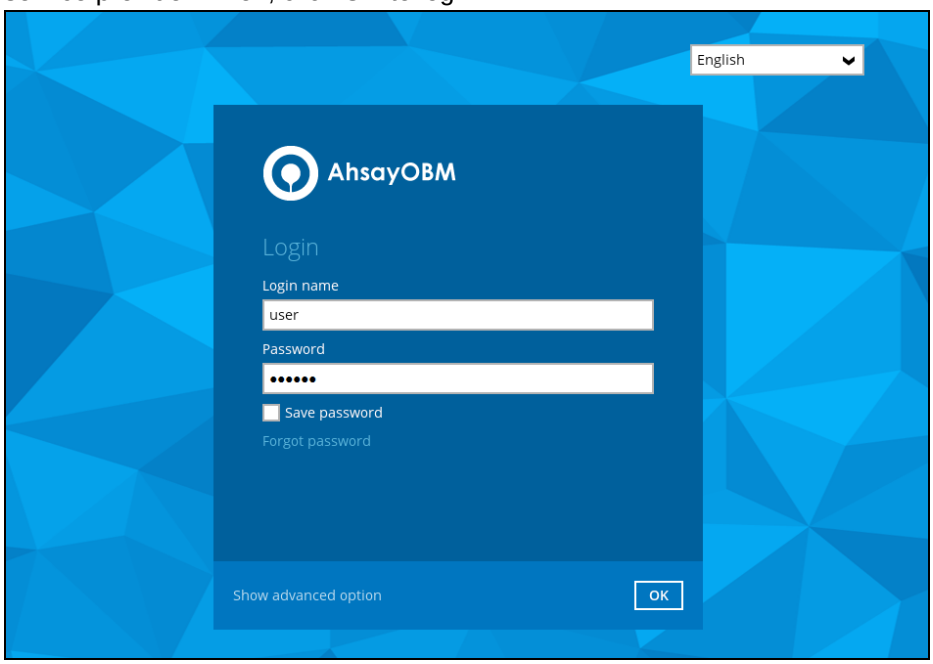
- Login to AhsayOBM without 2FA
- Login to AhsayOBM with 2FA using Ahsay Mobile Authenticator
  - Push Notification and TOTP 2FA
  - TOTP only 2FA
- Login to AhsayOBM with 2FA using Microsoft Authenticator
- Login to AhsayOBM with 2FA using Google Authenticator
- Login to AhsayOBM with 2FA using Twilio

8.1 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.

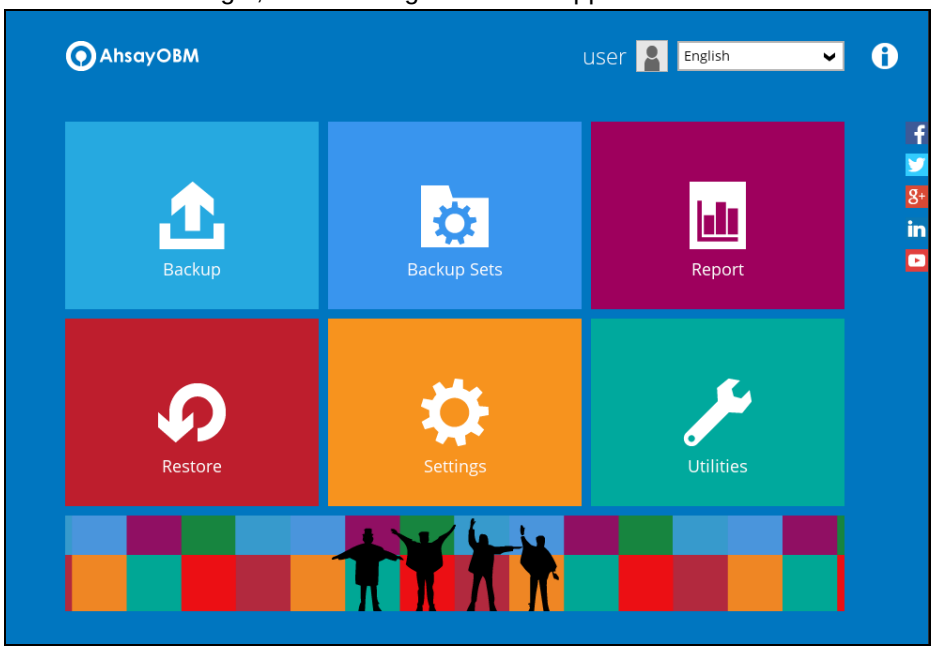
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.



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.

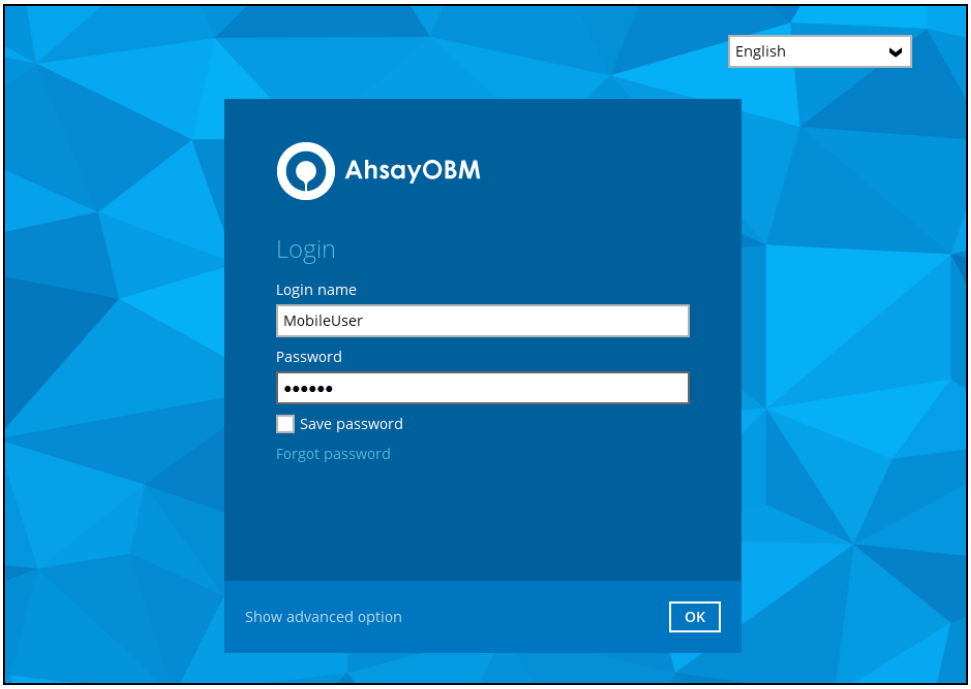


8.2 Login to AhsayOBM with 2FA using Ahsay Mobile Authenticator

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.



NOTE

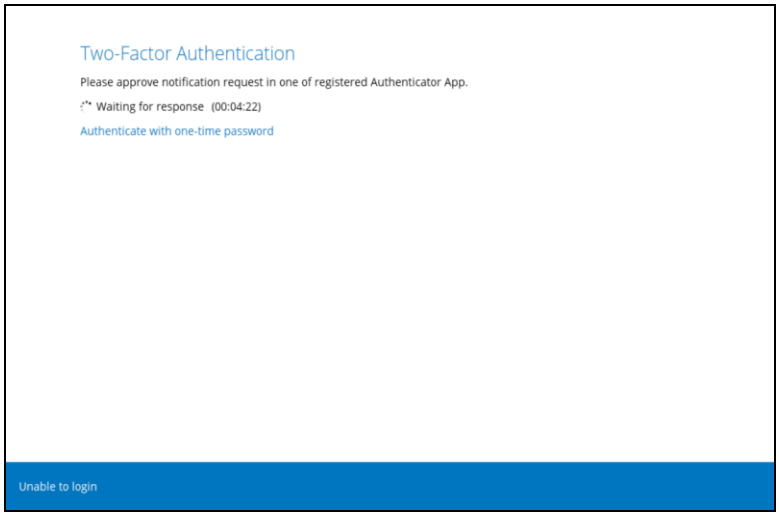
The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

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

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

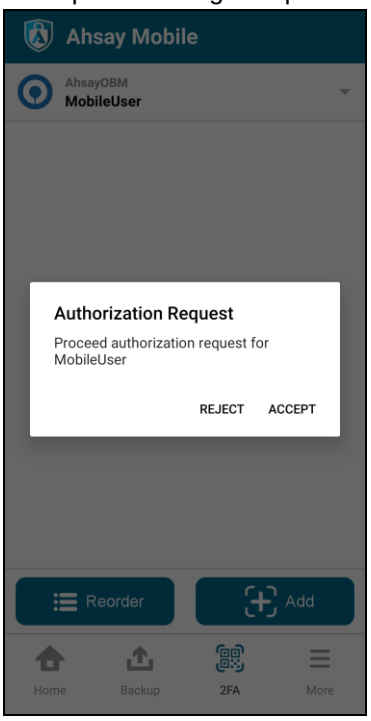
- **Push Notification and TOTP (default mode)**

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

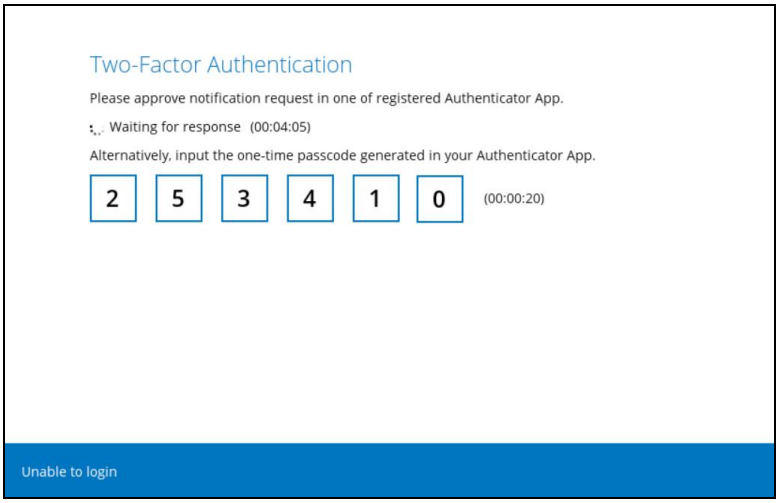


  Push notification is the default 2FA mode. Accept the login request on the Ahsay Mobile app to complete the login.

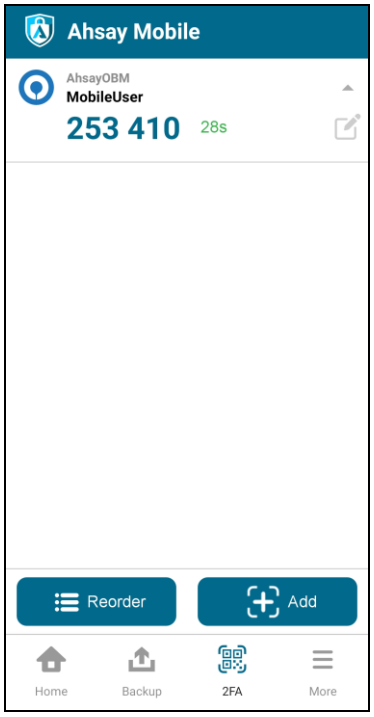
Example of the login request sent to the Ahsay Mobile:



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.



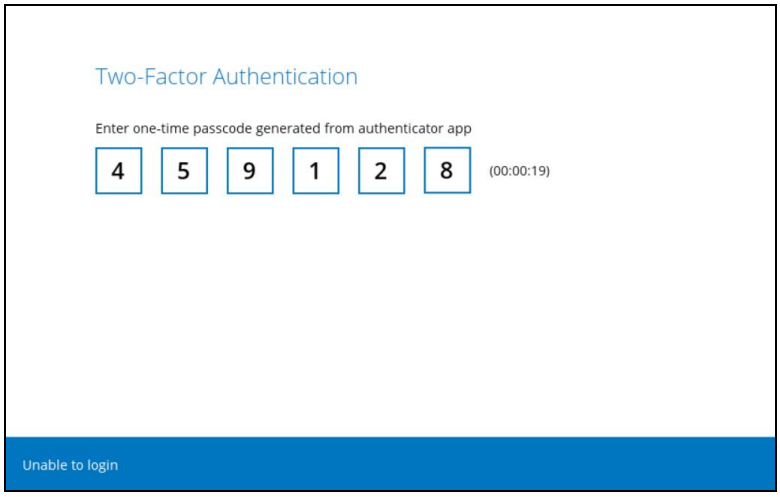
Example of the one-time password generated by Ahsay Mobile:



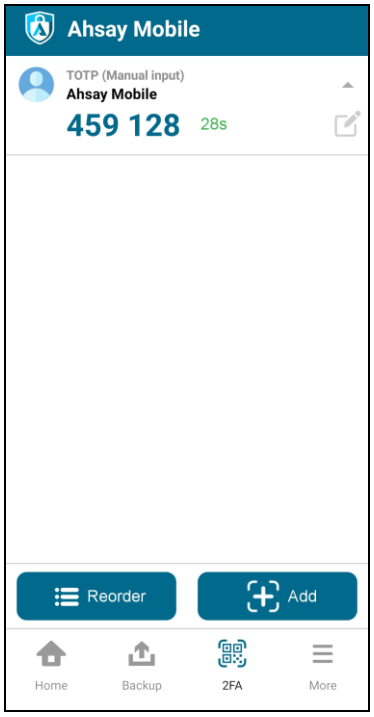
- **TOTP only**

  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.



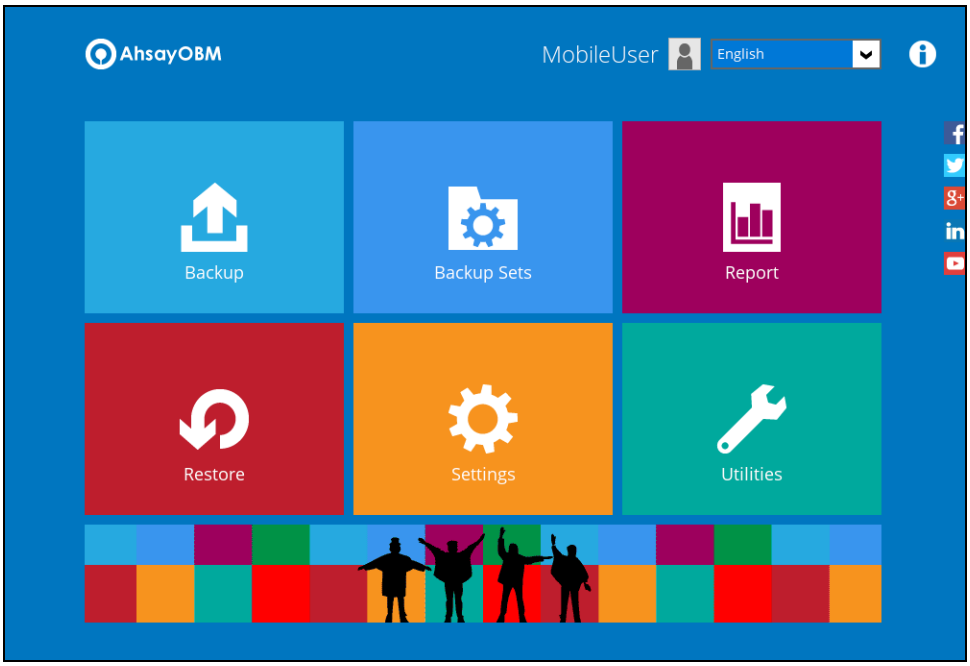
Example of the one-time password generated by Ahsay Mobile:



NOTE

If you are unable to log in using any of the authentication method, please refer to Chapter 9 Unable to log in to AhsayOBM with 2FA.

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

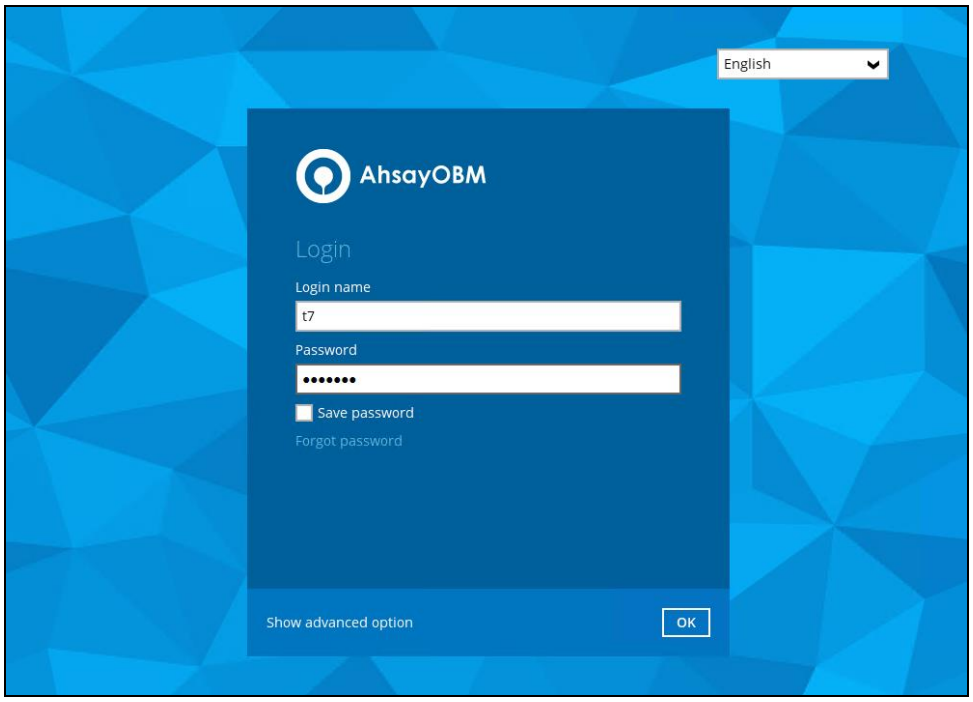


8.3 Login to AhsayOBM with 2FA using Microsoft Authenticator

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.

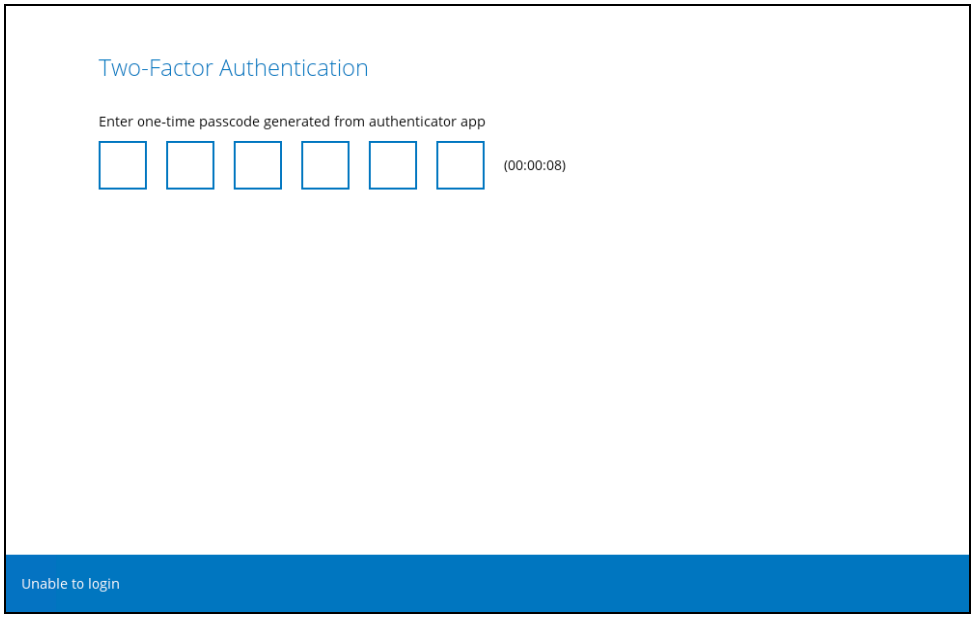
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.



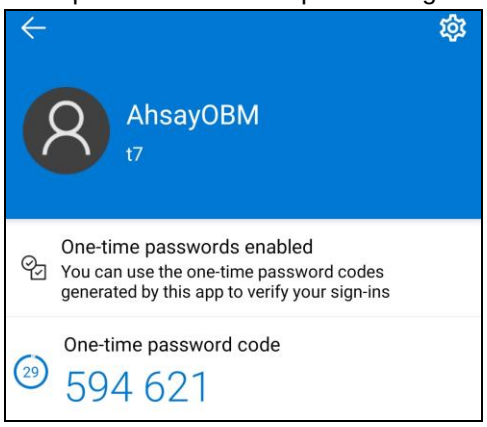
NOTE

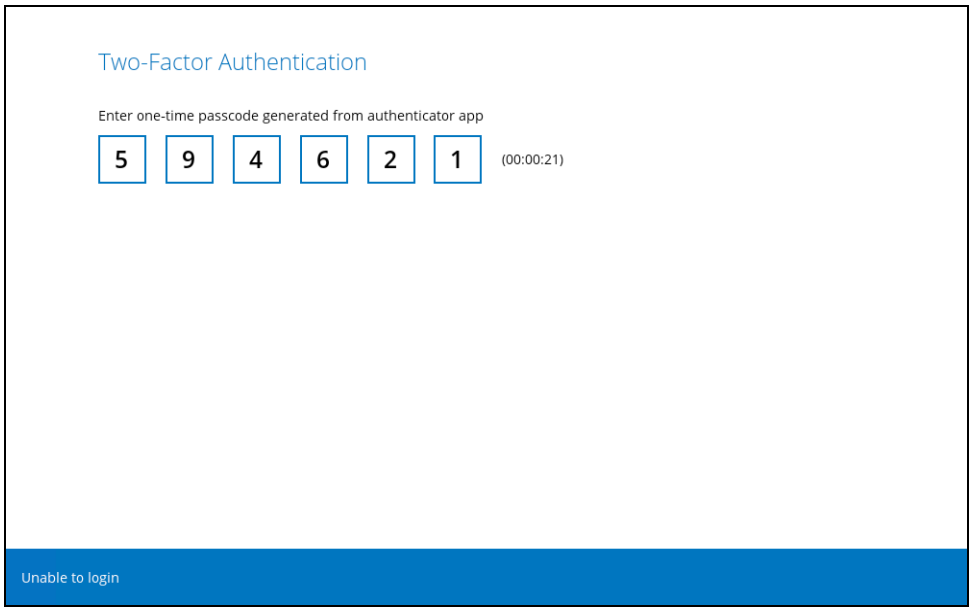
The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

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

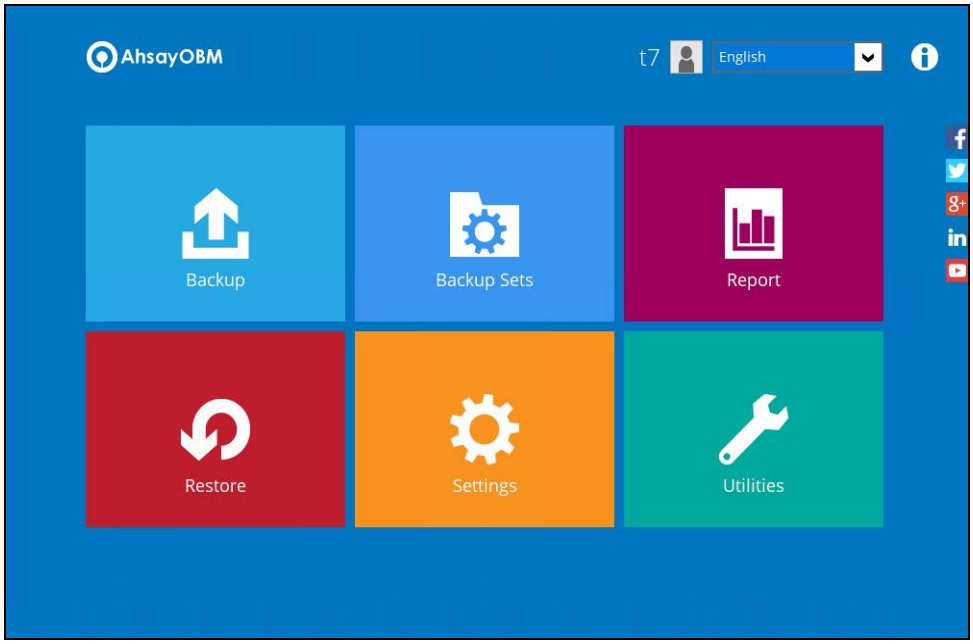


Example of the one-time passcode generated:





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

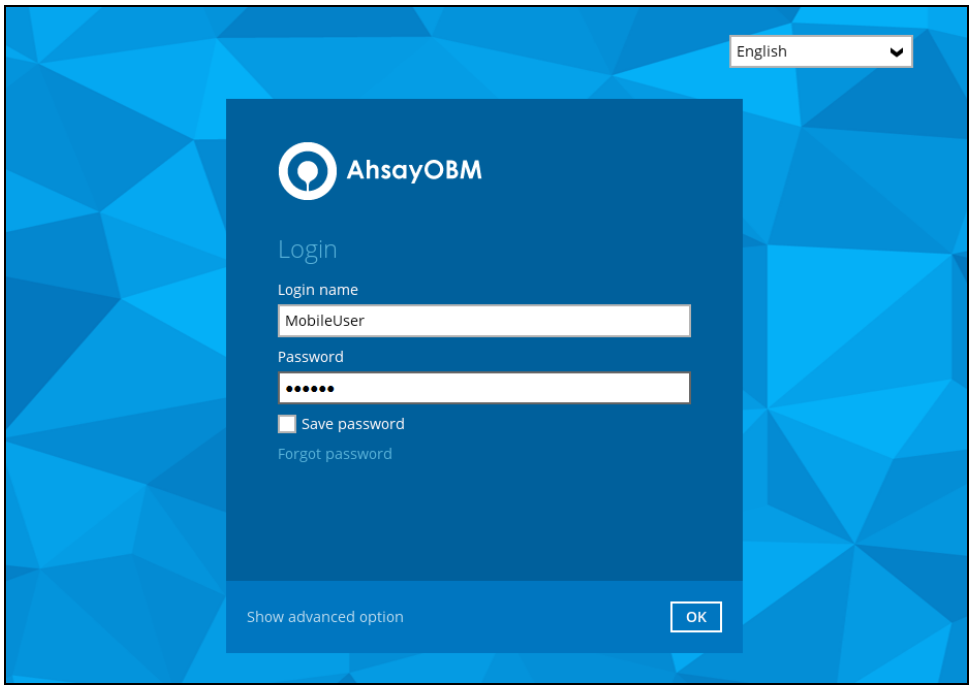


8.4 Login to AhsayOBM with 2FA using Google Authenticator

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.

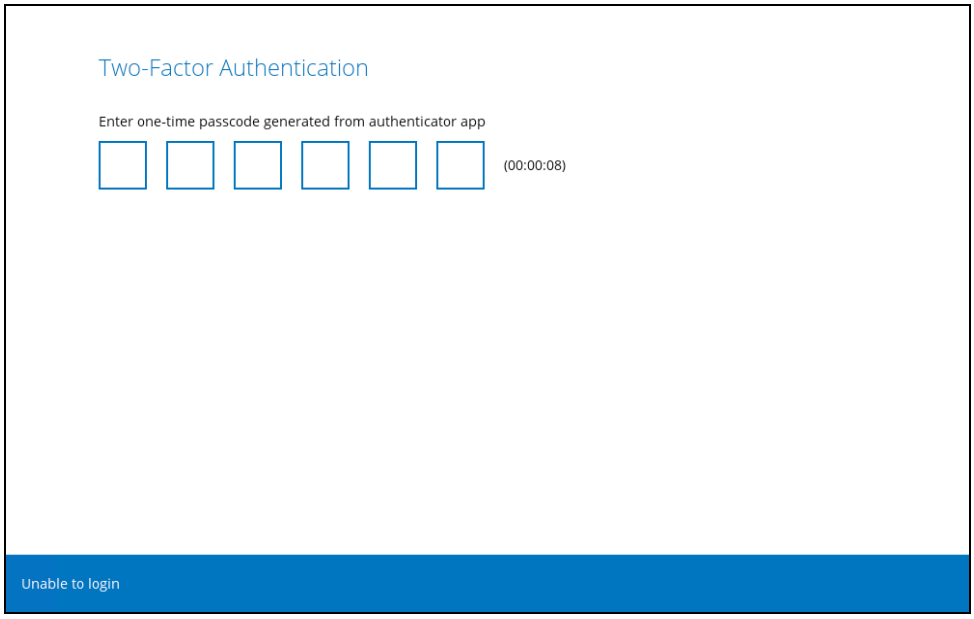
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.



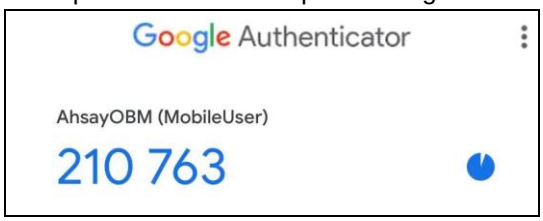
NOTE

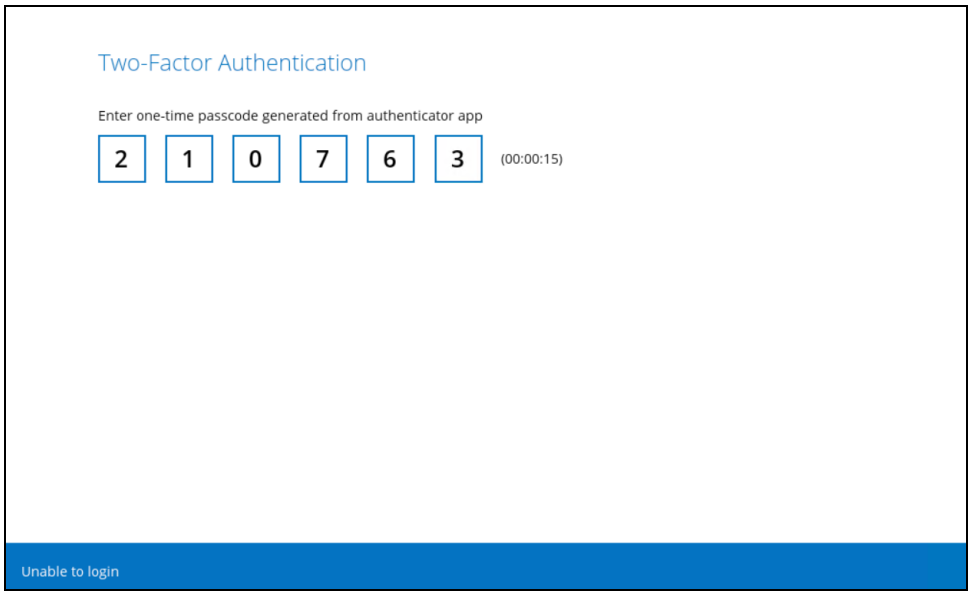
The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

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

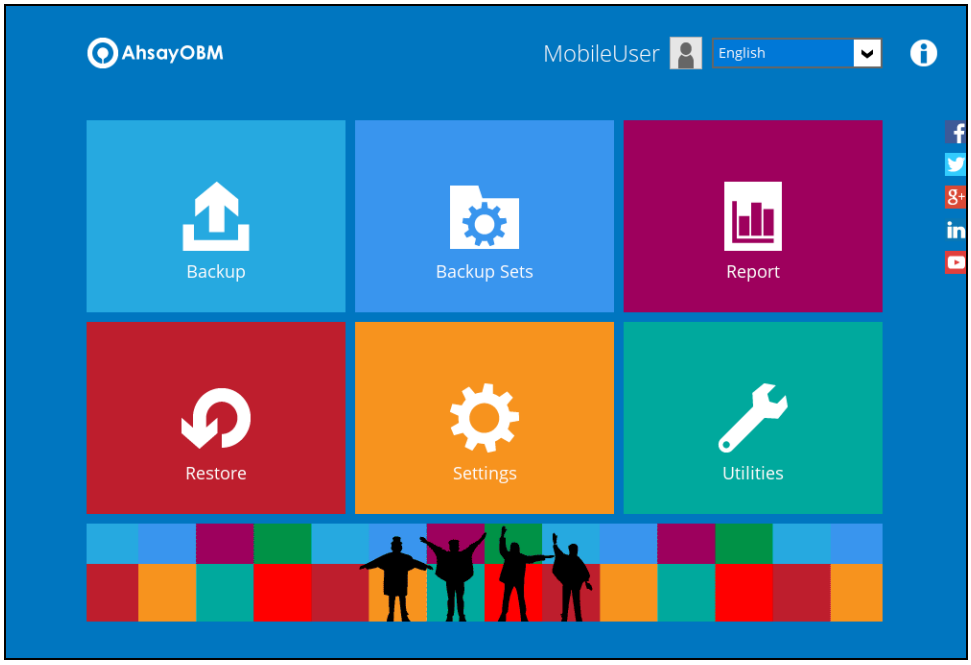


Example of the one-time passcode generated:





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

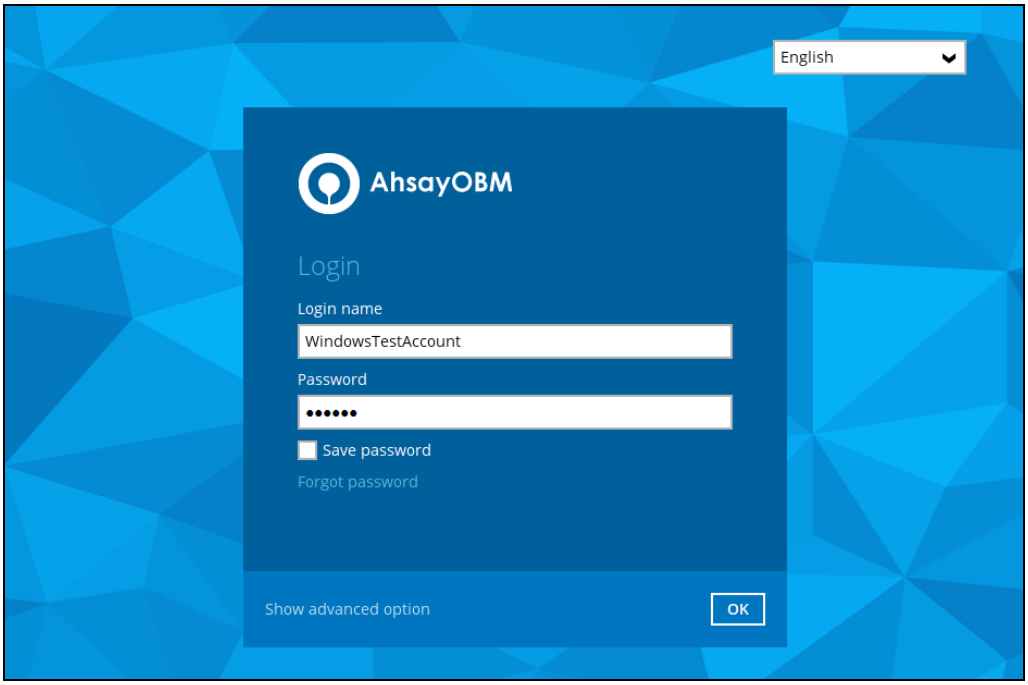


8.5 Login to AhsayOBM with 2FA using Twilio

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

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

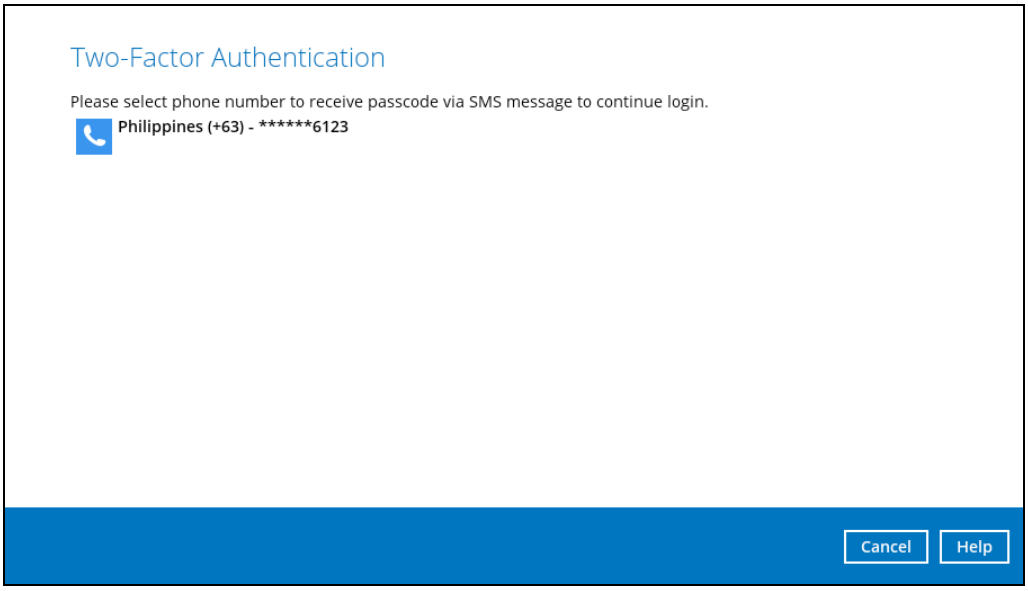
2. Enter the login name and password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to log in.



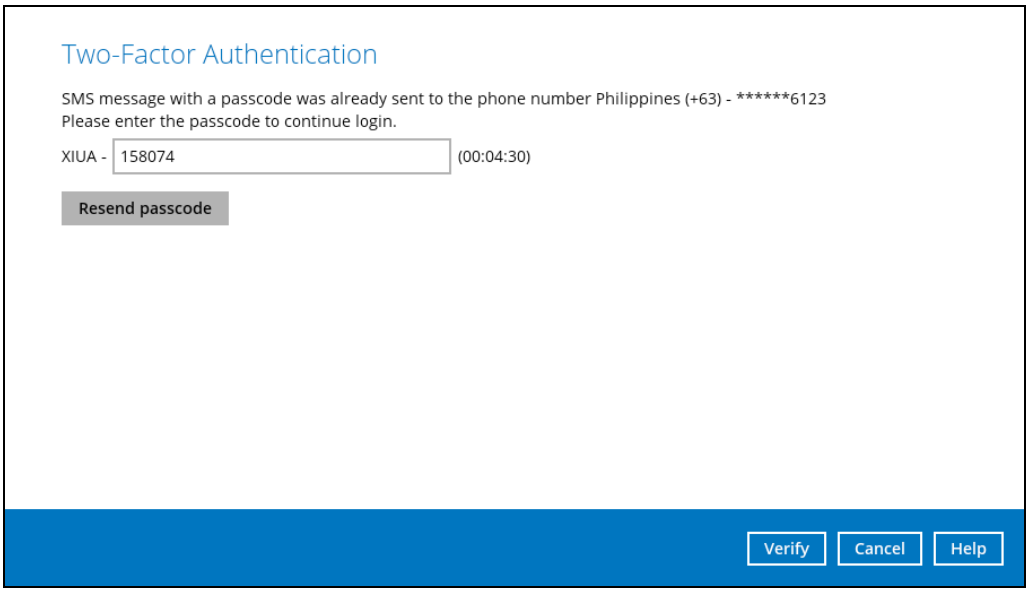
NOTE

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.

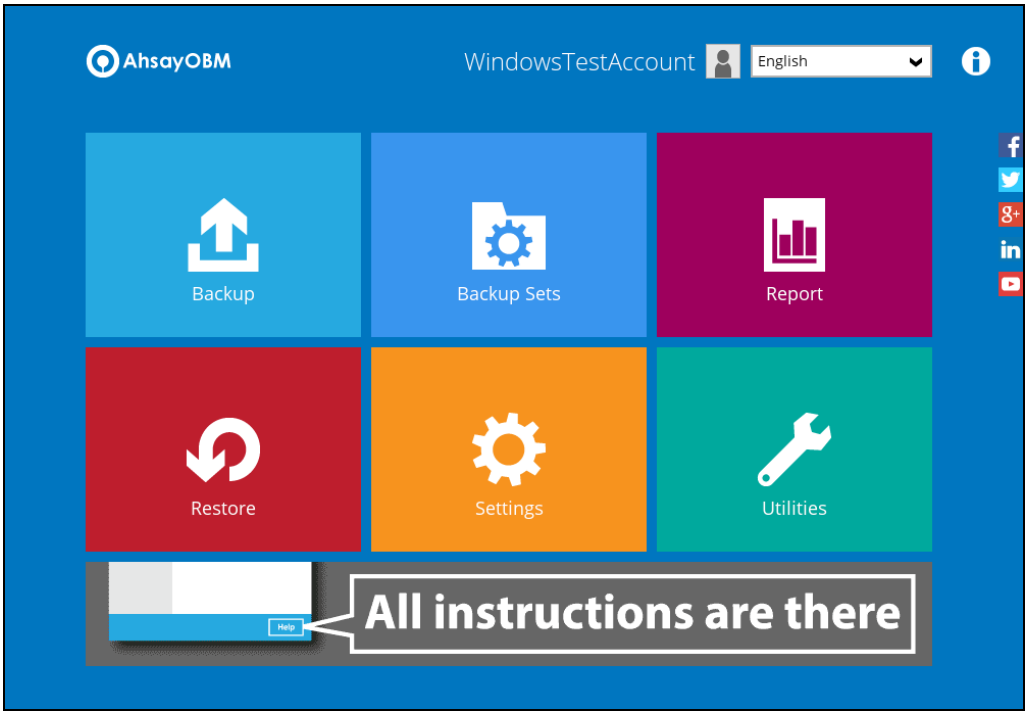
3. Select your phone number to receive the passcode.



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



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

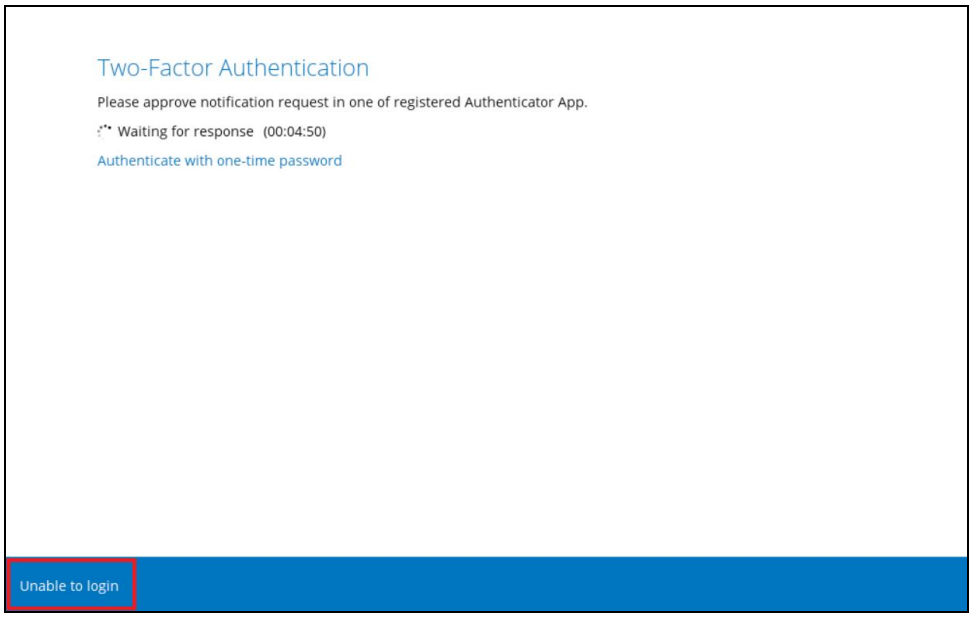


9 Unable to log in to AhsayOBM with 2FA

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.

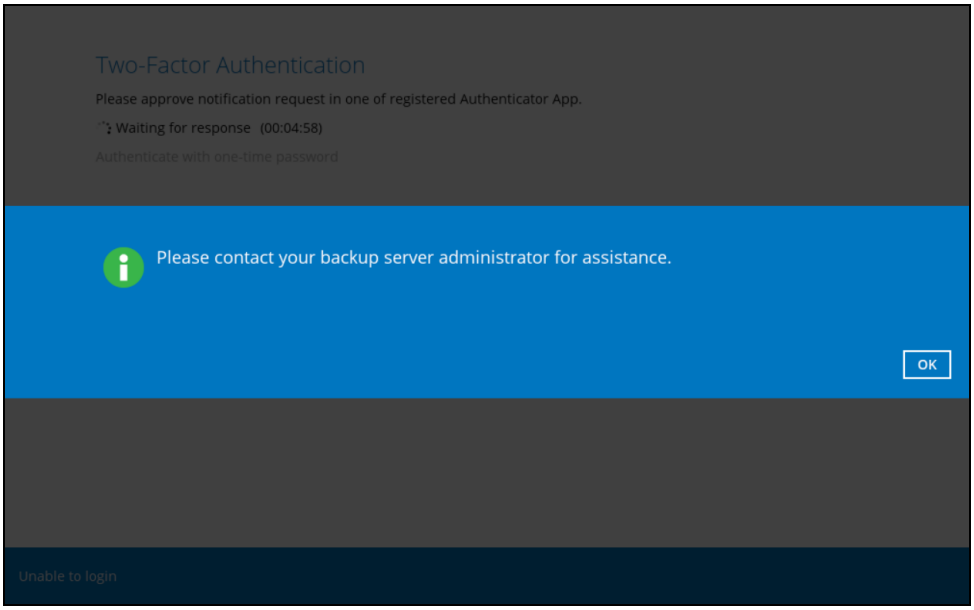
Here are the three scenarios after clicking the **Unable to login** link:

- 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

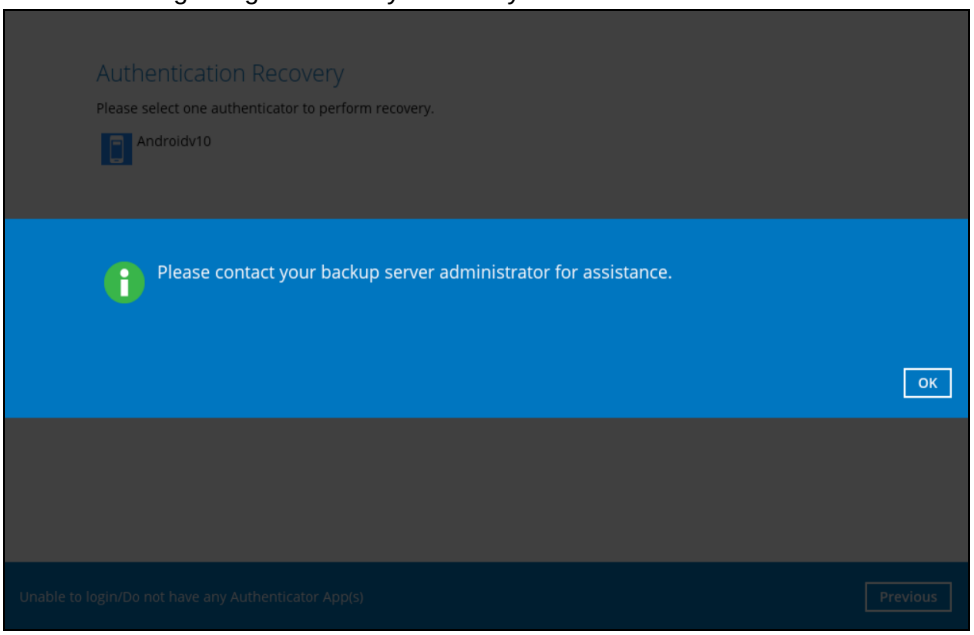
If a recovery number was registered on Ahsay Mobile for the 2FA account, then select the registered mobile device to perform the following "Authentication Recovery" procedure.

NOTE

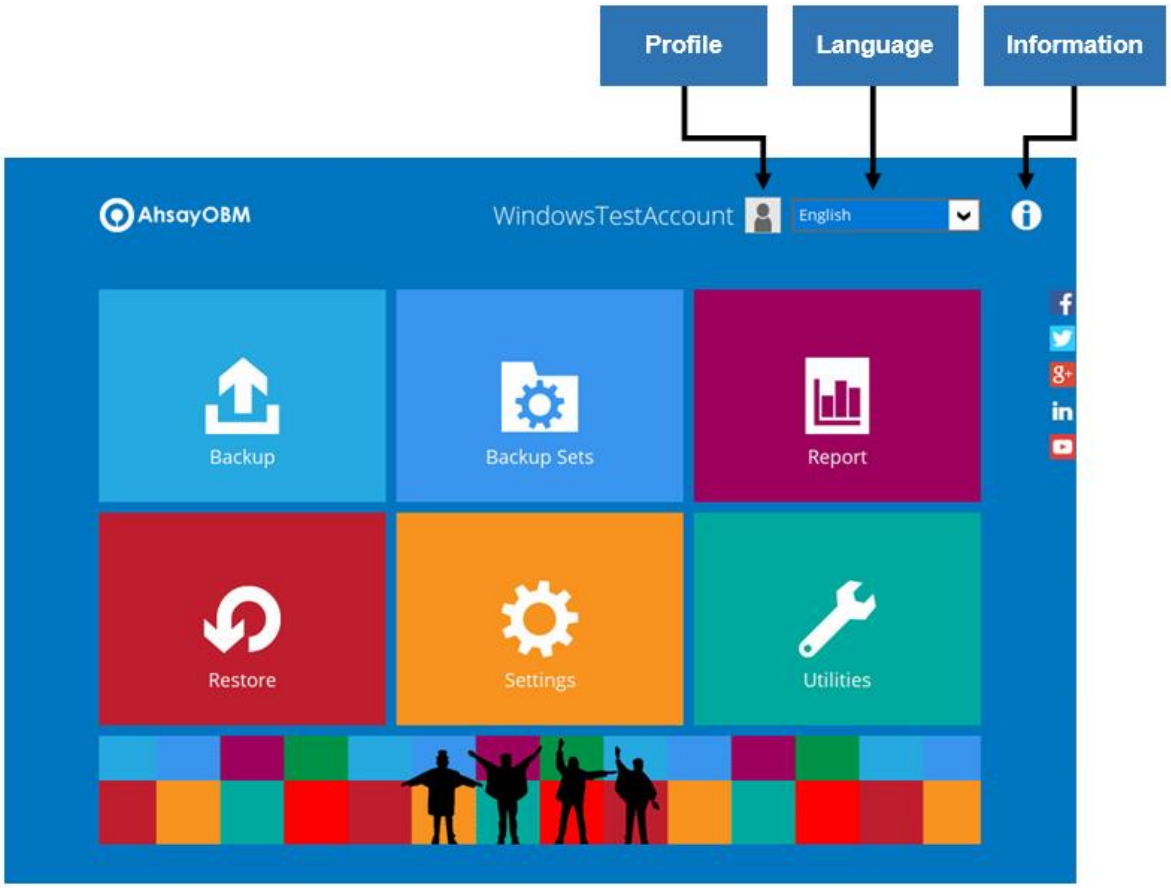
For the detailed steps in performing Authentication Recovery, please refer to the **Ahsay Mobile User Guide for Android and iOS – Appendix A: Troubleshooting Login**.

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.



10 AhsayOBM Overview



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

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

10.1 Profile

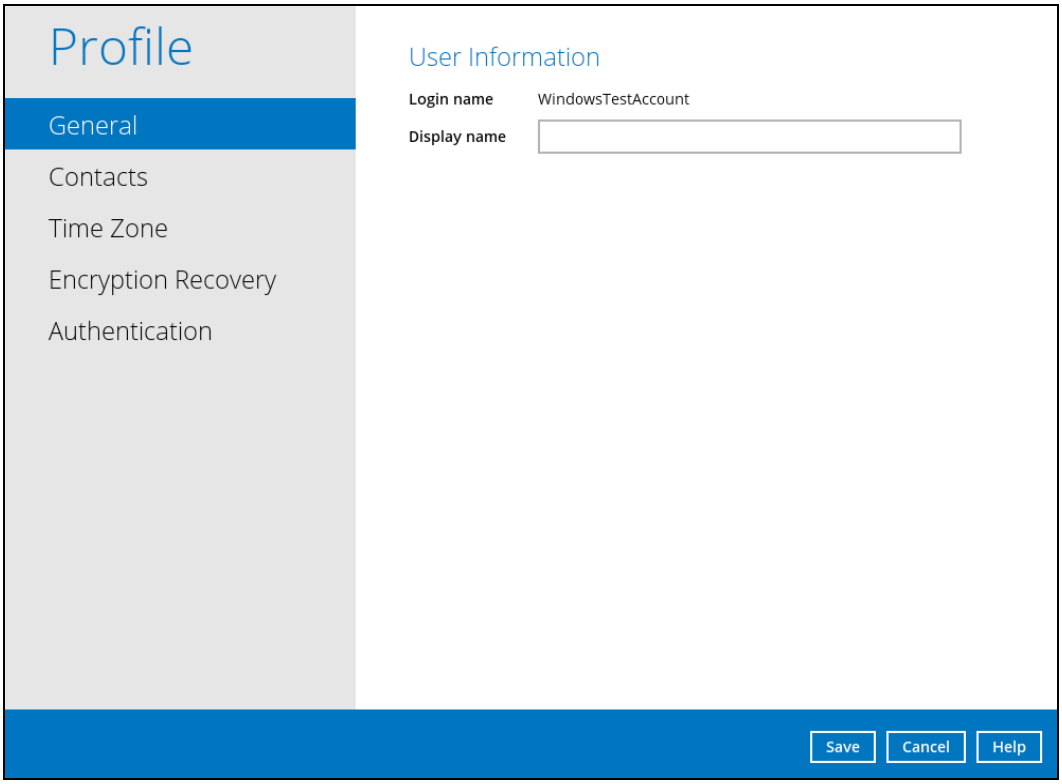
The **Profile** icon shows the settings that can be modified by the user. The features that will be shown will depend on if the user accounts was using Twilio Two-Factor Authentication in prior to upgrading to v8.5.0.0 or above and continues to use Twilio.

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.)

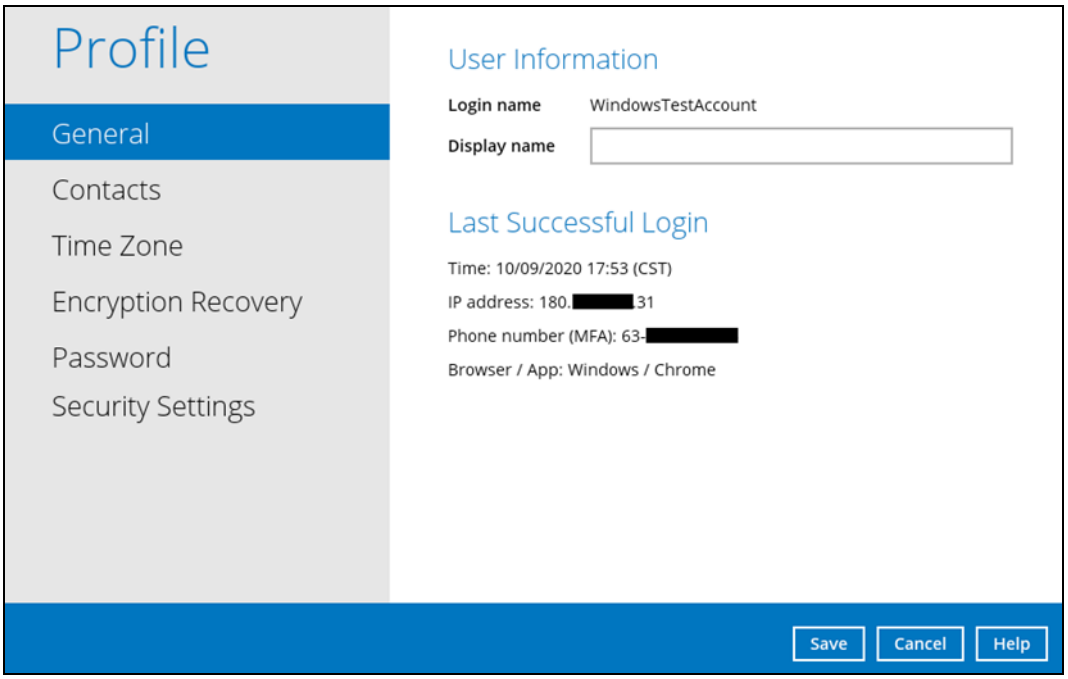
10.1.1 General

The General tab displays the user's information.



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.

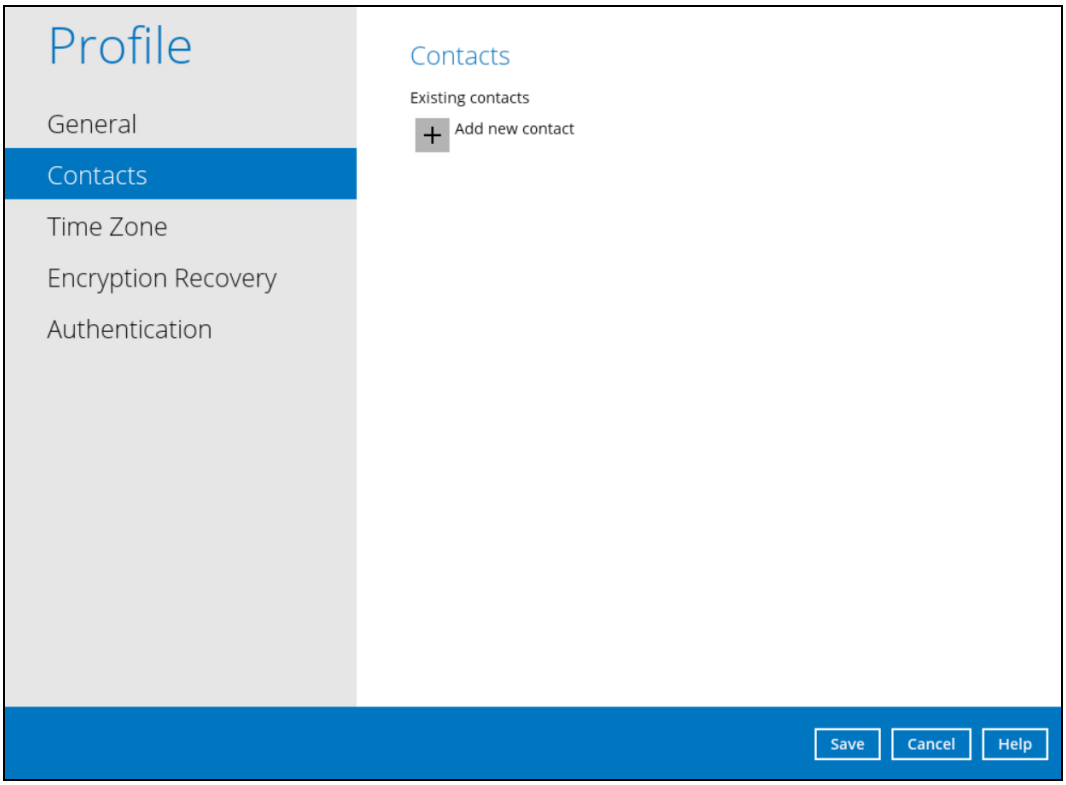
This will be the General tab for old backup account using Twilio for two-factor authentication.



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 log in in to AhsayCBS User Web Console or AhsayOBM.

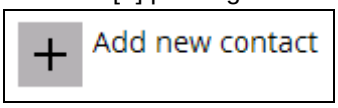
10.1.2 Contacts

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.

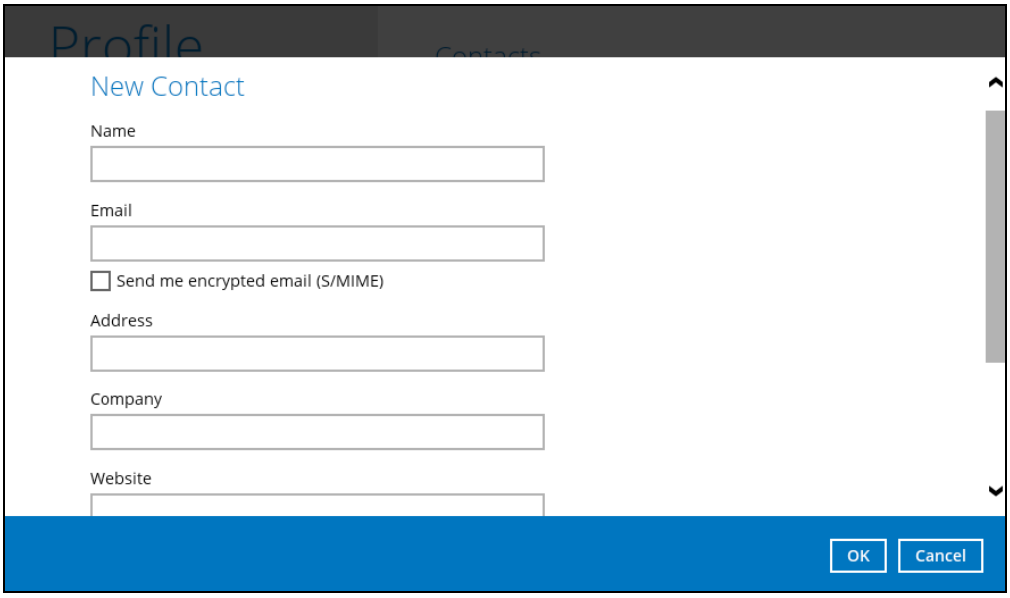


To add a new contact, follow the instructions below:

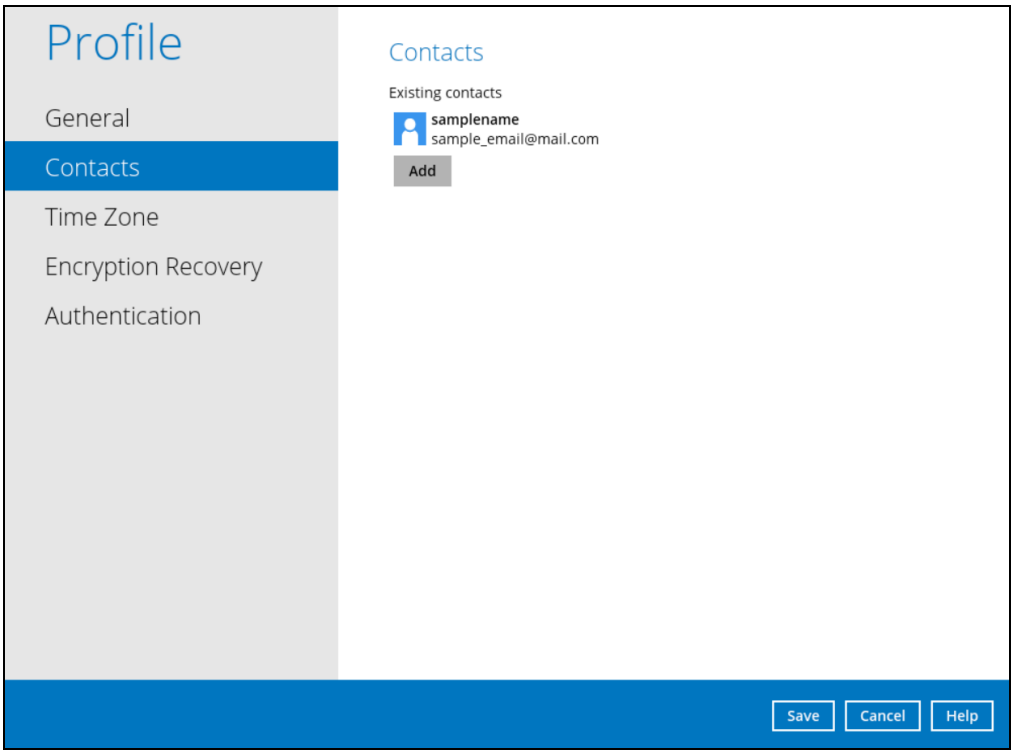
1. Click the [+] plus sign to add a new contact.



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

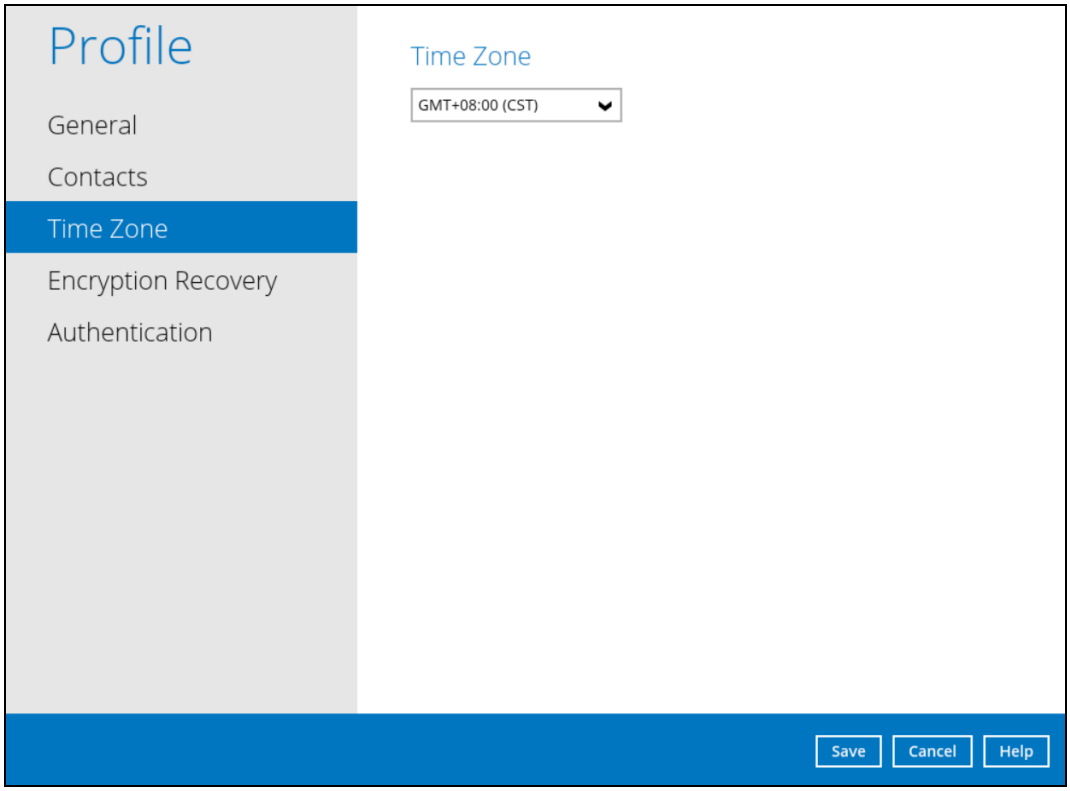


3. Click the [Save] button to store the contact information.



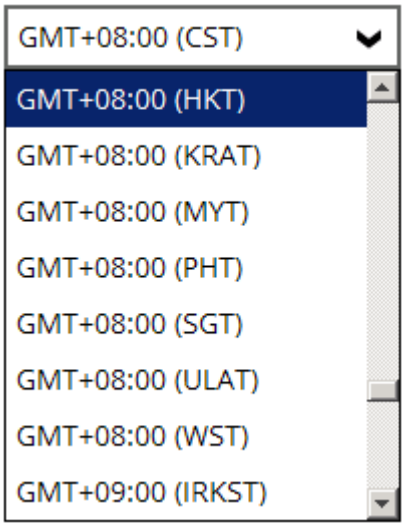
10.1.3 Time Zone

The time zone indicated.



To modify the time zone, follow the instructions below:

1. Select from the dropdown list.

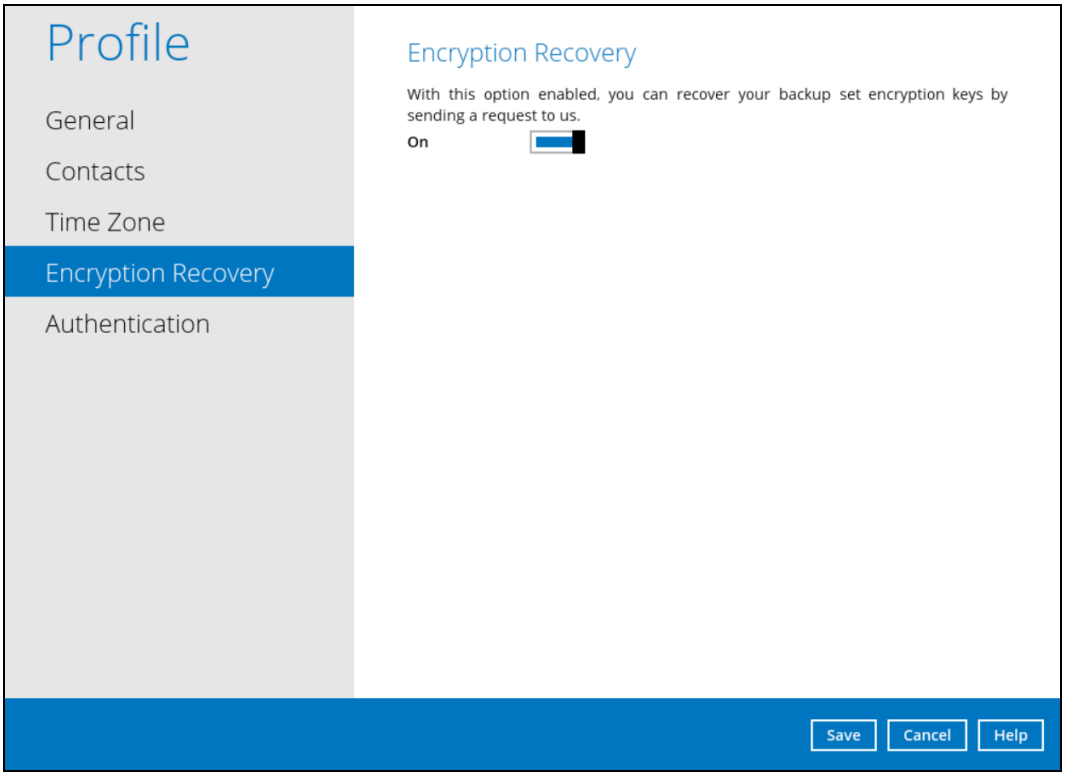


2. Click the [Save] button to save the updated time zone.

10.1.4 Encryption Recovery

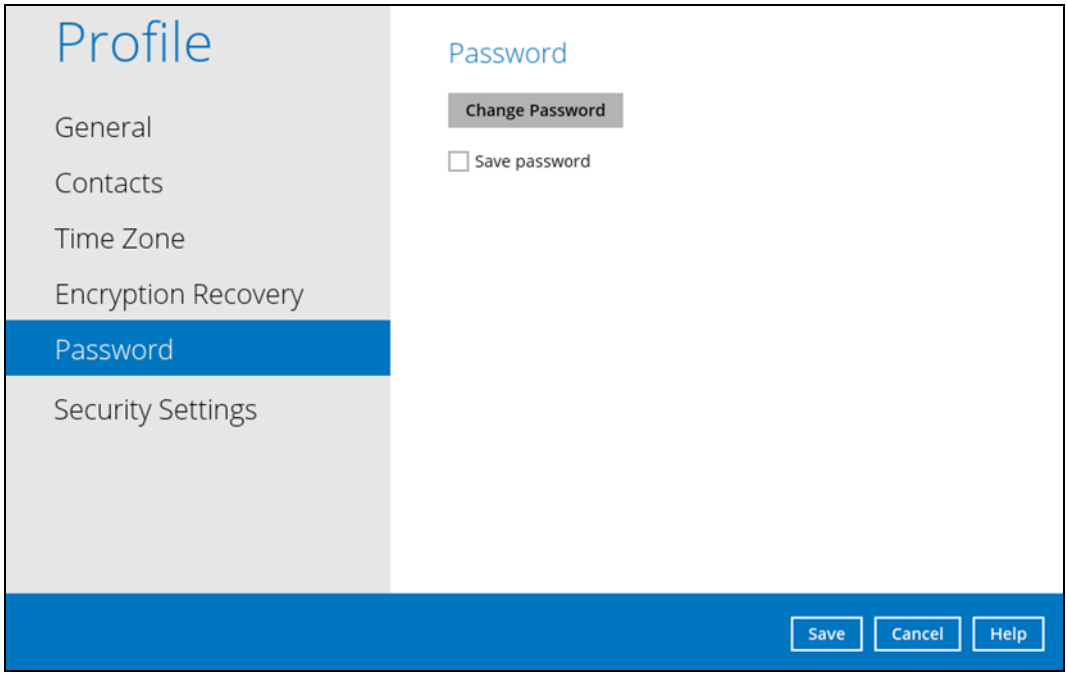
Backup set encryption key can be recovered by turning this feature on.

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



10.1.5 Password

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

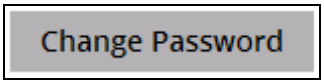


NOTE

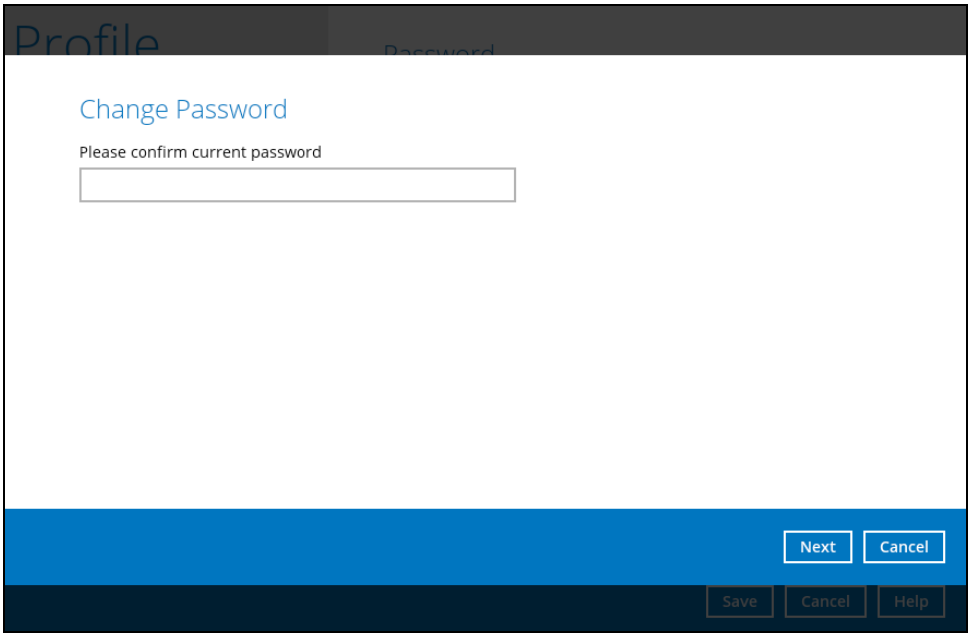
The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

To modify the password, follow the instructions below:

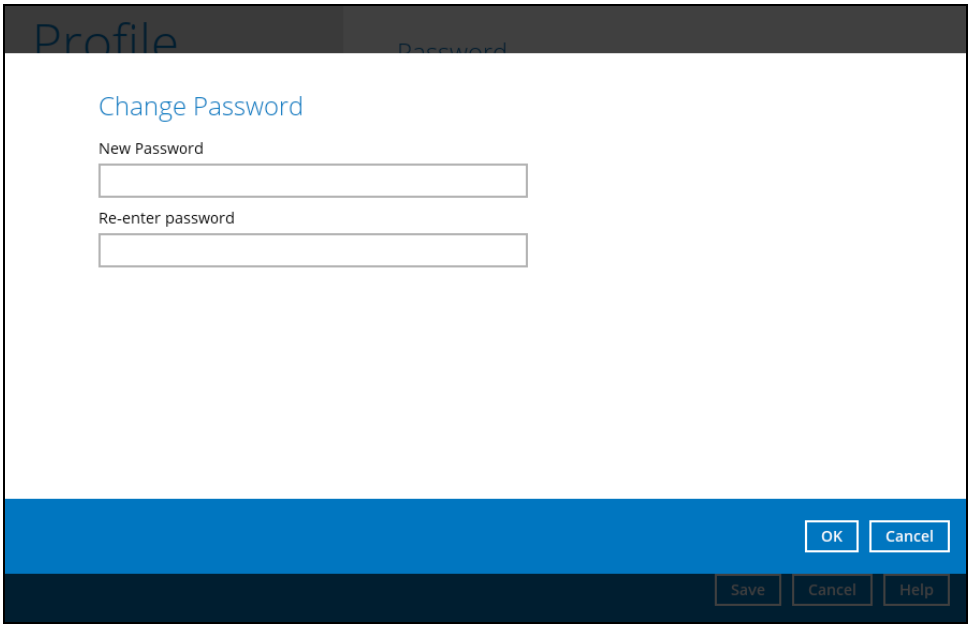
1. Click [Change Password].



2. Enter the current password, then click [Next].



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



4. Click the [Save] button to store the updated password.

10.1.6 Authentication

You can use the Authentication function to:

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

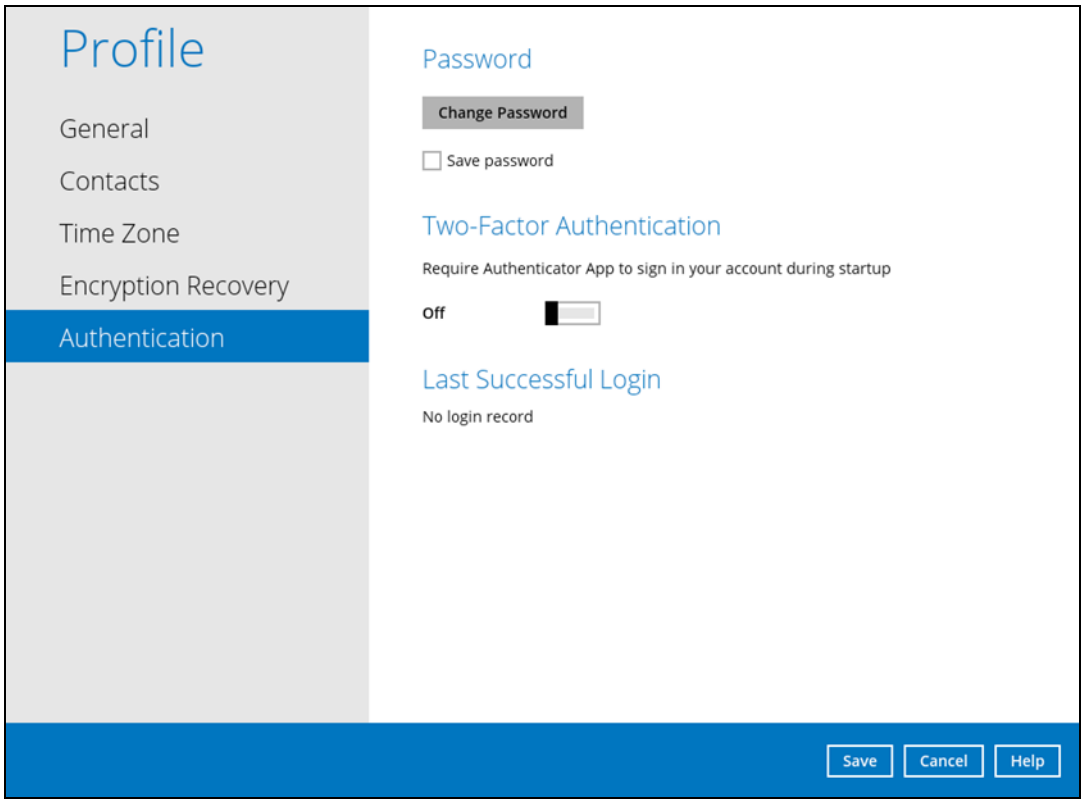
NOTE

Please refer to the **Ahsay Mobile App User Guide for Android and iOS – Chapter 6.3.1** for the detailed step-by-step procedure.

- Remove one or more device(s) registered for Two-Factor Authentication (2FA).
- Re-pair mobile device with AhsayOBM account.
- View details of the "Last Successful Login".

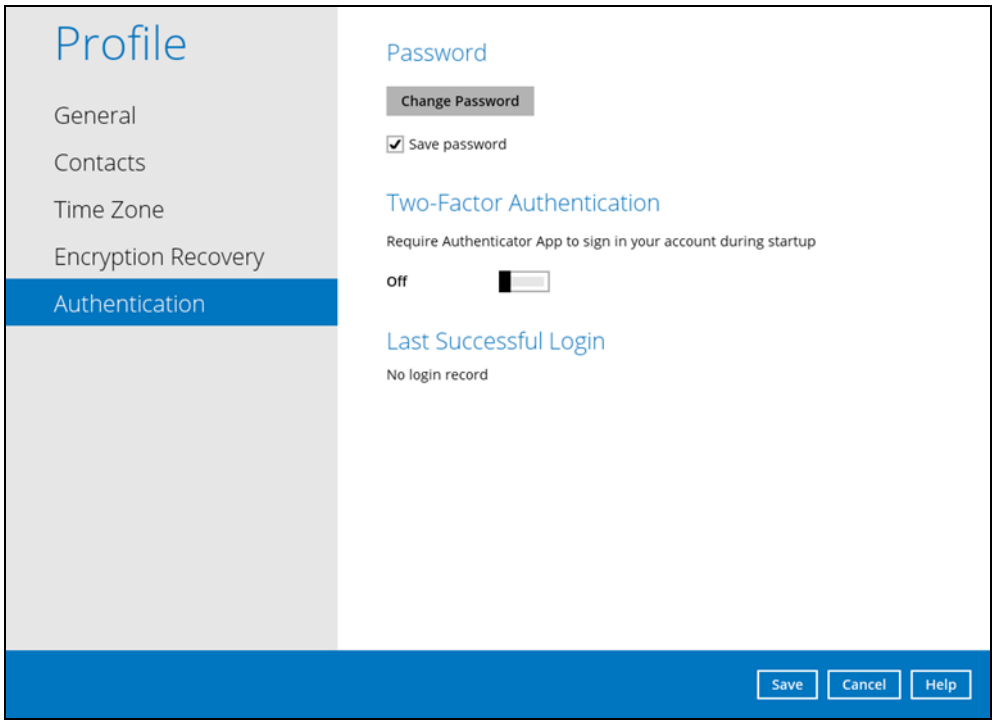
NOTE

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



Password

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

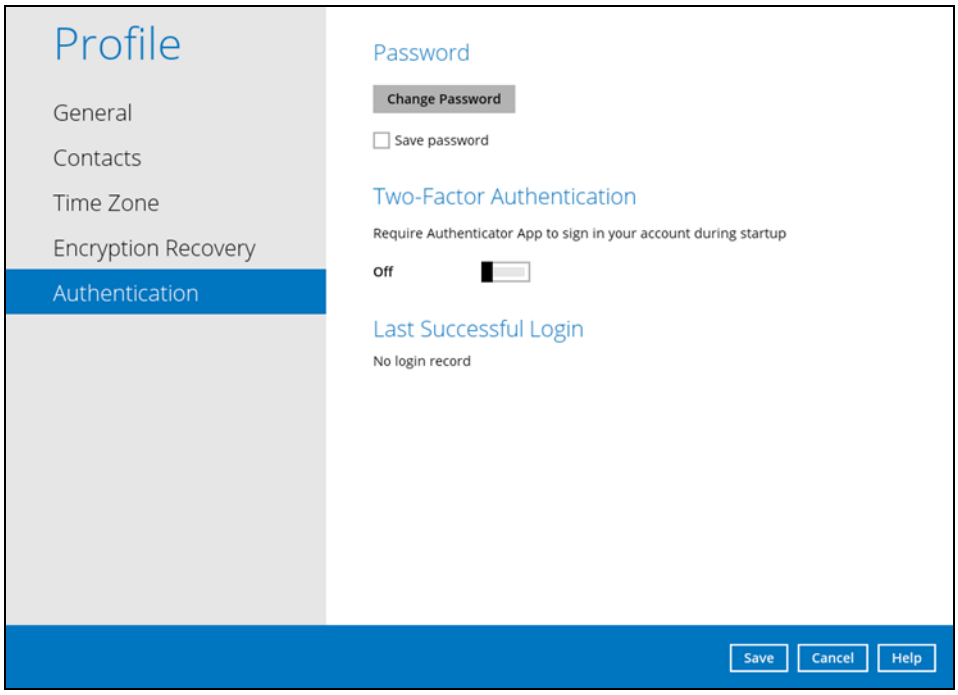


NOTE

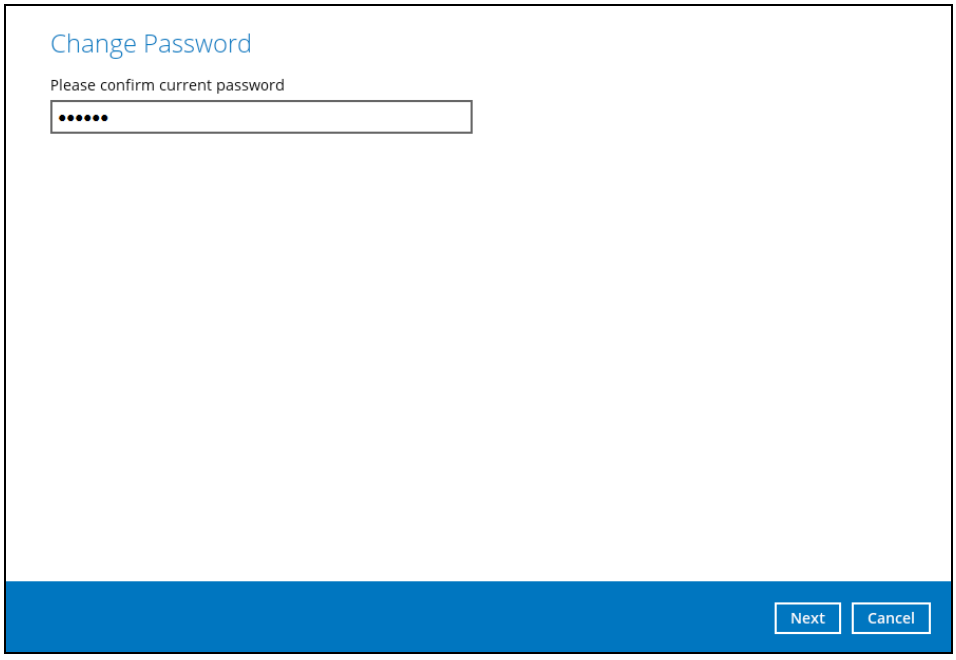
The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

To change the password, follow the instructions below:

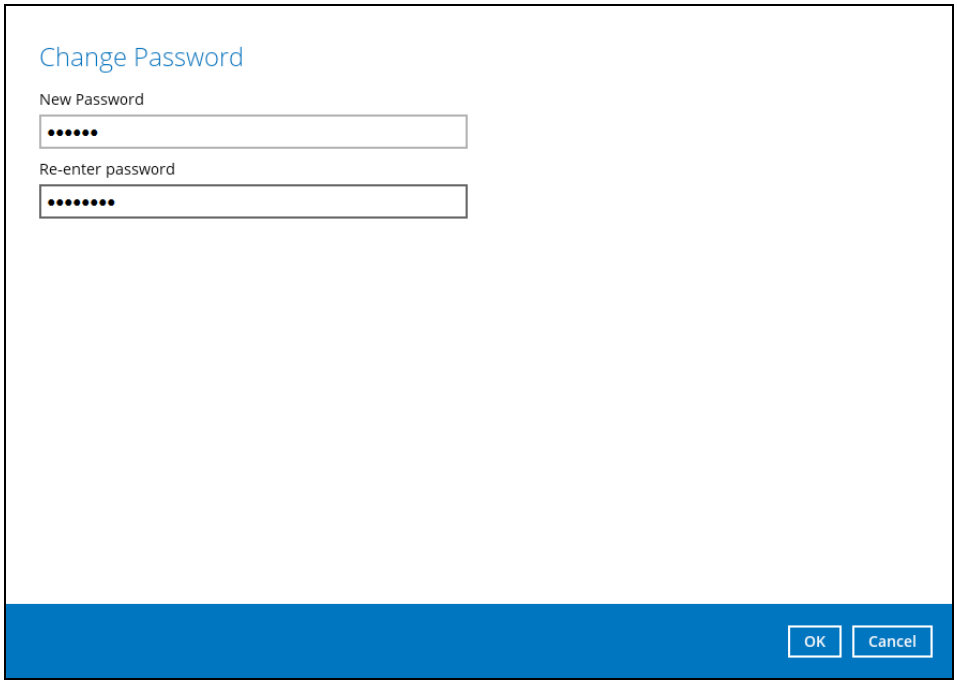
1. Click the **Change Password.**



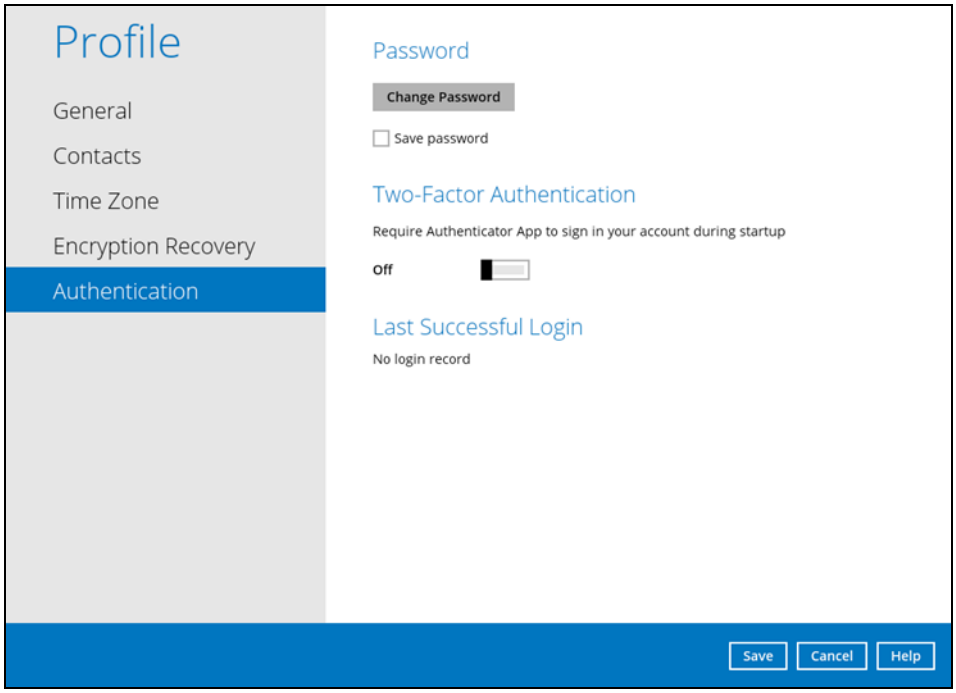
2. Enter the current password.



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



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

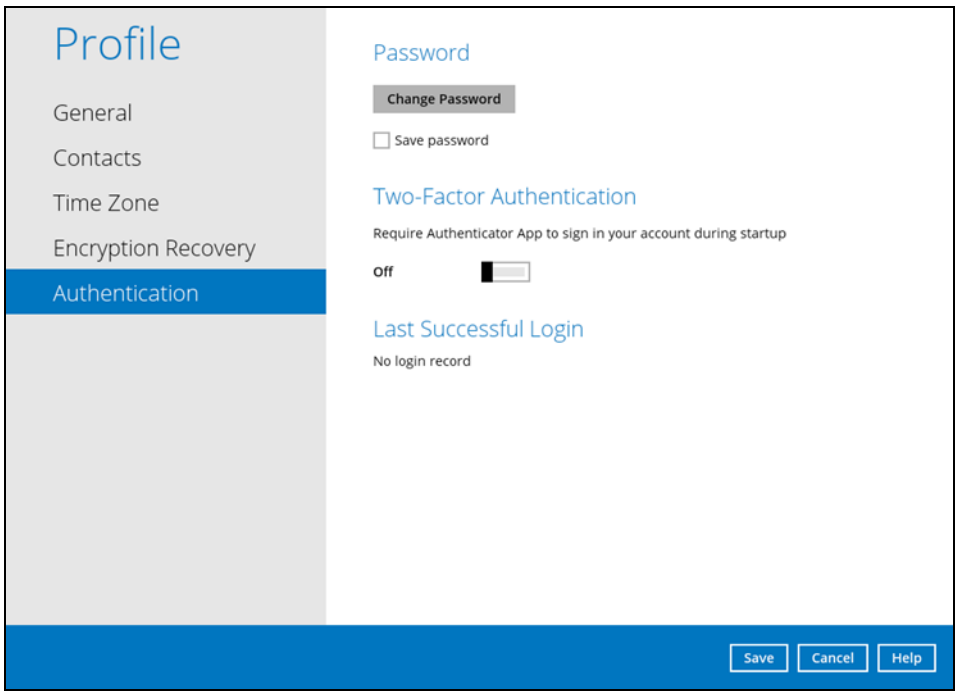


Two-Factor Authentication

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

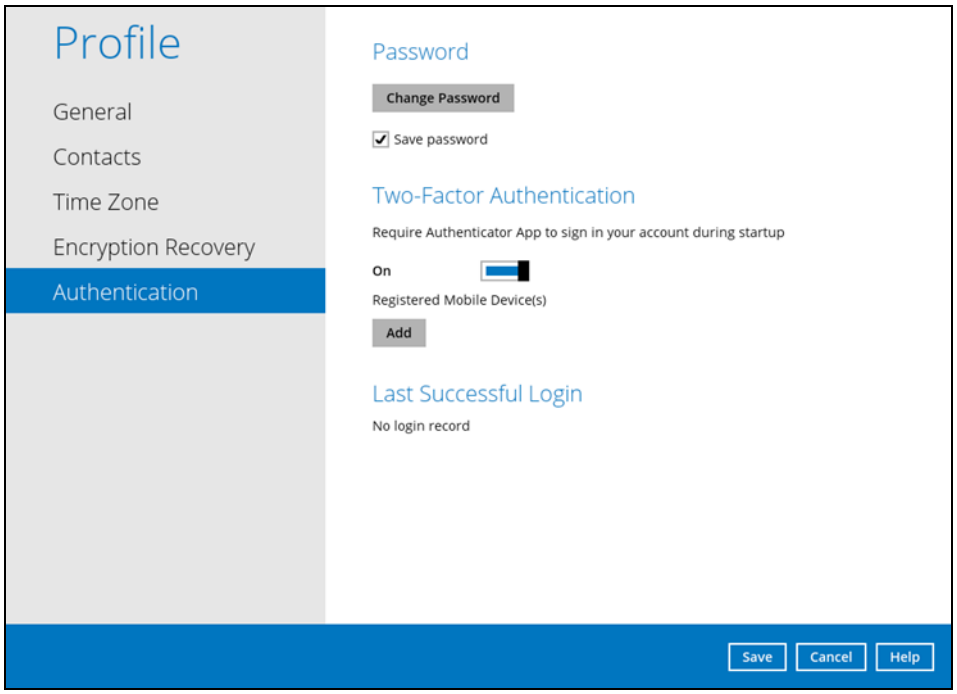
NOTE
The Ahsay Mobile app or a third-party authenticator app is needed for 2FA.

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



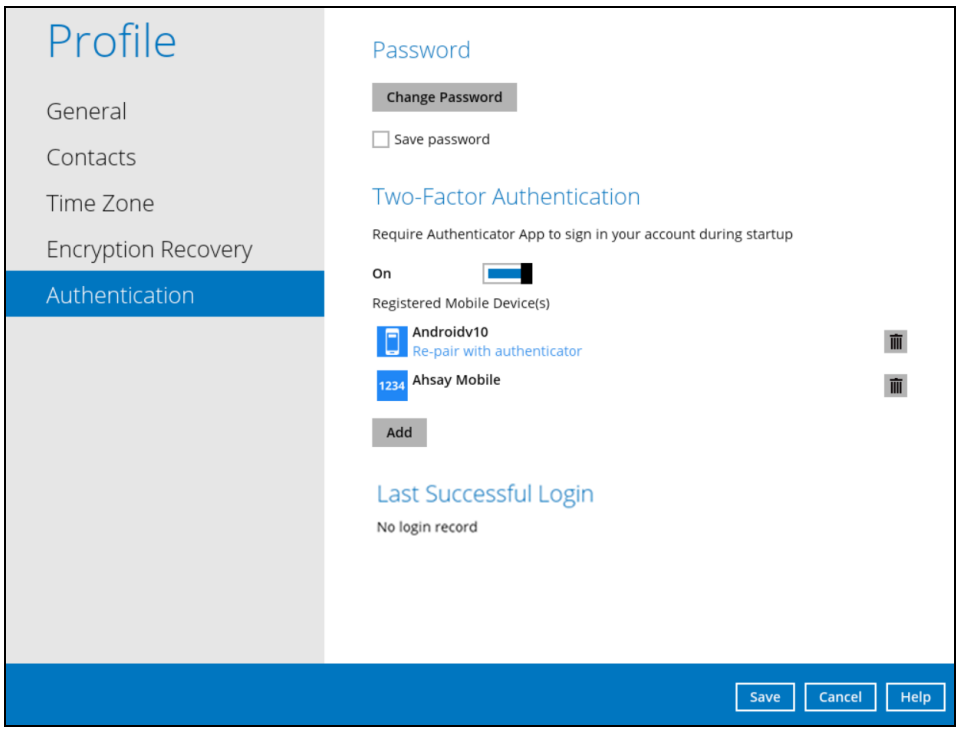
2. Swipe lever to the right to turn it on.

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

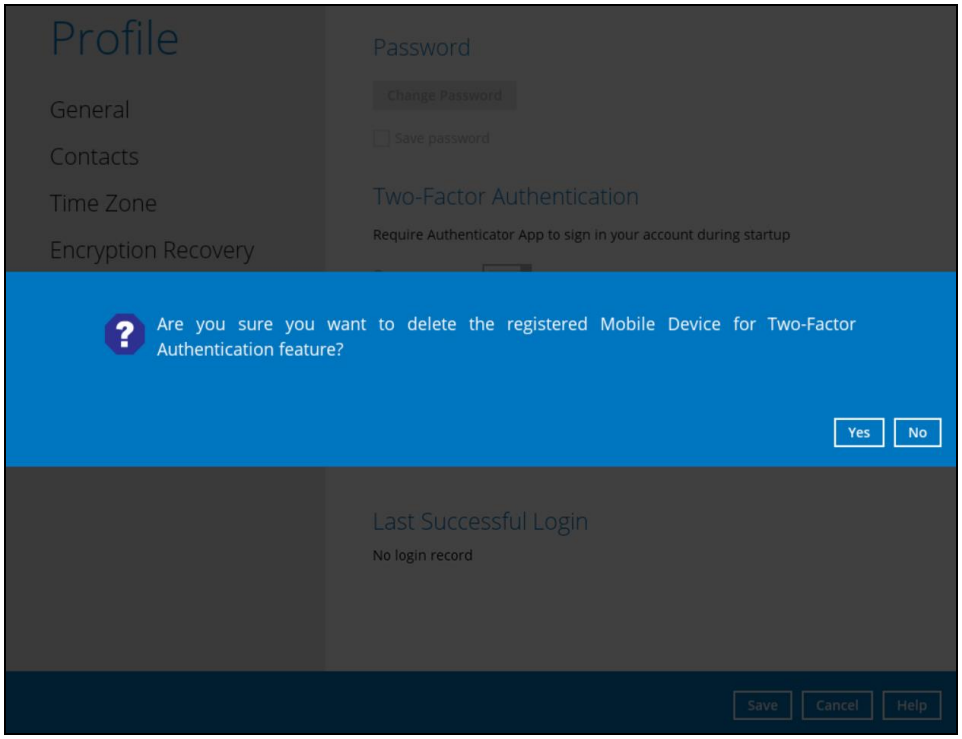


To remove a mobile device, follow the instructions below:

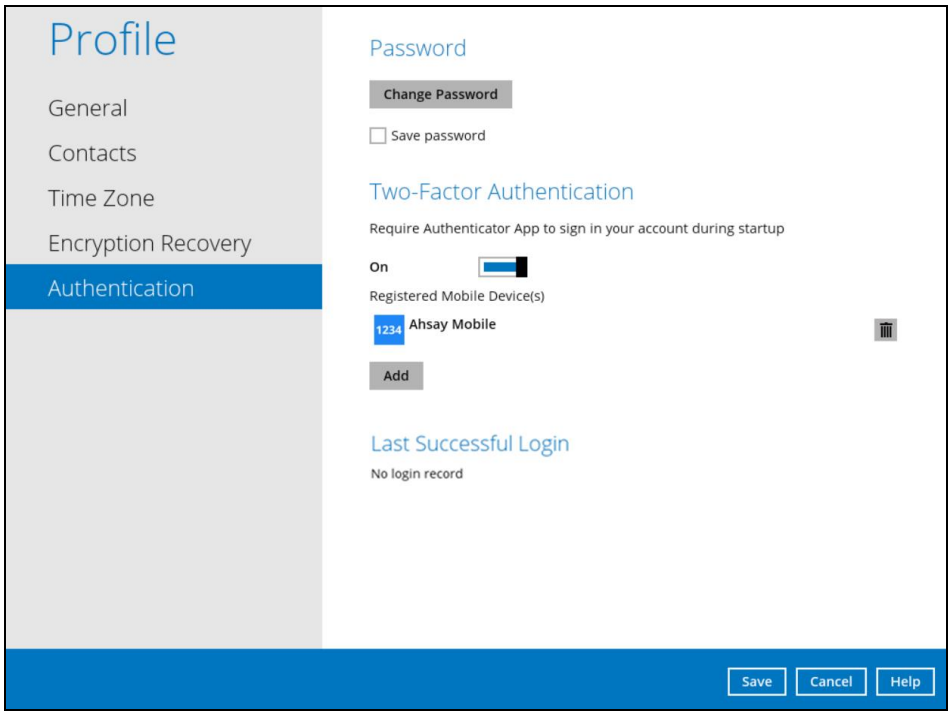
1. Click the button on the right side of the registered mobile device. In this example, we are going to delete the mobile device named “Androidv10”.



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



3. Mobile device is successfully removed.

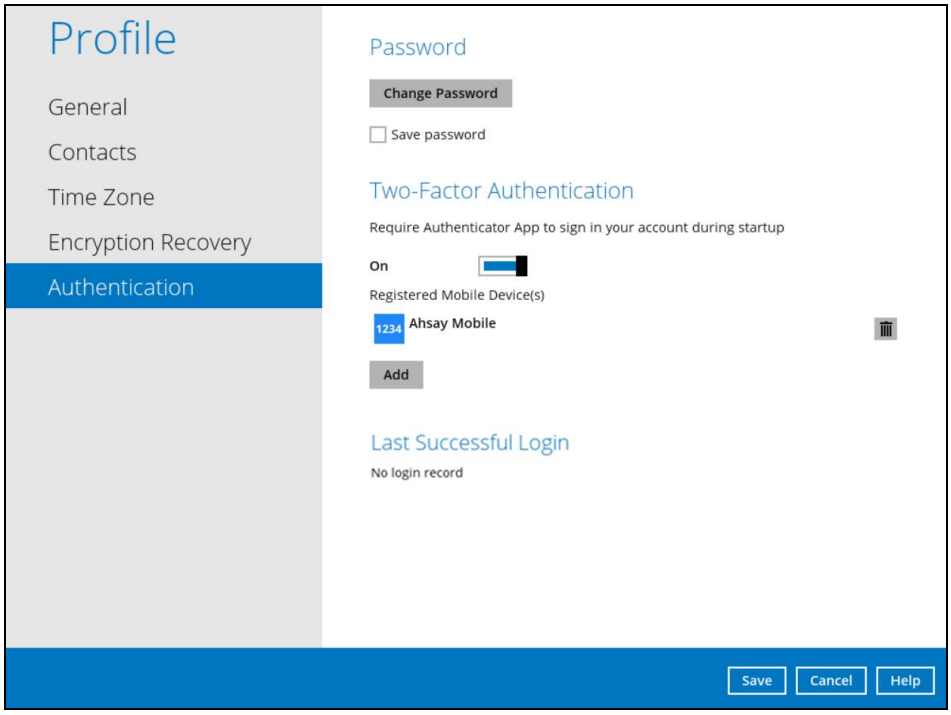


To disable the two-factor authentication feature, follow the instructions below:

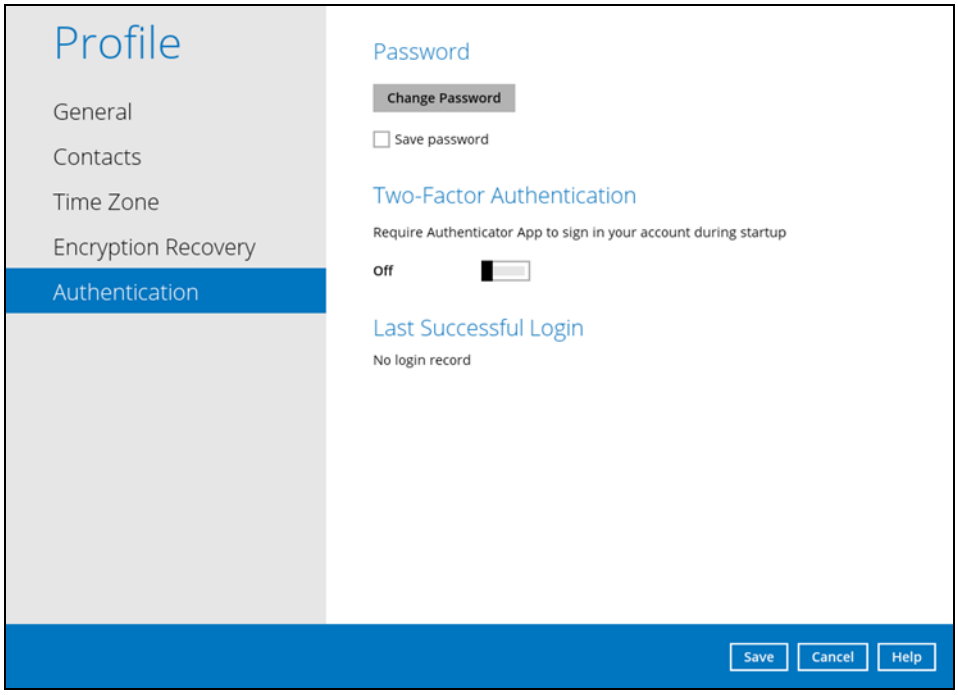
NOTE

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

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



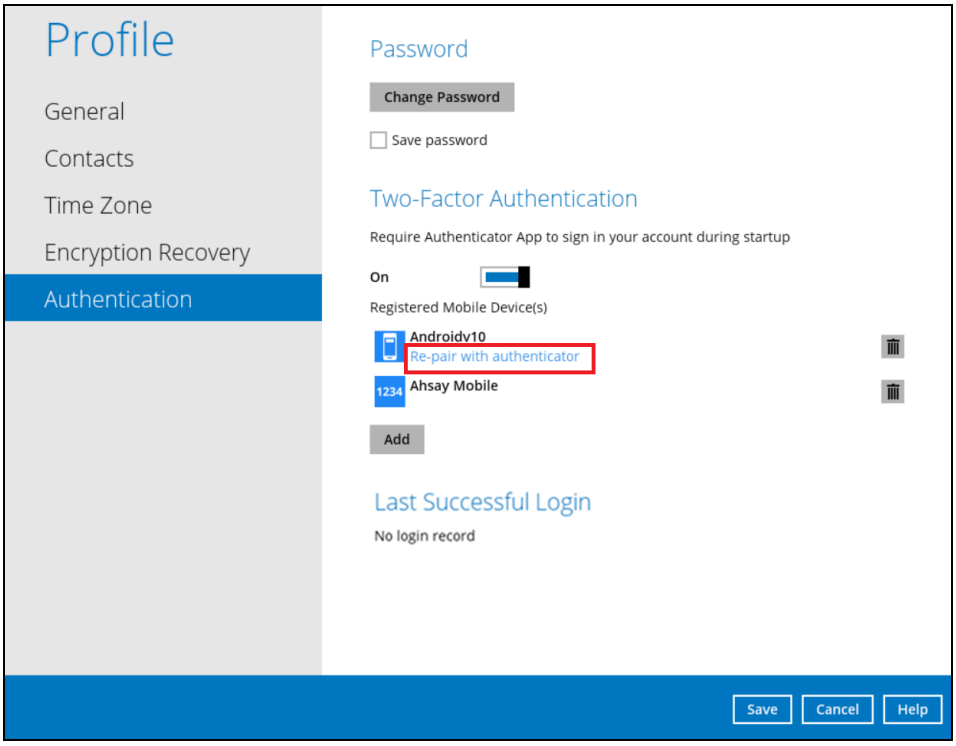
2. Click **Save** to save the settings.



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 AhsayOBM. This feature is used when:

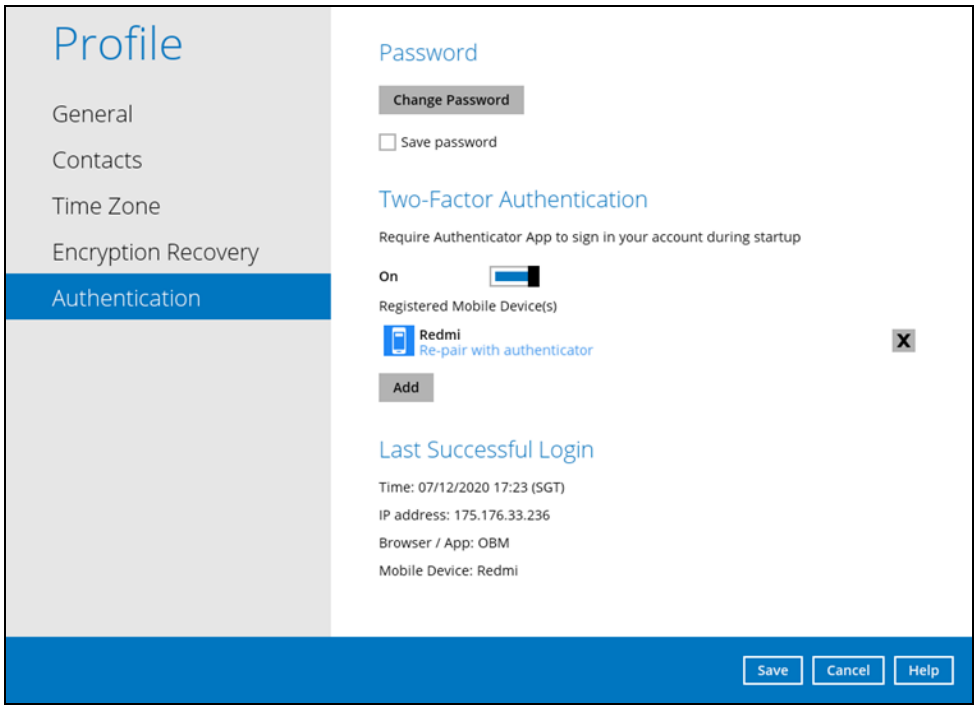
1. The registered profile for the 2FA is removed from the Ahsay Mobile app
2. The Ahsay Mobile app is accidentally uninstalled from the mobile device



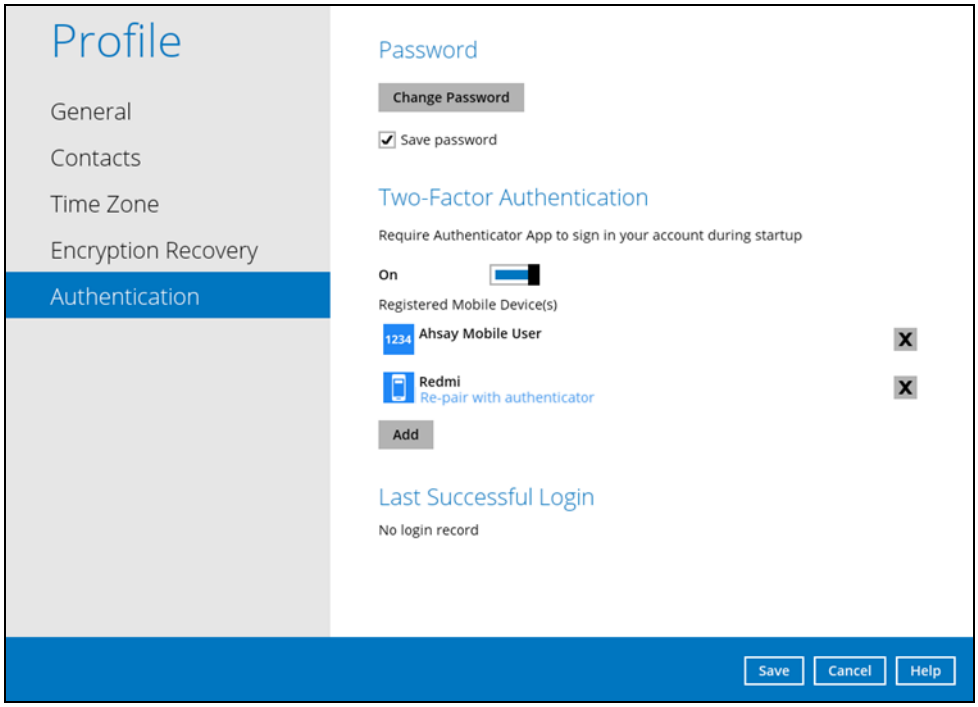
Last Successful Login

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 log in.
- Browser / App – the browser or app used to log in to AhsayCBS User Web Console or AhsayOBM.
- Mobile Device – the name of the device used for authentication when 2FA is enabled.



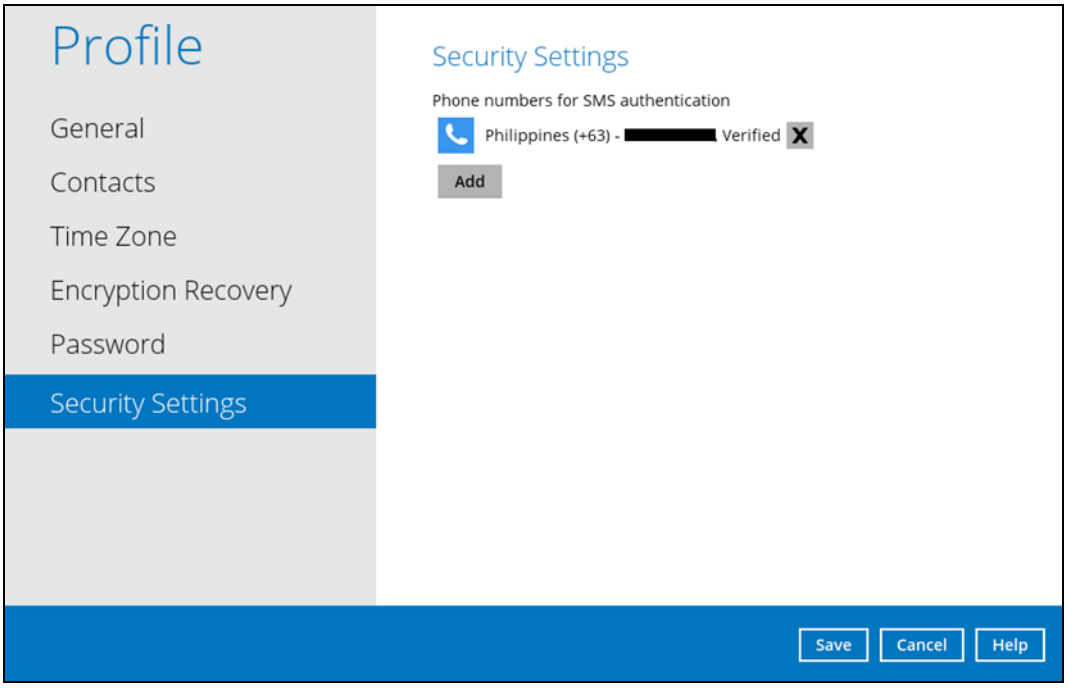
Below is the screenshot if there is no login record yet.



10.1.7 Security Settings

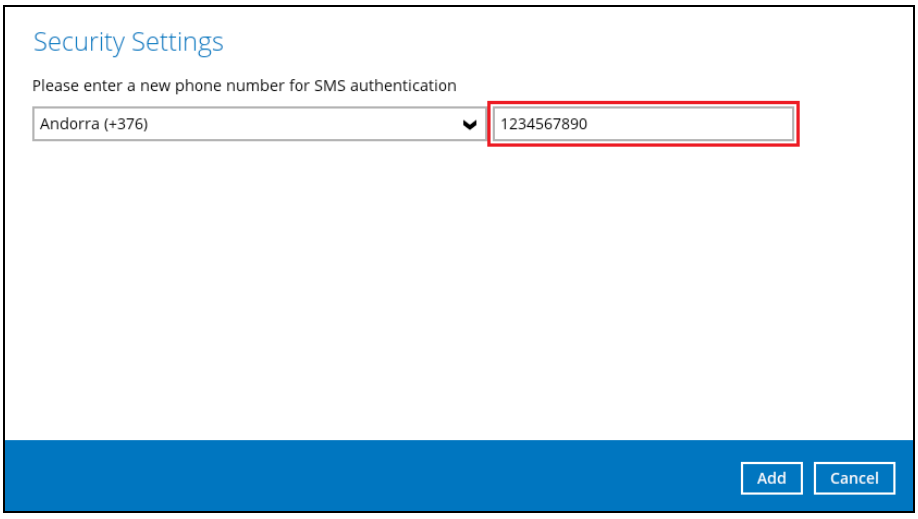
The Security Settings option is for backward compatibility with Twilio Two-Factor Authentication. It will only be visible if Twilio Two-Factor Authentication was enabled on the user account on pre-v8.5.0.0 AhsayOBM versions.

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.

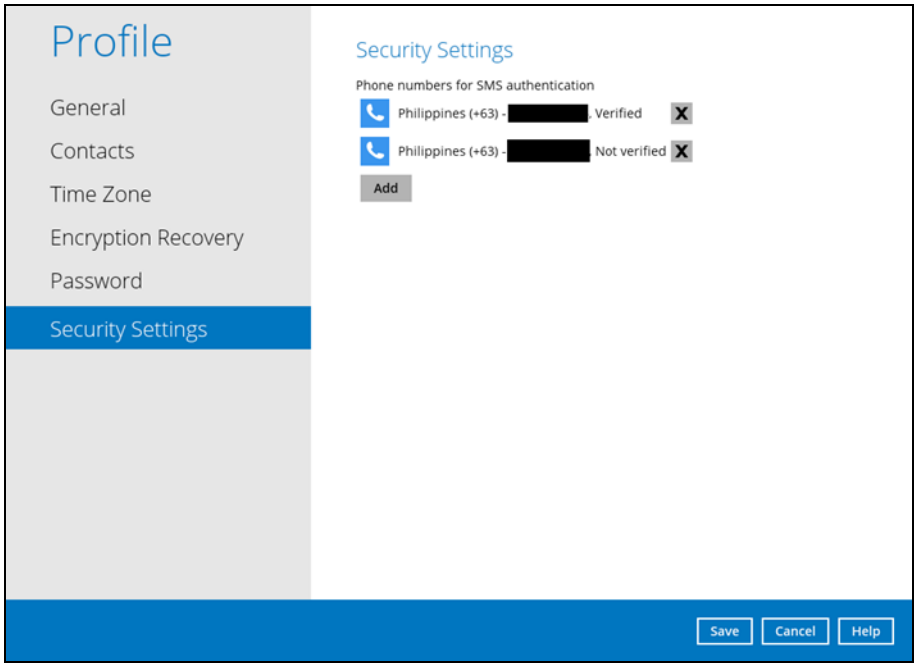


1. Click [Add].

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

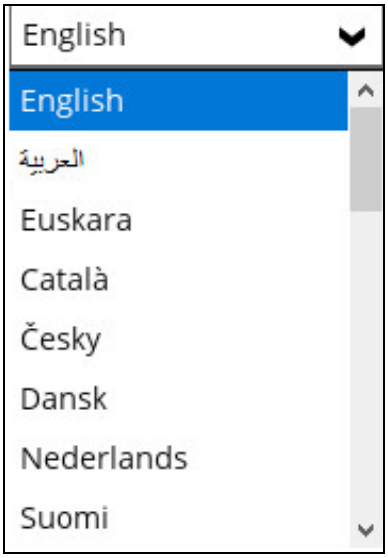


3. Click the [Save] button to save the phone number.



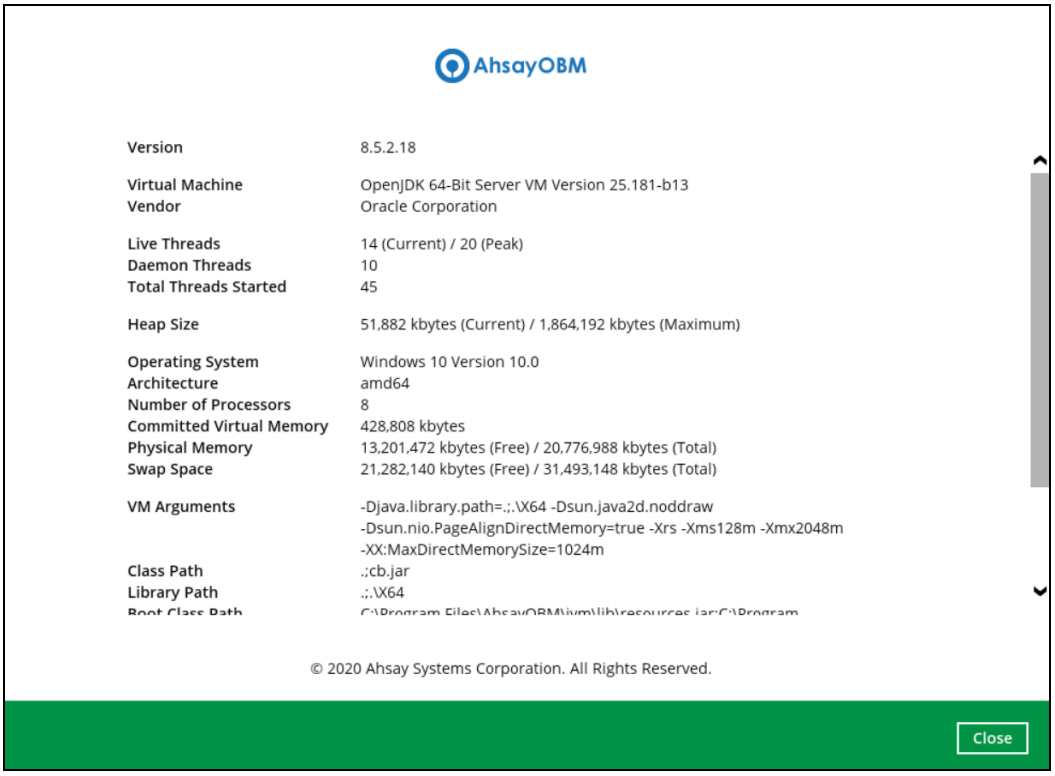
10.2 Language

The list of available languages depends on the backup service provider.



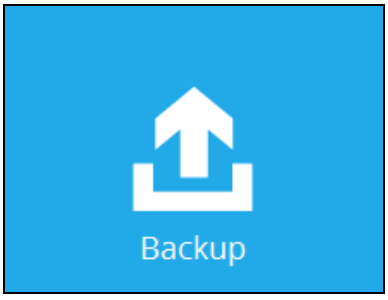
10.3 Information

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



10.4 Backup

This feature is used to run the backup set/s.



To start backing up, follow the instructions on Chapter 13 Run Backup Jobs

10.5 Backup Sets

A backup set is a place for files and/or folders of your backed up data. This feature allows the user to select files individually or an entire folder to backup. It is also used to delete backup set/s.

To create or modify a backup set, follow the instructions on Chapter 11 Create a Backup Set

Backup Set Settings

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

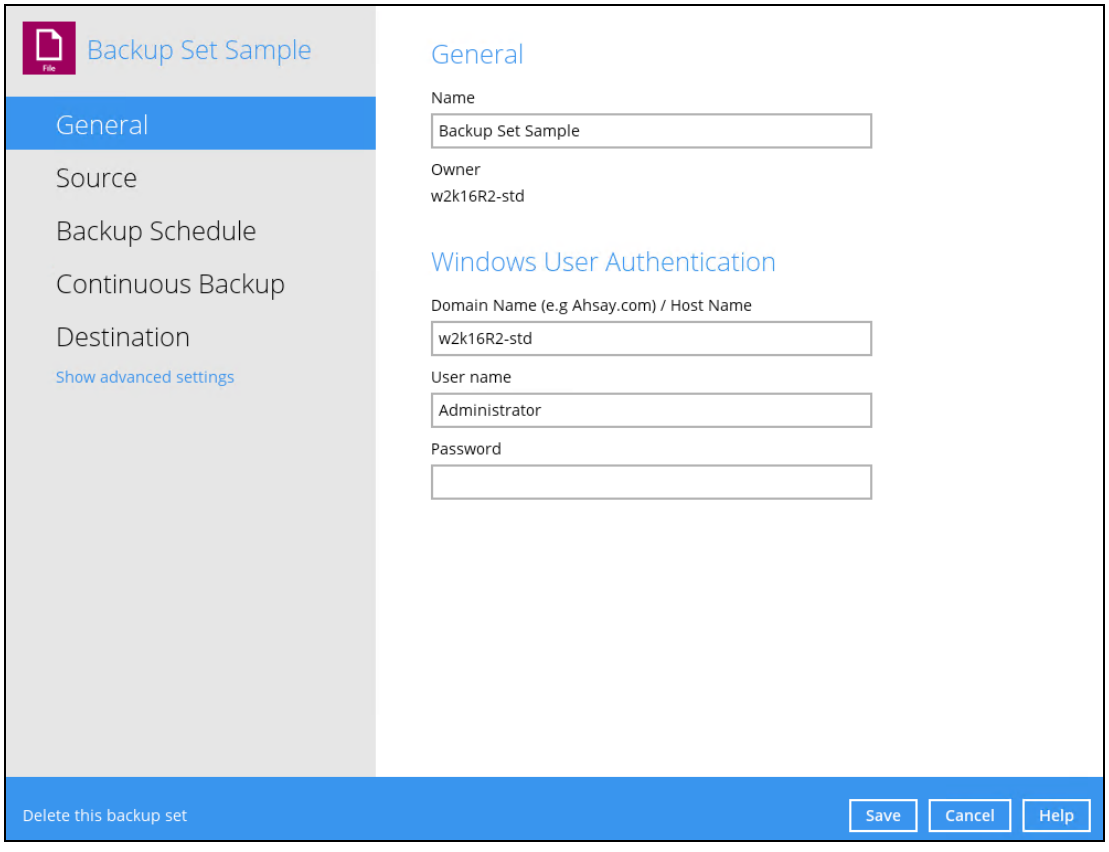
- General
- Source
- Backup Schedule
- Continuous Backup
- Destination

(Advanced settings)

- In-File Delta
- Retention Policy
- Command Line Tool
- Reminder
- Bandwidth Control
- Others

General

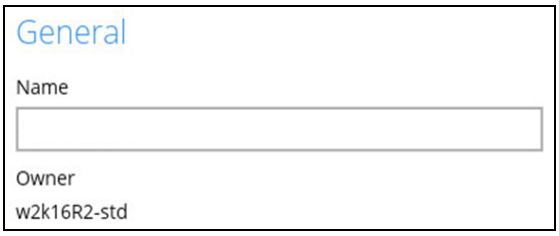
This feature allows the user to modify the backup set name and manage the Windows User Authentication login credentials in the backup set.



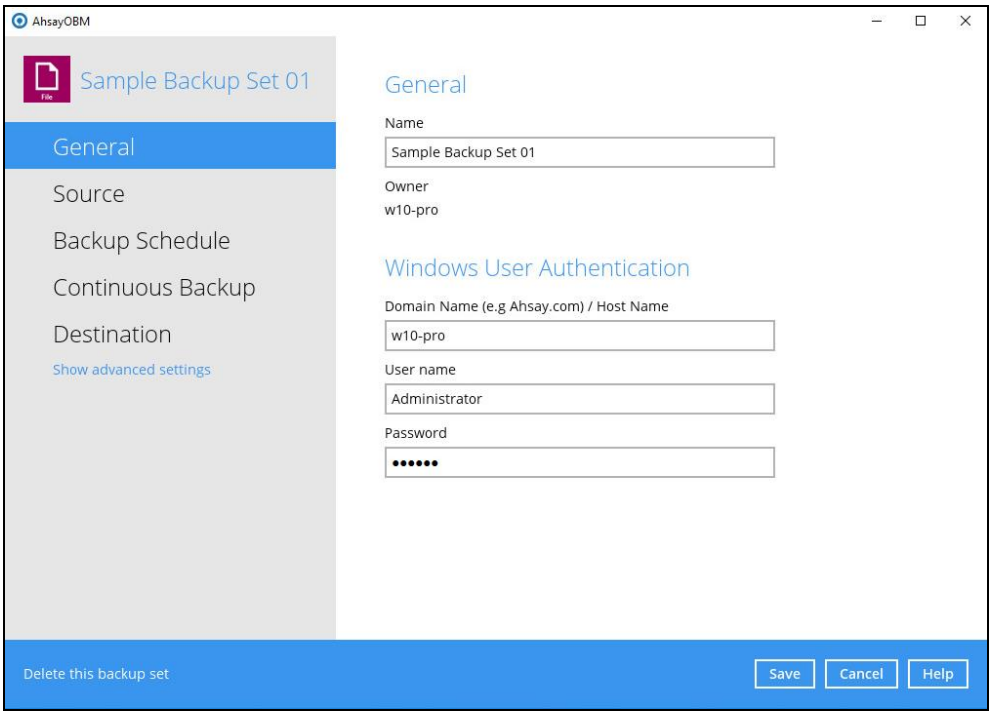
Backup Set Name

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

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



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



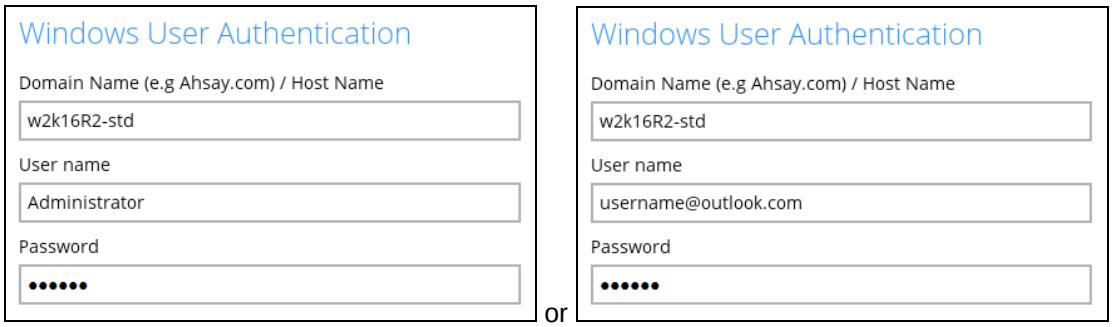
NOTE

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

Windows User Authentication

To successfully perform backup and restore operations, AhsayOBM requires both read and write permission to all the files/folders selected in the backup source.

The Windows User Authentication login credentials are used by the AhsayOBM to ensure it has sufficient permission to access files and/or folders selected in the Backup Source, the temporary folder location, and the backup destination if it is a network drive accessible from backup machine via LAN, especially when running scheduled backup jobs, as the default Windows account used by the AhsayOBM scheduler service is a local system account which does not have access to network resources.



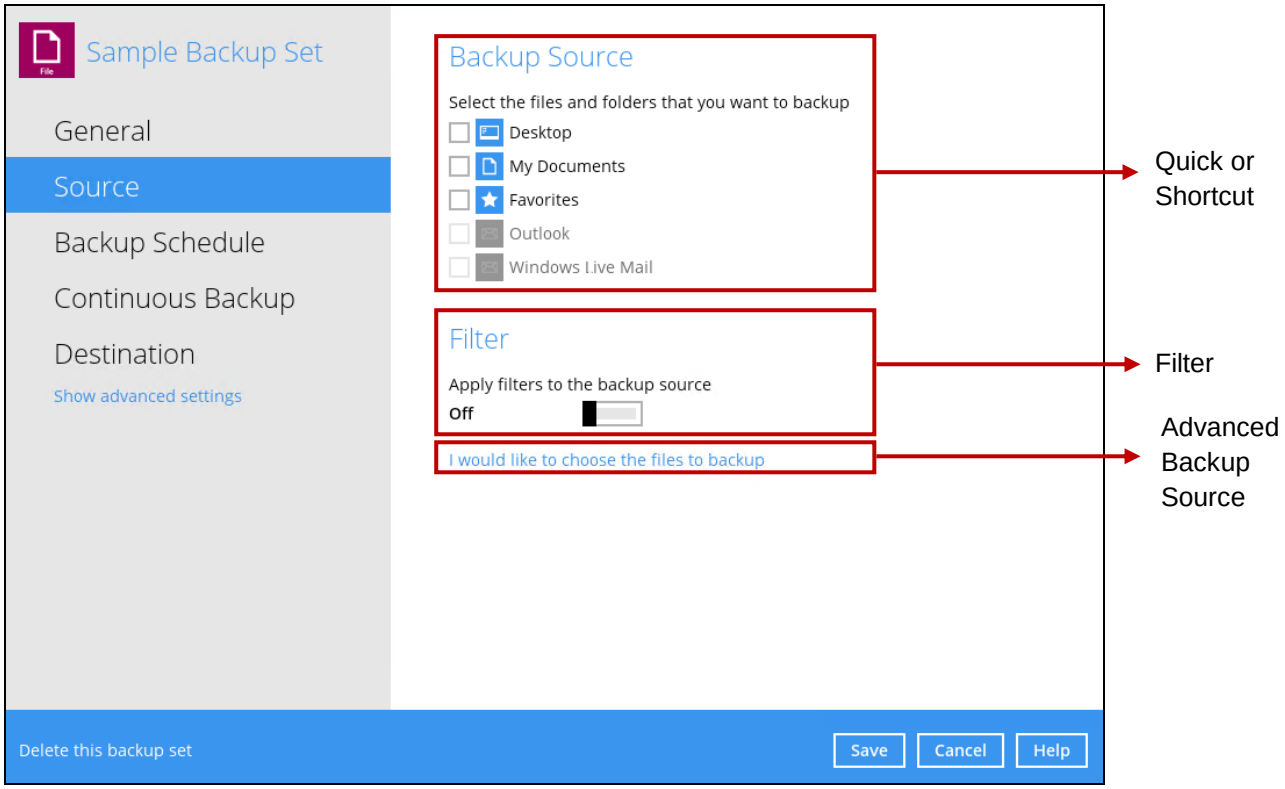
- If files and/or folders selected are located on network drive(s), the login credentials for the Windows User Authentication must have permission to access network resources, (e.g., an administrator account).
- If the machine is a file server shared by multiple users, then the AhsayOBM will require login credentials with read/write permissions to access all the selected files and/or folders in the backup source (e.g., an administrator account).
- For AhsayOBM installed on Microsoft Windows version 8, 8.1 and 10, using the Microsoft account for Windows User Authentication is supported, e.g., username@outlook.com.

  Some users prefer to use a pin to log in to Windows, this cannot be used for the Windows User Authentication. The pin can only be used for logging in to Windows and is not applicable for the Windows User Authentication. The password of the account must be provided instead of the pin to access files and/or folders in the backup source.

Field	Description
Domain Name	The domain or host name of the machine.
Username	Login username used by the AhsayOBM to access files and/or folders selected in the backup source.
Password	Login password used by the AhsayOBM to access files and/or folders selected in the backup source.

Source

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

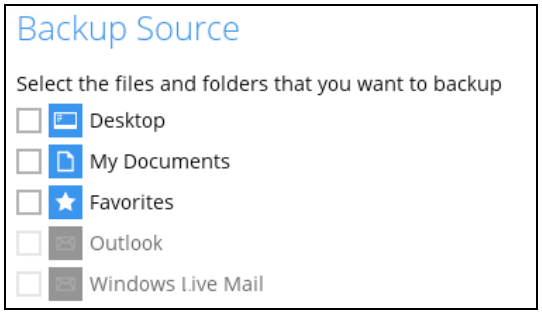


There are three (3) different ways to select files and/or folders to back up:

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

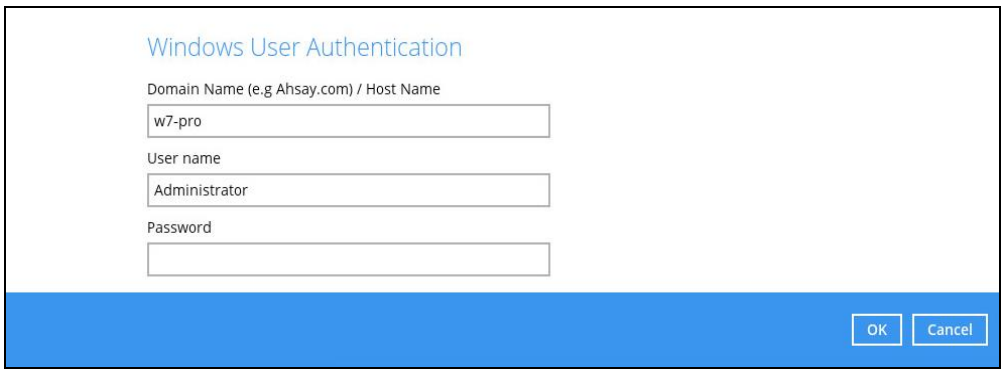
Option 1: Quick or Shortcut

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



If any of the following backup source is selected and the Backup Schedule is enabled, the Windows User Authentication will prompt the user to enter the login password. To select a backup source without entering the login password, the backup schedule must be disabled.

Desktop	
My Documents	
Favorites	
Outlook	
Windows Live Mail	



NOTE

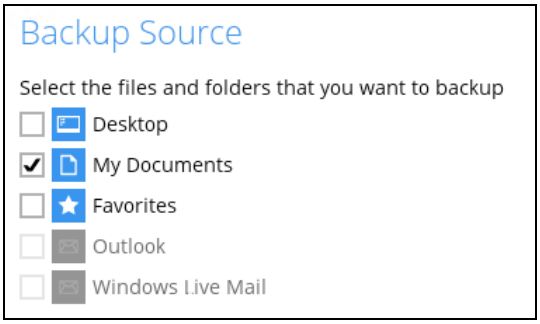
During the creation of backup set, if this type of backup source (Quick or Shortcut) is selected and the Schedule is set to “on”, the Windows User Authentication screen will be displayed. You will need to enter the login password, otherwise, the creation of backup set will not continue.

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

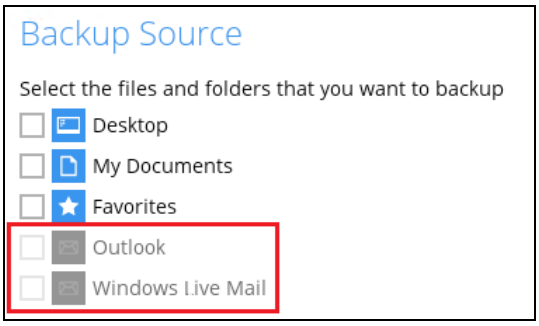
Backup Source		Description
Desktop		If Desktop is selected, all files and/or folders in the following location will be backed up: ***%UserProfile%\Desktop***
My Documents		If Documents is selected, all files and/or folders located in the following location will be backed up: ***%UserProfile%\Documents*** If the Follow Link is enabled, all files and/or folders located in the following locations will also be backed up: ***%UserProfile%\Music*** ***%UserProfile%\Pictures*** ***%UserProfile%\Videos*** **NOTE**: The Follow link is enabled by default.
Favorites		If Favorites is selected, all files and/or folders located in the following location will be backed up: ***%UserProfile%\Favorites***
Outlook		If Outlook is selected, all files and/or folders located in the following location will be backed up: ***%UserProfile%\AppData\Local\Microsoft\Outlook***
Windows Live Mail		If Windows Live Mail is selected, all files and/or folders located in the following location will be backed up: ***%UserProfile%\AppData\Local\Microsoft\Windows Live Mail***

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

1. Select a backup source.



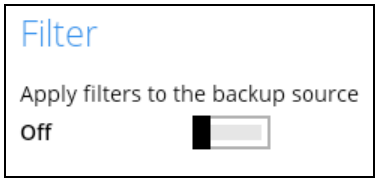
2. The Outlook and Windows Live Mail will be disabled if they were not installed on the machine.



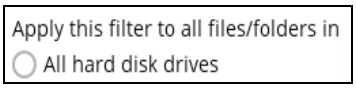
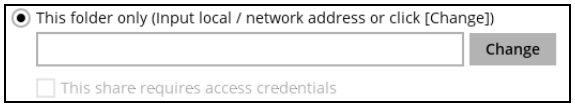
3. Click the **Save** button to store the selected backup source.

Option 2: Filter

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

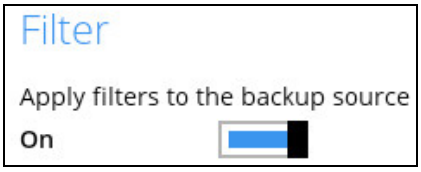


The following options in the filter backup source does not require Windows User Authentication login password:

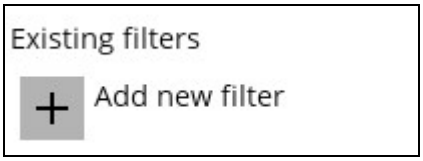
All hard disk drives	
Specific folder	

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

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

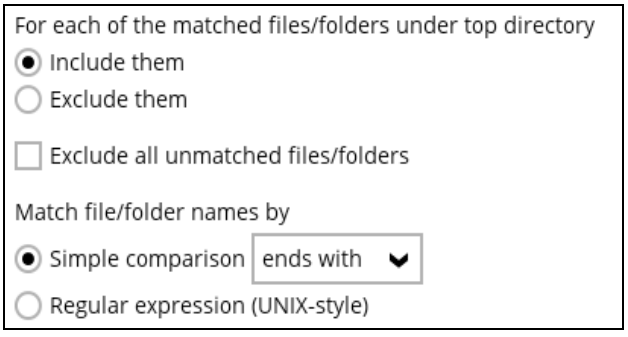


2. Click the **[+]** button to create filter.

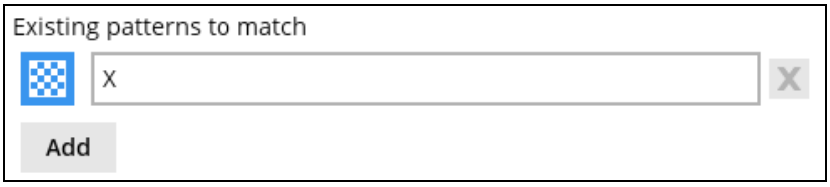


3. Assign a desired name to the backup filter.

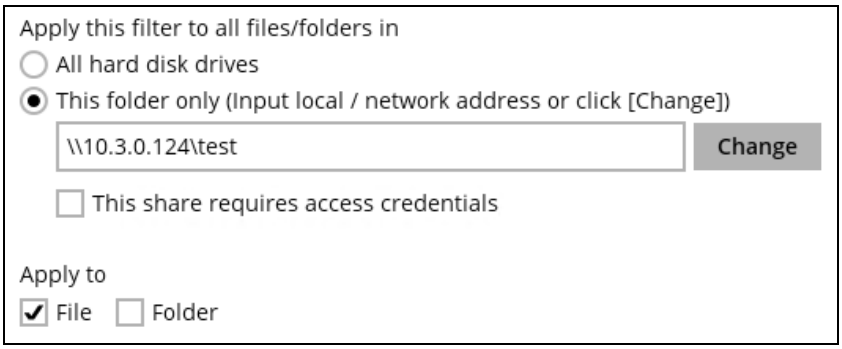
4. Select from the options below.



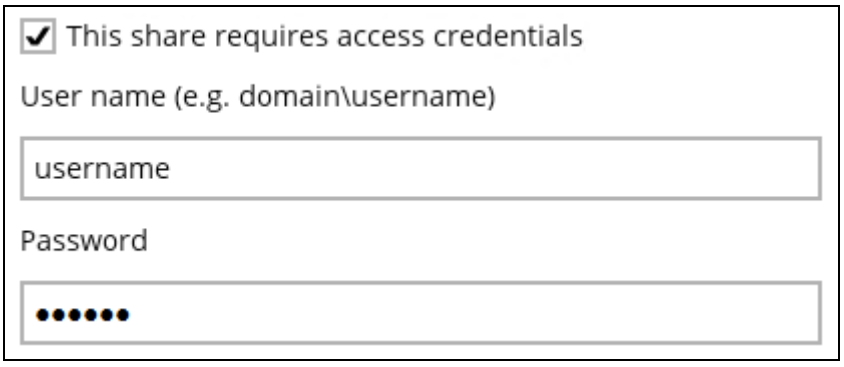
5. In this example, all files and/or folders that end with the letter 'X' will be included to the backup job. You can add multiple patterns here.



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

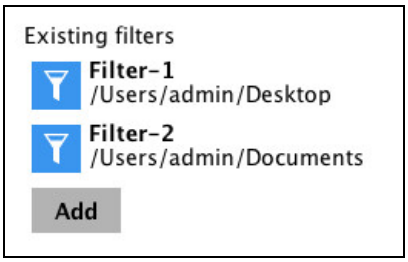


7. If 'This share requires access credentials' is checked, enter the User name and Password of the local or network drive. This checkbox will only be enabled if a local or network address is detected.



8. 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.

   Multiple backup filters can be created by clicking the [Add] button.

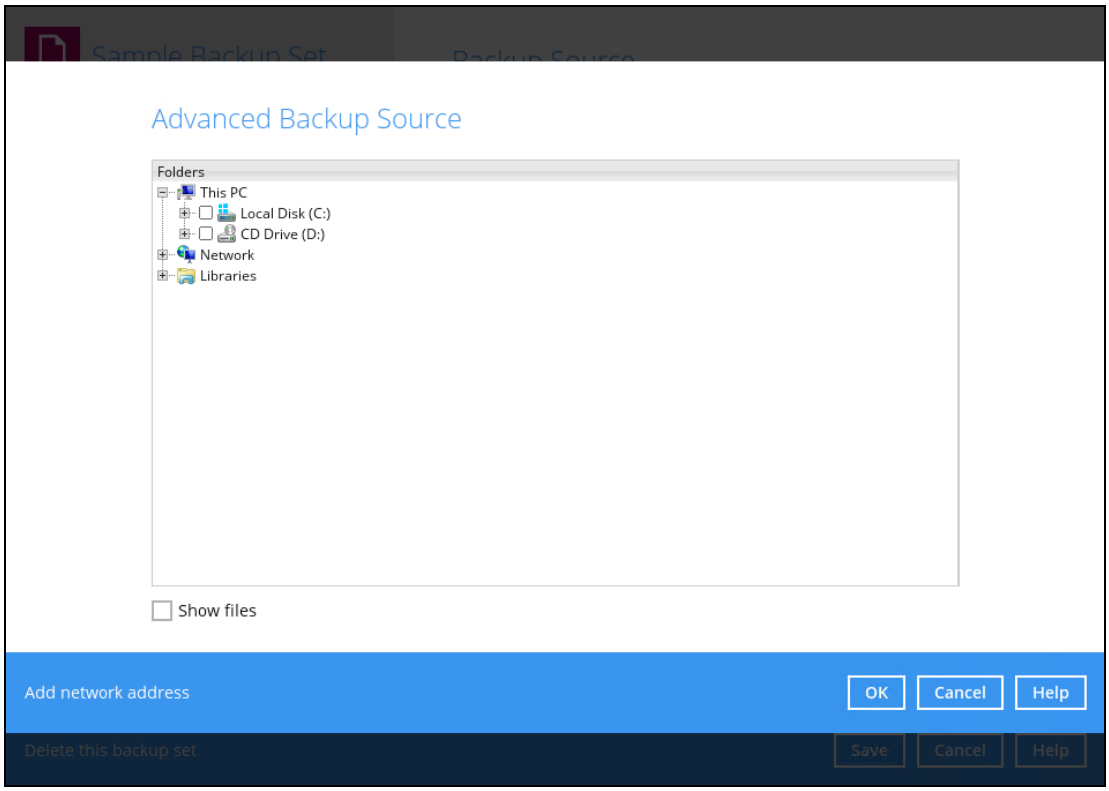


NOTE

For more details about backup source file filtering, please refer to **Chapter 4.1 Create a backup set with filter** in the Ahsay Online Backup Manager v8 Backup Source File Filter Guide.

Option 3: Advanced Backup Source

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



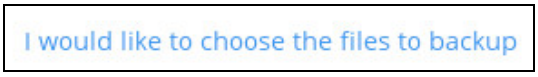
The following table shows the list of options in the Advanced Backup Source which require and does not require Windows User Authentication login password:

Advanced Backup Source		Description
Local Disk		Does not require Windows User Authentication login password.
Network drive		Requires Windows User Authentication login password. For network drive/s, you will need to enter the login credentials which has permission to access network resources in order to back up selected files and/or folders.
Libraries		Does not require Windows User Authentication login password. **NOTE:** This type of backup source may not be supported on other versions of Windows. **This feature is not supported on:** Windows 10 Windows 8.1

		Windows 8 and Windows Server 2012 R2 **Supported on:** Windows 7 Windows Server 2016 and Windows Server 2008 R2
Add network address		Requires Windows User Authentication login password. For network drive/s, you will need to enter the login credentials which has permission to access network resources in order to back up selected files and/or folders.

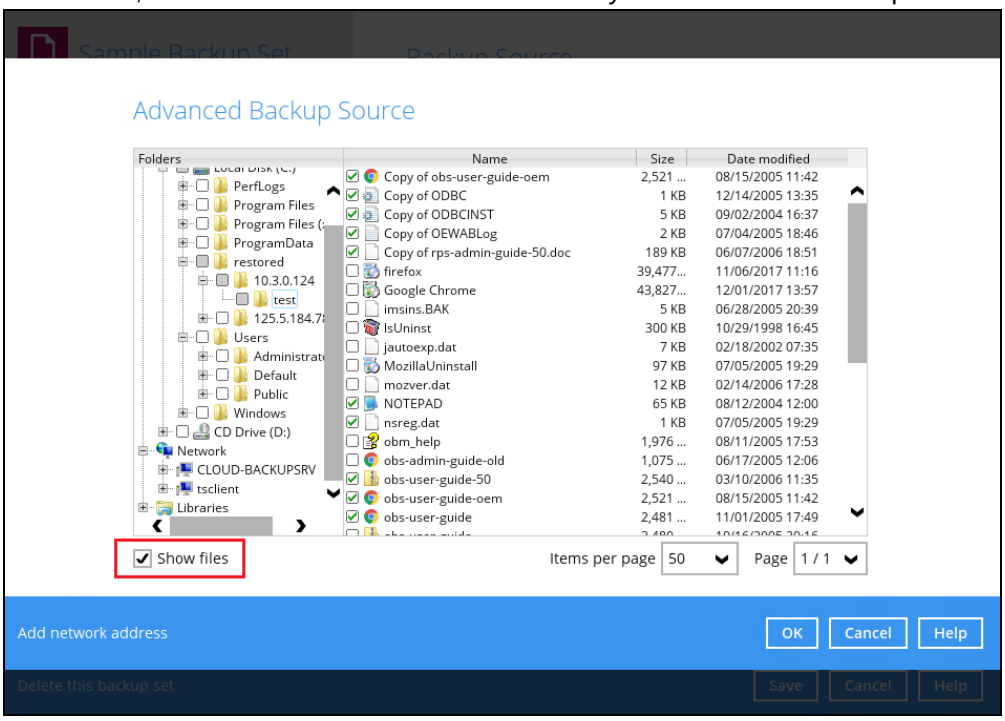
To select files and/or folders using the Advanced Backup Source, follow the steps below:

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

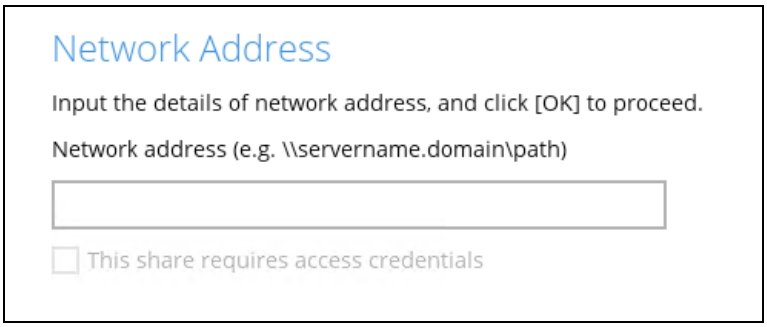


There are two (2) ways to select files and/or folders, one is when the files and/or folders are located in the local machine and another way is when the files and/or folders are located in the network.

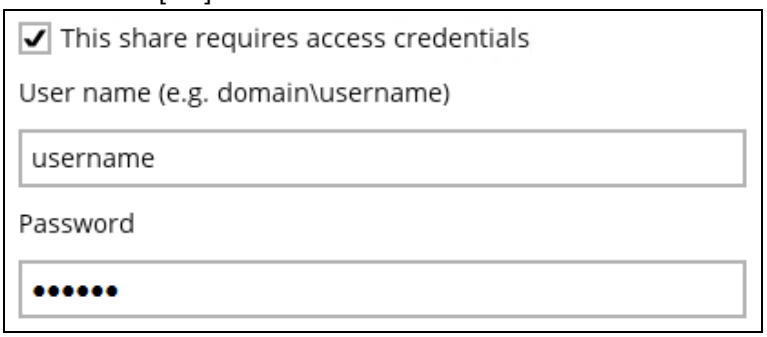
- In the Advanced Backup Source window, select 'Show files' to display the files inside each folder, then select the files and/or folders that you would like to back up.



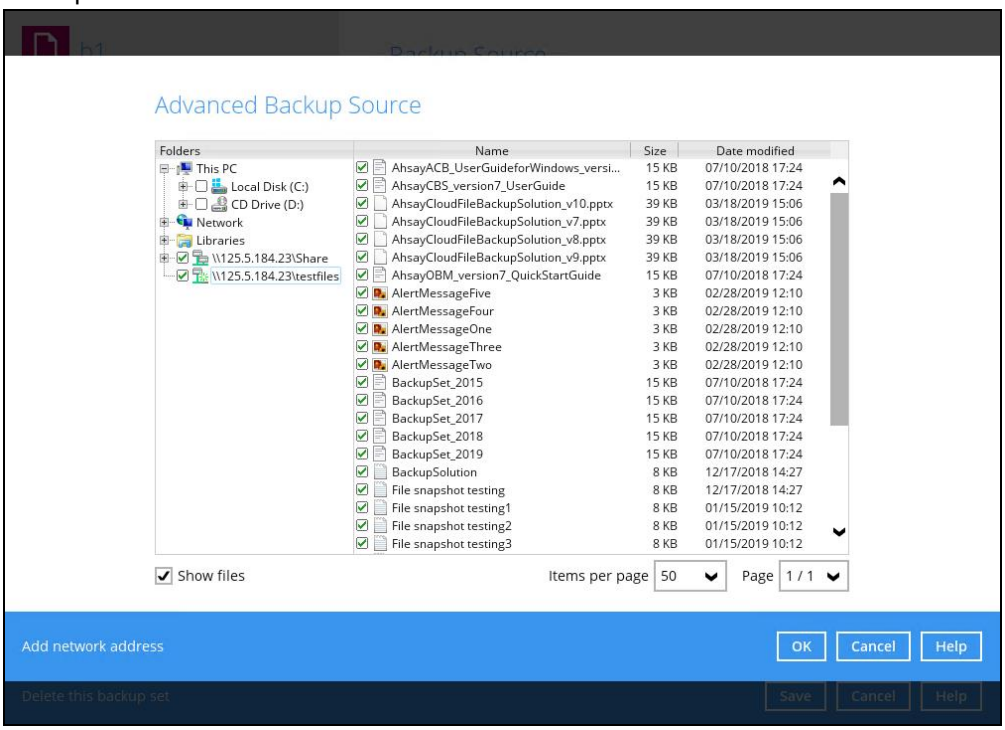
- If the files and/or folders are located in a network drive, click the 'Add network address' link. Enter the network address.



If access credentials are required to access the network, then check the "This share requires access credentials' checkbox. The checkbox will only be enabled once the network address is entered. Enter the User name and Password of the network drive and click the [OK] button.



By default all the files inside the folder in the network drive is selected for backup. But there is still an option to deselect files that you do not want to be included in the backup.



NOTE

- There must be a specific folder that is shared in the network drive that will be entered in the network address e.g. \\125.5.184.23\Share
- Temporary folders location are not supported for individual login credentials but can still be setup separately using existing Windows User Authentication login.

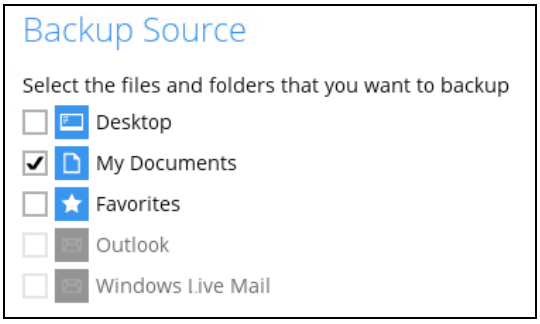
Click the [OK] button to save the selection, then click the [Save] button to store settings.

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:

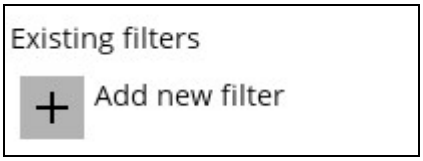
Scenario 1 (Quick or Shortcut + Filter)

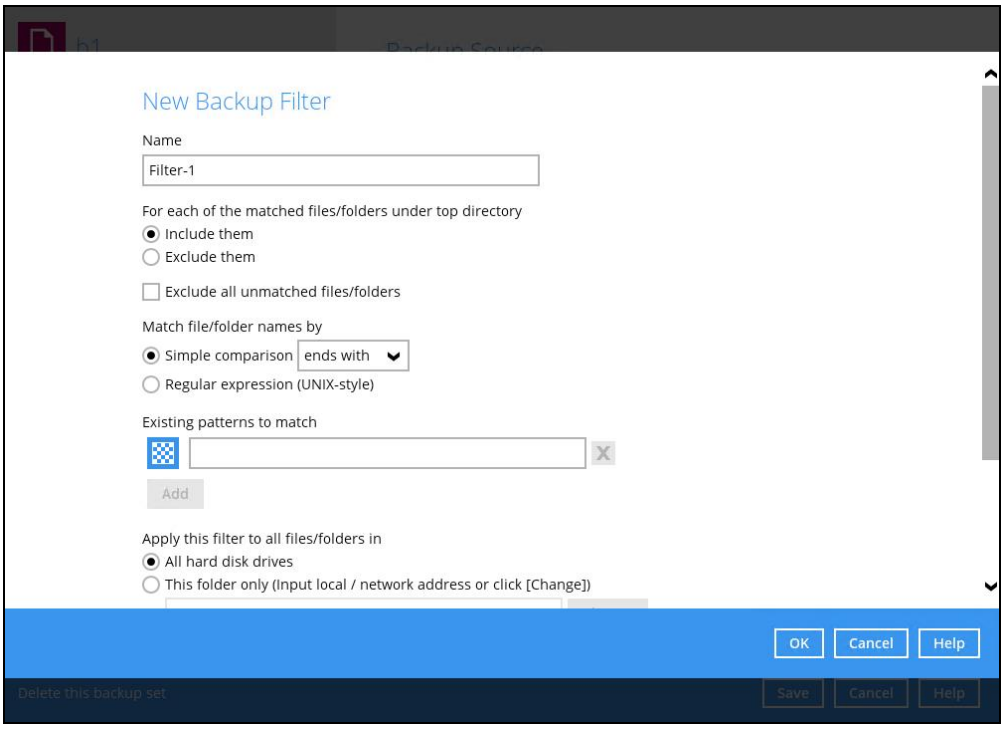
You can use the quick or shortcut option and apply filter to the selected backup source at the same time. To use this type of combination, follow the steps below:

1. Choose a backup source.



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



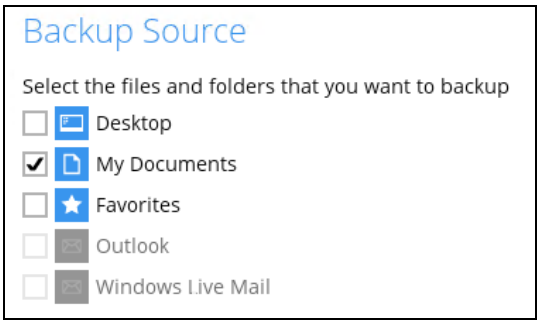


3. Click the [OK] button to save the created filter, then click the [Save] button to store settings.

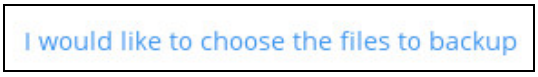
Scenario 2 (Quick or Shortcut + Advanced Backup Source)

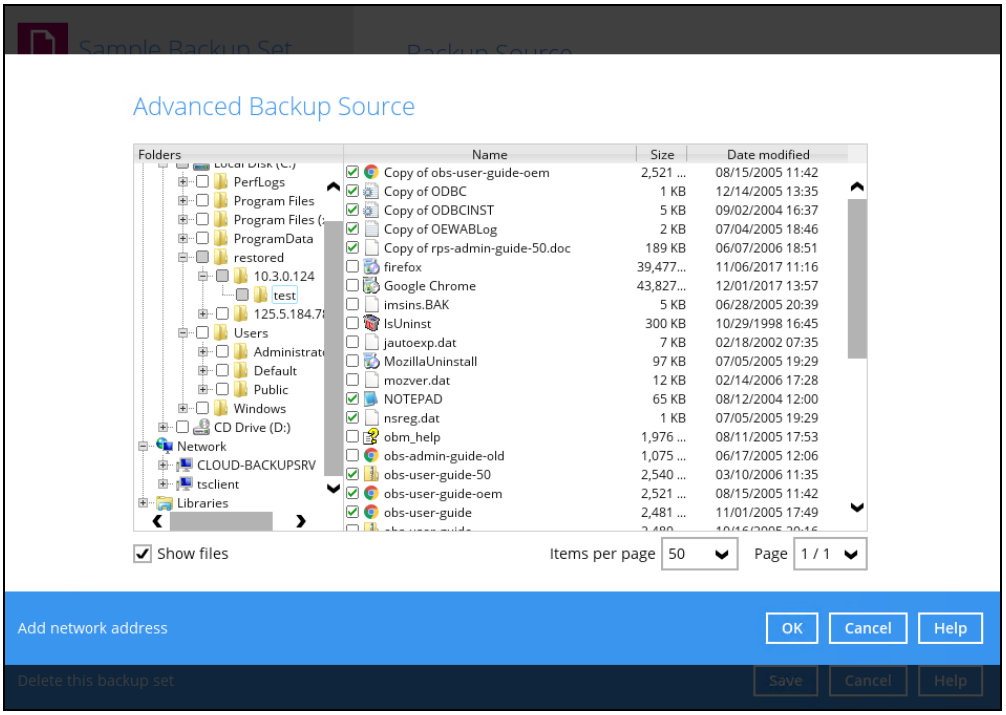
You can use the quick or shortcut option and select files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

1. Choose a backup source.



2. In the source window, click 'I would like to choose the files to backup' and select the files and/or folders that you would like to back up. Or click 'Add network address' to backup files and/or folders located in a network drive.



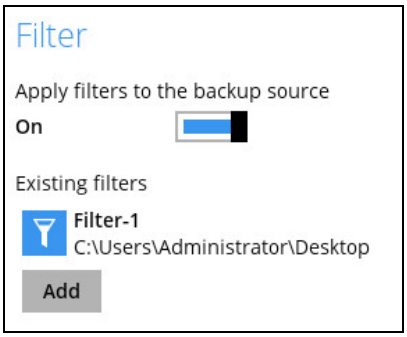


3. Click the [OK] button to save the selection, then click the [Save] button to save settings.

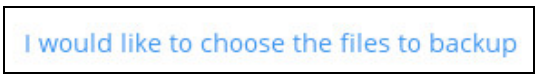
Scenario 3 (Filter + Advanced Backup Source)

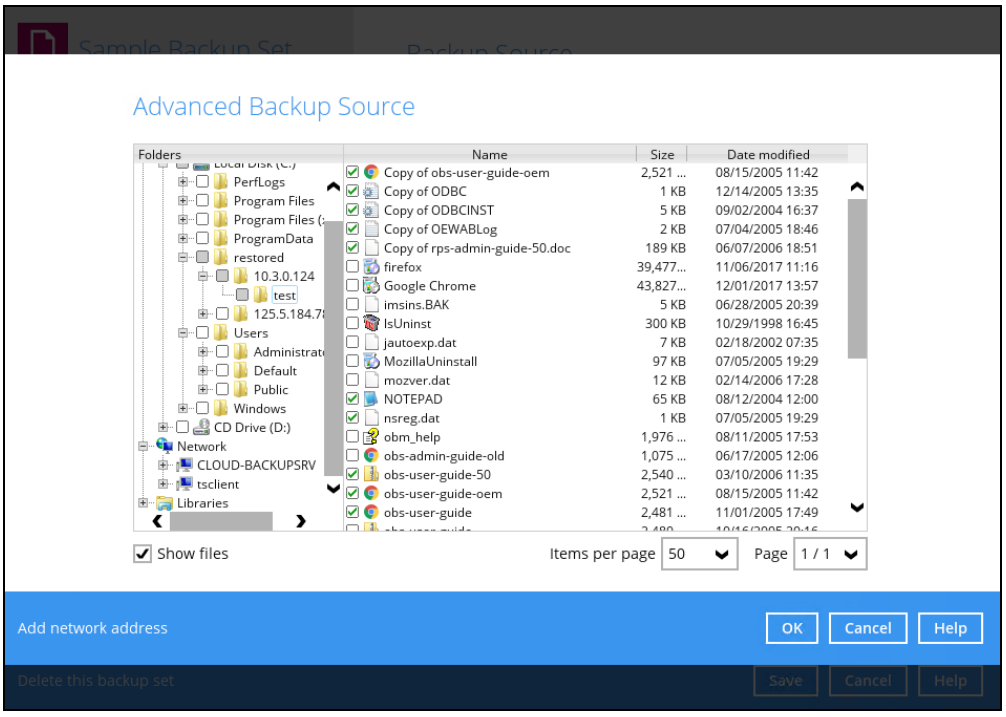
You can use the filter backup source and select files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

1. Create a filter.



2. In the source window, click 'I would like to choose the files to backup' and select the files and/or folders that you would like to back up. Or click 'Add network address' to backup files and/or folders located in a network drive.

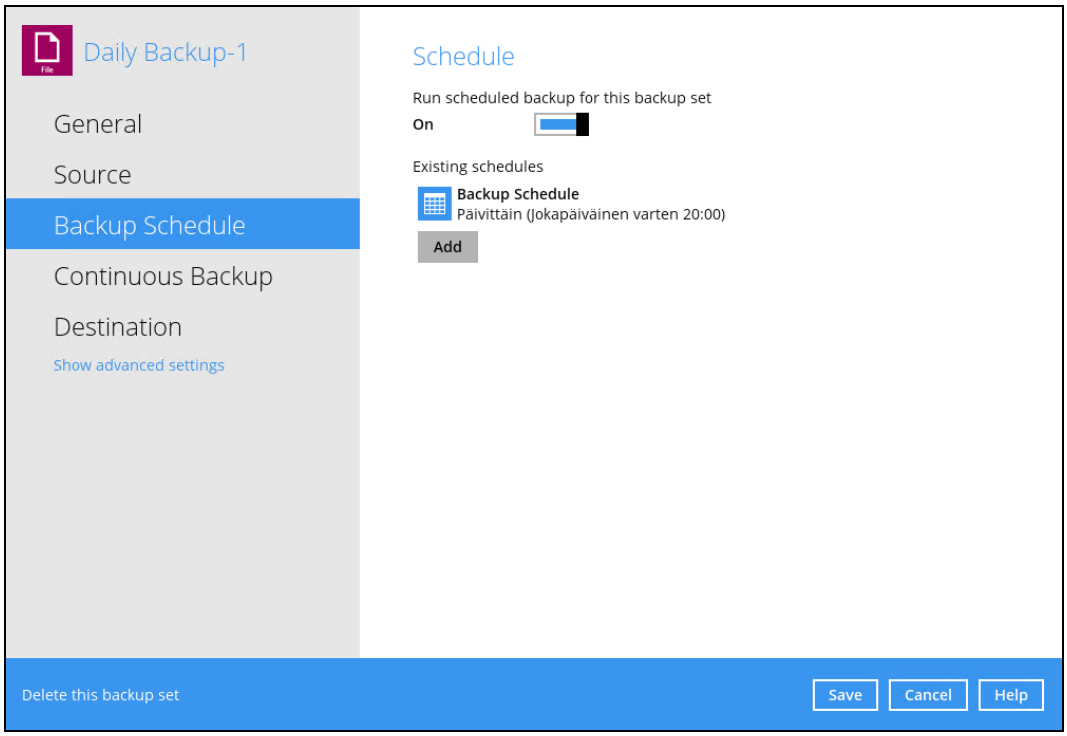


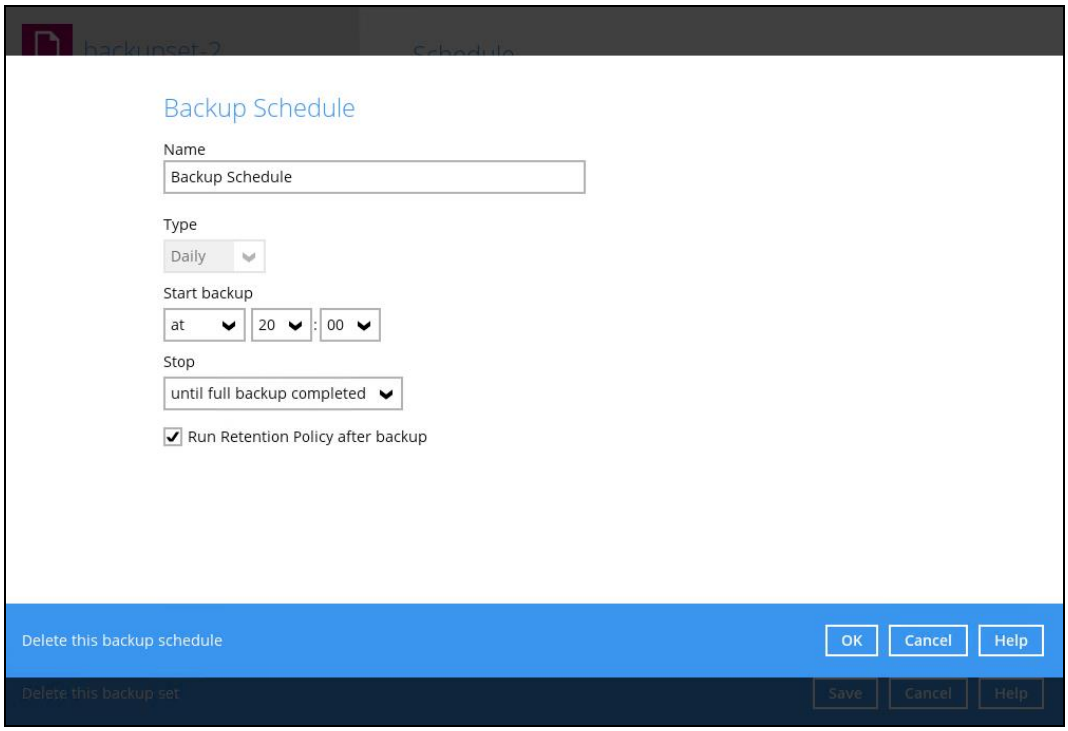


3. Click the [OK] button to save the selection, then click the [Save] button to store settings.

Backup Schedule

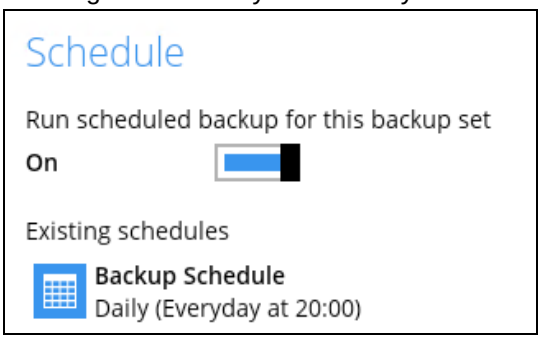
This feature allows the user to assign a backup schedule for the backup job to run automatically.



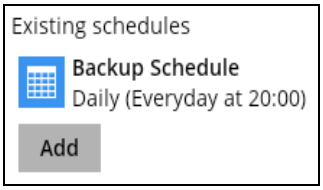


To configure a backup schedule, follow the steps below:

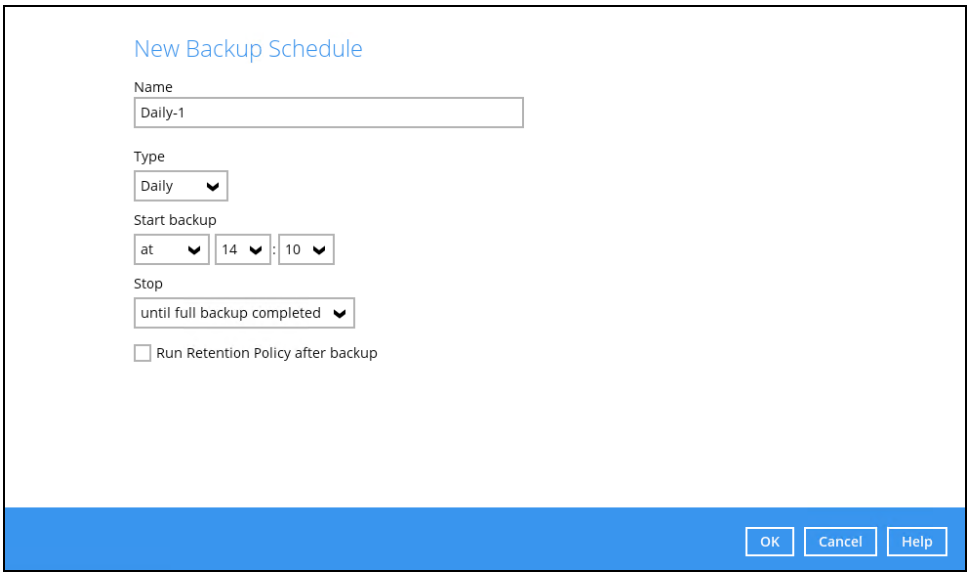
1. Swipe the lever to the right to turn on the backup schedule setting. The backup schedule is configured as “Daily at 20:00” by default.



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

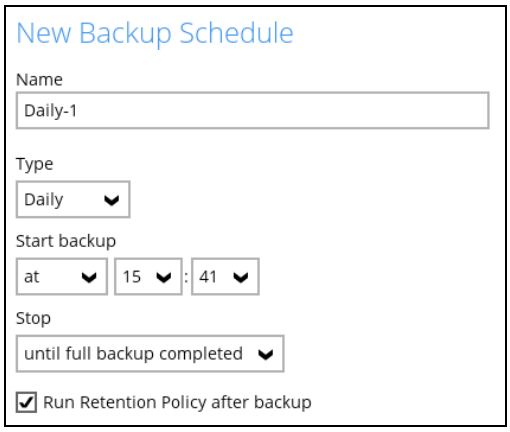


3. In the New Backup Schedule window, configure the following backup schedule settings.

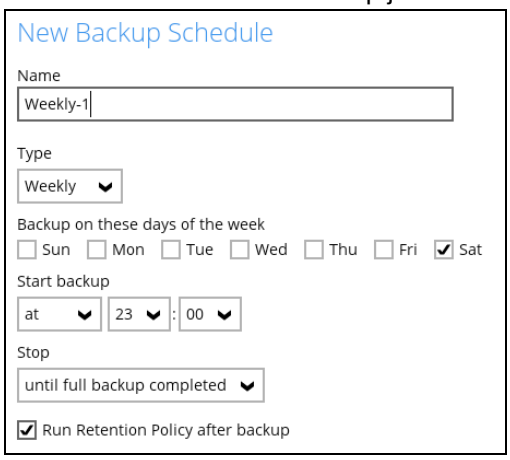


- **Name** – the name of the backup schedule.
- **Type** – the type of backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.

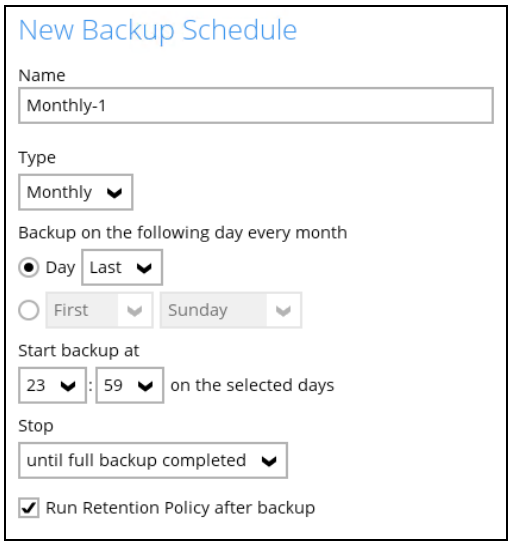
Daily – the time of the day or interval in minutes/hours when the backup job will run.



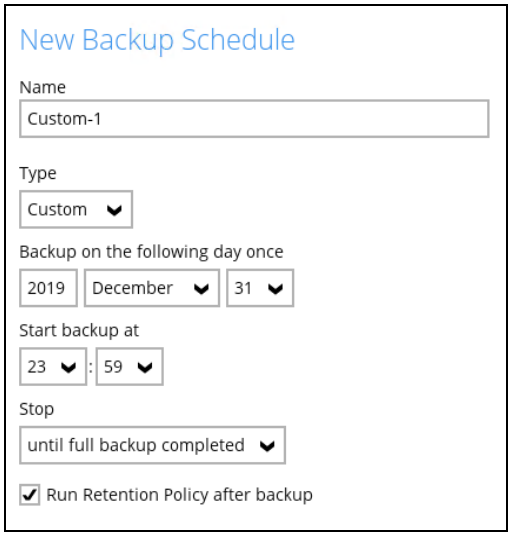
Weekly – the day of the week and the time of the day or interval in minutes/hours when the backup job will run.



Monthly – the day of the month and the time of that day which the backup job will run.



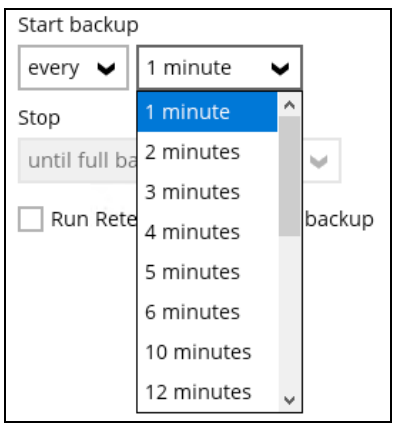
Custom – a specific date and the time of that date when the backup job will run.

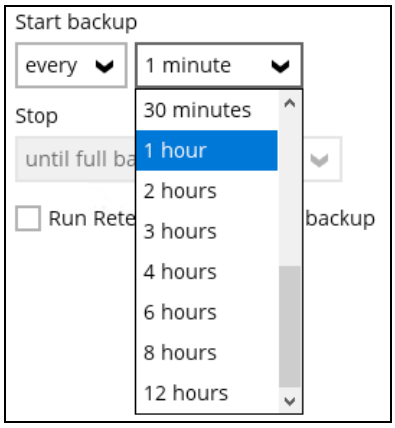


- **Start backup** – the start time of the backup job.

  at – this option will start a backup job at a specific time.

  every – this option will start a backup job in intervals of minutes or hours.





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

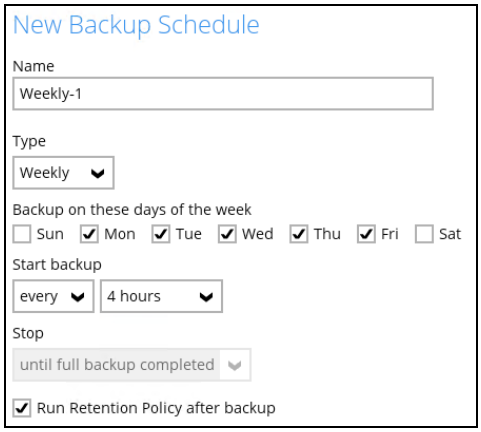


Figure 1.1

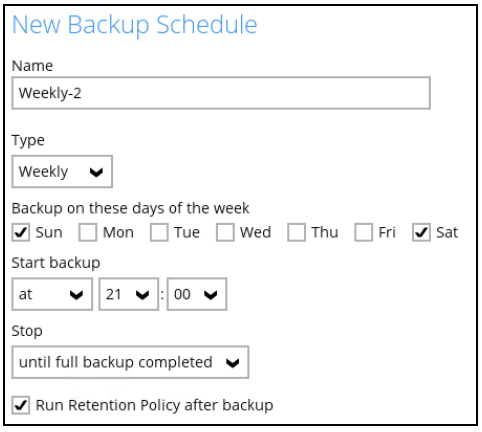


Figure 1.2

Figure 1.1 – Periodic backup schedule runs every 4 hours from Monday – Friday during business hours

Figure 1.2 – Normal backup schedule runs at 21:00 or 9:00 PM on Saturday and Sunday on weekend non-business hours

- **Stop** – the stop time of the backup job. This only applies to schedules with start backup "at" and is not supported for periodic backup schedule (start backup "every")

  until full backup completed – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.

  after (defined no. of hrs.) – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

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

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

  The partially backed up data will have to be removed by running the Data Integrity Check.

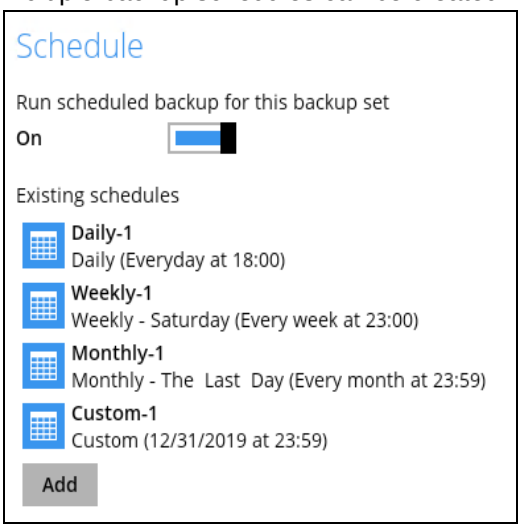
  As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.

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

4. Click the [OK] button to save the configured backup schedule settings.

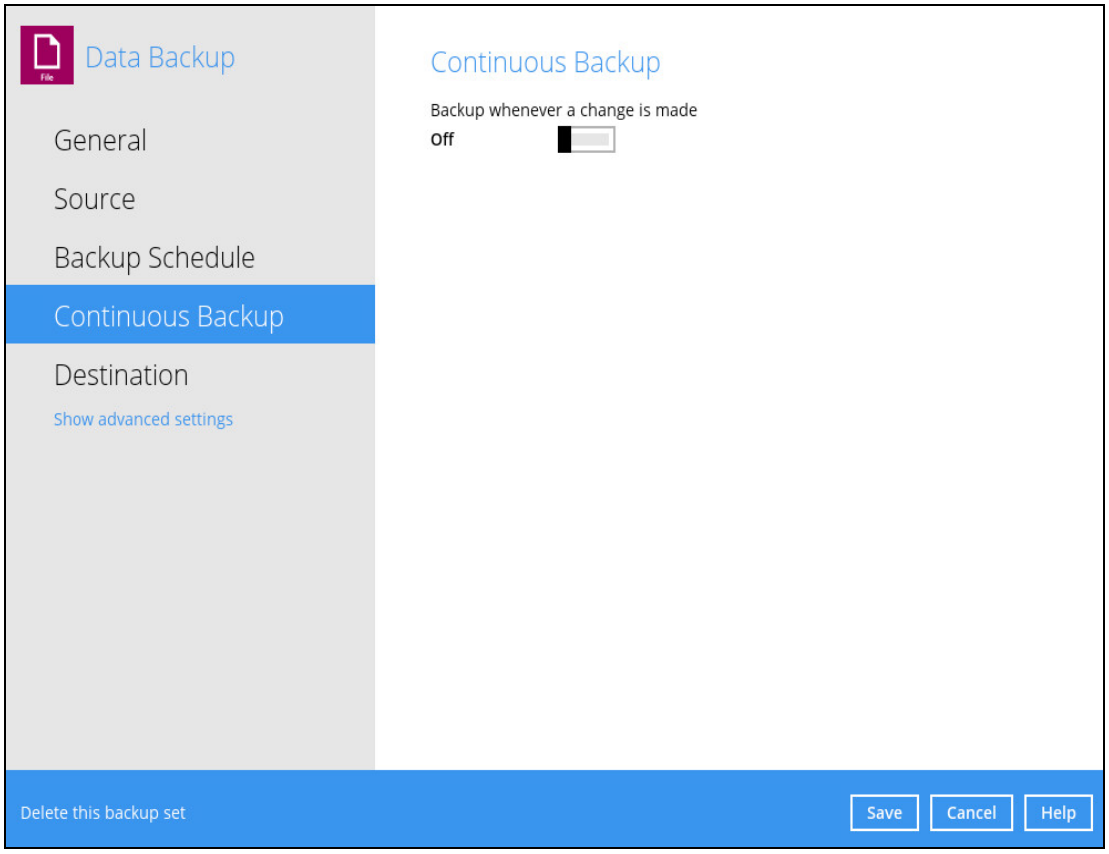
5. Click the [Save] button to save settings.

6. Multiple backup schedules can be created.



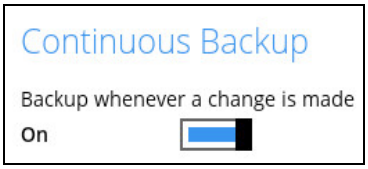
Continuous Backup

This feature provides backup for selective data whenever a change is made. This feature is disabled by default.

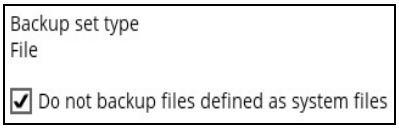


To enable the continuous backup, follow the steps below:

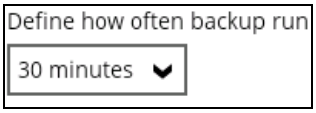
1. Swipe the lever to the right to turn on the continuous backup setting.



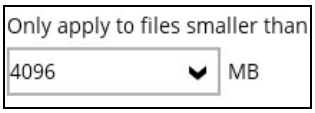
2. It is recommended to select this option to avoid backing up files that are marked as system files.



3. Define how often the continuous backup job will run. The backup time interval can be set from 1 minute to 12 hours.



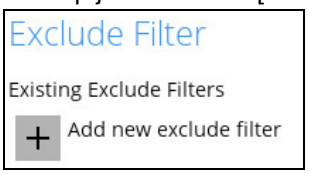
4. This applies the continuous backup on small regular update files. The file size can range from 25MB to unlimited MB.



NOTE

For large file size, the continuous backup may not run with a short time interval. You may need to adjust the continuous backup time interval (in step 3).

5. This allows the user to create an exclude filter to exclude files and/or folders from the backup job. Click the [Add] button to create an exclude filter.



6. If an exclude filter is created, click the [OK] button to save the created exclude filter, then click the [Save] button to save the configured continuous backup settings.

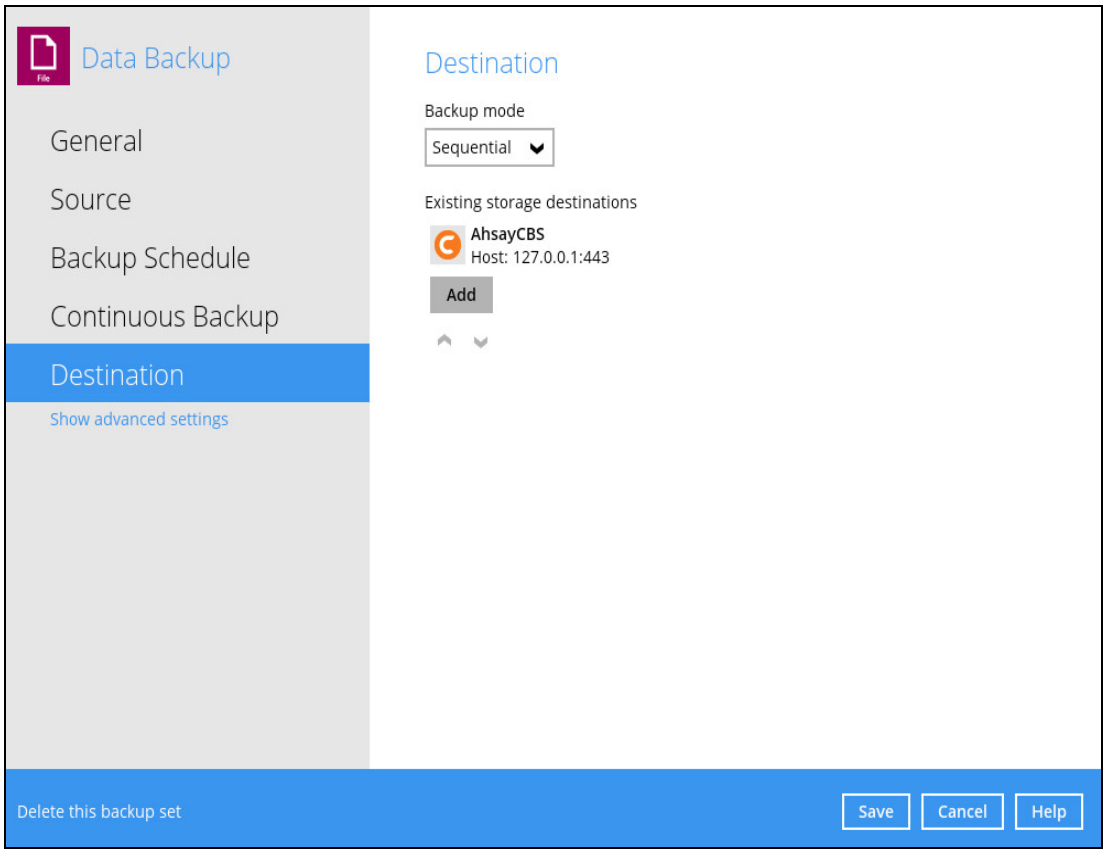
NOTE

Only File backup sets on Windows operating system will support Continuous Backup Schedule on v8.3.4.0 (or above)

All v7 and pre-v8.3.4.0 Windows non-File backup sets with Continuous Backup Schedules will be automatically converted to periodic backup schedules after upgrading to v8.3.4.0 (or above)

Destination

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



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

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

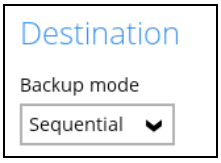
Comparison between Sequential and Concurrent Backup mode

Backup mode	Pros	Cons
Sequential	➢ Takes less resources in the local machine (e.g., memory, CPU, bandwidth, etc.) to complete a backup job.	➢ Backup job is slower than in concurrent mode since the backup job will upload the backup data to the selected backup destinations one at a time.

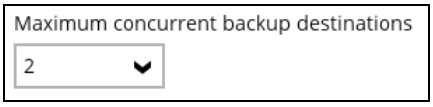
Concurrent	➢ Backup job is faster than in Sequential mode. ➢ Maximum number of concurrent backup destinations can be configured.	➢ Requires more resources in the local machine (e.g. memory, CPU, bandwidth, etc.) to complete a backup job.

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.



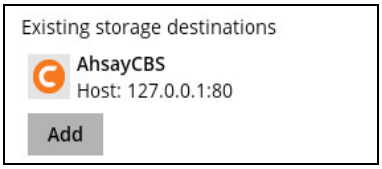
4. If “Concurrent” is selected, click the drop-down button to select the no. of maximum concurrent backup destination.



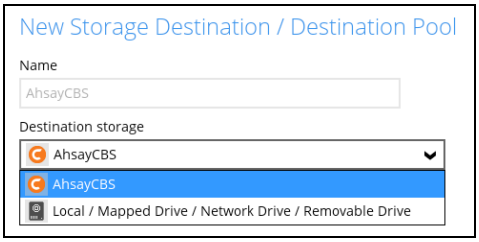
5. Click the [Save] button to save the selected backup mode.

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

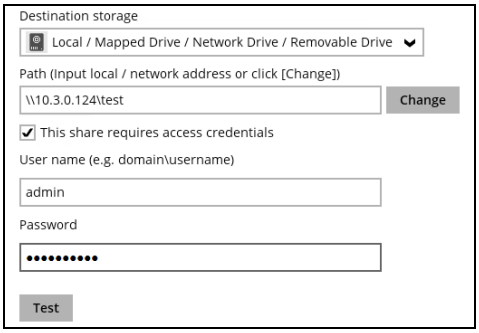
1. Click the [Add] button.



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



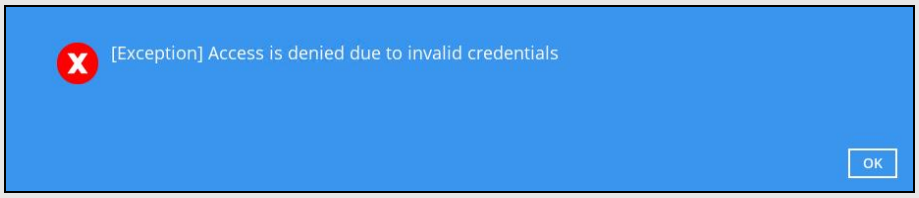
3. If the Local / Mapped Drive / Network Drive / Removable Drive is selected, click the [Change] button to select a new storage destination or input the local or network address. Check ‘This share requires access credentials’ if required then click the [Test] button to validate access to it.



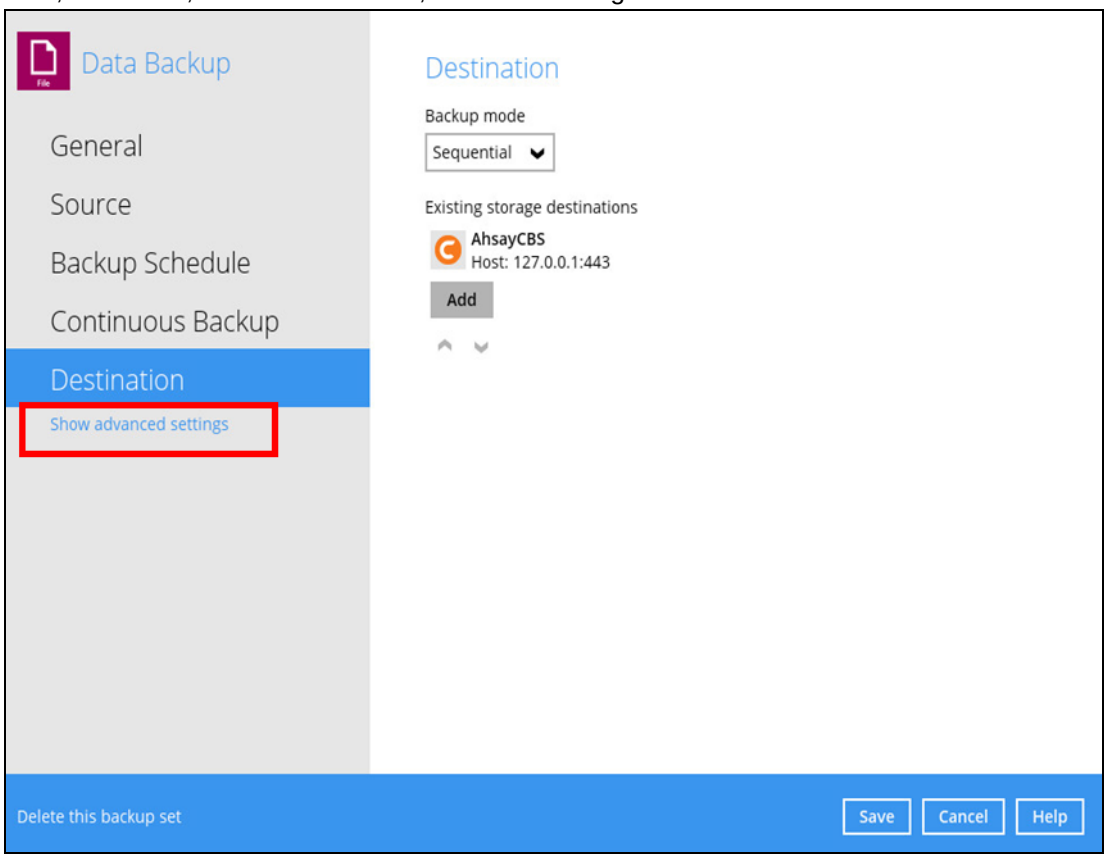
4. If there is an added storage destination, click the [OK] button to save the added one. Then click the [Save] button to save the updated backup mode and the added storage destination.

NOTE

The error below will appear if 'This share requires access credentials' is not checked and access credentials are setup in the storage destination.

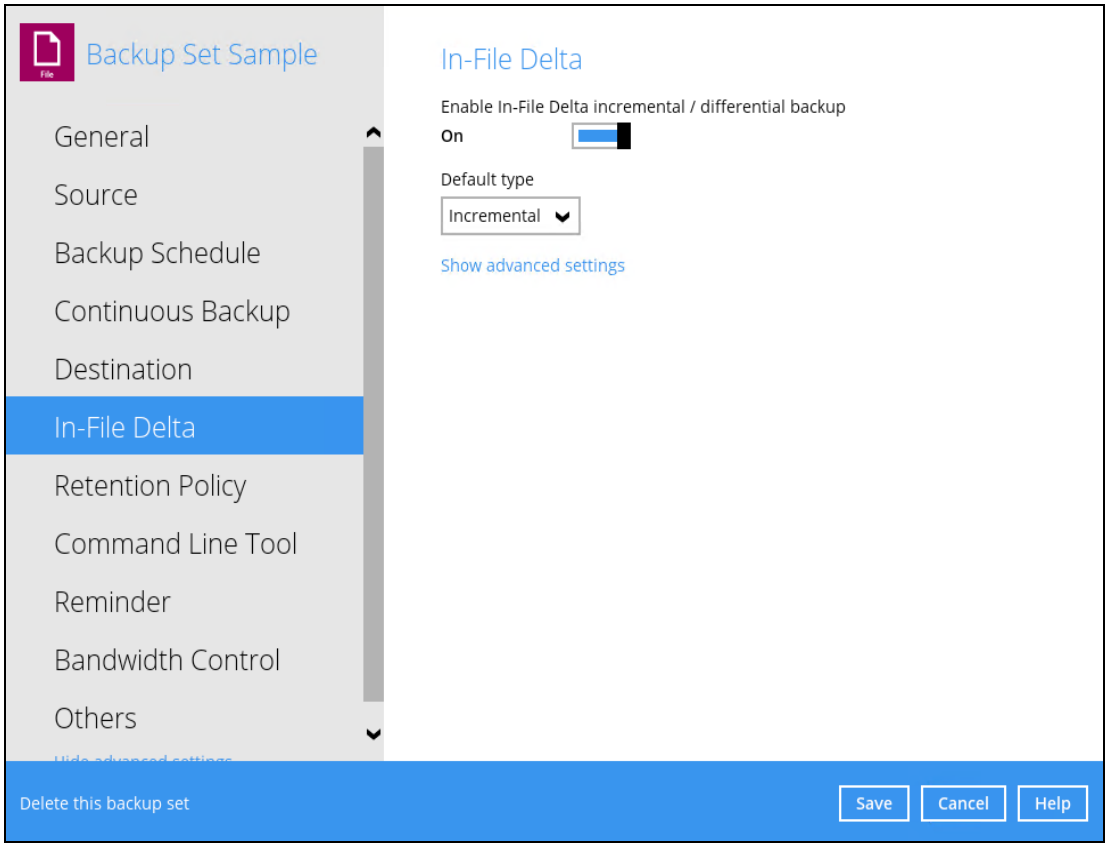


Select **Show advanced settings** to modify the In-File Delta, Retention Policy, Command Line Tool, Reminder, Bandwidth Control, and other configurable items.



In-File Delta

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



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

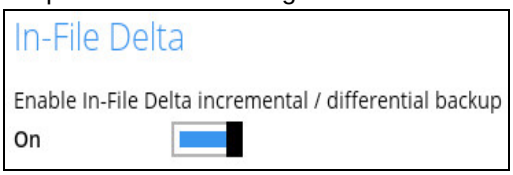
In-File Delta Type	Description
Differential	The delta is generated by comparing with the last uploaded full file only. Delta generated with this method will grow daily and uses more bandwidth.
Incremental	This is the configured In-file delta by default. The delta is generated by comparing with the last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

Comparison between Incremental and Differential In-File Delta

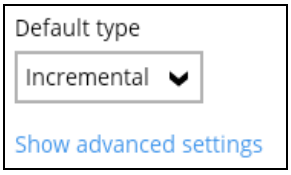
In-File Delta Type	Pros	Cons
Differential	➢ Backup speed is faster than Full backup. ➢ Restoration is faster than data backup with Incremental In-File Delta. Less storage space is need than a Full backup.	➢ Backup process is slower than Incremental In-File Delta backup. ➢ Restoration is slower than data backup with Full backup.
Incremental	➢ Backup process is fastest among all three (3) types; Full, Differential, and Incremental ➢ Least storage space is required.	➢ Restoration is slowest among all three (3) types; Full, Differential, and Incremental. ➢ For restoration, the full file and all deltas that does not chain up to the required point-in-time may result to broken delta chain.

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

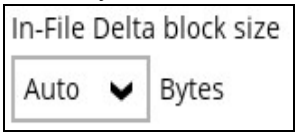
1. Swipe the lever to the right to enable the In-File Delta.



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

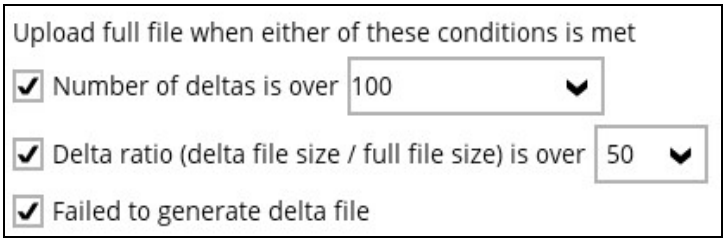


3. Click the drop-down button to specify the In-File Delta block size. This is configured as "Auto" by default.



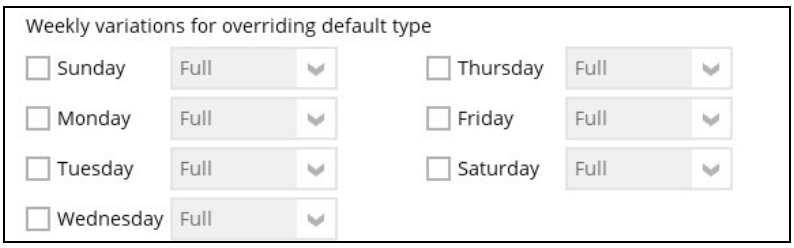
4. Click the drop-down button to select how much of the file size (MB) the In-File Delta logic will apply to. By default, the In-File Delta logic is configured to apply to files larger than 25 MB.

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

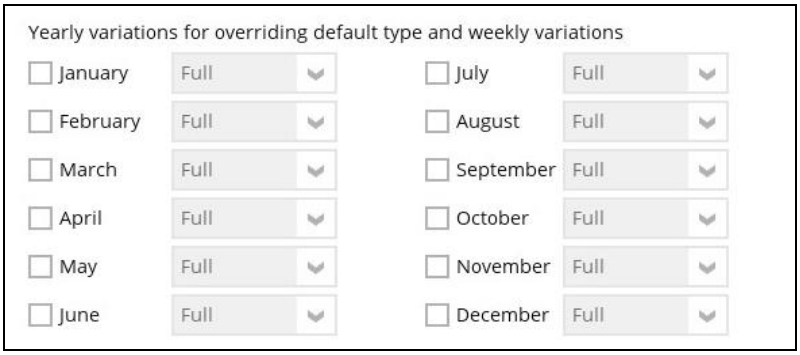


- This allows the user to configure a different In-File Delta setting to override the default In-File Delta.

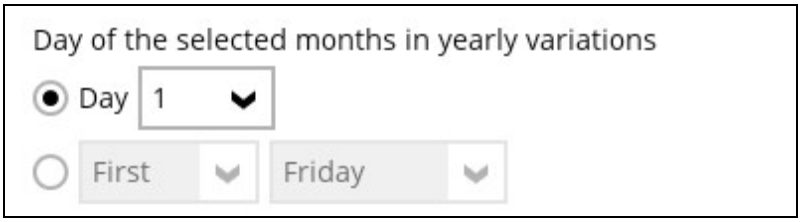
  Weekly variations – for example, you set Sunday to perform a full backup, for the rest of the week, a backup based on the default In-File Delta will be run.



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



  This allows the user to specify which day of the selected months in yearly variations the backup job will be run. (e.g., First of January, March, May...)



6. Click the [Save] button to save the modified In-File Delta settings.

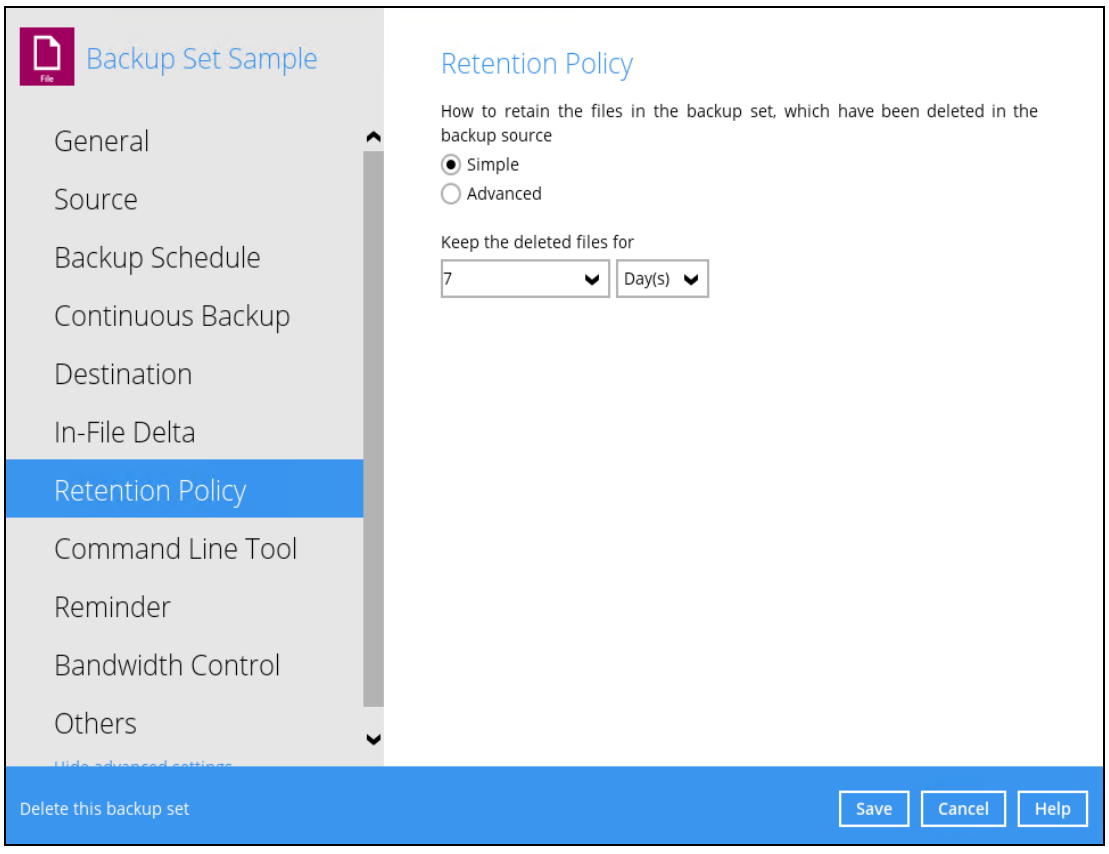
Retention Policy

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

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

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

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



NOTE

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

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

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

Comparison between Simple and Advanced Retention Policy

Control	Simple	Advanced
Backup Jobs	Can keep the deleted files 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	➢ Daily ➢ Weekly ➢ Monthly ➢ Quarterly ➢ Yearly ➢ Custom
User-defined name	Not applicable	Applicable

WARNING

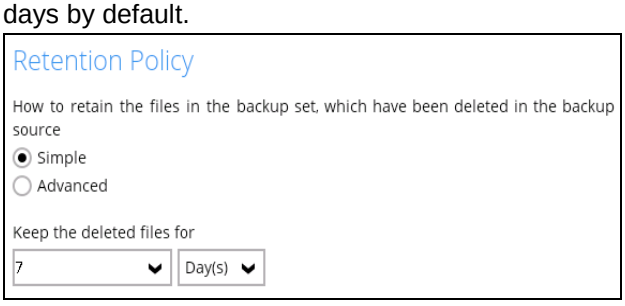
When files and/or folders in the retention area exceed the Retention Policy setting, they are permanently removed from the backup set and cannot be restored

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

1. 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.



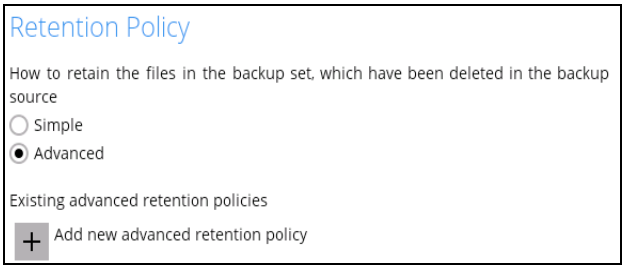
4. Click the [Save] button to save the configured retention policy settings.

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.

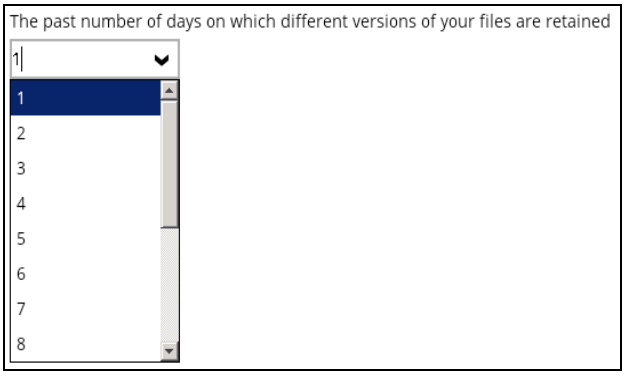
3. Select [Advanced] from the options, then click the [Add] button to create.



4. Assign a desired name to the retention policy.

5. Click the drop-down button to display the retention type, then select one.

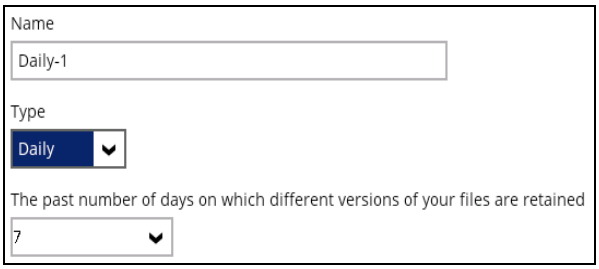
6. Click the drop-down button to specify the period on which the deleted files will be kept in the backup set.



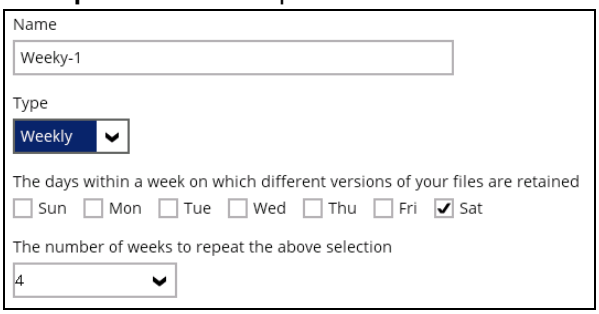
7. Click the [OK] button to save the configured advanced retention policy, then click [Save] to save the settings.

For further details about how to configure an advanced retention policy for each type (Daily, Weekly, Monthly, Quarterly, Yearly), refer to the examples below:

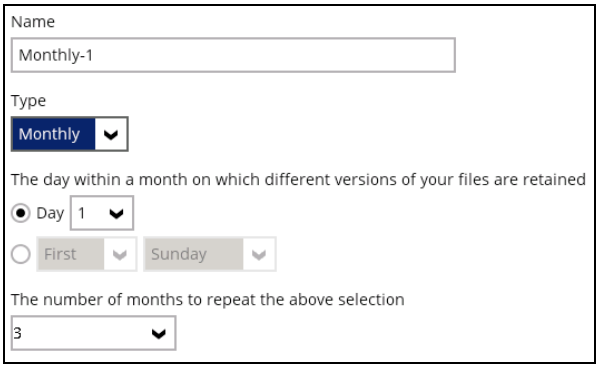
- **Example no. 1**: To keep the retention files for the last seven (7) days:



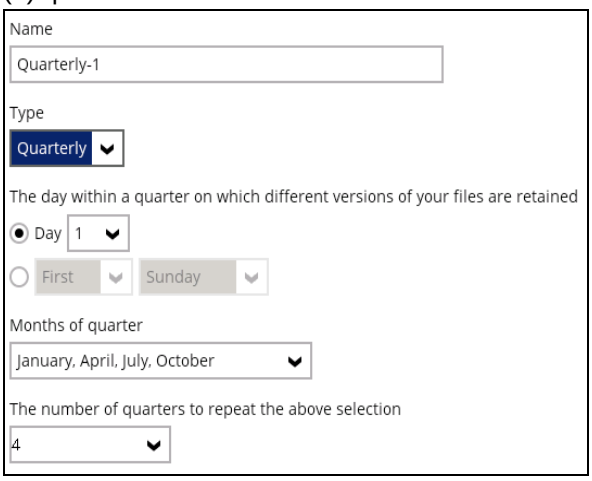
- **Example no. 2**: To keep the retention files for the last four (4) Saturdays:



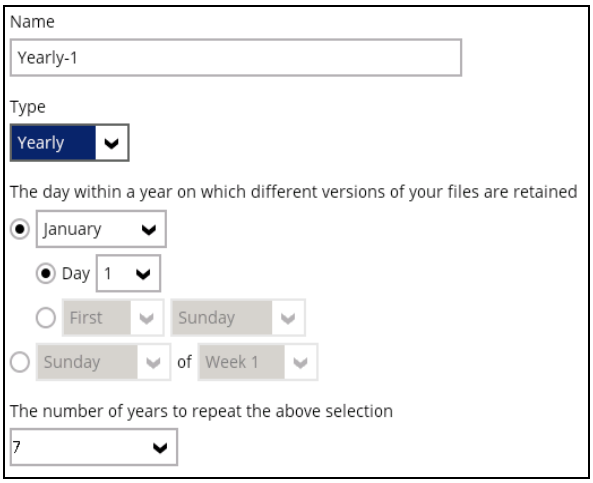
- **Example no. 3**: To keep the retention files for the 1st day of each month for the last three (3) months:



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



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



NOTE

Multiple advanced retention policy can be created.

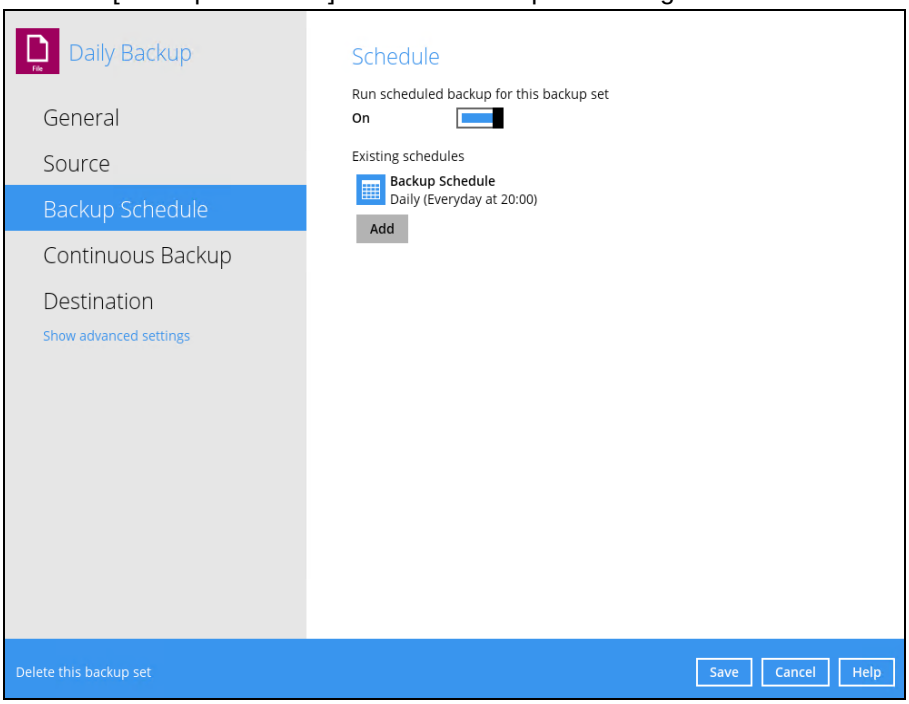
There are three (3) ways to run the Retention Policy:

- Backup Scheduler
- Manual Backup
- Space Freeing Up

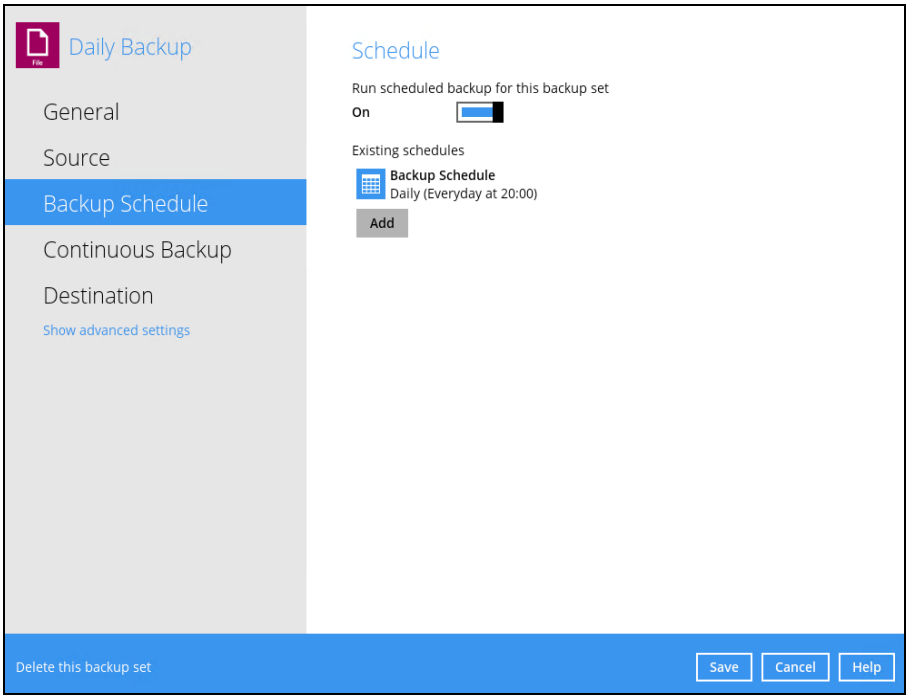
Backup Scheduler (Recommended)

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

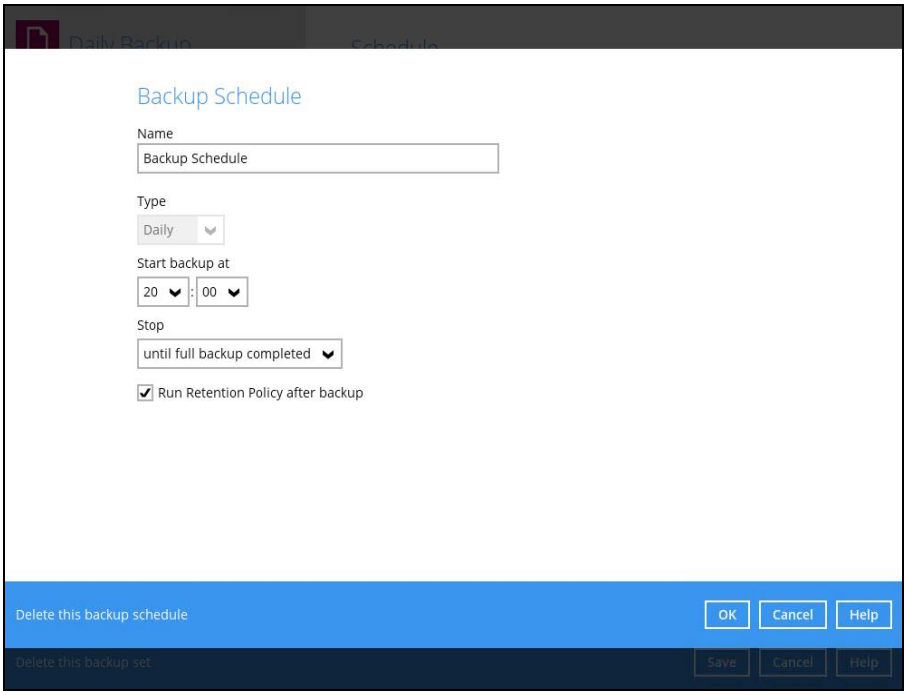
1. Click the [Backup Schedule] tab in the backup set settings.



2. Select an existing backup schedule or add a new one.



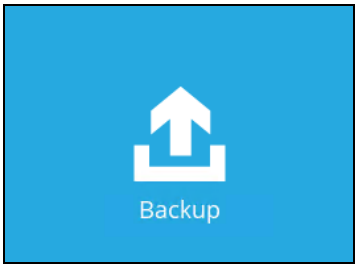
3. In the Backup Schedule window, select ‘Run Retention Policy after backup’ to run a retention policy job after a scheduled backup job.



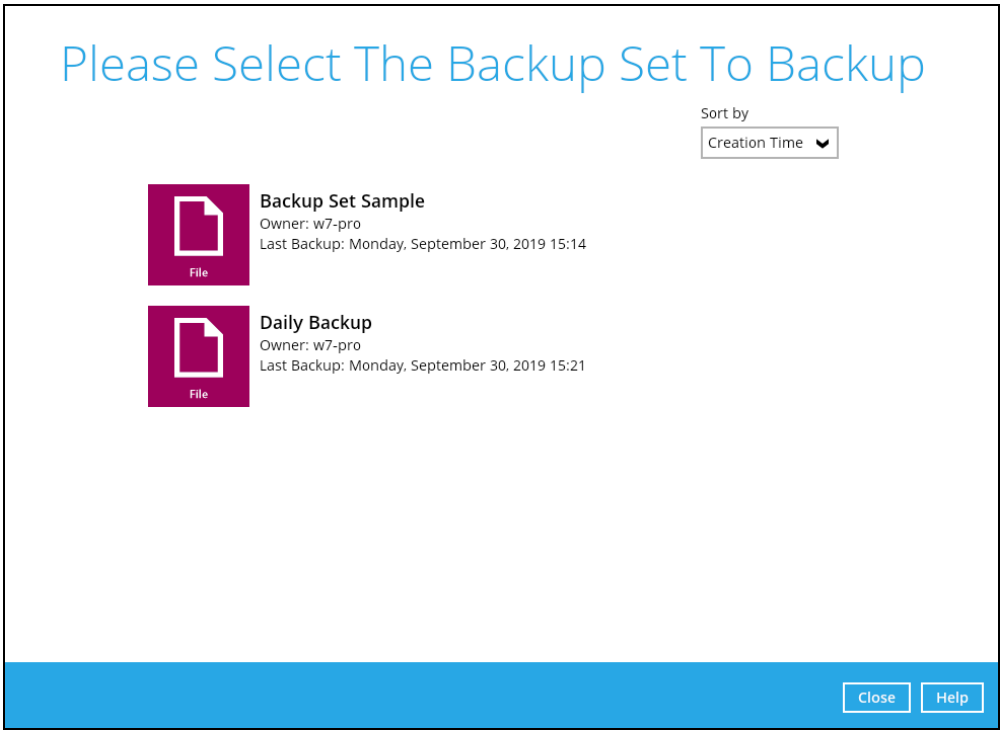
Manual Backup

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

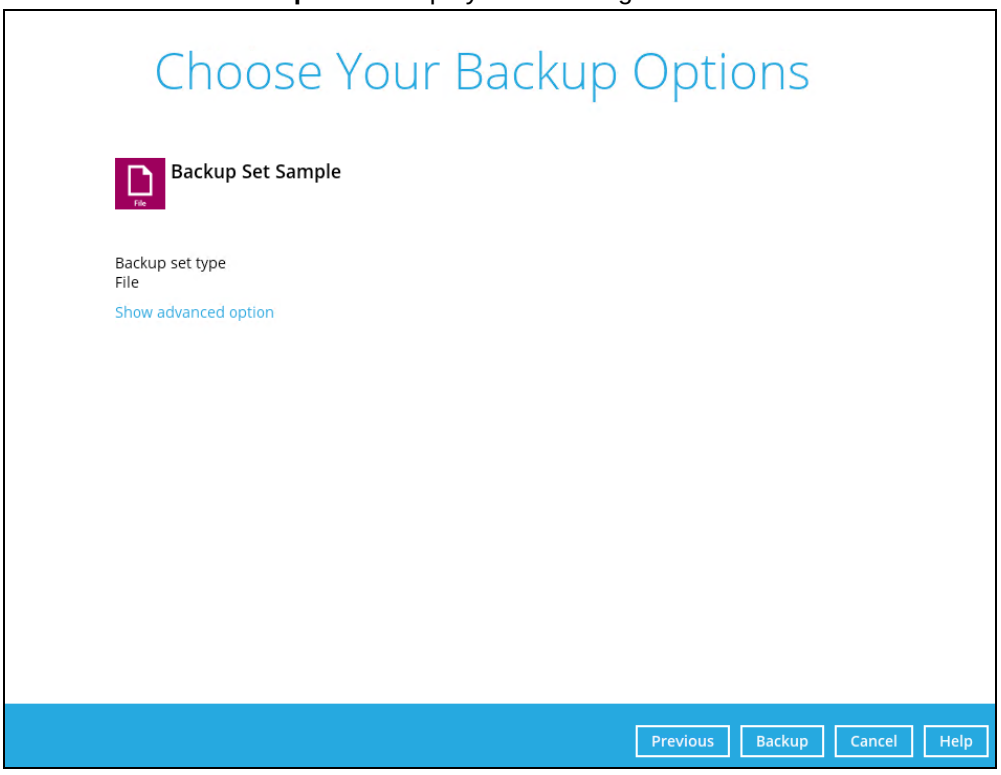
1. Click the **Backup** icon in the AhsayOBM main interface.



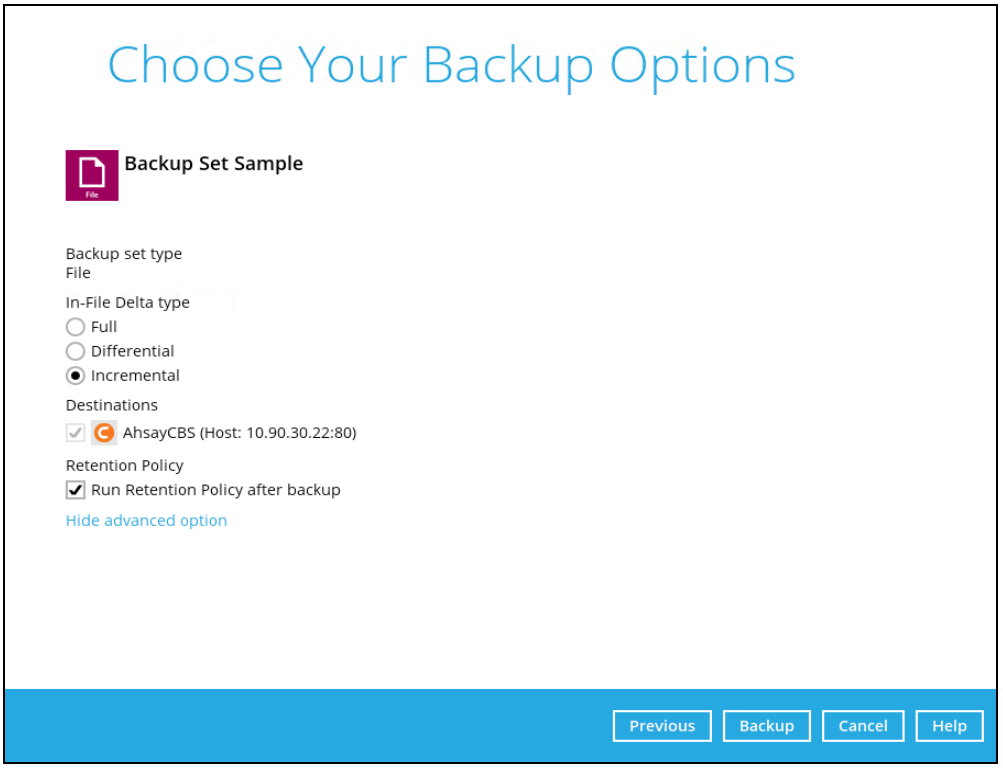
2. Select the backup set that you would like to back up and run the retention policy job on.



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



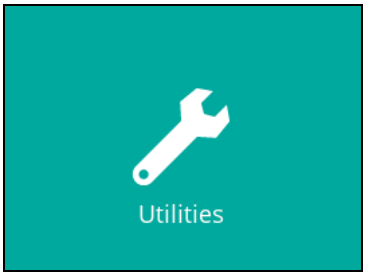
4. Select 'Run Retention Policy after backup' to run a retention policy job after a backup job.



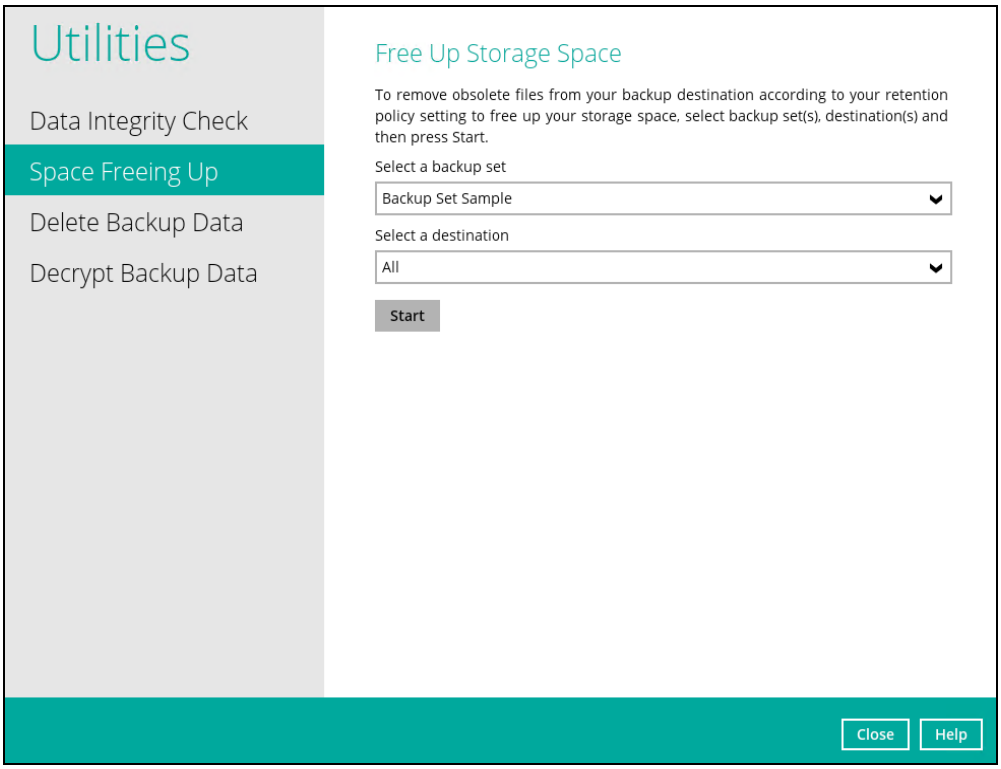
Space Freeing Up

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

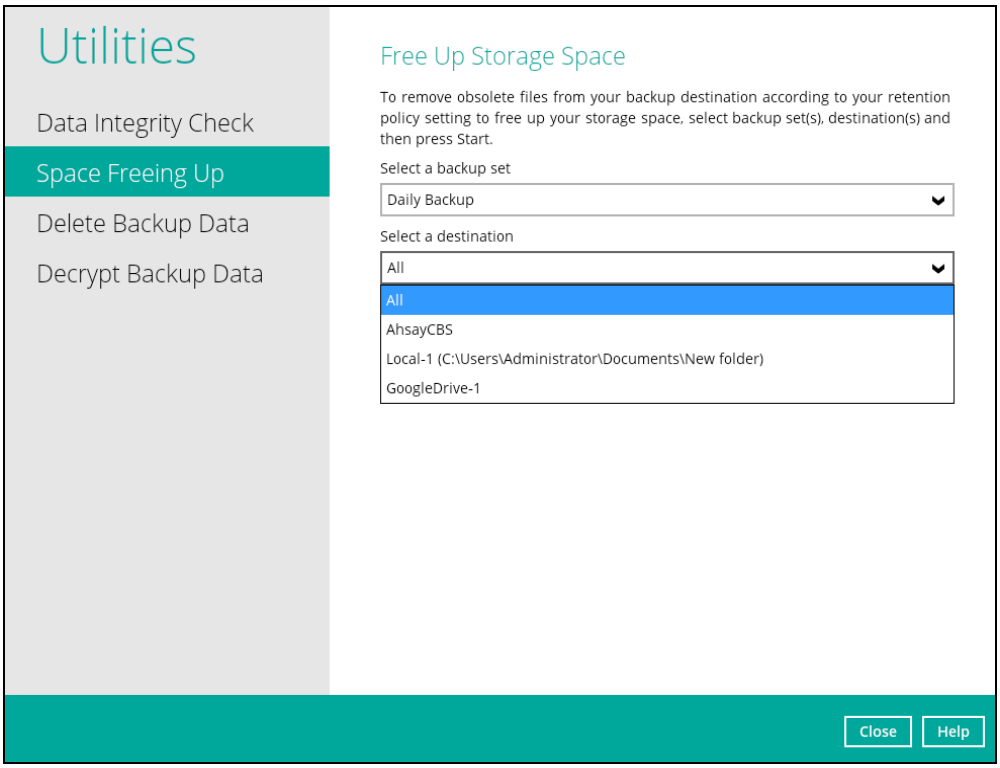
1. Click the **Utilities** icon in the AhsayOBM interface.



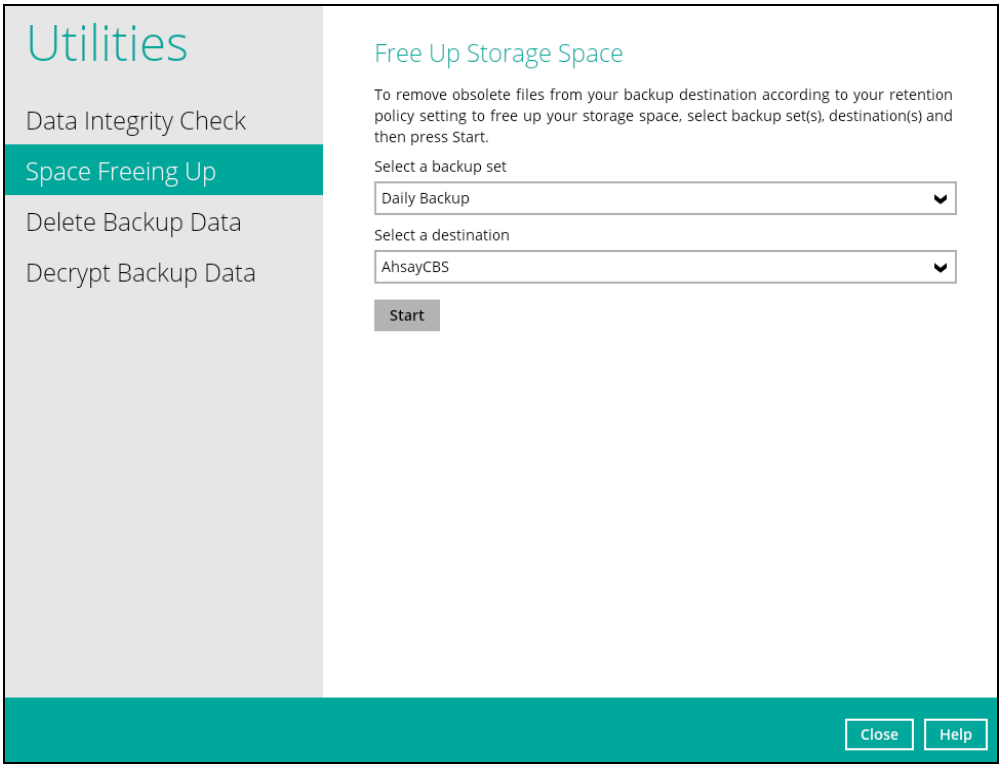
2. Select the [Space Freeing Up] tab in the Utilities settings.



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.



4. Click the [Start] button to run the retention policy job.



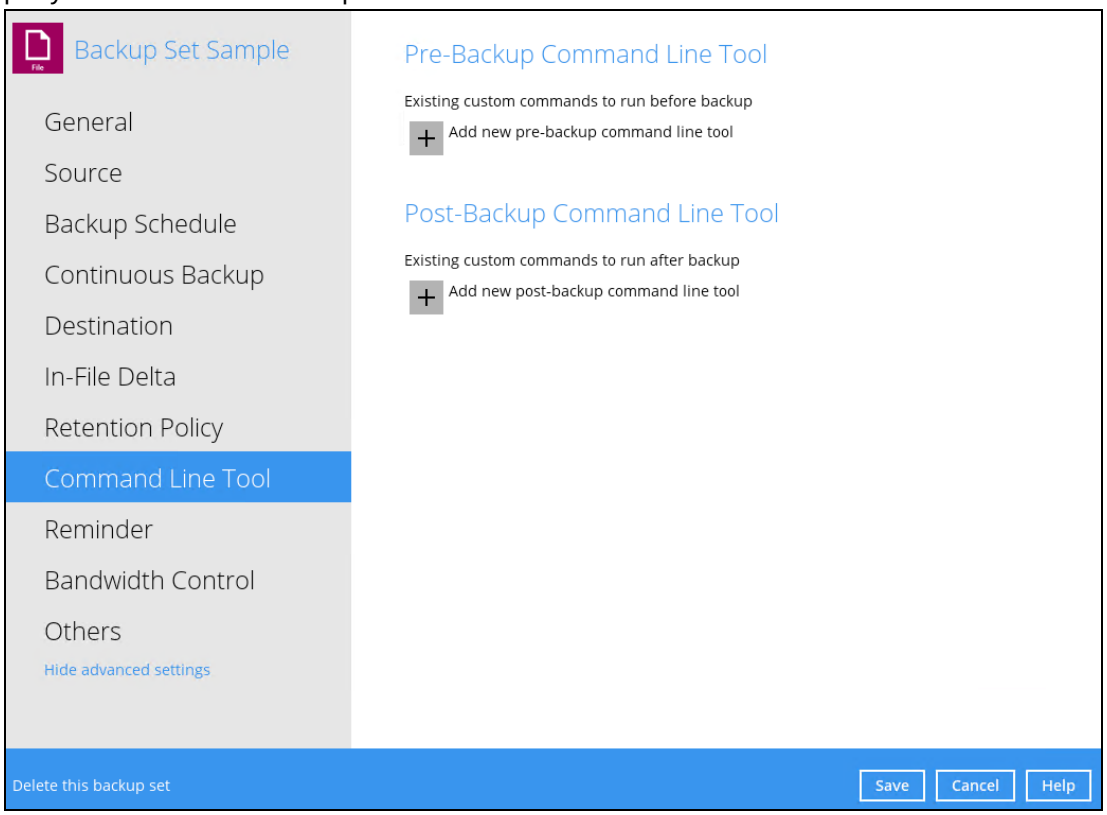
NOTE

For more details about Space Freeing Up, please refer to Space Freeing Up in **Chapter 10 AhsayOBM Overview**.

Command Line Tool

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

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



Requirements and Best Practices

Error and Exception Handling

Each pre-backup command or batch file should have an error and exception handling. If a pre-backup command contains an error, although an unhandled error may not hinder the backup job process, and the backup job is successful, it will result to a status indicating completed backup with warning(s). For more details about backup report status, please refer to Backup Reports in **Chapter 10 AhsayOBM Overview**.

Command or Batch File Compatibility

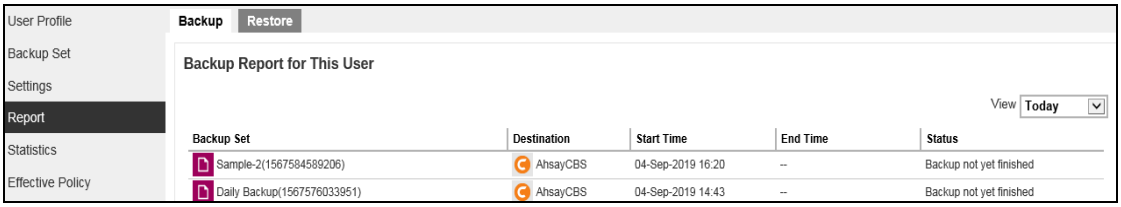
Make sure that each command (pre-backup and post-backup) are tested thoroughly before including them to the backup job.

Scheduled Backup

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

Pre-backup Command Limitation

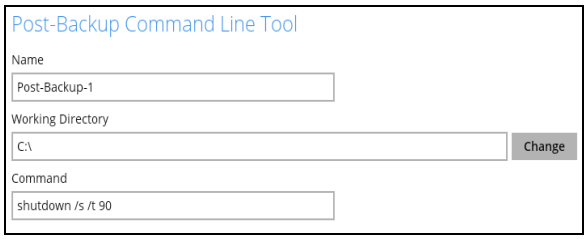
A Windows reboot or shutdown must not be used in the pre-backup command. Otherwise, the machine will shut down immediately that will result to a status indicating “Backup not yet finished”, which can be viewed in the AhsayCBS User Web Console. Please refer to AhsayCBS Backup Reports for more details.



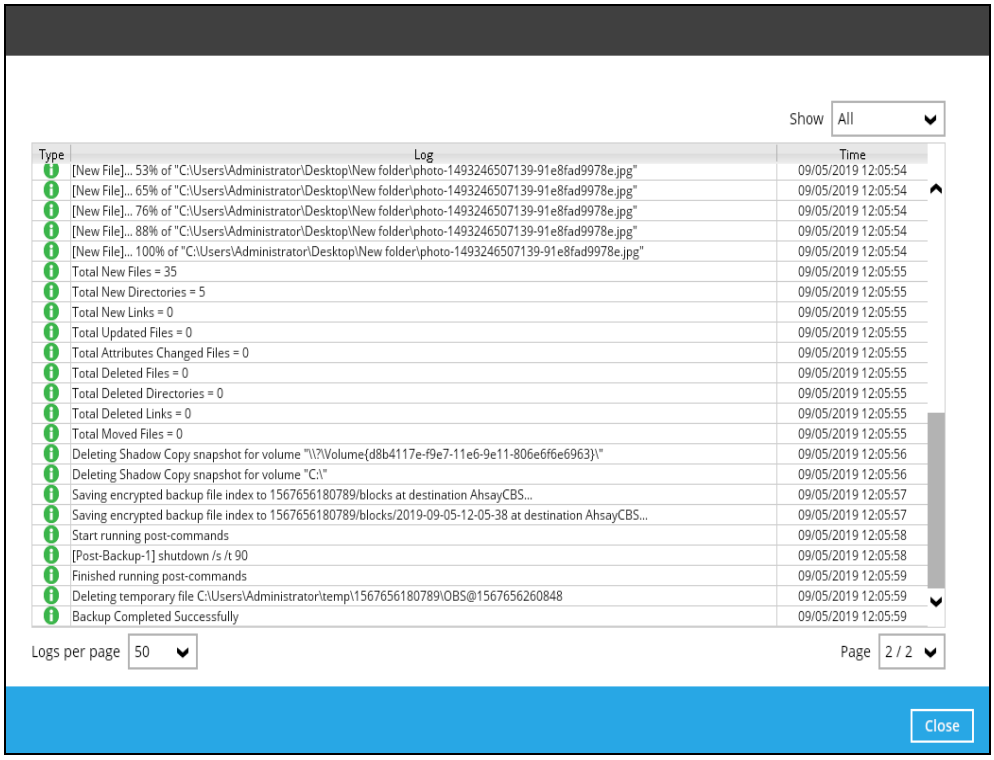
Post-backup Command Recommendation

It is recommended to include a timeout for a post-backup command to shut down the machine. The timeout must be adjusted until when the AhsayOBM sends the backup job status to the AhsayCBS.

In this example, the configured post-backup command is to shut down the machine that has a timeout set to ninety (90) seconds. The machine will shut down automatically after the specified time.



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. See screenshot below:



NOTE

For more details about detailed backup report, please refer to Backup Reports in **Chapter 10 AhsayOBM Overview**.

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 command to execute a batch file, command, or a VBScript (exclusively for Windows).

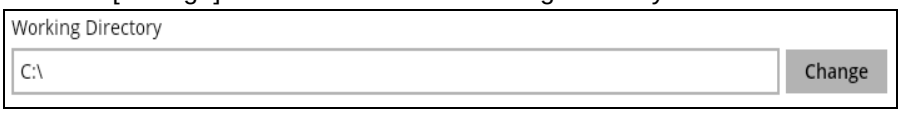
Pre-backup Command

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

1. Click the [Add] button.

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

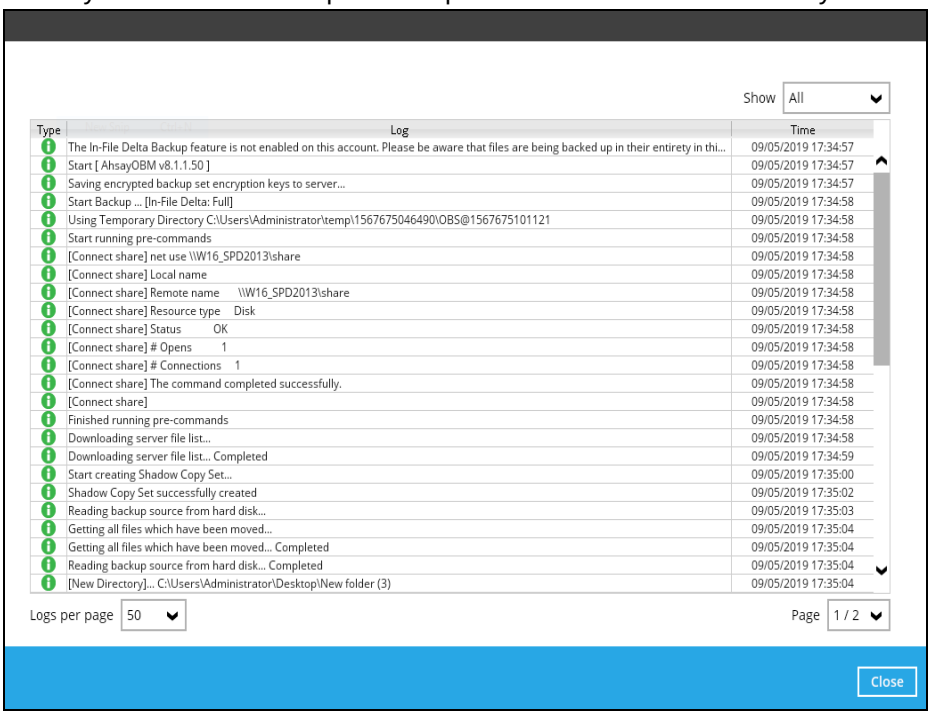
3. Click the [Change] button to locate the working directory of the command.



4. Input a command to be run before a backup job. In this example, the pre-backup command will connect to a network drive before the backup process.

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

6. Once the backup job is complete, click the button to display the backup report log where you can check if the pre-backup command has run successfully.

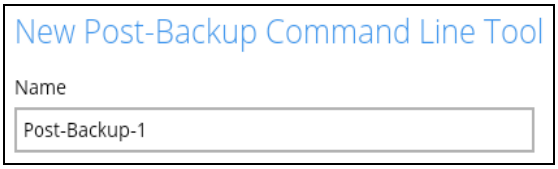


Post-backup Command

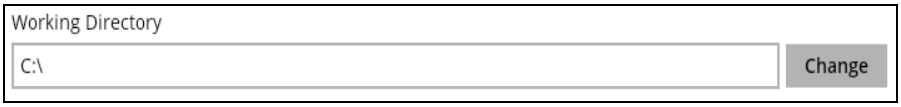
A post-backup command is used to execute an action or process after a backup job. To create a post-backup command, follow the steps below:

1. Click the [Add] button.

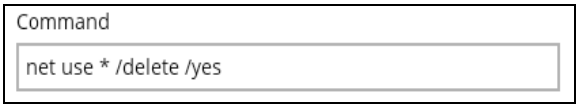
2. Assign a desired name to the post-backup command.



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

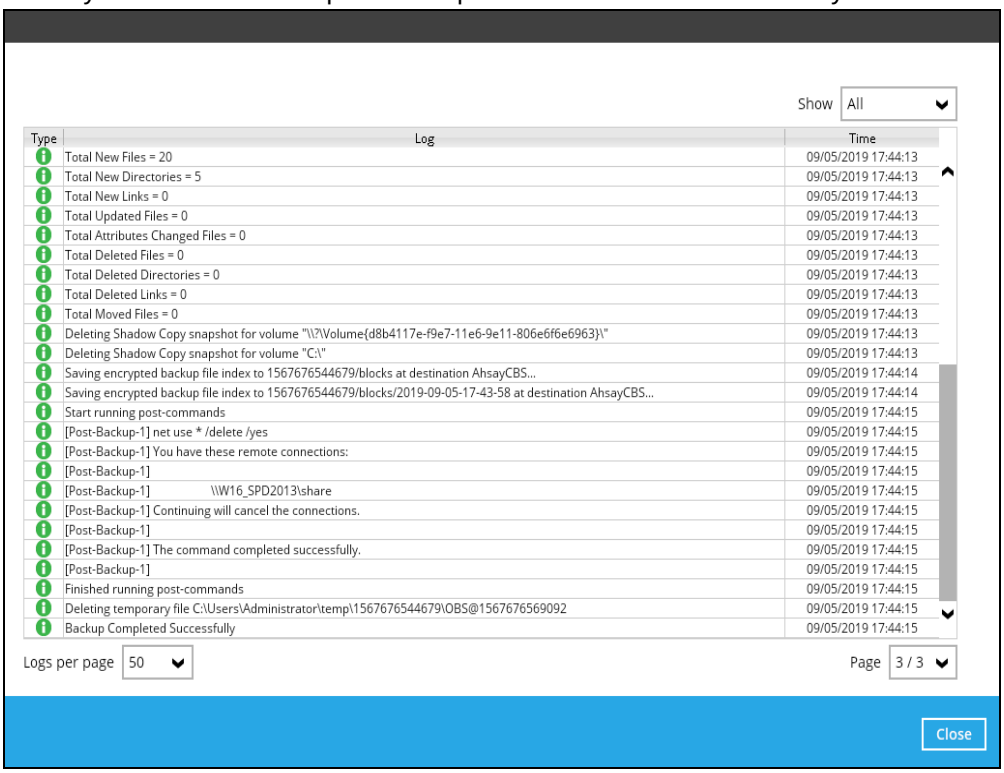


4. Input a command to be run after a backup job. In this example, the post-backup command will disconnect a network drive after the backup process.



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

6. Once the backup job is complete, click the button to display the backup report log where you can check if the post-backup command has run successfully.

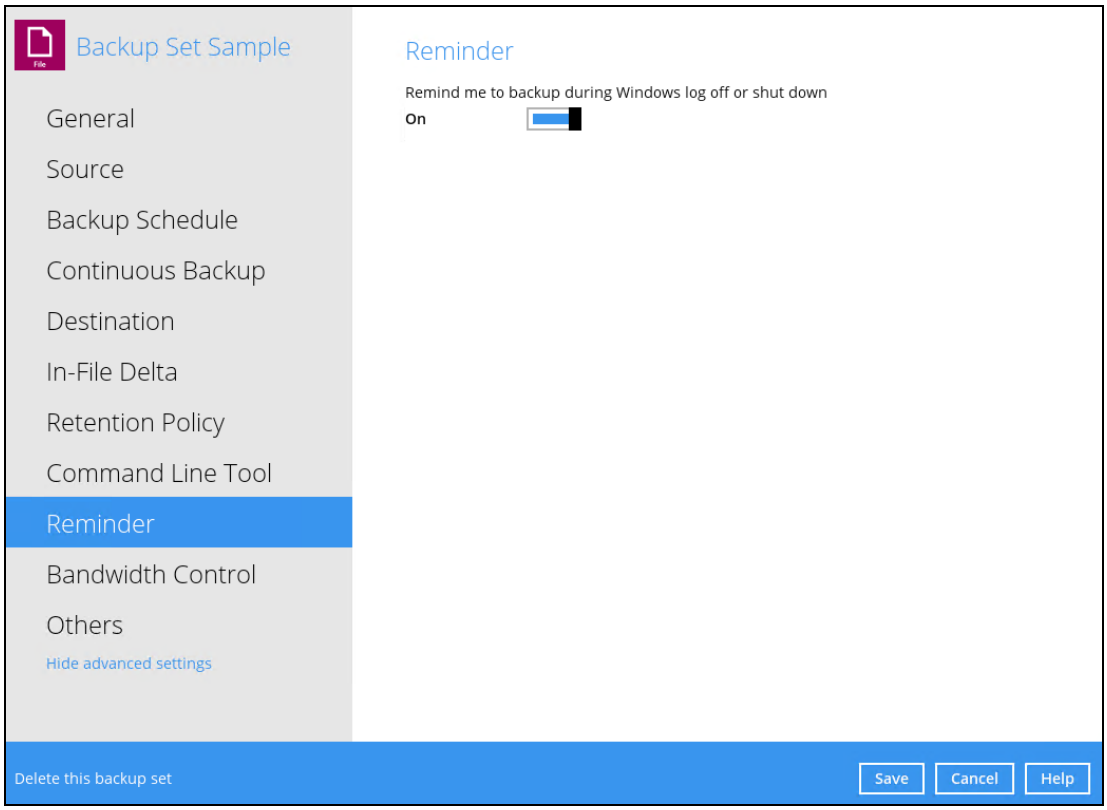


NOTE

Multiple commands (pre-backup and post-backup) can be created in the Command Line Tool

Reminder

This feature is enabled by default. When enabled, a backup confirmation dialog box will prompt the user to run a backup job during Windows log off, restart or shut down.



To enable the Reminder setting, follow the steps below:

1. Go to Backup Sets, then select a backup set.
2. Choose the [Reminder] tab in the backup set settings.
3. Swipe the lever to the right to turn on the reminder.
4. Click the [Save] button to save settings.

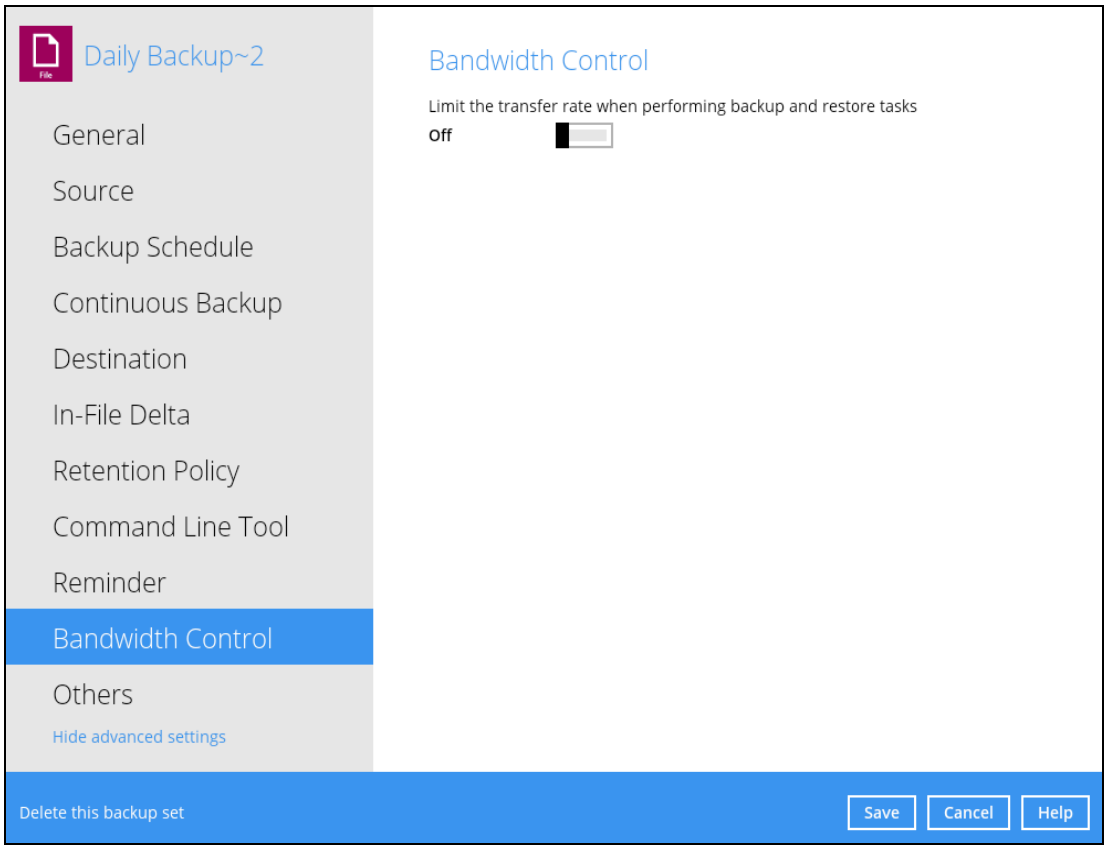
NOTES

1. This feature is not supported on Windows 10, Windows Server 2016, and Windows Server 2019.
2. The dialog box will only appear if there is a backup set with enabled Reminder setting.
3. The dialog box will only be displayed for four (4) seconds.
4. If there are multiple backup sets displayed, you cannot select one (1) backup set to back up. It is recommended to only enable the Reminder setting for the backup sets you regularly back up.

For more detailed examples of the reminder feature, please refer to Appendix D: Example Scenarios for the Reminder.

Bandwidth Control

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



There are two (2) different modes in assigning a 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.

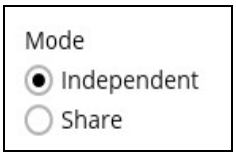
NOTE

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

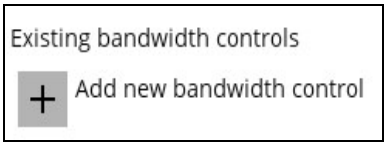
To enable the bandwidth control setting, follow the steps below:

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

2. Select a bandwidth control mode.



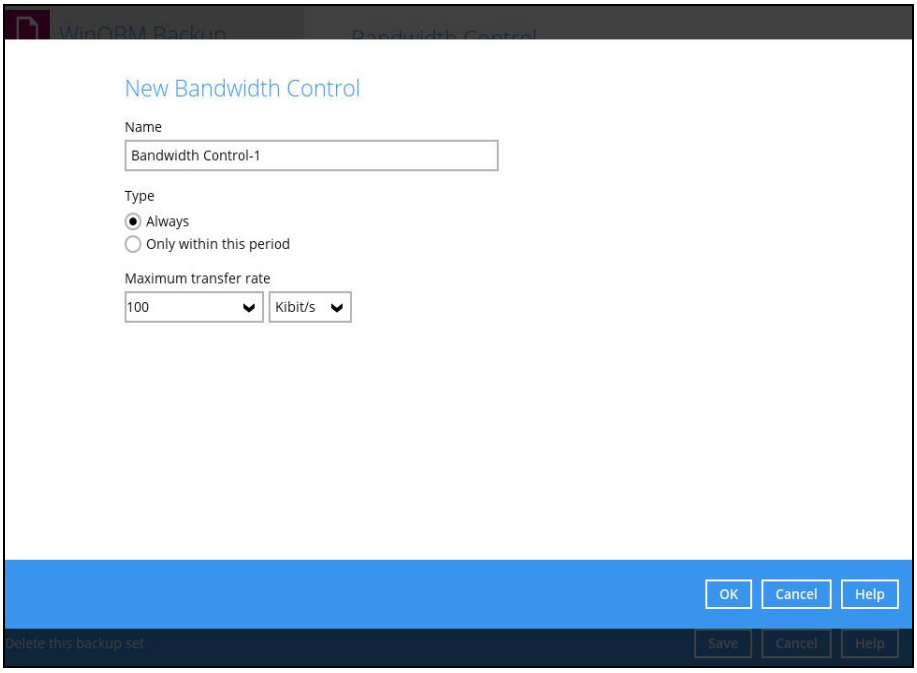
3. If you want to add a modified bandwidth control, click the [Add] button.



4. Complete the following fields:

   - Name
   - Type
   - Maximum transfer rate

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

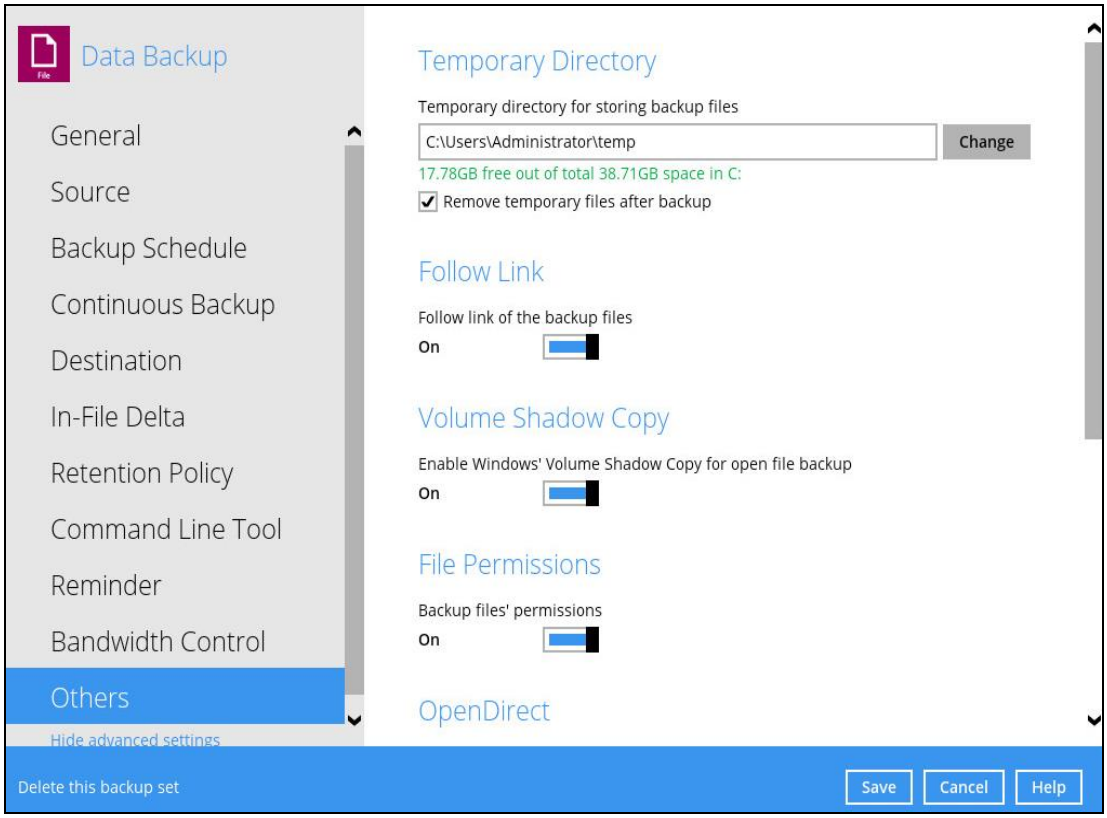


5. Click the [OK] button to save the created bandwidth control set, then click the [Save] button to save settings.

Others

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

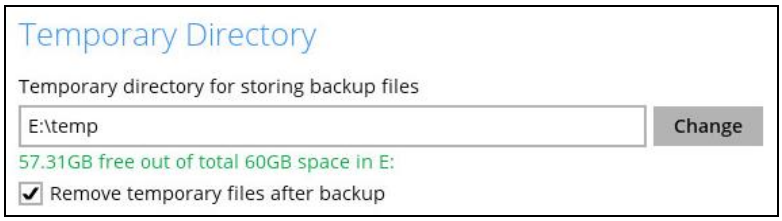
- Temporary Directory
- Follow Link
- Volume Shadow Copy
- File Permissions
- OpenDirect
- Compressions
- Encryption



Temporary Directory

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

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



- Backup set index files. An updated set of index files is generated after each backup. The index files are synchronized to each individual backup destination at the end of each backup job.
- Incremental/Differential delta files generated during backups.

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

- Full and Incremental/Differential delta files retrieved from the backup destination.
- Merging of the Full and Incremental/Differential delta files as part of the restore process.

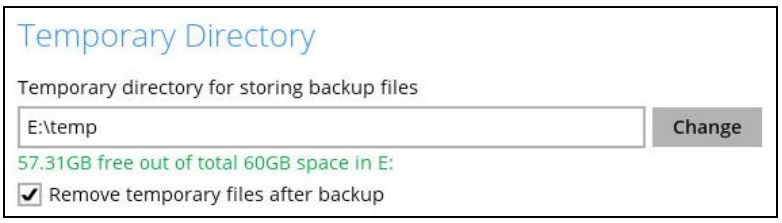
NOTES

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

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

To change the temporary directory, follow the steps below:

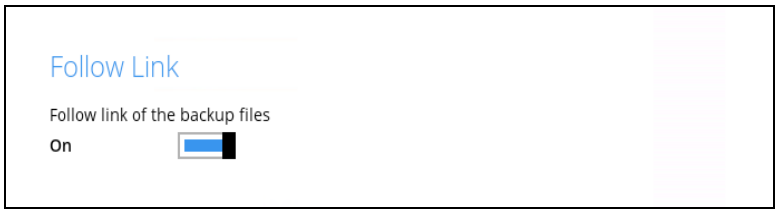
1. Click the [Change] button to select a directory path for storing temporary data.



Click the [Save] button to save 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 option is enabled by default.



NOTE

Applicable for File Backup Sets only.

Volume Shadow Copy

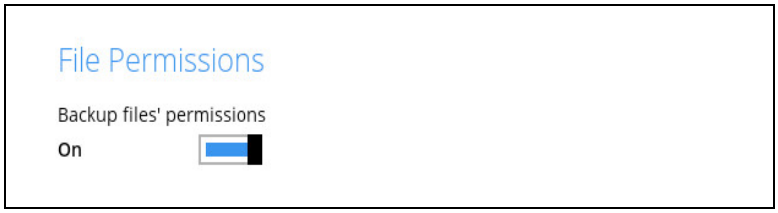
This feature allows the AhsayOBM to use the Windows Volume Shadow Copy service to create a snapshot of the selected files and/or folders on the local drive(s) of the machine, so that the AhsayOBM can continue to back up files even if they are opened and/or have been updated by the user. This feature is enabled by default.

WARNING

1. To use the Volume Shadow Copy, the license module must first be enabled on your backup user account. Otherwise, just enabling this setting on the AhsayOBM will not activate this feature and can result in possible backup errors if the backup job encounters an open file. Please contact your backup service provider for more details.
2. Volume Shadow Copy does not support open file backups on network drives.

File Permissions

This option defines whether to back up operating system file permission of the data selected as backup source. This option is enabled by default.

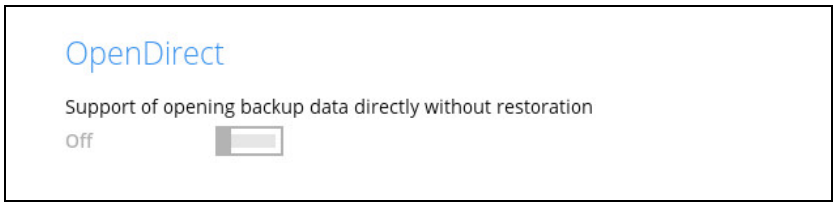


NOTE

Applicable for File Backup Sets only.

OpenDirect

This feature is used to add additional restore options in restoring files from a File Backup Set. This feature can only be enabled during the creation of backup set. For more details about OpenDirect Restore, please refer to Chapter 5 OpenDirect Restore.

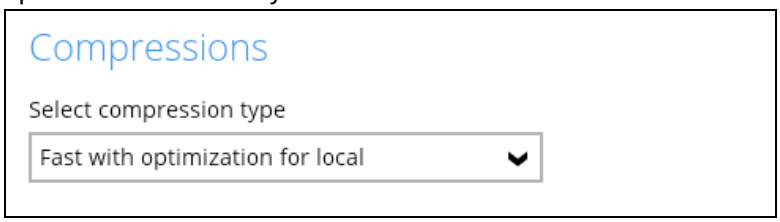


WARNING

1. To use this feature, the OpenDirect license module must first be enabled with the correct number of modules on your user account. If you enable this setting on the AhsayOBM without an OpenDirect license, or your account does not have enough OpenDirect licenses, then your backup job will not run. Please contact your backup service provider for more details.
2. When OpenDirect is enabled, to optimize restore performance, both compression and encryption will be disabled for this backup set. Therefore, it is not recommended to assign your backup destination on a cloud or on an offsite location.
3. Once the OpenDirect is enabled and the setting is saved, it cannot be disabled without re-creating the backup set.

Compressions

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



There are four (4) different data compression types:

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

NOTE

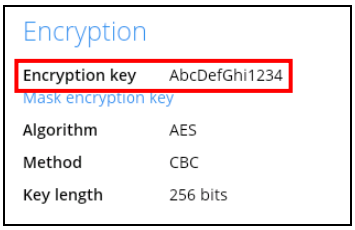
The compression type can be changed anytime even after a backup job. The modified compression type will be applied on the next run of a backup.

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, select 'Unmask encryption key' to display the encryption key of the backup set.

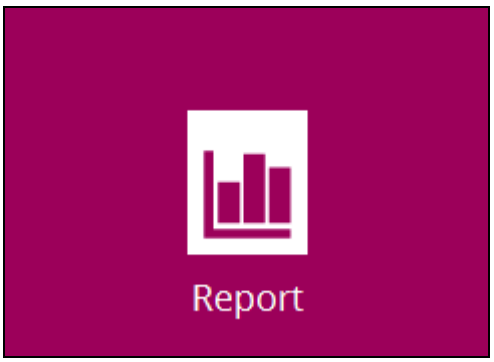


NOTE

For more details about encryption settings, please refer to step no. **13** in Chapter 11 Create a Backup Set.

10.6 Report

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



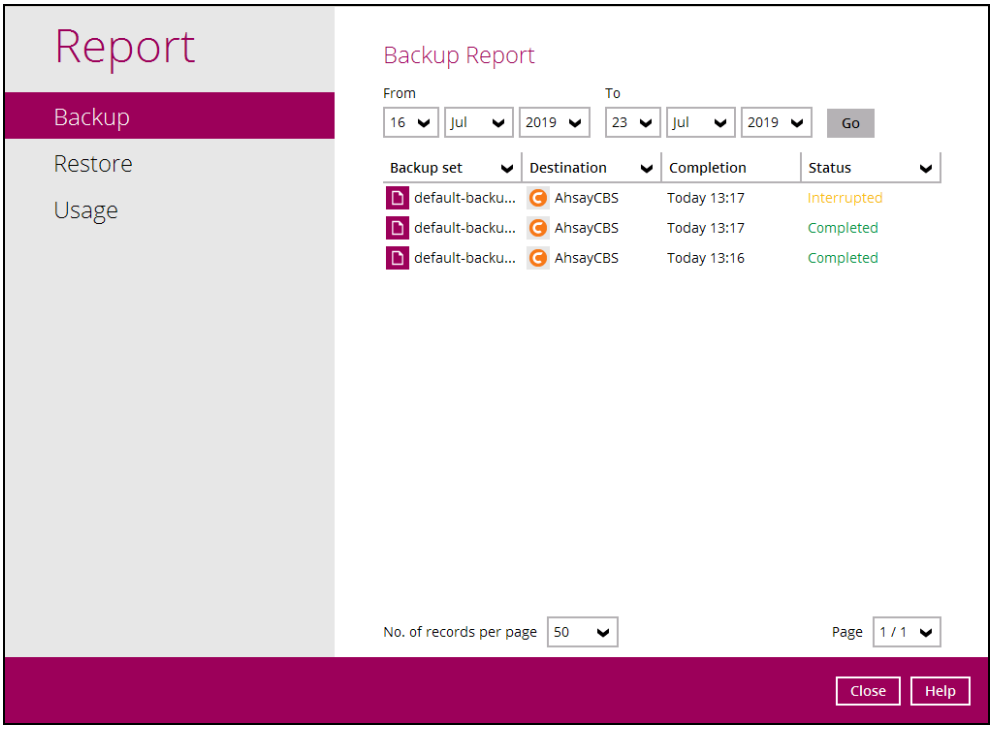
There are three (3) functions available for this feature:

- Backup
- Restore
- Usage

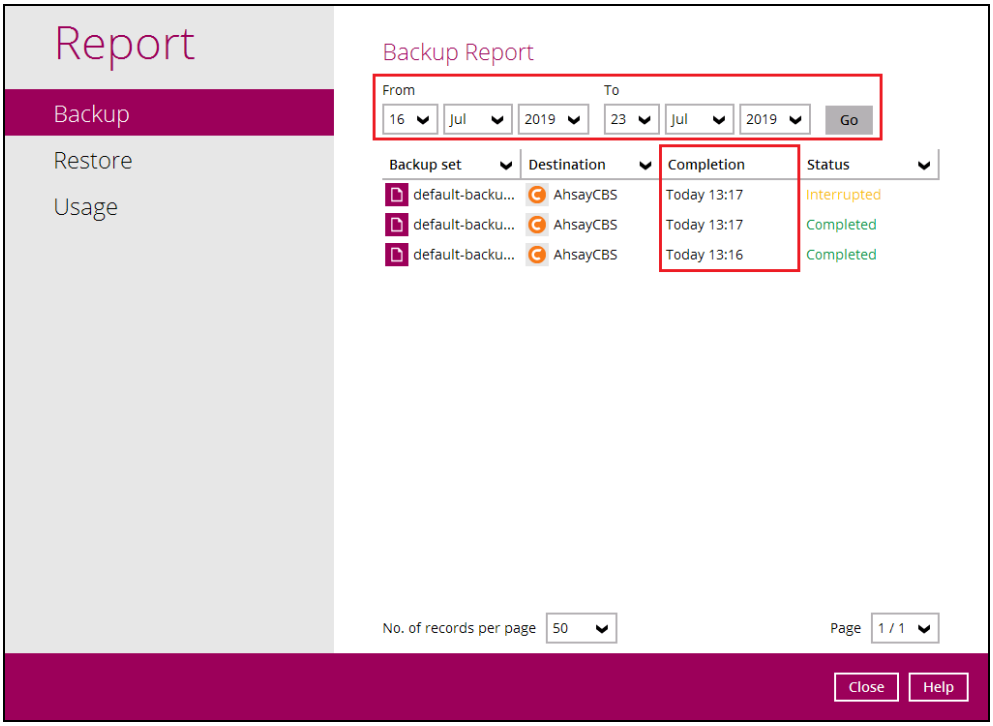
10.6.1 Backup

This shows the backup reports. There are four (4) filters that can be applied on this feature:

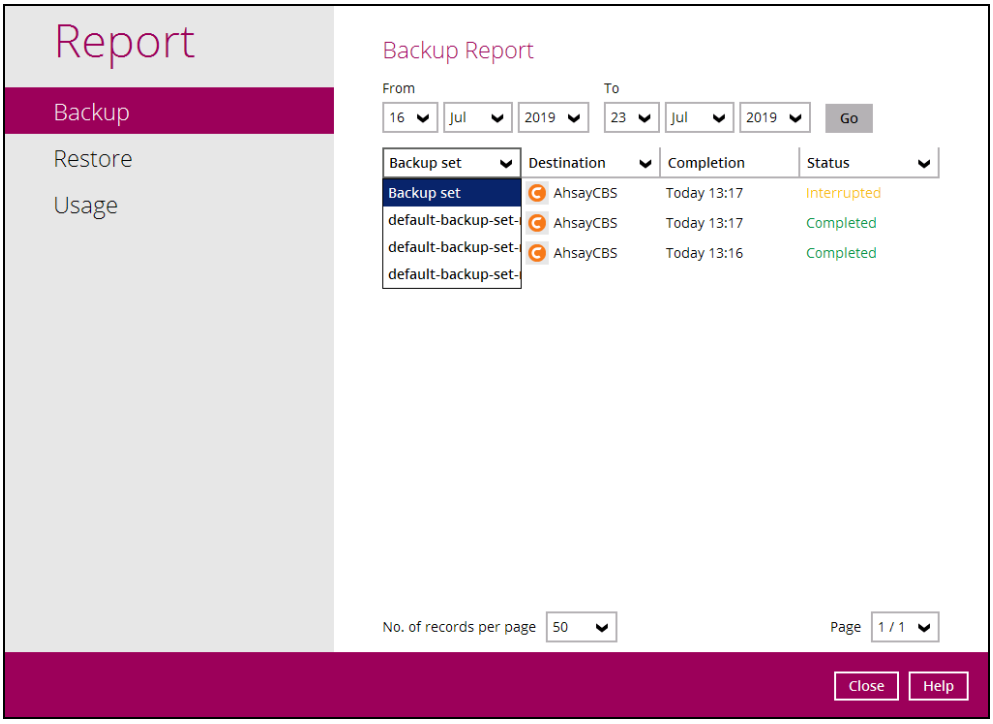
- Date
- Backup Set
- Destination
- Status



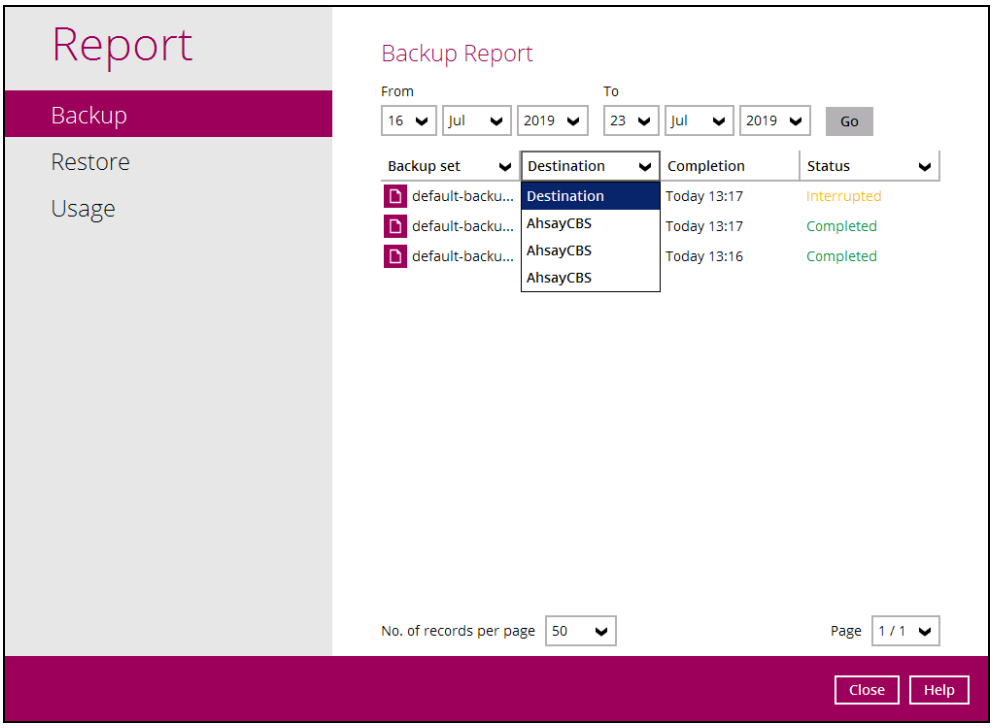
You can filter and view the backup report using the Date filter.



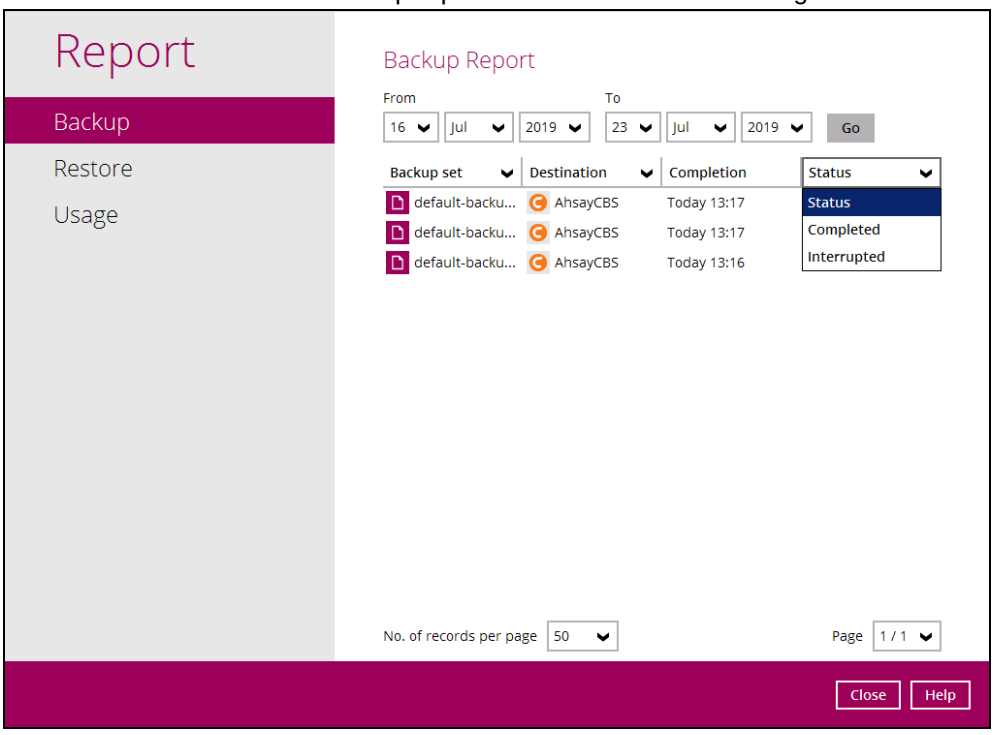
You can filter and view the backup report using the Backup set filter.



You can filter and view the backup report to your selected storage location using the Destination filter.

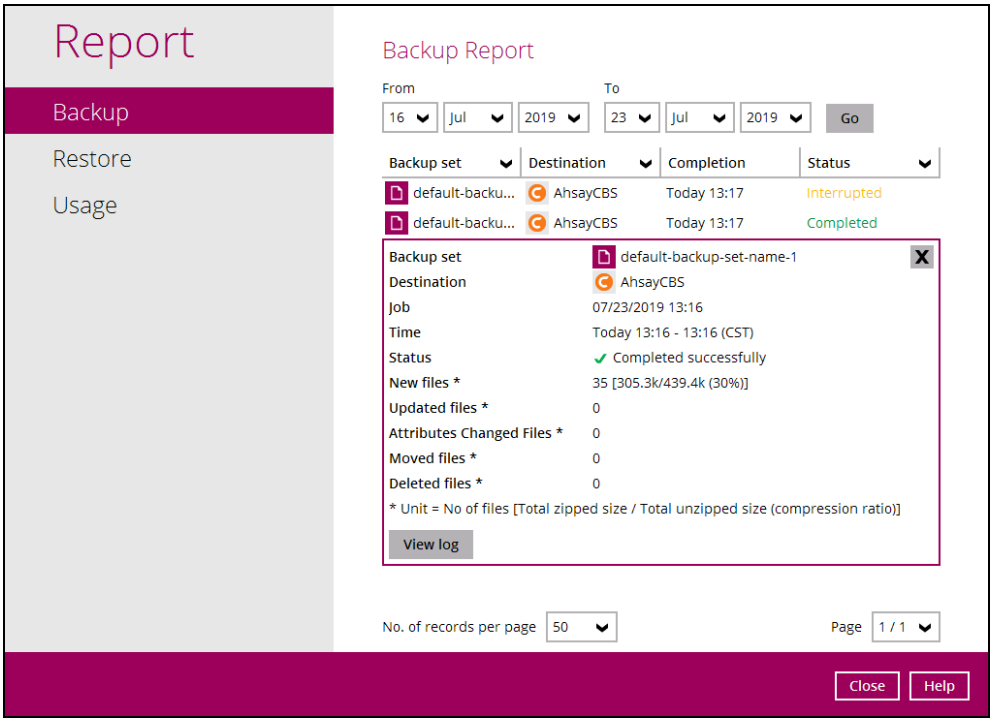


You can filter and view the backup report with the same status using the Status filter.

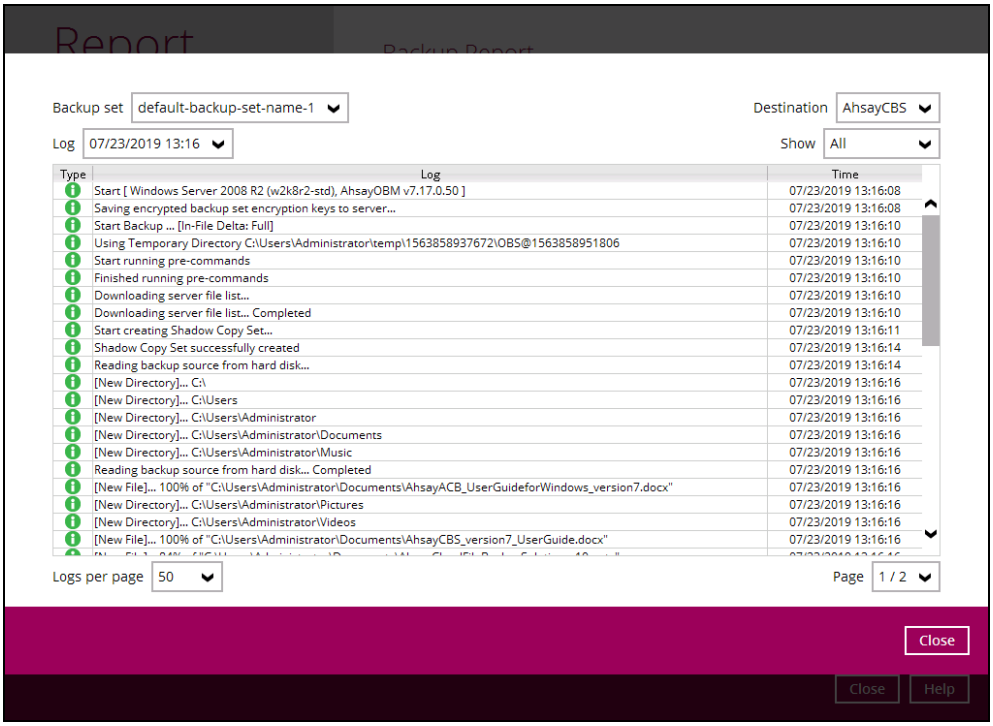


To view the backup log, follow the instructions below:

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



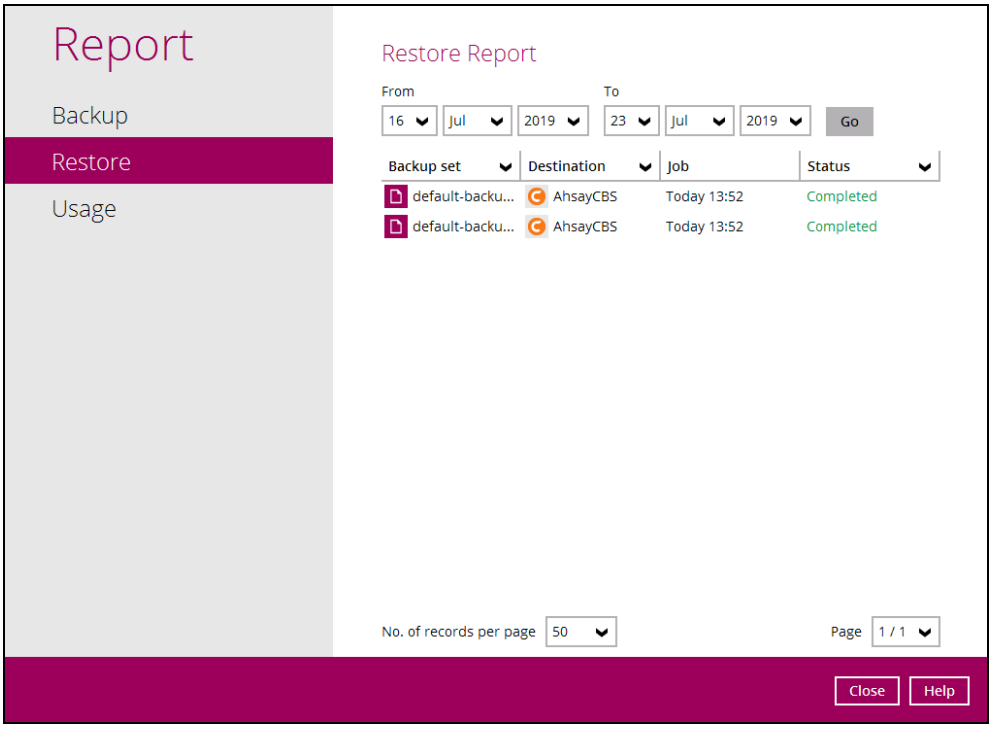
2. Backup set, Destination, Log Date and Time, and Status can also be filtered as well as the number of logs per page.



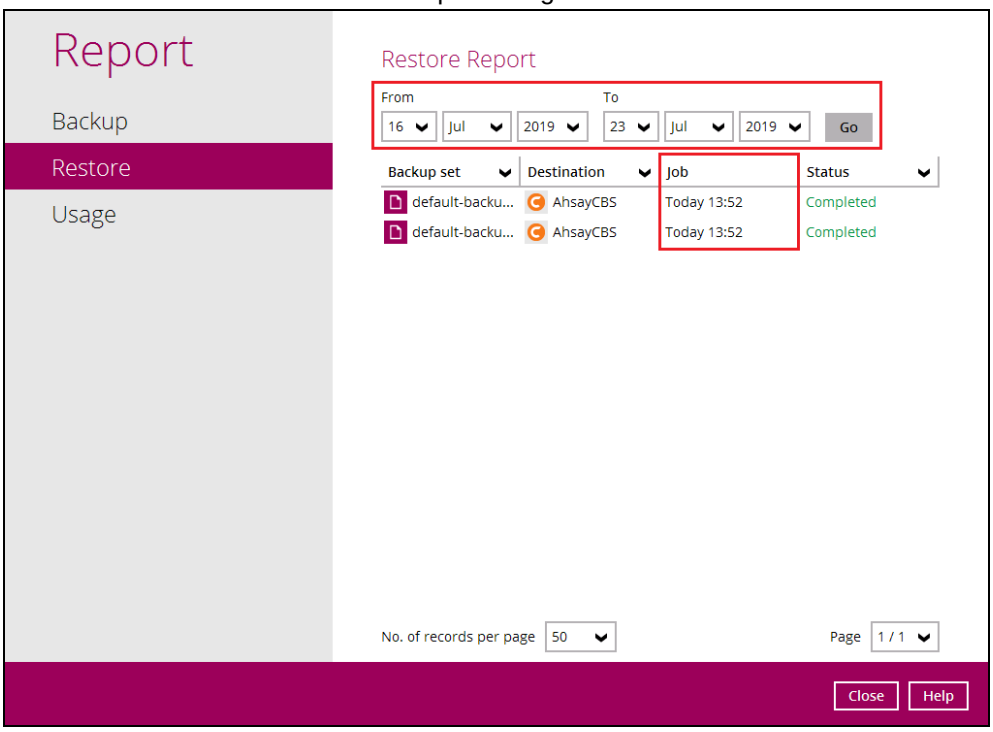
10.6.2 Restore

This shows the restore reports. There are four (4) filters that can be applied on this feature:

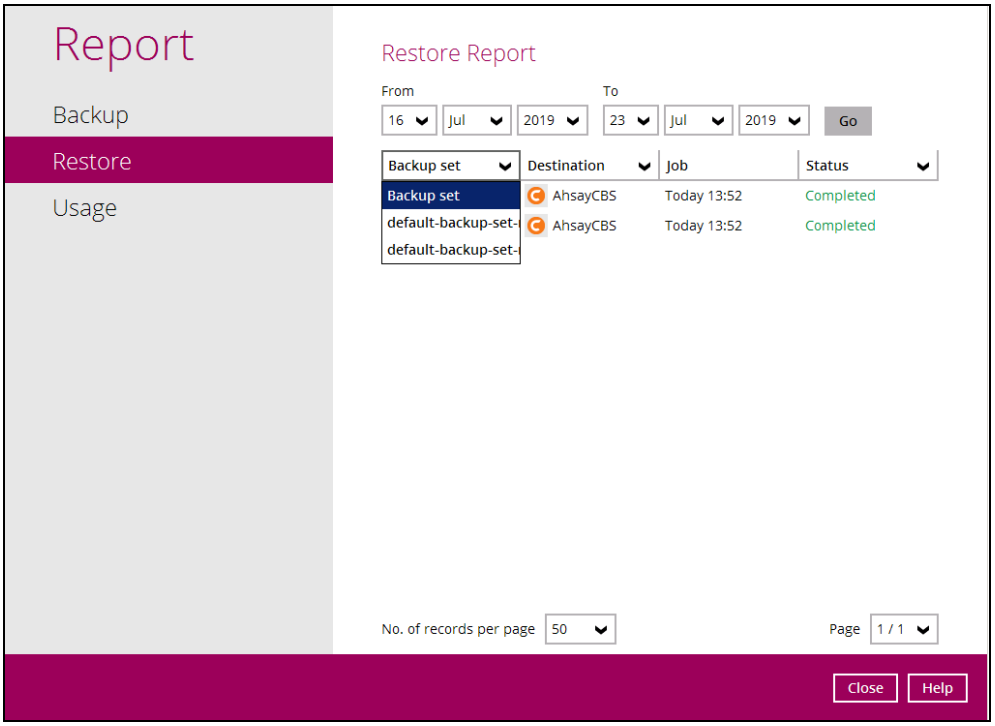
- Date
- Backup Set
- Destination
- Status



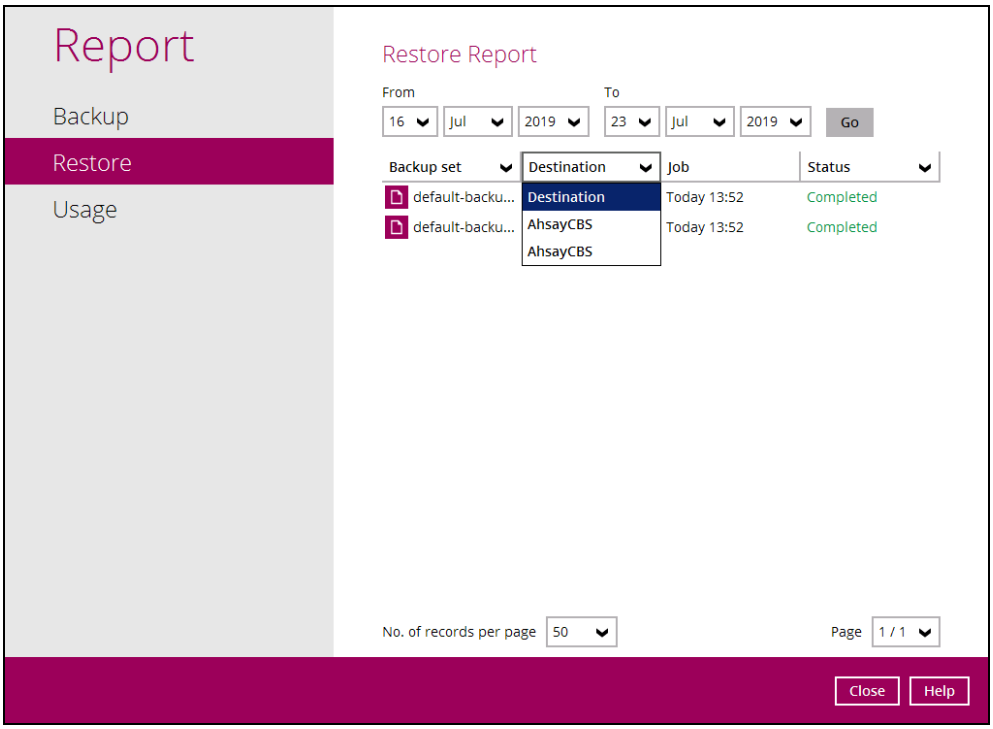
You can filter and view the restore report using the Date filter.



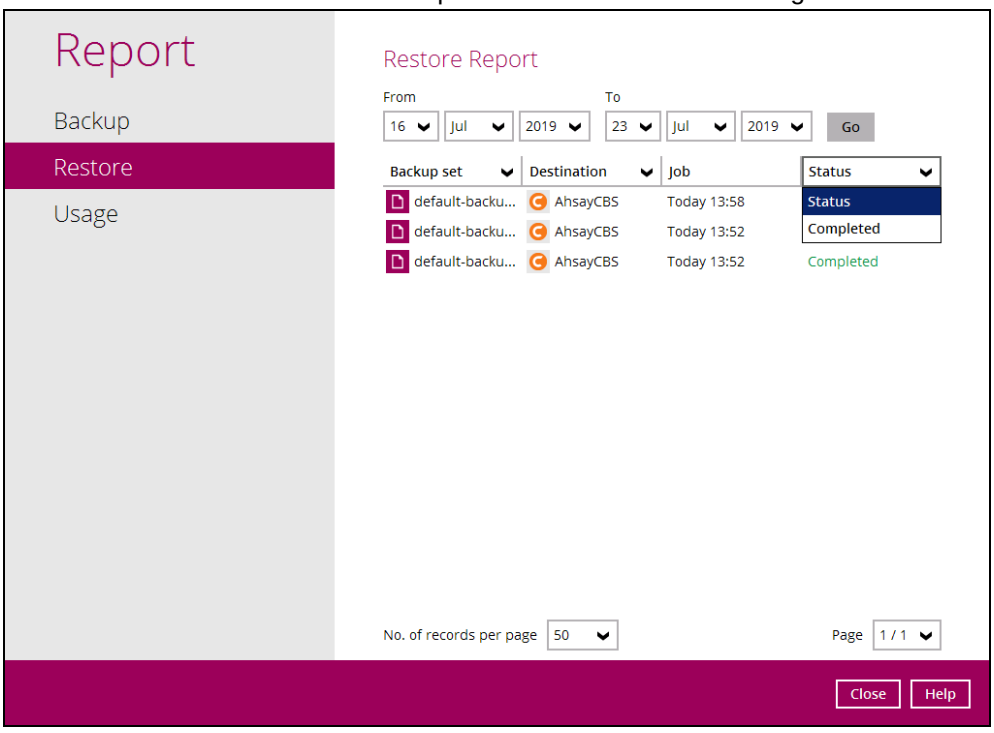
You can filter and view the restore report using the Backup set filter.



You can filter and view the restore report to your selected storage location using the Destination filter.

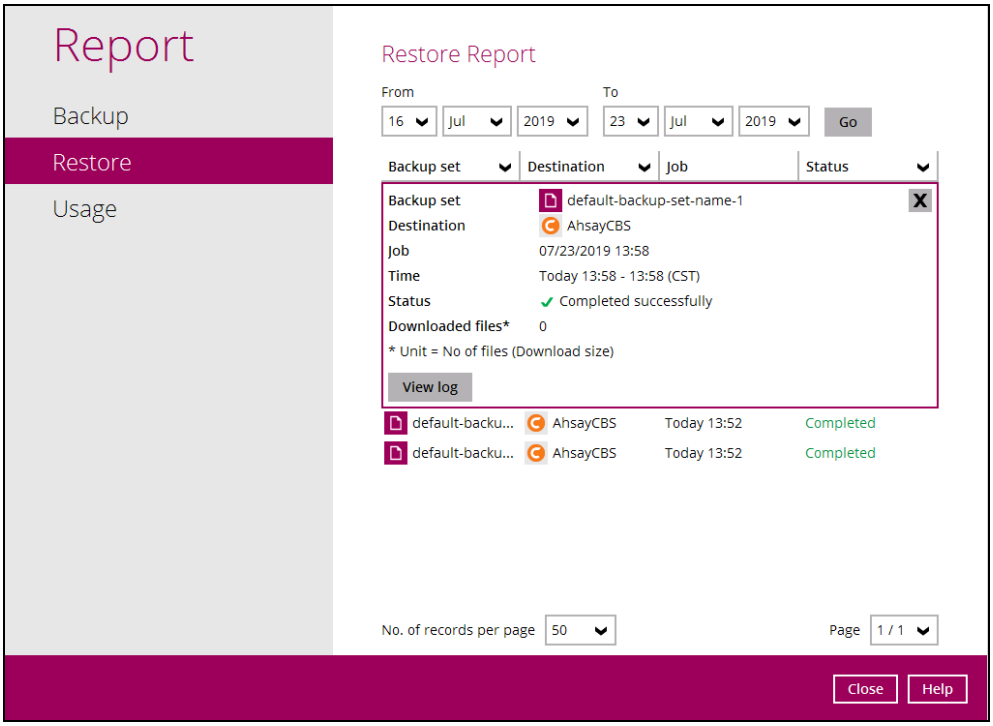


You can filter and view the restore report with the same status using the Status filter.

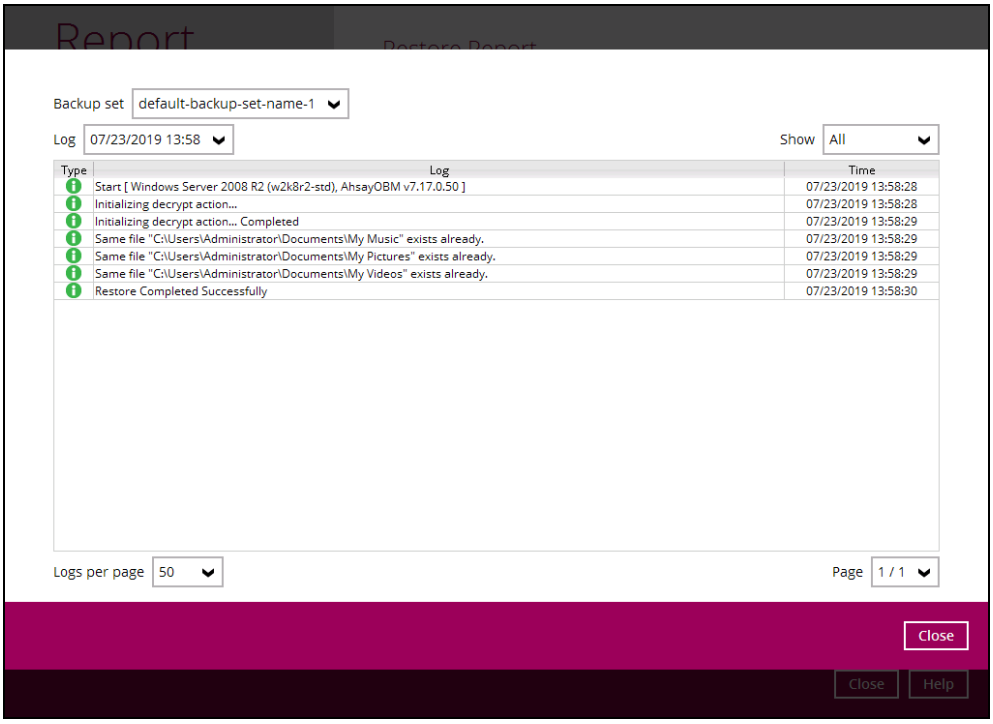


To view the restore log, follow the instructions below:

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

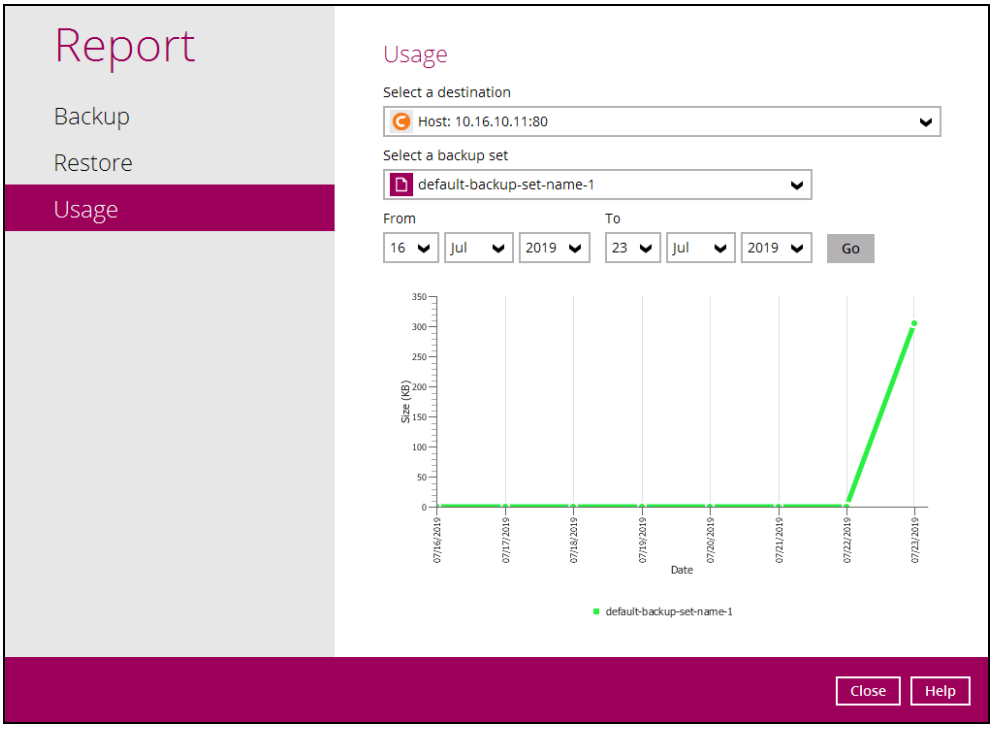


2. Backup set, Log Date and Time, and Status can also be filtered as well as the number of logs per page.



10.6.3 Usage

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



- Storage statistics

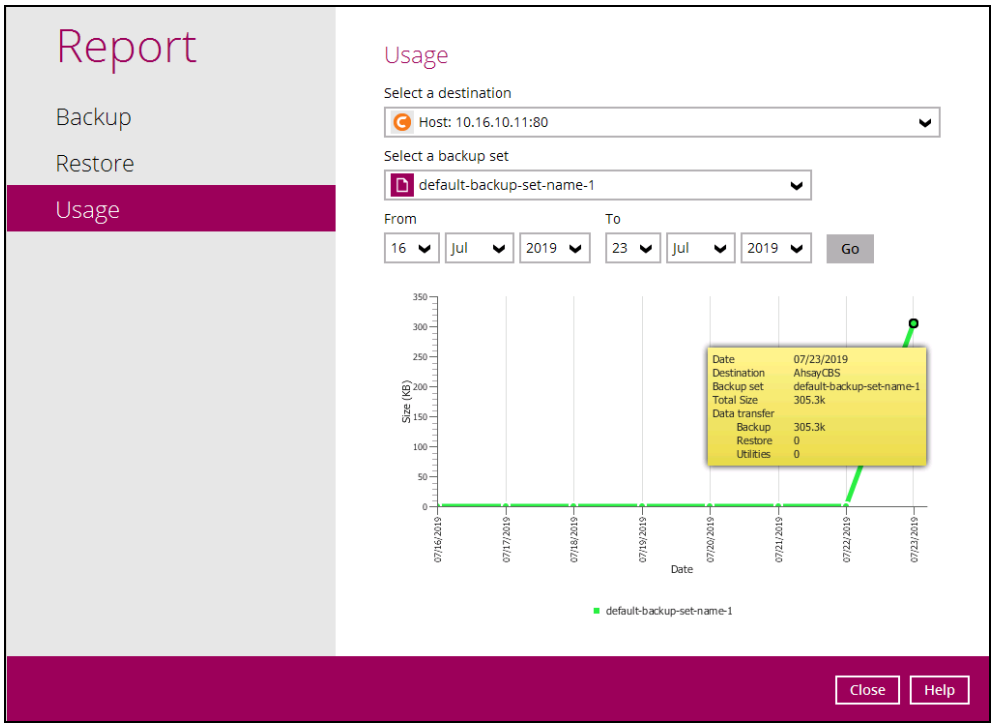
  Total Size: displays the total amount of backed up data on the backup destination

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

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

Example:

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



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

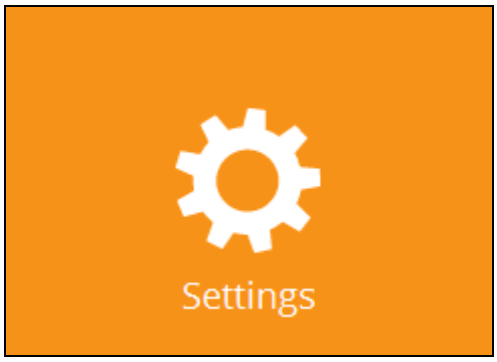
10.7 Restore

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 14 Restore Data.

10.8 Settings

This feature allows the user to enable the **Proxy Settings** and **Windows Event Log**.



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

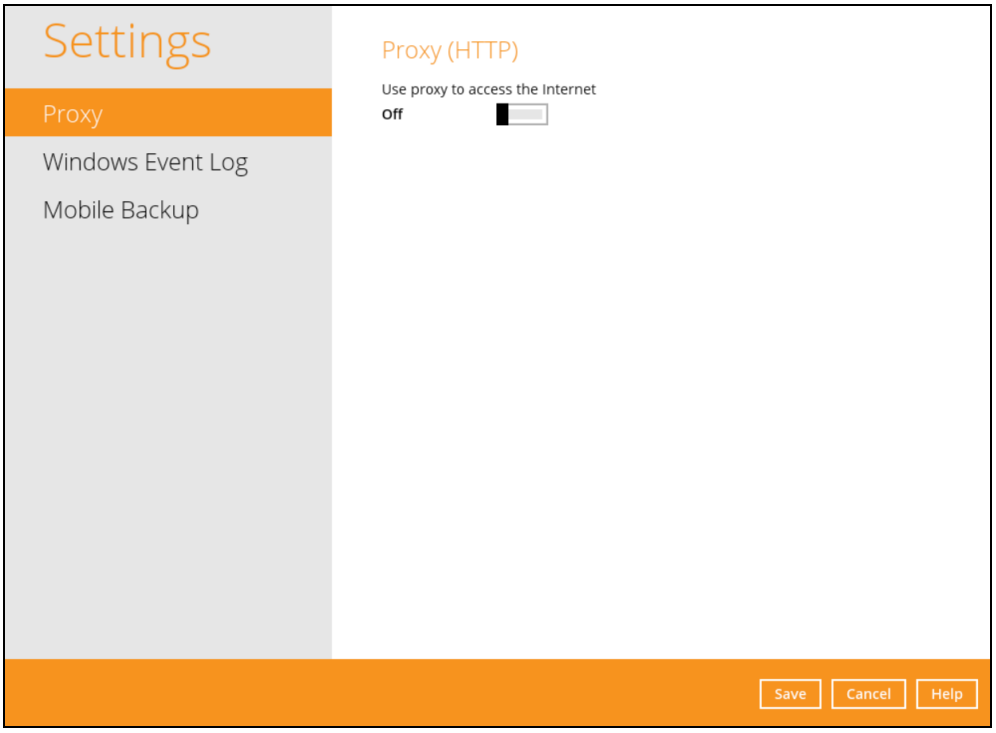
- Proxy
- Windows Event Log
- Mobile Backup

10.8.1 Proxy

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

To enable the Proxy Settings, follow the instructions below:

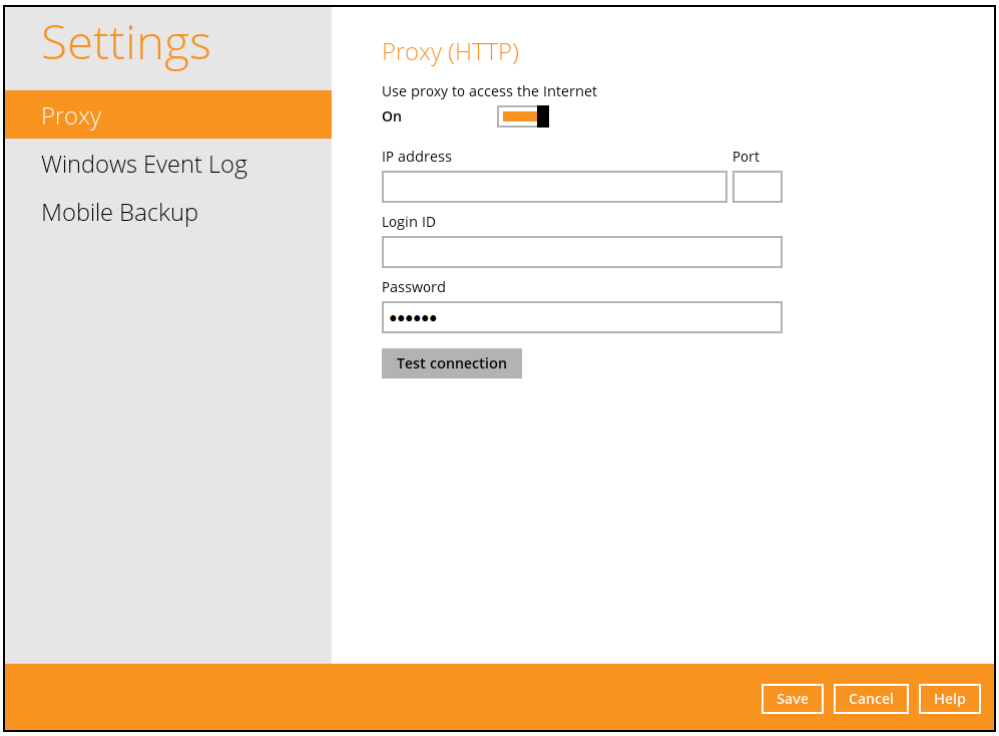
1. Slide the lever to the right to turn it on.



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

2. Complete the following fields:

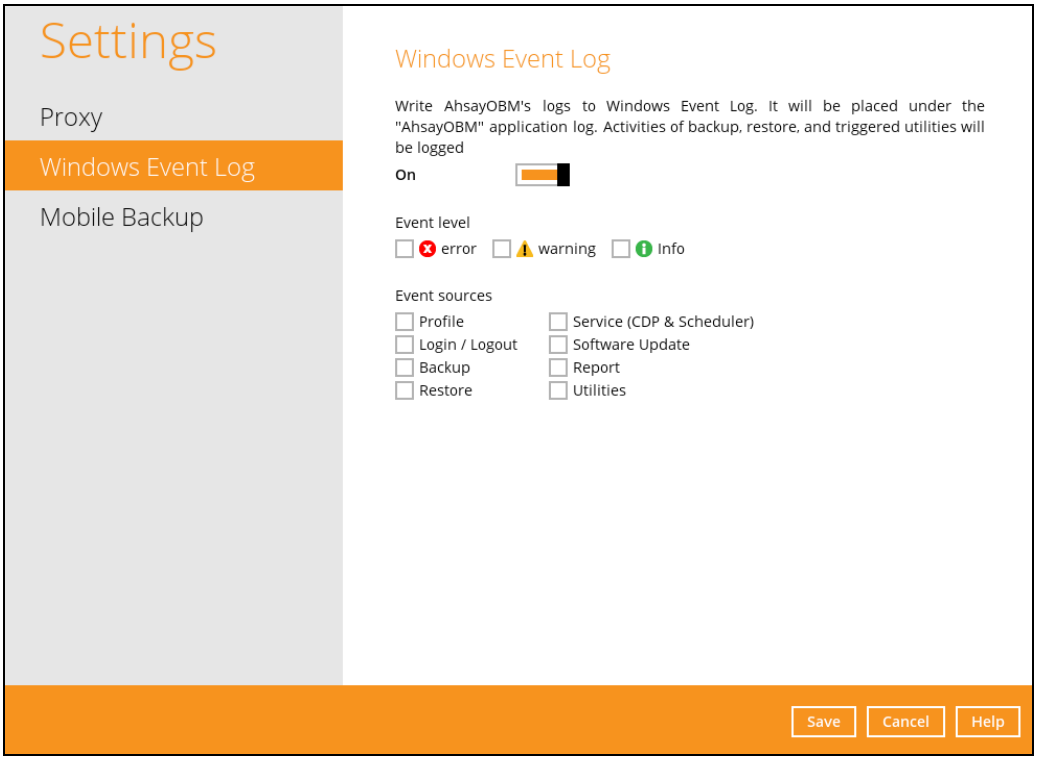
- IP address
- Port
- Login ID
- Password



3. Click the [Test Connection] button to validate the connection.
4. Click the [Save] button to store the settings.

10.8.2 Windows Event Log

When this feature is on, all AhsayOBM system log information will be written under **Applications and Services Logs**. User may access them through **Windows event viewer** in the local machine.



NOTE: This feature is only applicable for Windows OS.

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

10.8.3 Mobile Backup

Mobile Backup (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

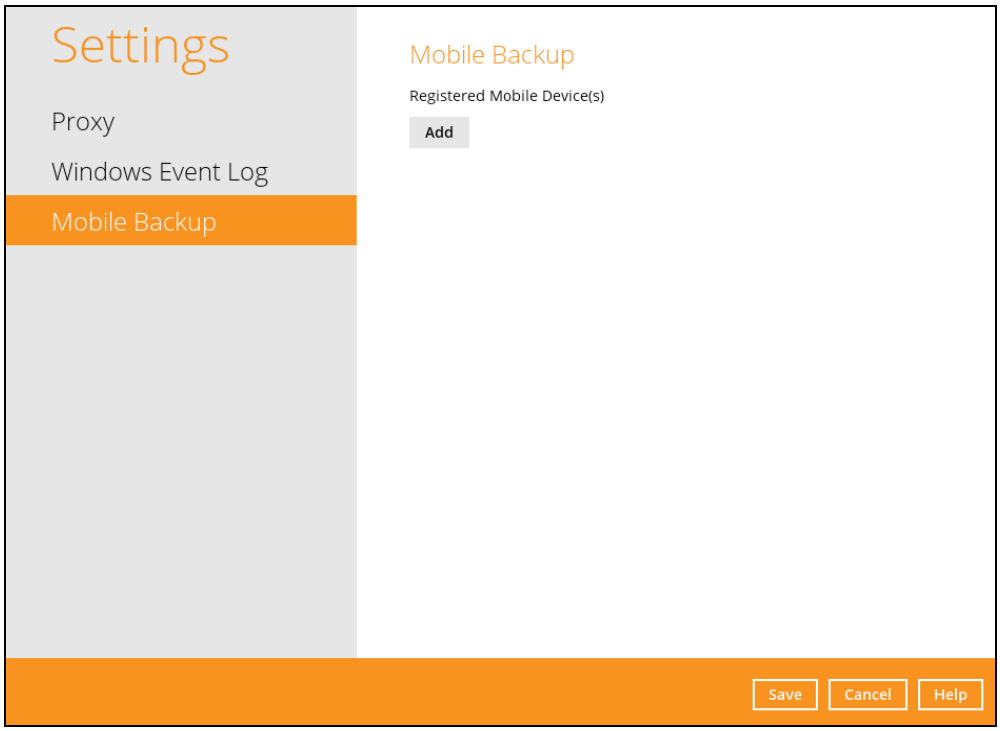
  Please refer to the **Ahsay Mobile App User Guide for Android and iOS – Chapter 7** for the detailed step-by-step procedure.

- View backed up photos and videos saved in the mobile backup destination.
- Change the mobile backup destination location 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 and 2FA accounts to an alternate mobile device, the other mobile devices must be registered first for mobile backup on AhsayOBM.

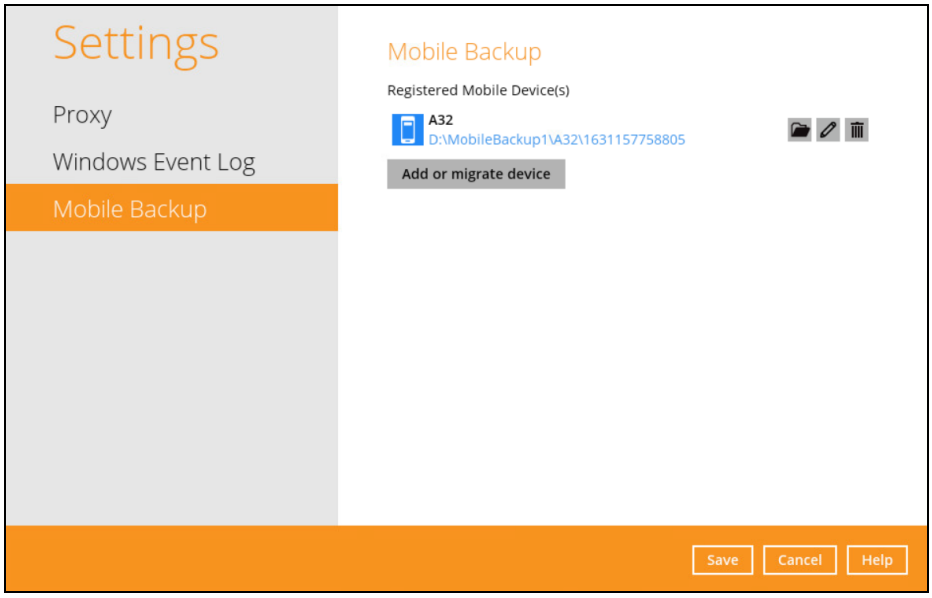
- Restore to a different mobile device on the same operating system.
- Restore to a different mobile device on another operating system, i.e., Android to iOS or iOS to Android.



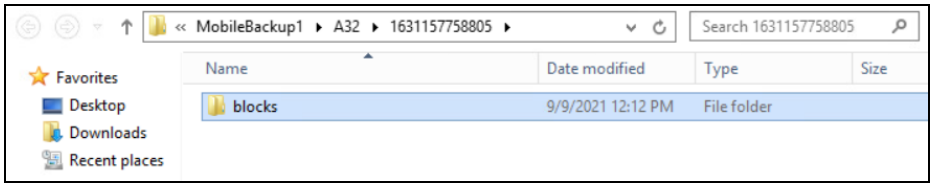
View backed up photos and videos saved in the mobile backup destination

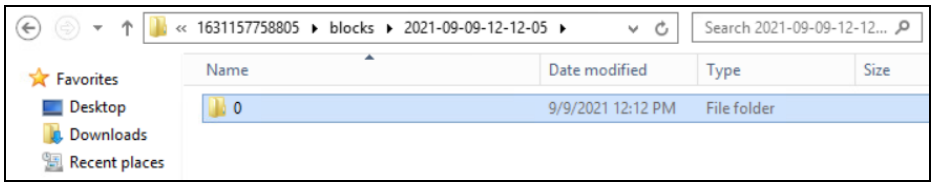
To view backed up photos and videos saved in the mobile backup destination, follow the instructions below:

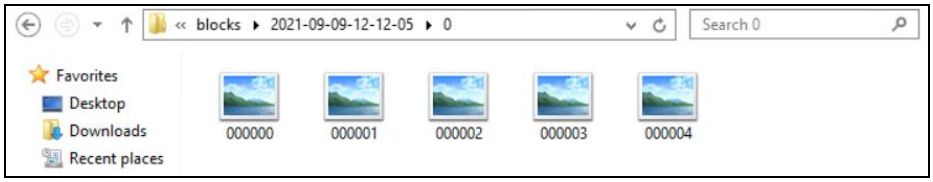
1. Either click the link under the registered mobile device or click the **Browse** icon on the right side of the registered mobile device.



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 and 2FA accounts to the new location to prevent missing data. As some of the backed-up photos, videos 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 and 2FA accounts again from the mobile device, this will not include the photos, videos 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 and 2FA accounts to the new location or continue to back up in the new location.

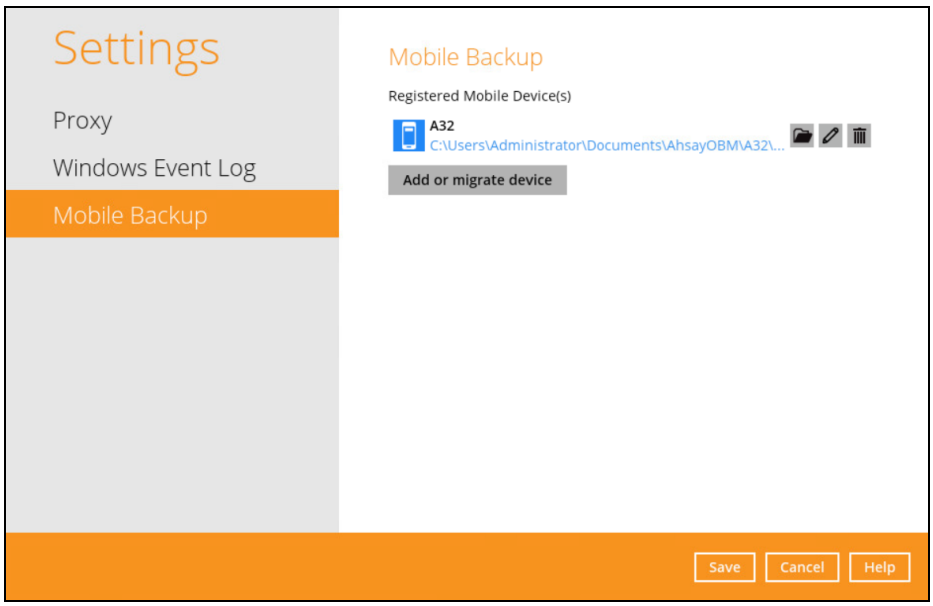
In case the previously backed-up photos, videos and 2FA accounts were not copied to the new location, the backup will re-upload all the photos, videos and 2FA accounts again from the mobile device.

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

Example: Change backup destination from **C:\Users\Administrator\Documents\AhsayOBM\%registered_mobile_device%\%backupsetID%** to **D:\MobileBackup1**

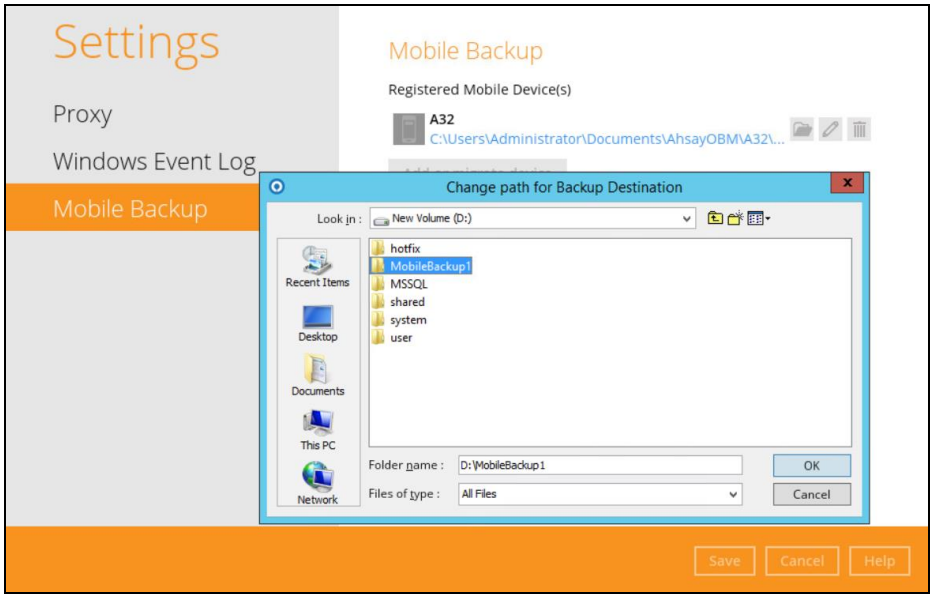
1. From the old location, secure a copy of the previously backed-up photos, videos and 2FA accounts.
2. Copy the previously backed-up photos, videos and 2FA accounts from the original location to the new mobile backup destination (if applicable).
3. Go to **Settings** > **Mobile Backup**. Click the **Edit** icon on the right side of the registered mobile device.

In this example, the old mobile backup destination is **C:\Users\Administrator\Documents\AhsayOBM\%registered_mobile_device%\%backupsetID%.**



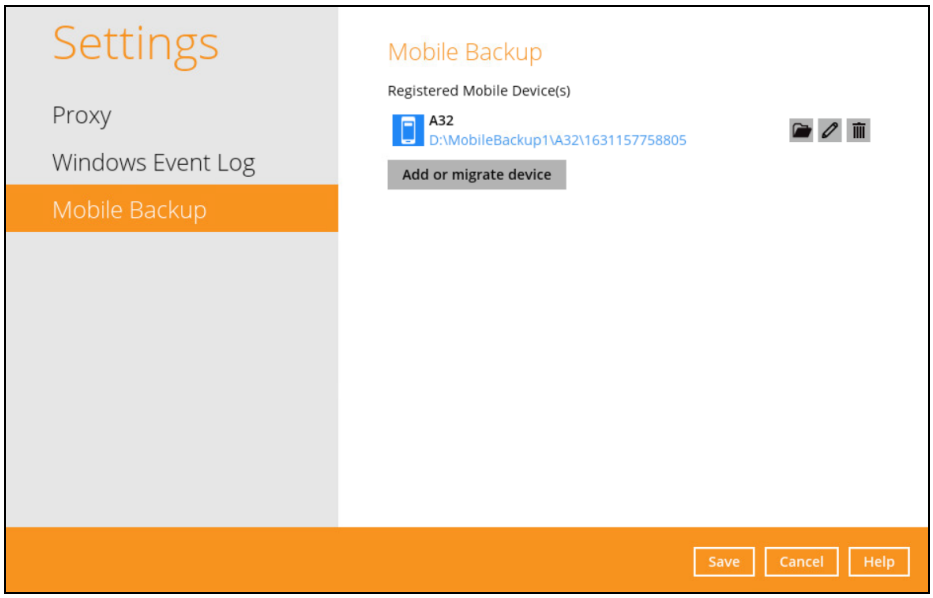
4. **Change path for Backup Destination** screen will be displayed. Select a new mobile backup destination then click **OK**.

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



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

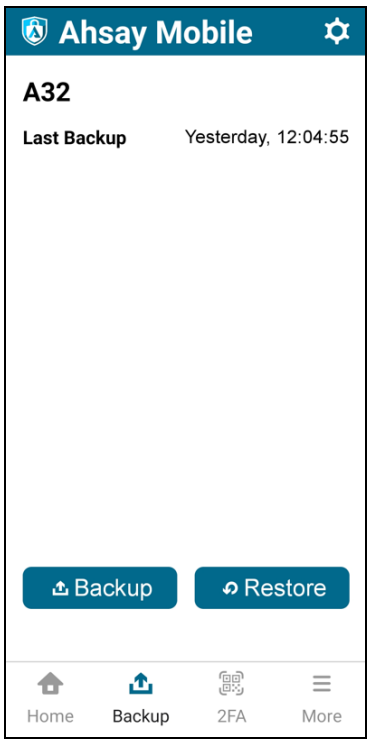
   Mobile backup destination is successfully changed to **D:\MobileBackup1**. All mobile backups will now be saved to this destination.



NOTE

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

6. Resume backup of photos and videos.



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 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 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 and 2FA accounts to the new machine otherwise the photos, videos and 2FA accounts on the mobile device will be backed-up again from scratch.

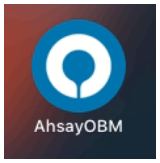
NOTE

- 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 photos, videos and 2FA accounts again.
- Changing the mobile backup destination to a new machine with a different operating system is supported, e.g. from a Windows machine to macOS machine or macOS machine to Windows machine etc.

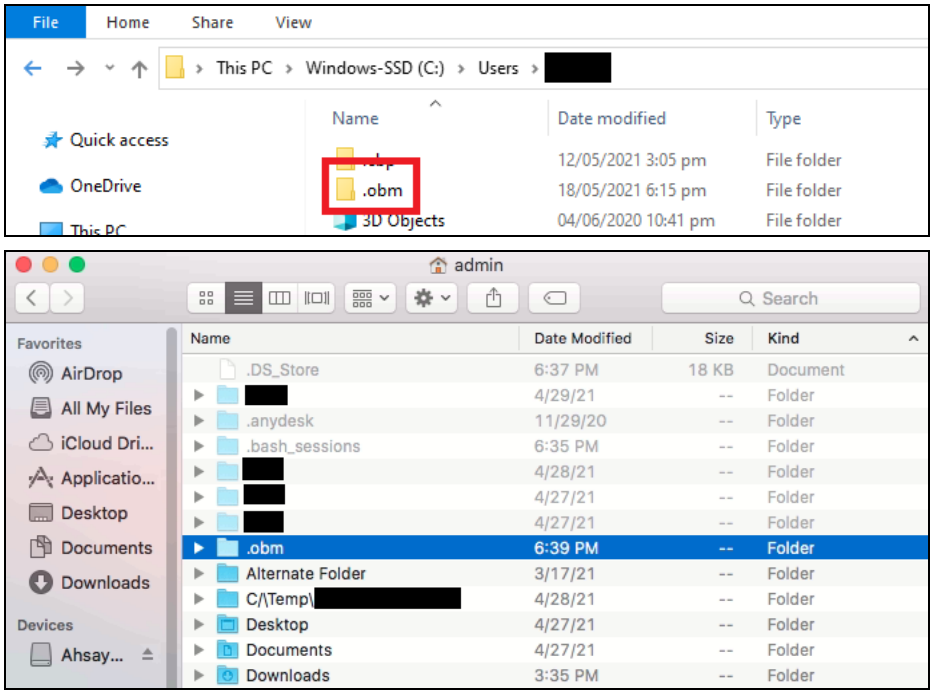
To change the mobile backup destination to a new machine, follow the instructions below:

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

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



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



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

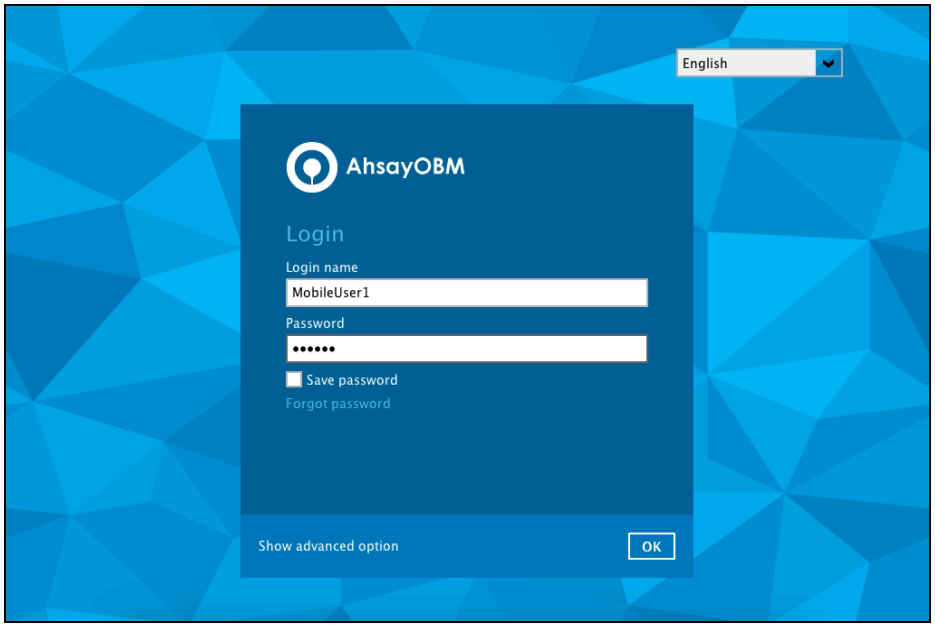
NOTE

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.

```
#cd /Applications/AhsayOBM.app/bin
#sh StopScheduler.sh
#sh Scheduler.sh
```

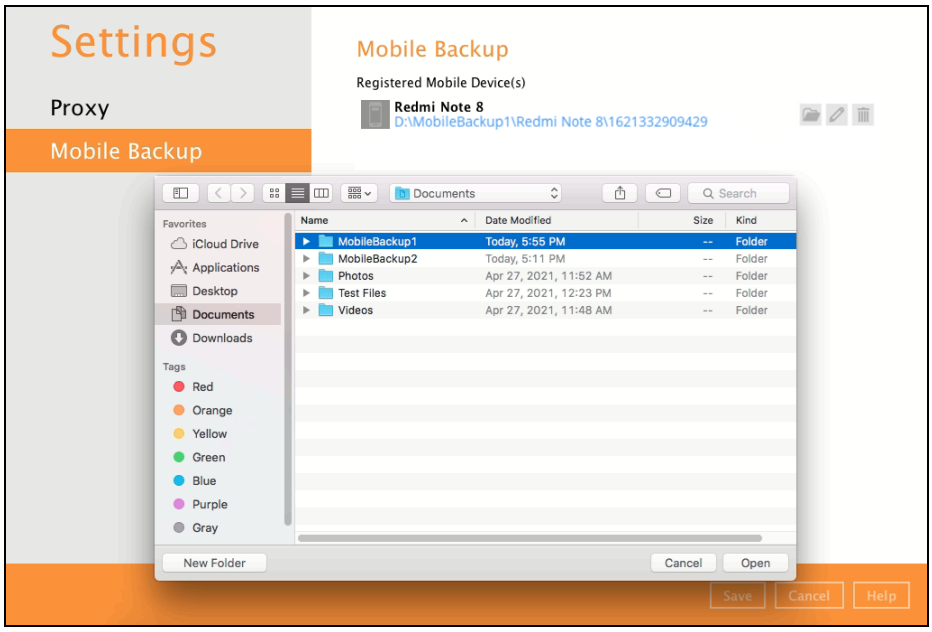
5. Login to **AhsayOBM**. Enter the login name and password of your AhsayOBM account. Then, click **OK** to log in



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

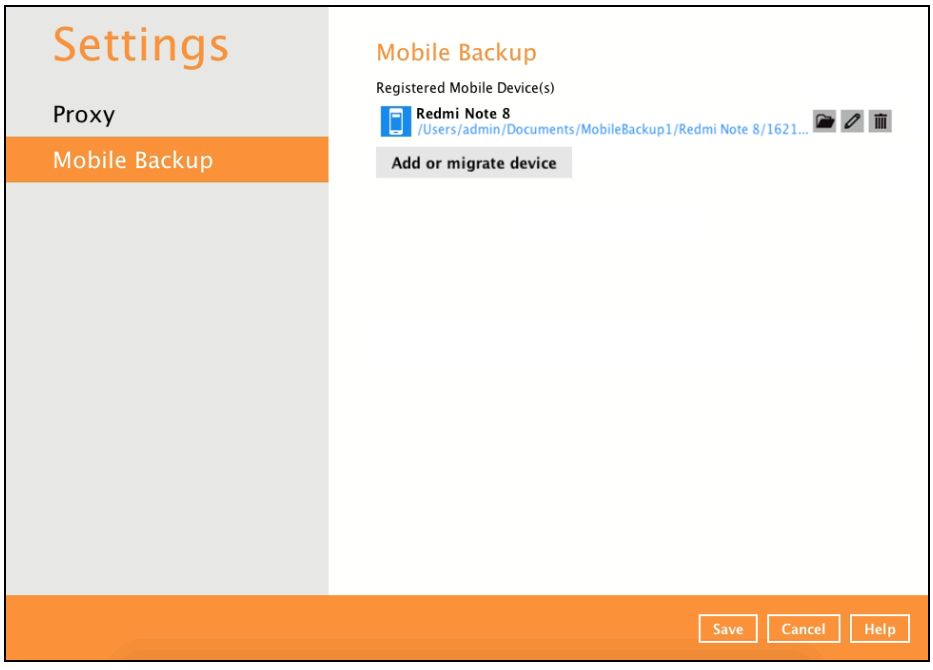
7. A new screen will be displayed, select the new mobile backup destination then click **Open**.

   In this example, the new mobile backup destination will be **/Users/admin/Documents/MobileBackup1**.



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

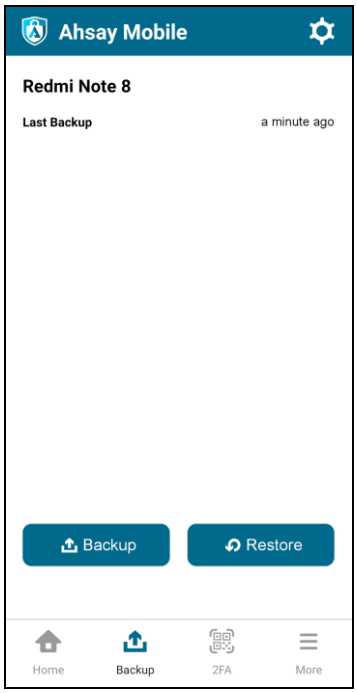
   Mobile backup destination is successfully changed to **/Users/admin/Documents/MobileBackup1**. All mobile backups will now be saved to this destination.



NOTE

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

9. Resume backup of photos and videos.



NOTE

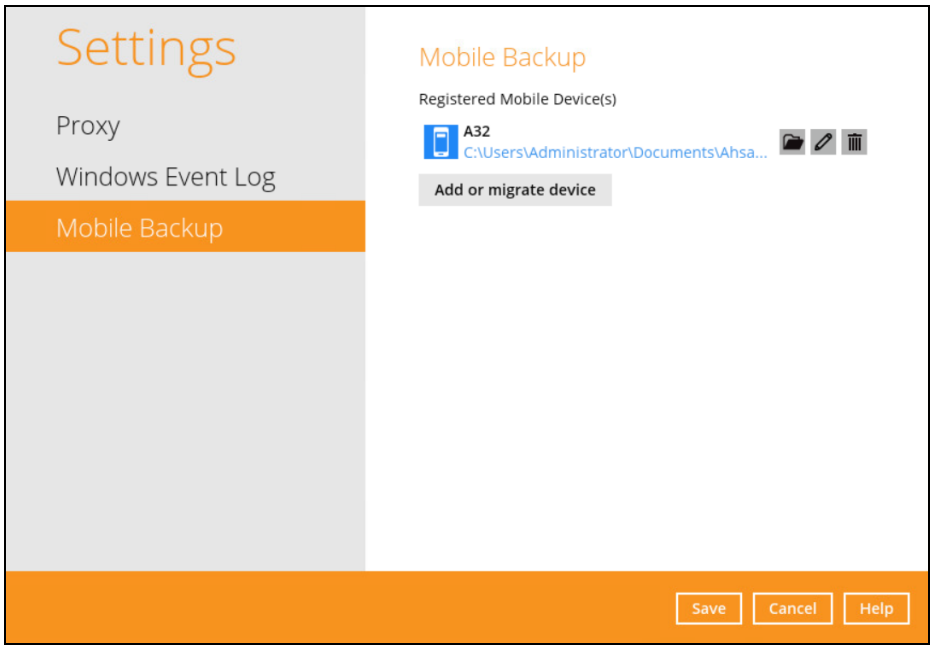
For instructions on changing the mobile backup destination of:

- a macOS machine to a Windows machine please refer to Ch.9.8.2 of the AhsayOBM v8 Quick Start Guide for Mac.
- a Linux machine to a Windows machine please refer to Ch. 9.8.2 of the AhsayOBM v8 Quick Start Guide for Linux (GUI).

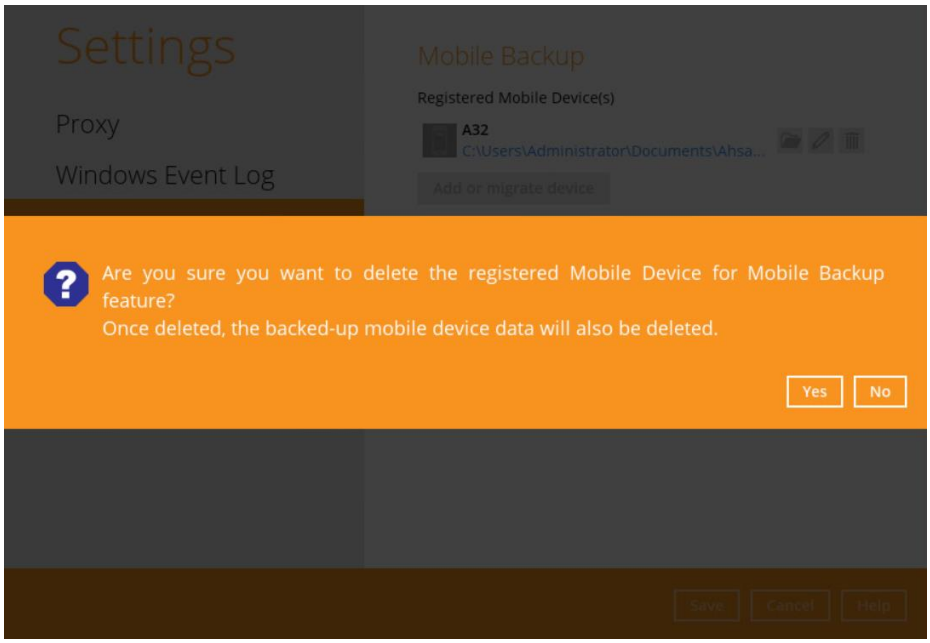
Remove one or more device(s) registered for Mobile Backup

To remove a mobile device, follow the instructions below:

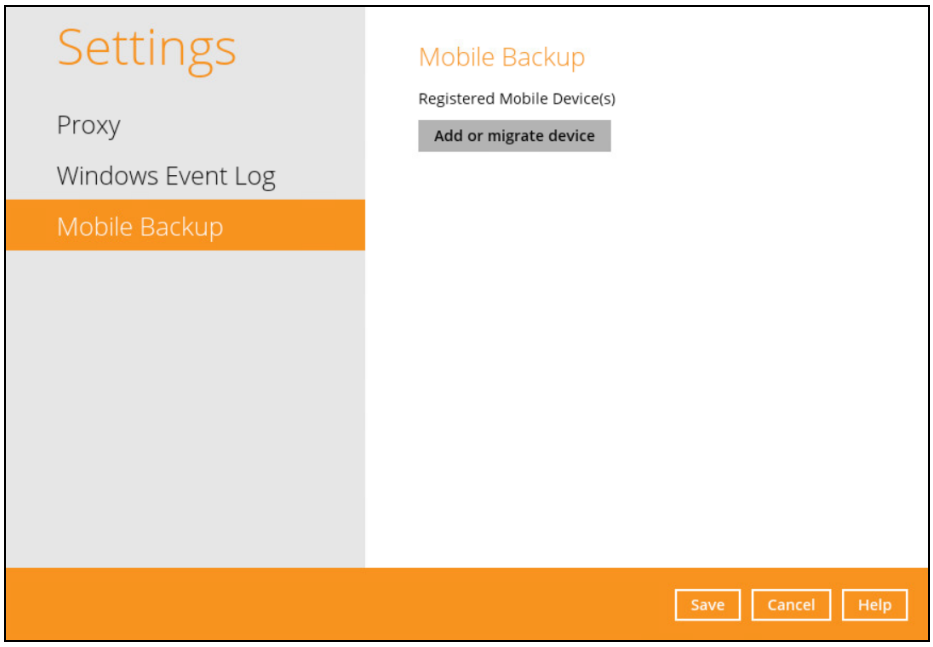
1. Click the **Delete** icon on the right side of the registered mobile device.



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

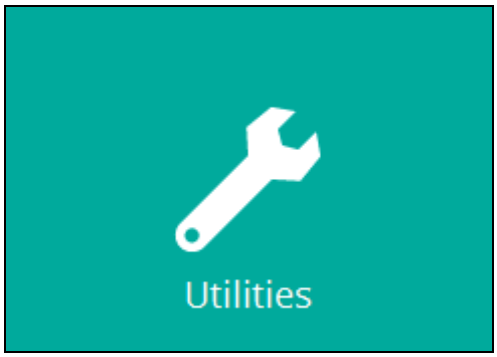


3. Mobile device is successfully removed along with any photos, videos and 2FA accounts backed up in the mobile backup destination.



10.9 Utilities

This allows the 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

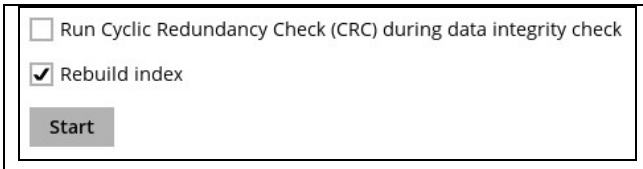
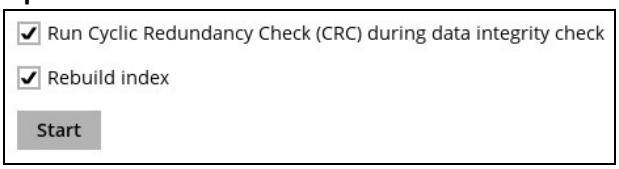
10.9.1 Data Integrity Check

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

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

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

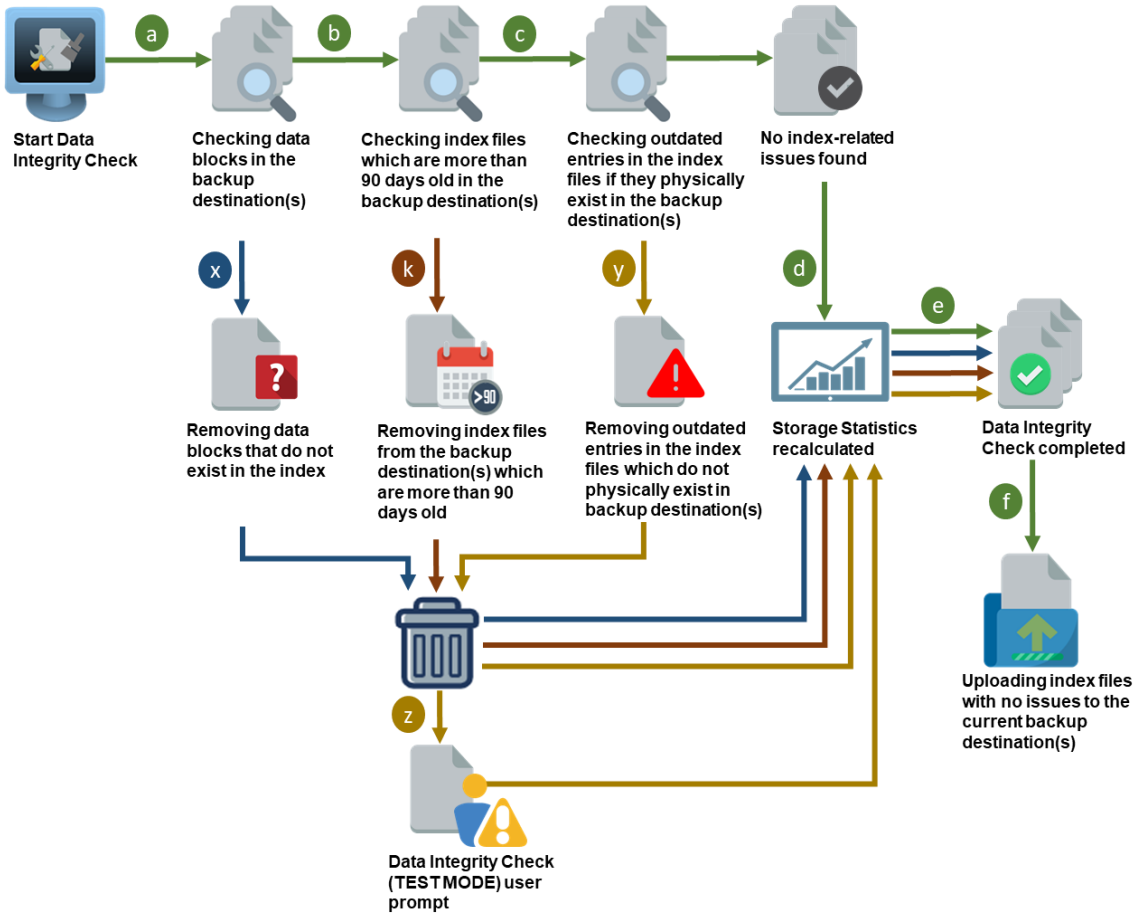
Option 1 ☐ Run Cyclic Redundancy Check (CRC) during data integrity check ☐ Rebuild index Start	For checking of index and data.
Option 2 ☑ Run Cyclic Redundancy Check (CRC) during data integrity check ☐ Rebuild index Start	For checking of index and integrity of files against the checksum file generated at the time of the backup job.
Option 3	For checking and rebuilding of index.

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

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

- **Option 1**
  Disabled Run Cyclic Redundancy Check (CRC) and Rebuild index - **(Default mode)**
- **Option 2**
  Enabled Run Cyclic Redundancy Check (CRC) and **Disabled** Rebuild index
- **Option 3**
  Disabled Run Cyclic Redundancy Check (CRC) and **Enabled** Rebuild index
- **Option 4**
  Enabled Run Cyclic Redundancy Check (CRC) and Rebuild index

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



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

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

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

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

e Data integrity check is completed.

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

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

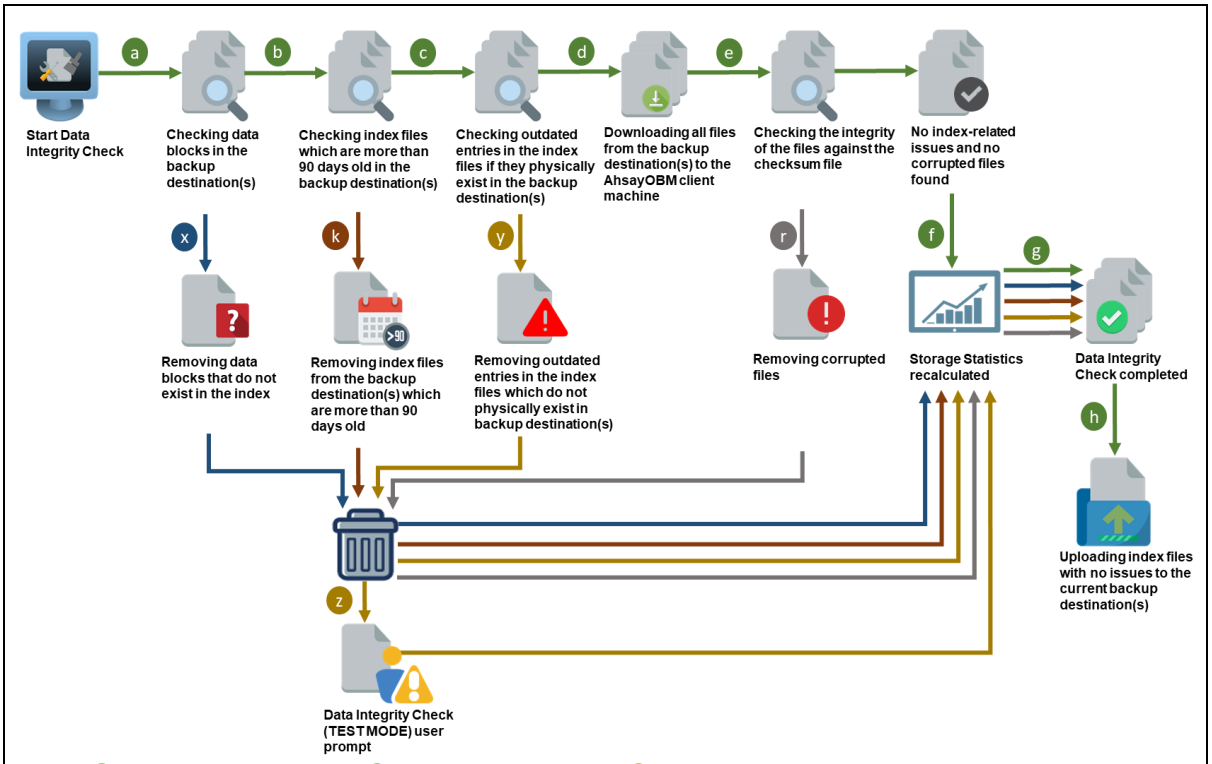
k Index files which are more than 90 days old will be removed from the backup destination(s).

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

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

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

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



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

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

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

d For **Run on Client (agent-based)** backup sets, files in the backup set are downloaded from the backup destination(s) to the AhsayOBM client machine.

For **Run on Server (agentless)** backup sets, proceed to e

e Check the integrity of files in the backup destination(s) against the checksum file generated at the time of the backup job.
- If any discrepancy is **FOUND**, proceed to r
- If **NO** discrepancy is found, proceed to f

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

g Data integrity check is completed.

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

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

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

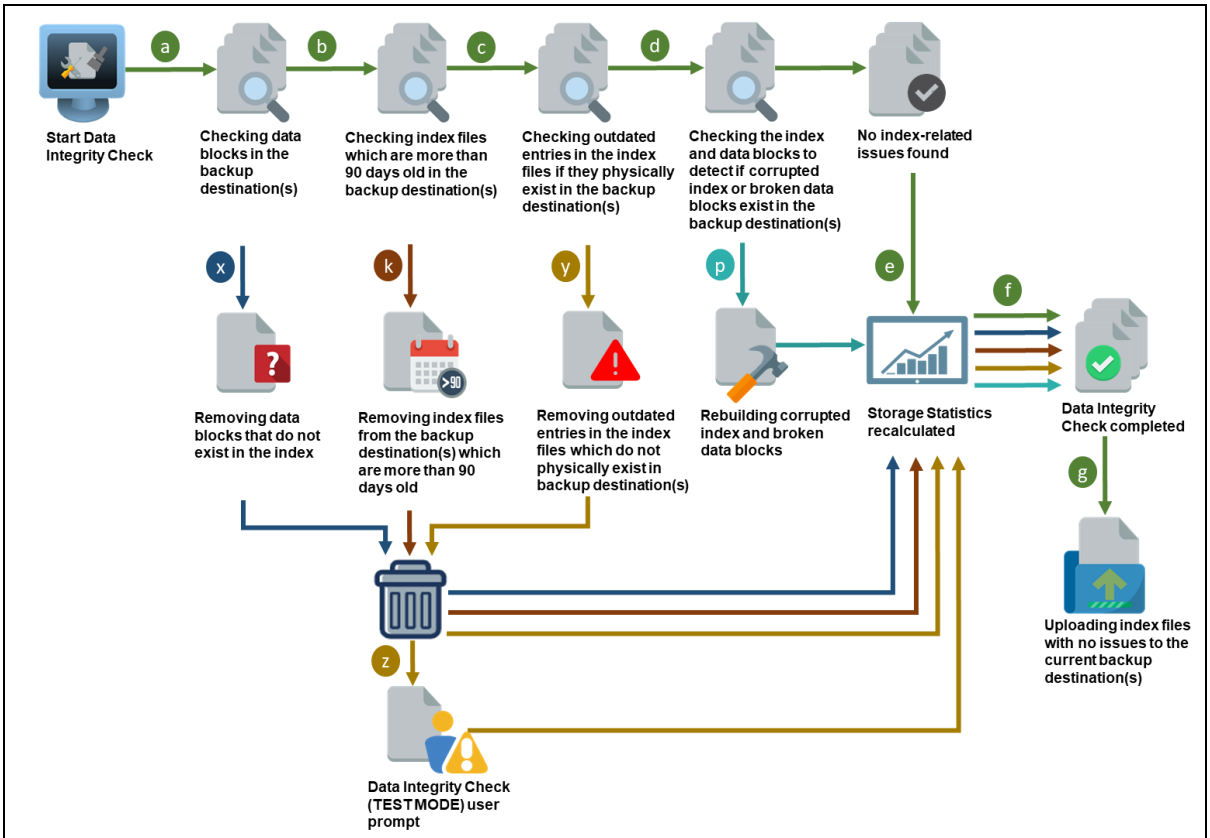
y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.
- If the backup data matches either of the criteria, proceed to z
- If **NOT**, proceed to d

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

r Corrupted files will be automatically removed from the backup destination(s).

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

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



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

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

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

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

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

f Data integrity check is completed.

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

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

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

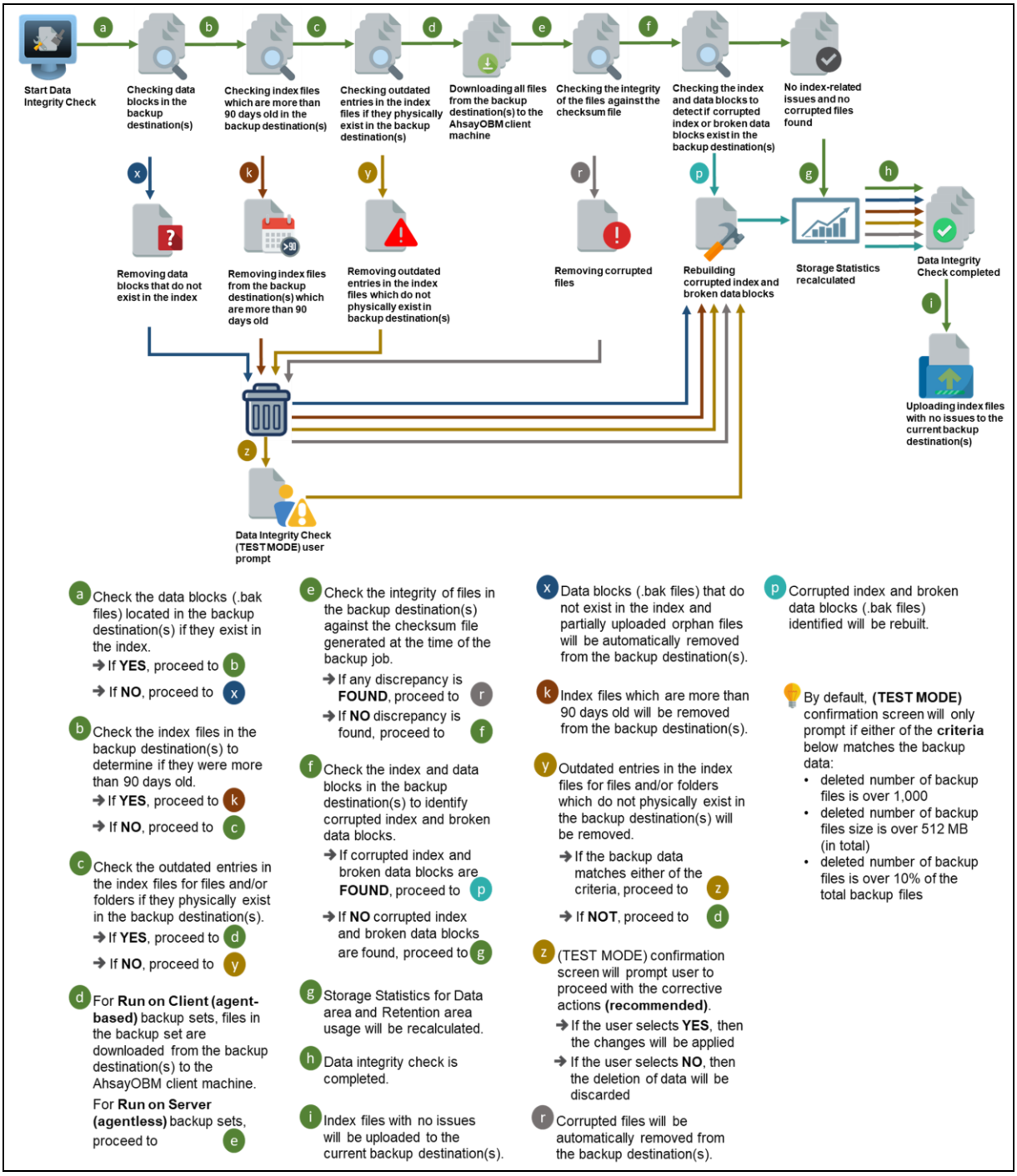
y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.
- ➔ If the backup data matches either of the criteria, proceed to z
- ➔ If **NOT**, proceed to d

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

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

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

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



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

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

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

d For **Run on Client (agent-based)** backup sets, files in the backup set are downloaded from the backup destination(s) to the AhsayOBM client machine.
For **Run on Server (agentless)** backup sets, proceed to e

e Check the integrity of files in the backup destination(s) against the checksum file generated at the time of the backup job.
→ If any discrepancy is **FOUND**, proceed to r
→ If **NO** discrepancy is found, proceed to f

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

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

h Data integrity check is completed.

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

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

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

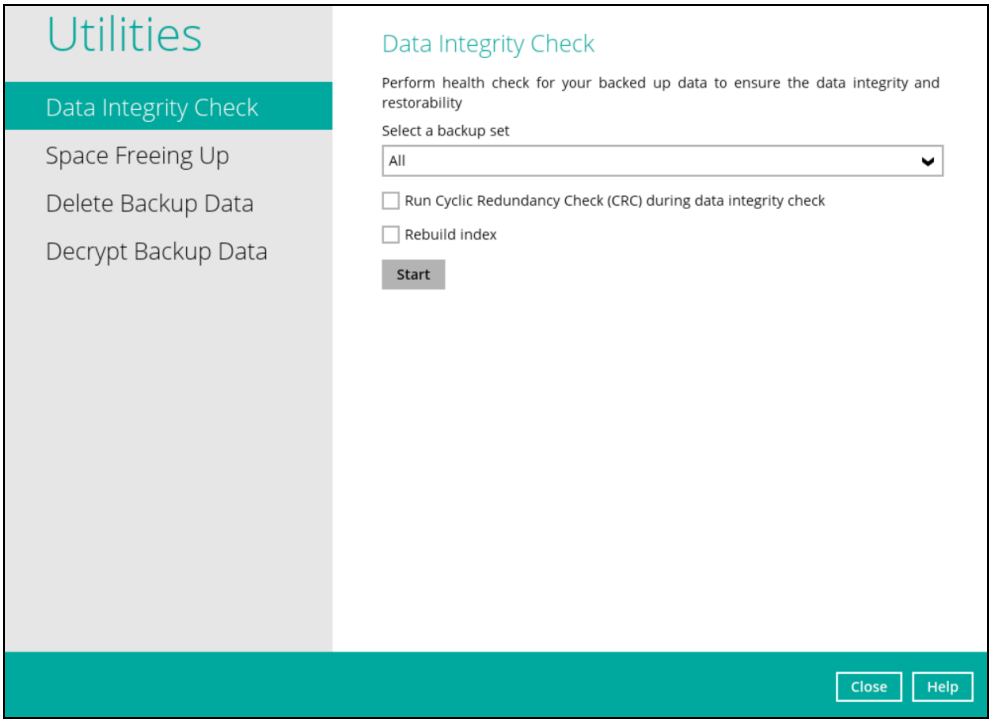
y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.
→ If the backup data matches either of the criteria, proceed to z
→ If **NOT**, proceed to d

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

r Corrupted files will be automatically removed from the backup destination(s).

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

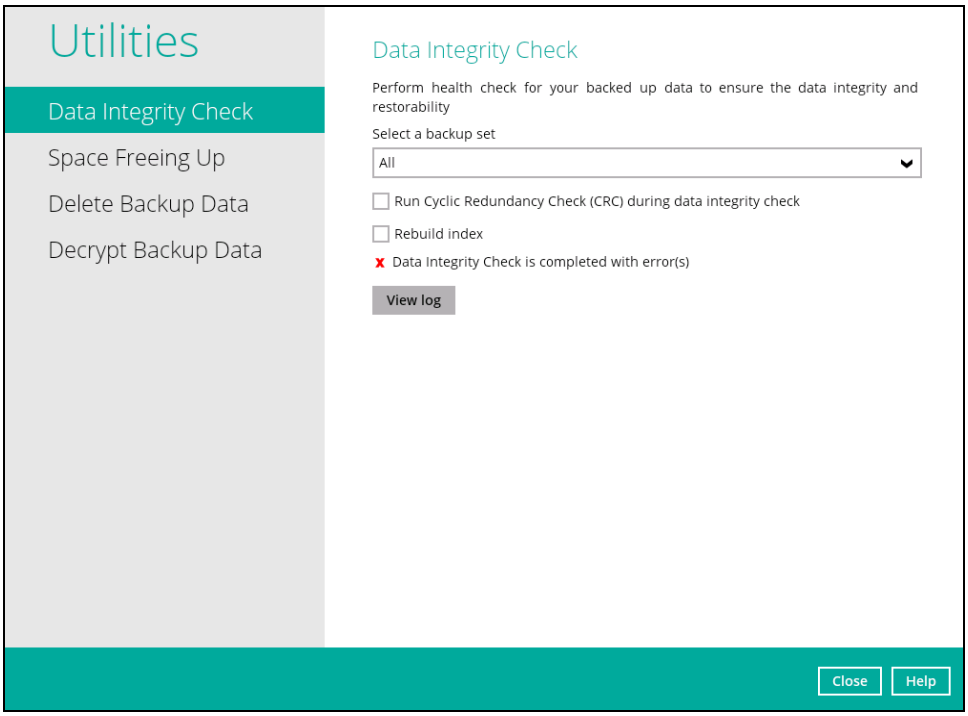
By default, **(TEST MODE)** confirmation screen will only prompt if either of the **criteria** below matches the backup data:
- deleted number of backup files is over 1,000
- deleted number of backup files size is over 512 MB (in total)
- deleted number of backup files is over 10% of the total backup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

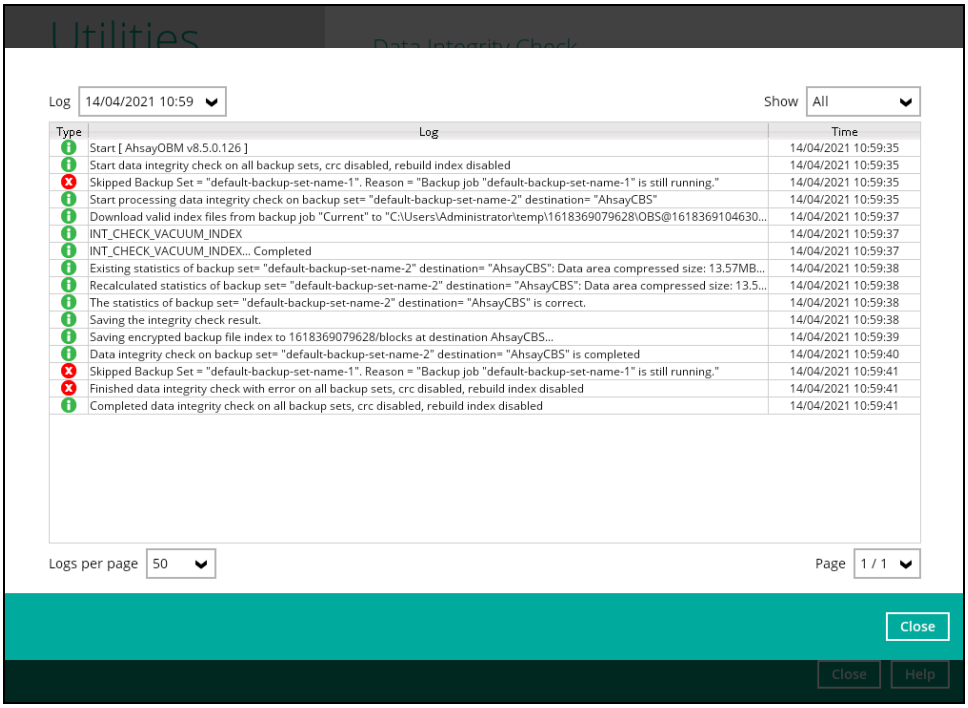


NOTES

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.

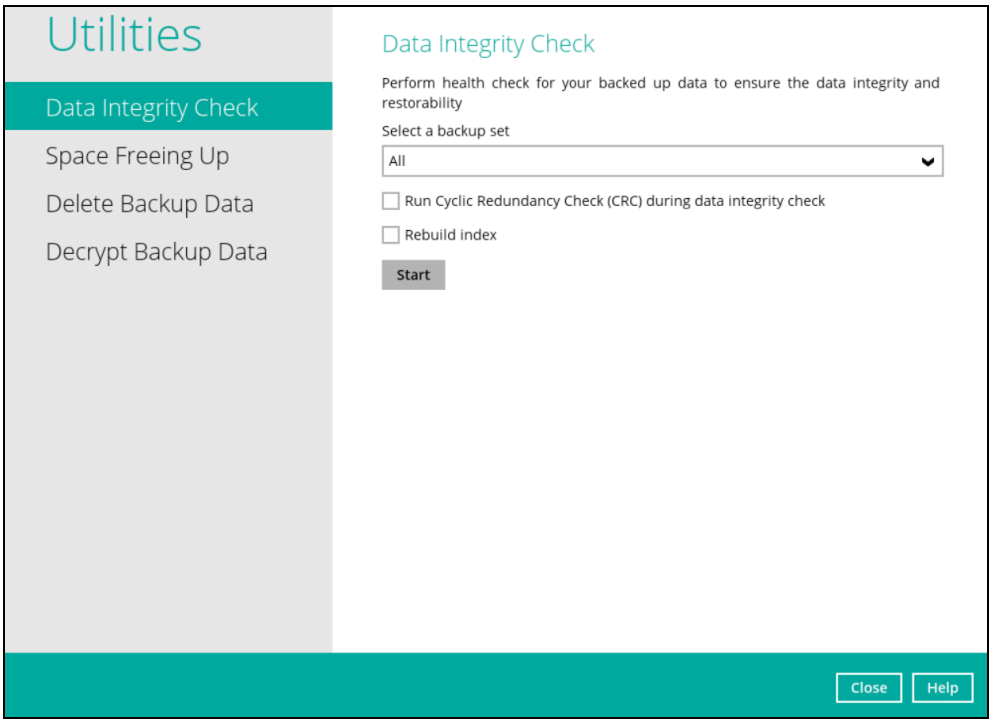
The following screenshot is an example of a Data Integrity Check completed with error(s). A Data Integrity Check is run on a backup set with an active backup job running which resulted the Data Integrity Check to stop with error(s). Clicking the **View log** button will display the details of the Data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



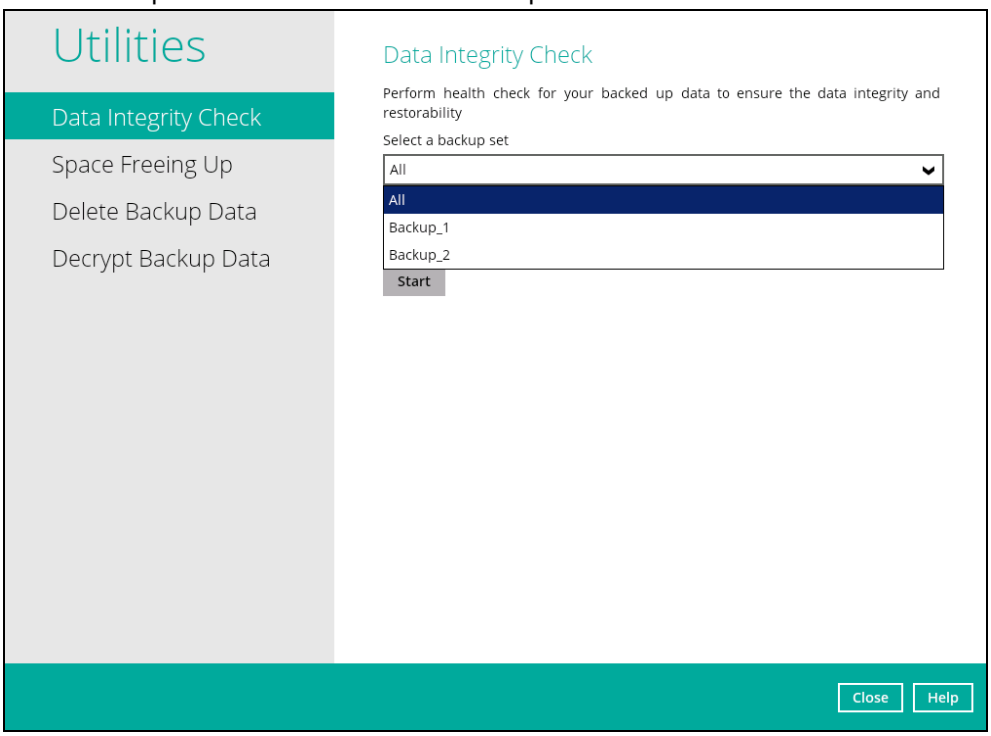


To perform a Data Integrity Check, follow the instructions below:

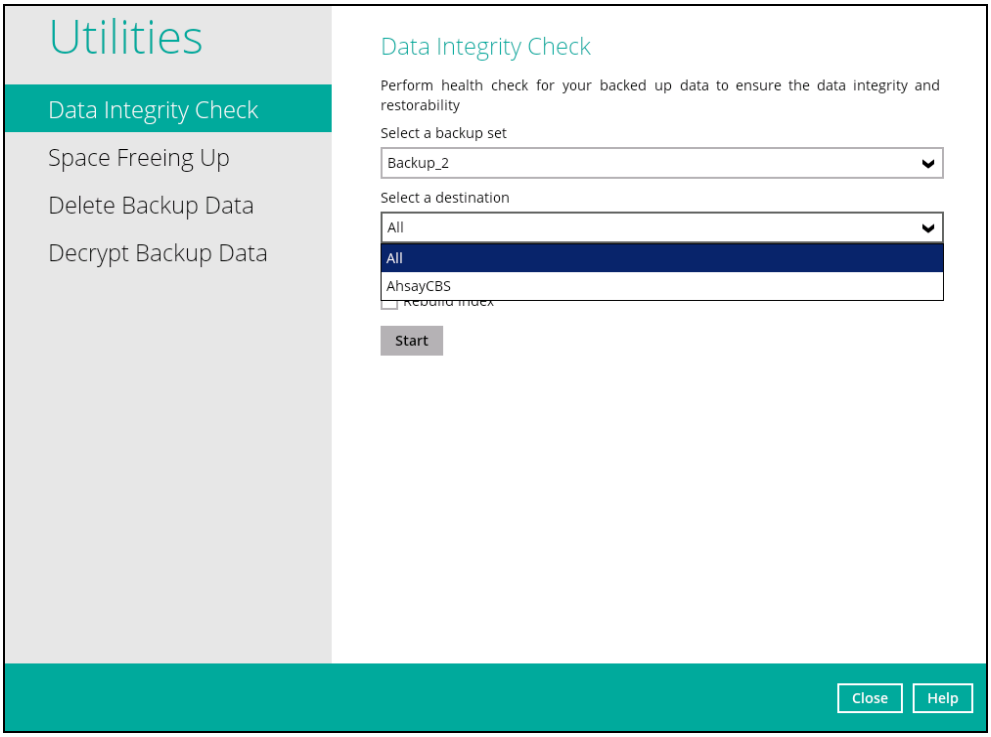
1. Go to the Data Integrity Check tab in the Utilities menu.



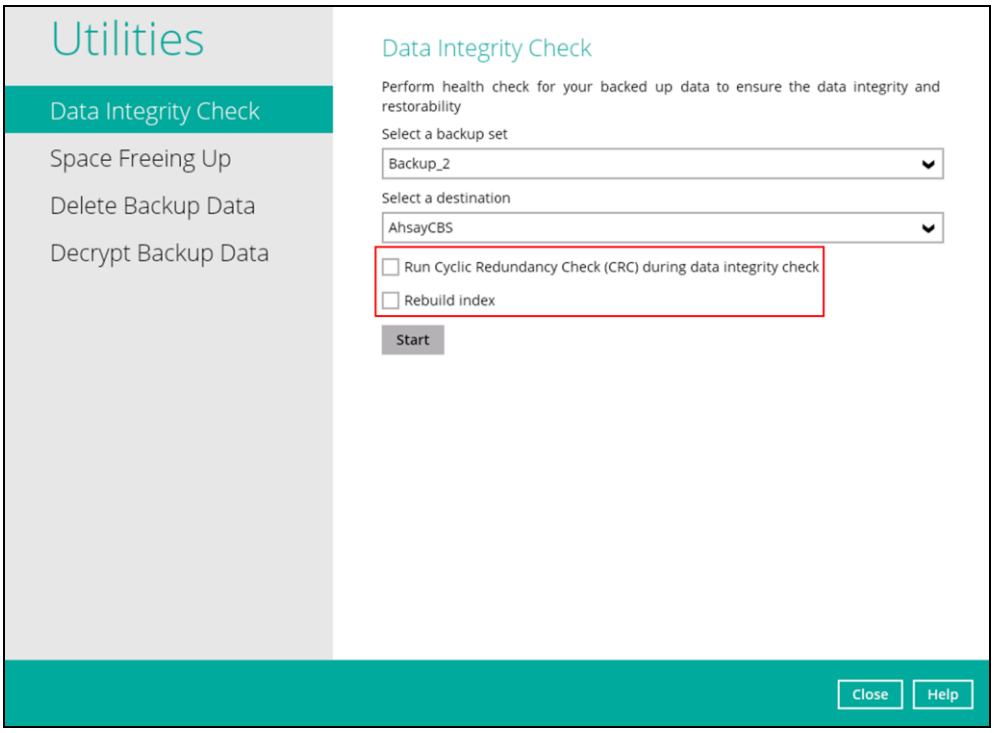
2. Click the drop-down button to select a backup set.



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



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



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

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

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

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

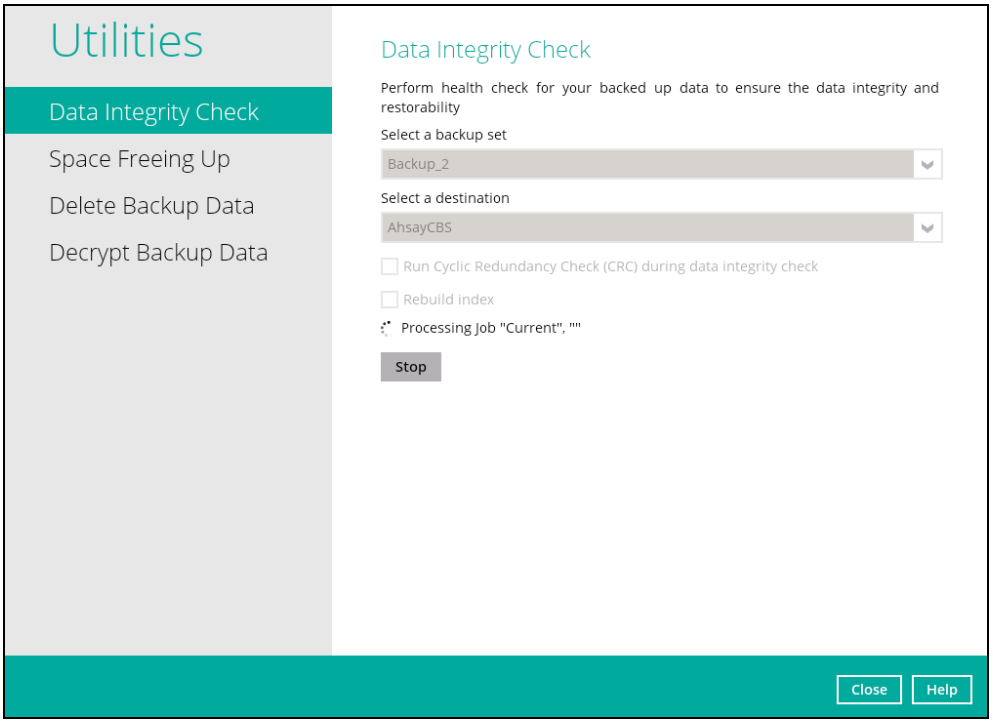
- number of files and/or folders in the backup set(s)
- bandwidth available on the client computer
- hardware specifications of the client computer such as, the disk I/O and CPU performance

NOTES

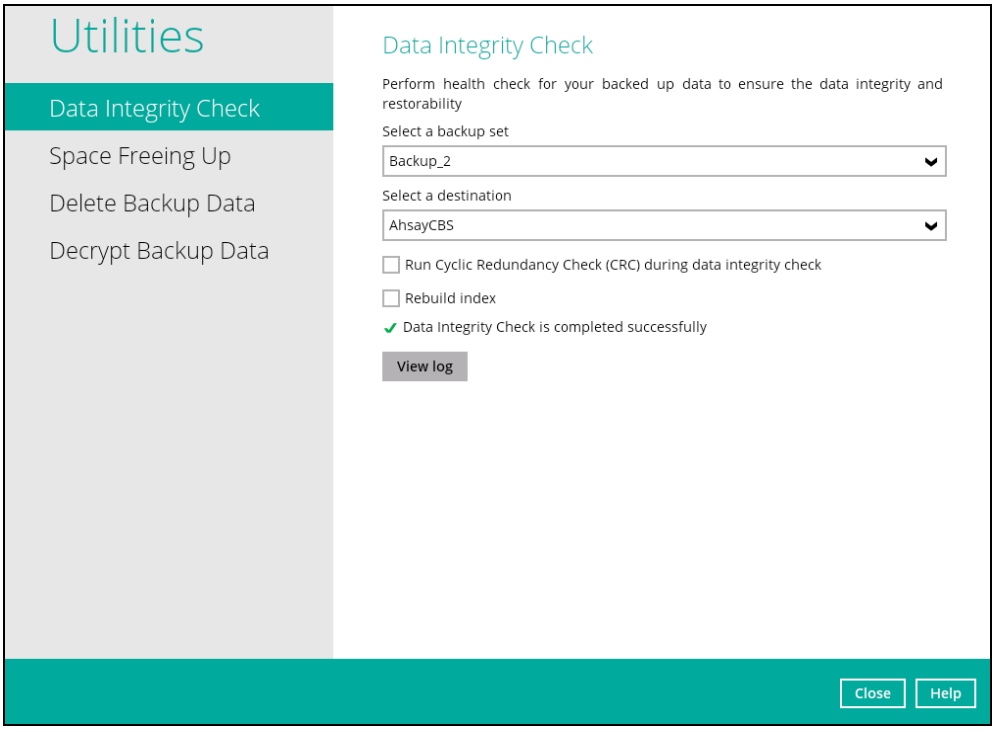
1. For user(s) with metered internet connection, additional data charges may be incurred if the Cyclic Redundancy Check (CRC) is enabled. As CRC data involves downloading the data from the backup destination(s) to the client machine in order to perform this check.
2. To find out how much data is downloaded from the backup destination(s) for the CRC check, please refer the value for **Utilities** in the Data Transfer statistics on chapter 10.6.3.

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

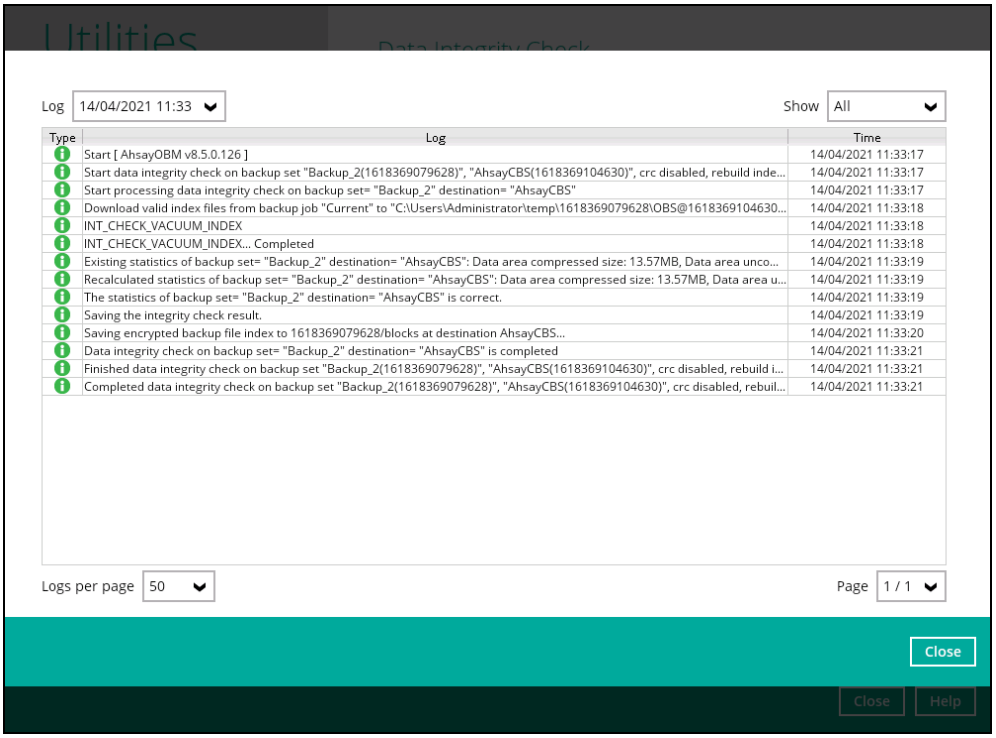
5. Click the [Start] button to begin the Data Integrity Check.
6. Data Integrity Check will start running on the selected backup set(s) and backup destination(s).



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

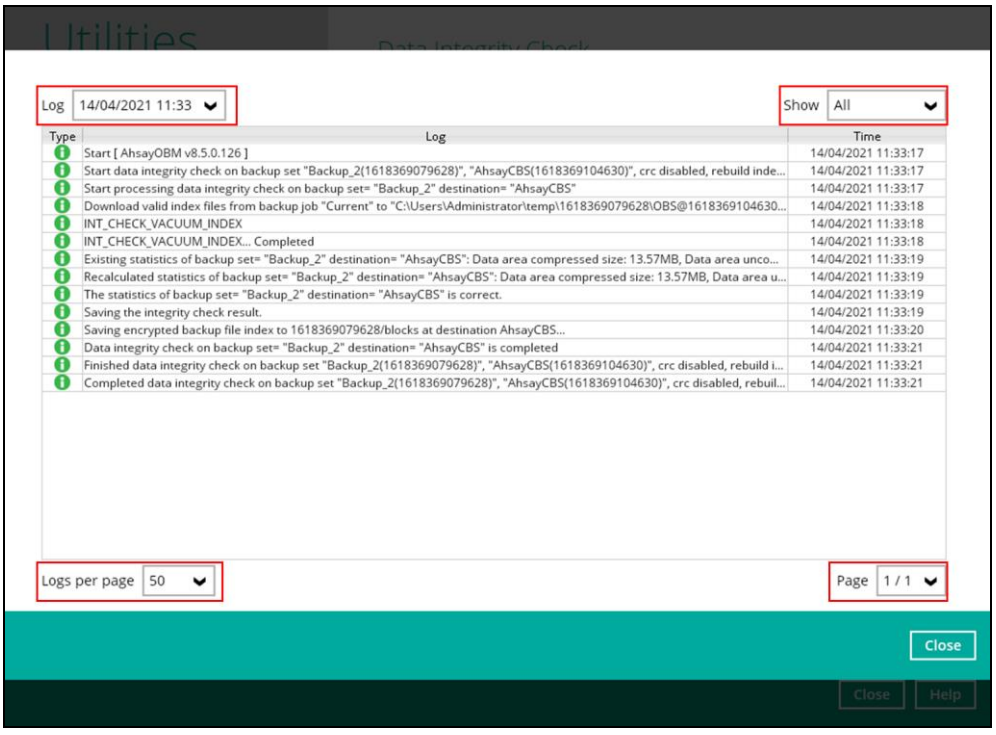


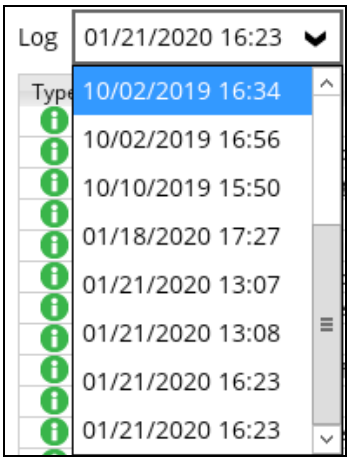
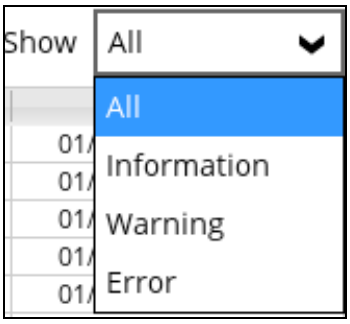
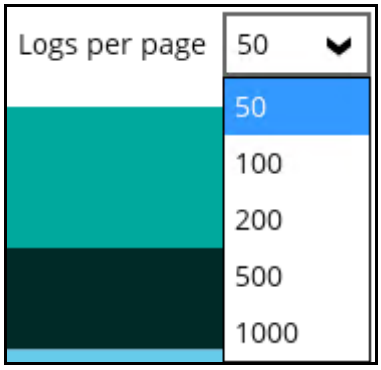
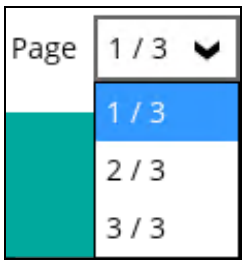
8. The detailed log of data integrity check process will be displayed.



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

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



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

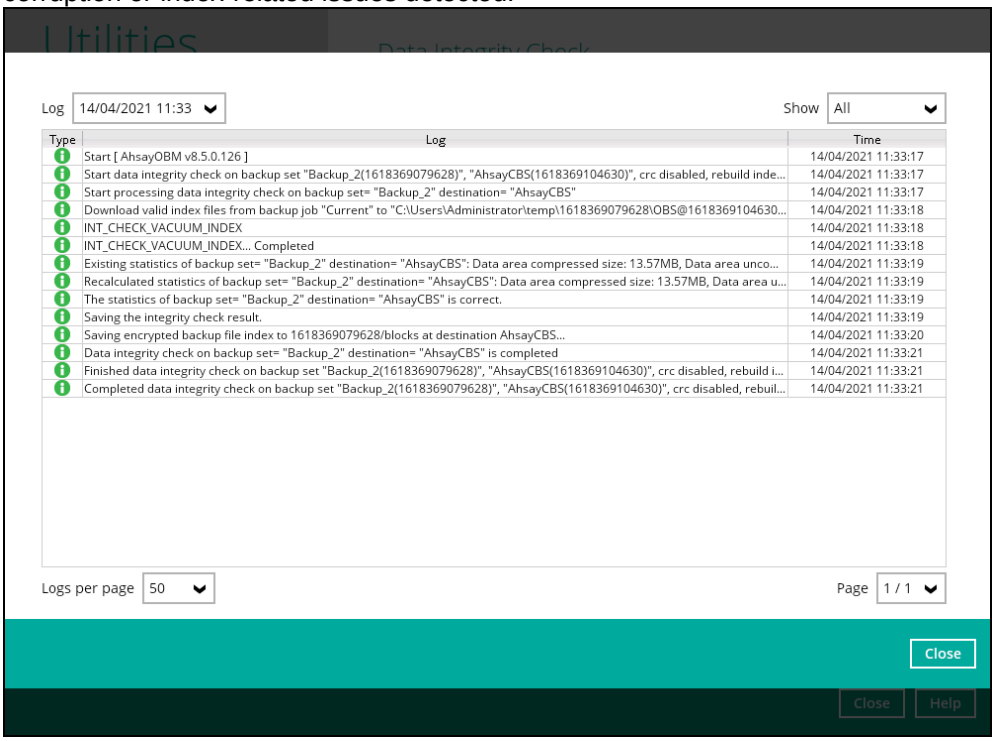
Data Integrity Check Result

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

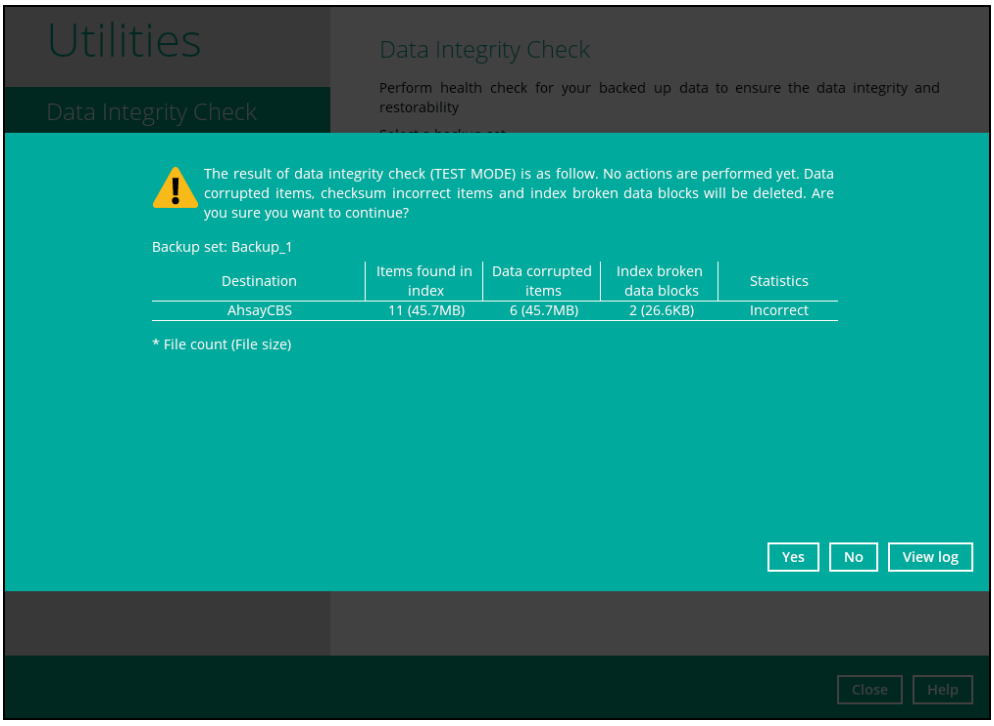
- Data Integrity Check is completed successfully with no data corruption or index-related issues detected;

- Corrupted data (e.g. index files, checksum files and/or broken data blocks) has been detected

The screenshot below shows an example of a data integrity check log with NO data corruption or index-related issues detected.



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



This is to inform the user of the following details:

- Backup set that contains an error
- Backup Destination
- Items found in index

- Data corrupted items
- Index broken data blocks
- Statistics (i.e. Correct or Incorrect)

Test Mode confirmation

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

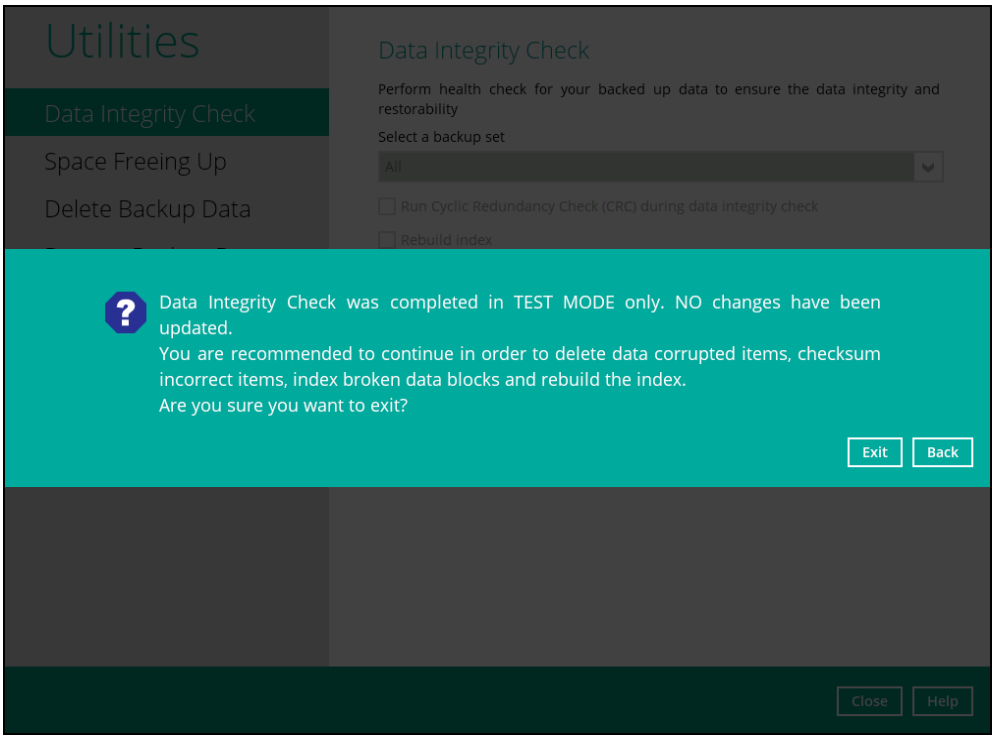
- deleted number of backup files is over 1,000
- deleted number of backup file size is over 512 MB (in total)
- deleted number of backup files is over 10% of the total backup files

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

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

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

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



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

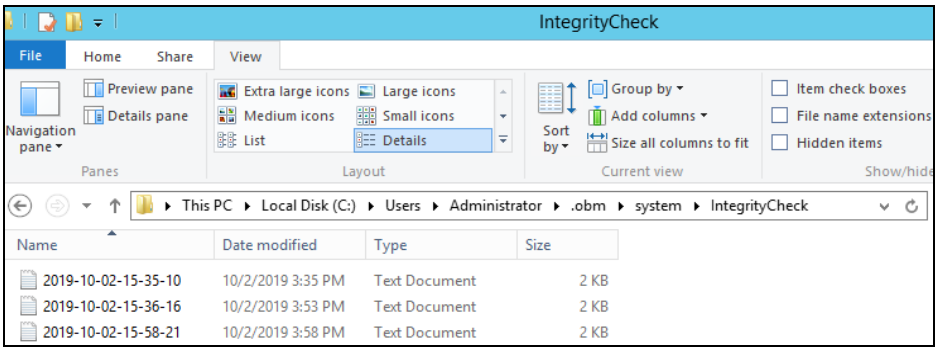
If the **[Back]** button is clicked, it will go back to the (TEST MODE) confirmation screen.

NOTES

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

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

%UserProfile%\.obm\system\IntegrityCheck

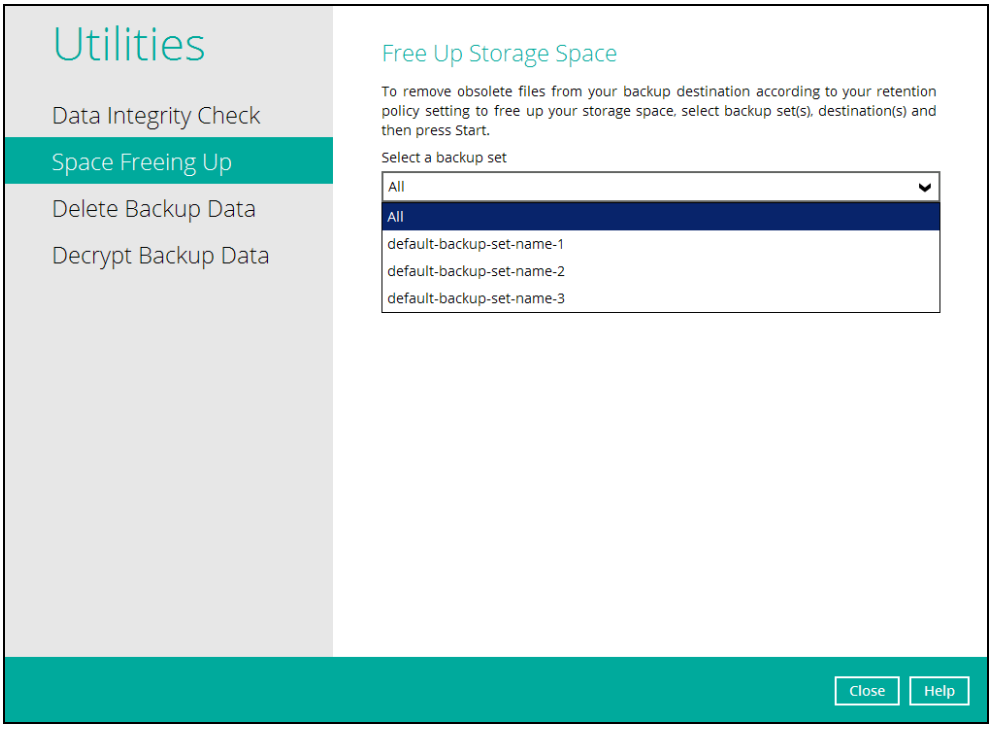


10.9.2 Space Freeing Up

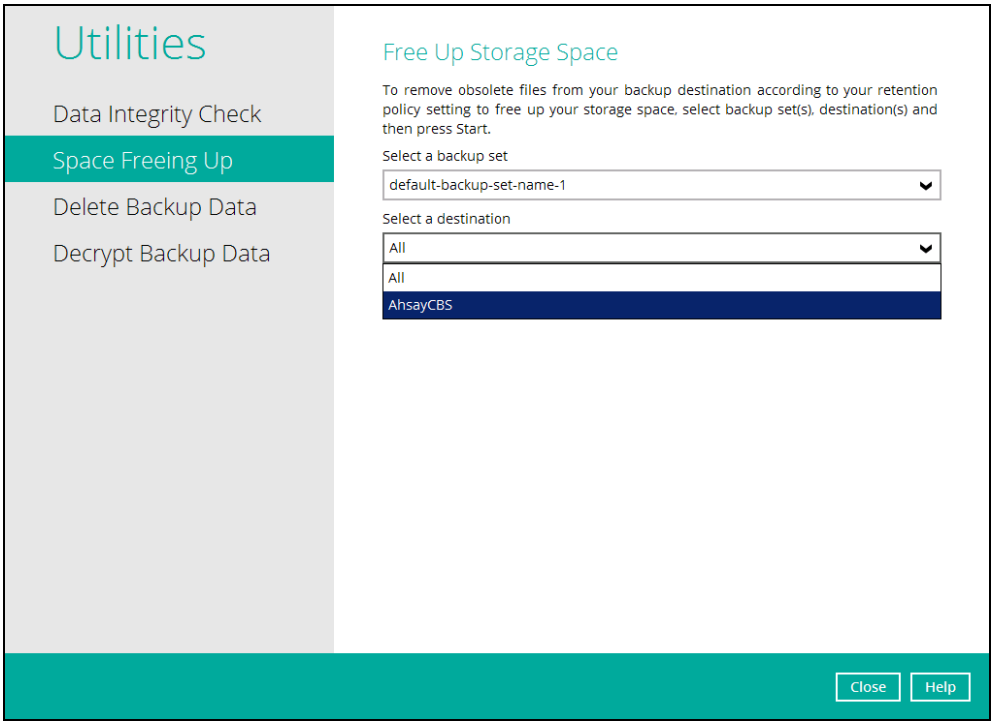
This feature is used to remove obsolete file(s) from your backup set and destination (manually start retention policy). After the Space Freeing Up job is completed, the storage statistics of the backup set(s) are updated.

To perform Space Freeing Up, follow the instructions below:

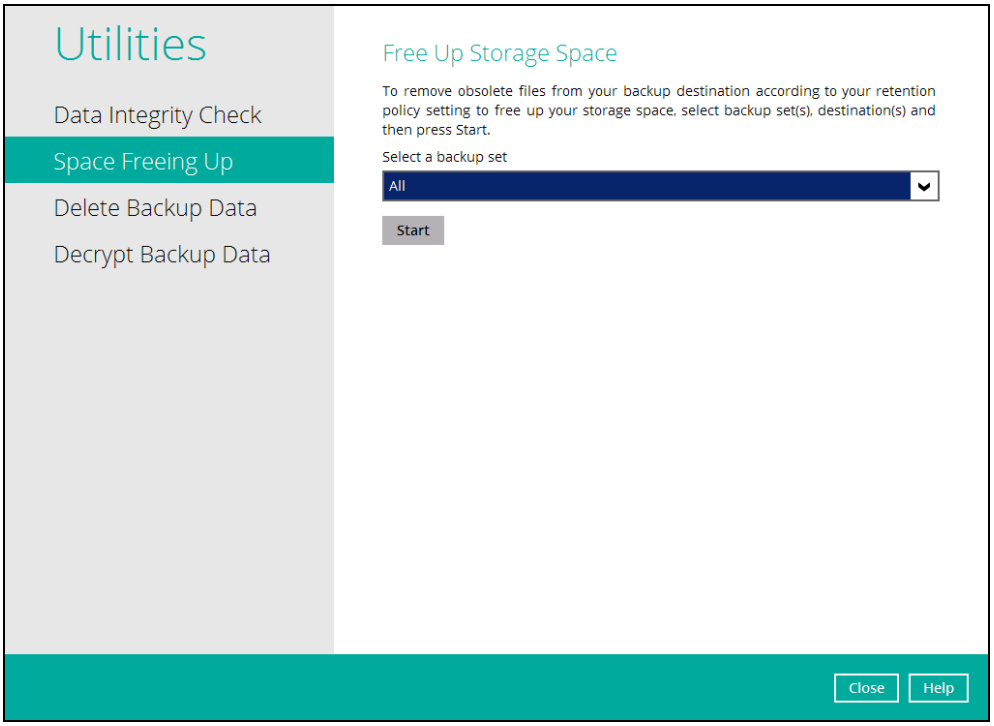
1. Select a backup set from the drop-down list.



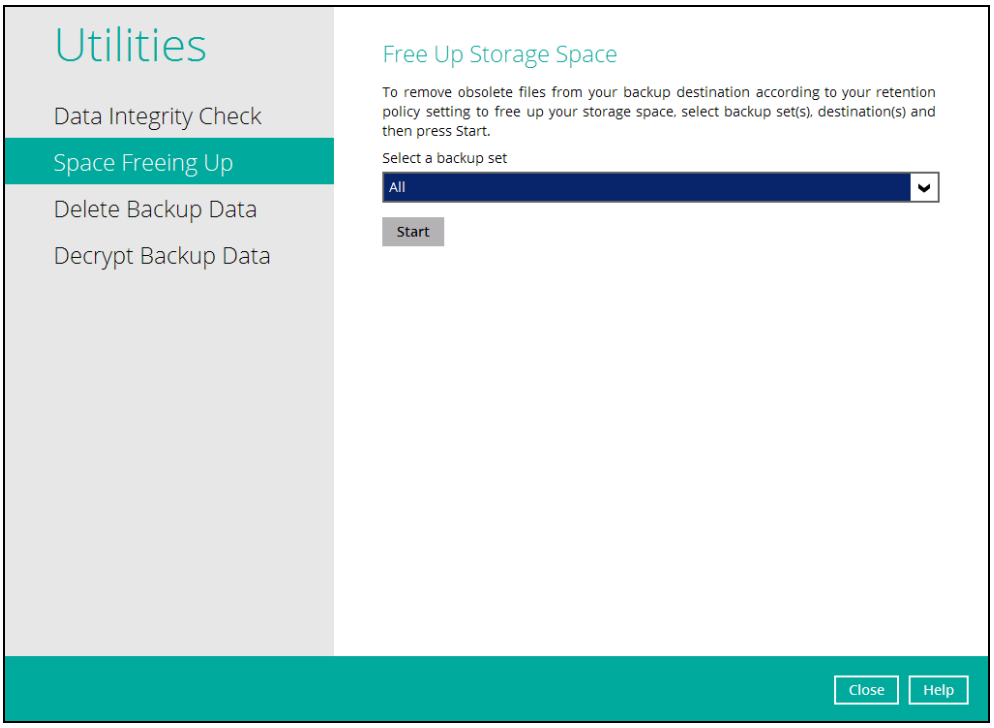
If you select a specific backup set, then you will also have to select a specific destination or all destinations.



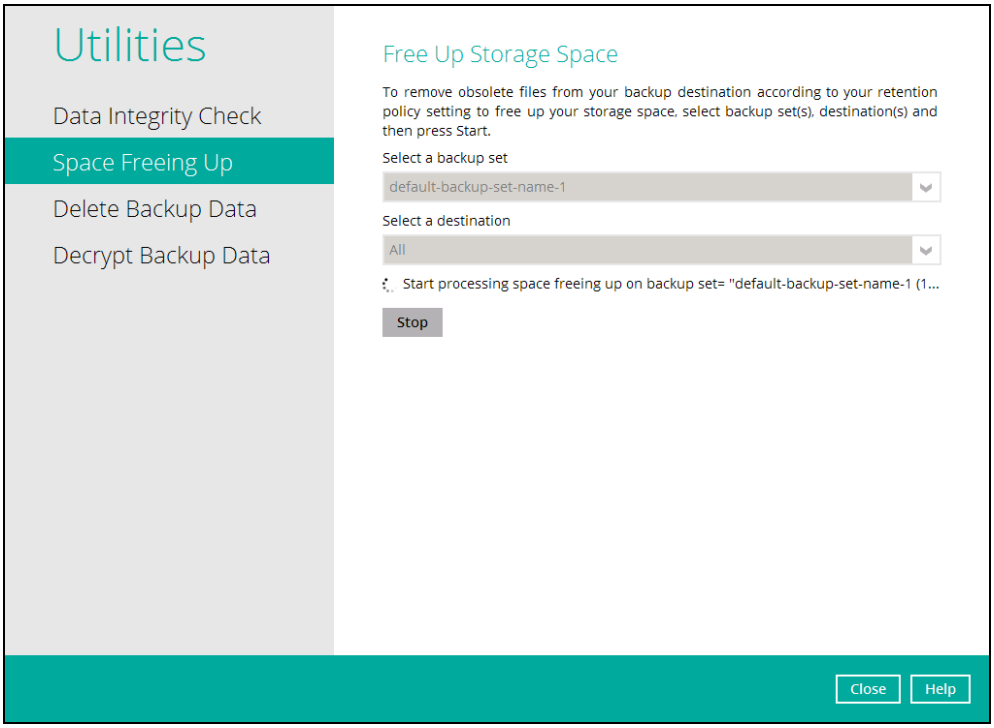
If you select All backup sets, then there is no need to select a destination.



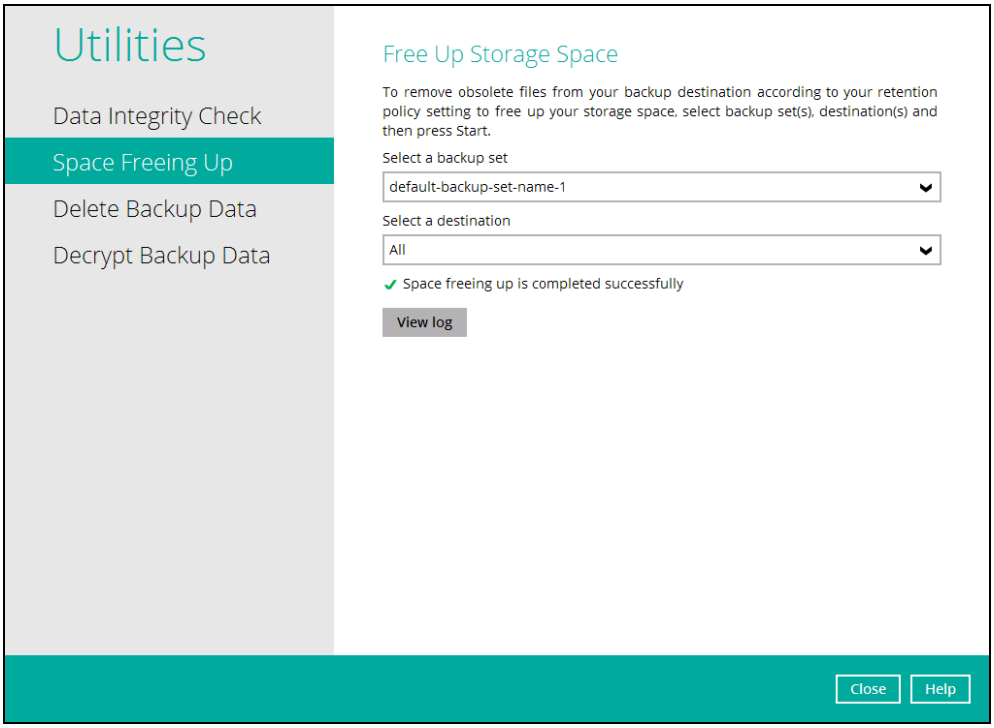
2. Click the [Start] button to perform space free up.

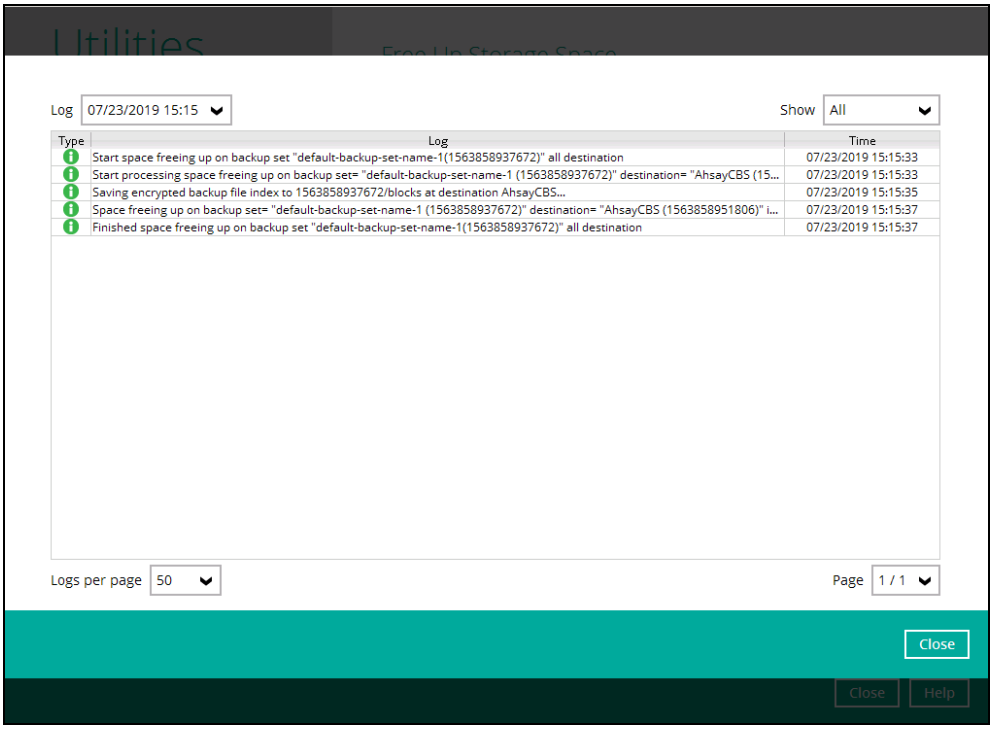


3. Space freeing job will start running on the selected backup set(s) and backup destination(s).



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



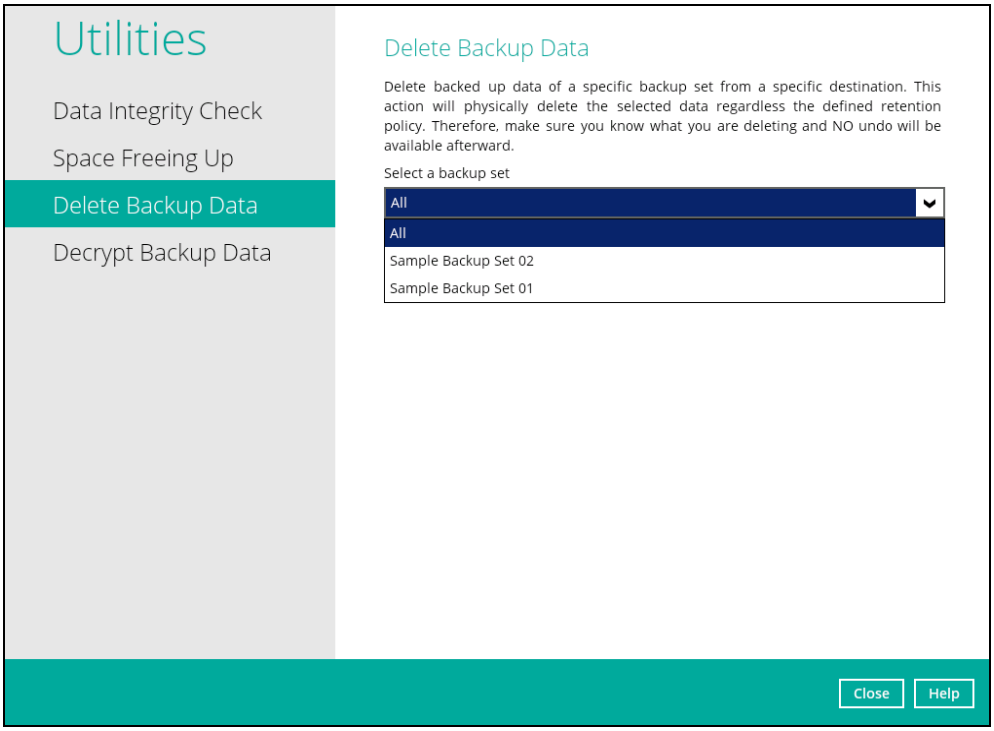


10.9.3 Delete Backup Data

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.

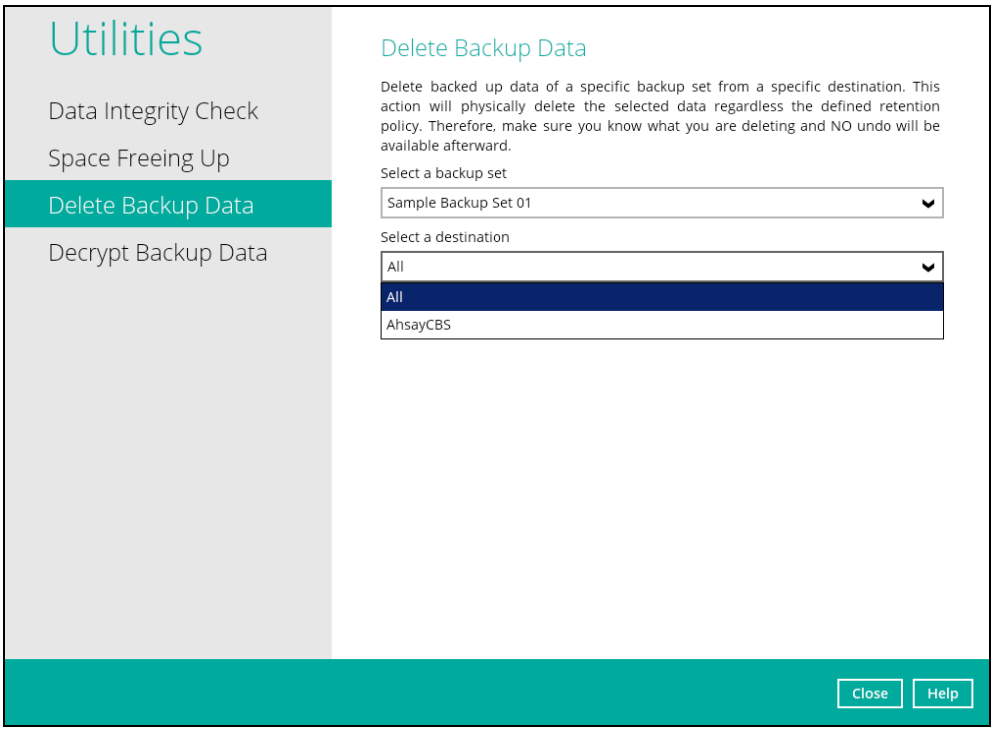
To perform deletion of backup data, follow the instructions below:

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

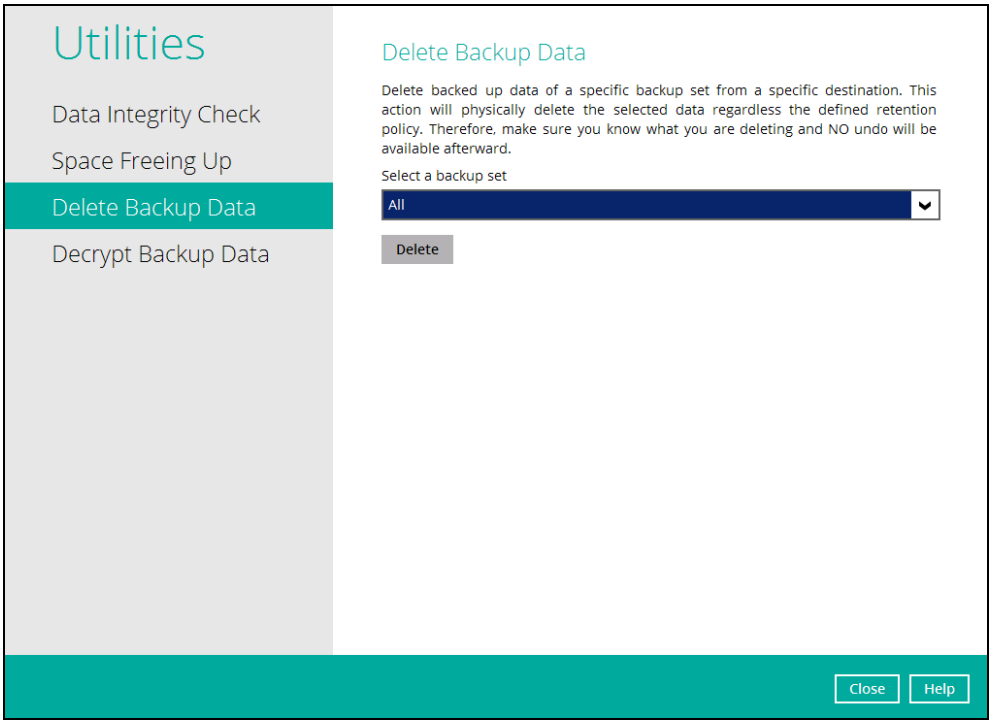


NOTE: This will only delete the backed up files in a backup set(s) and destination(s), but the backup set and destination will remain.

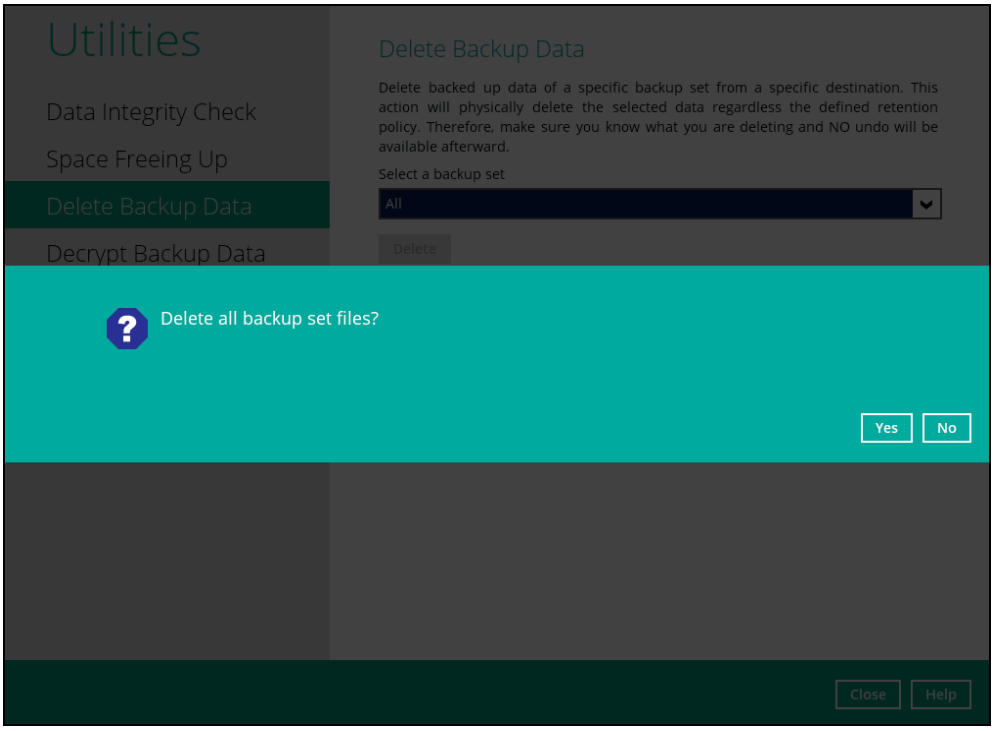
If you select a specific backup set, then you will also have to select a specific destination or all destinations.



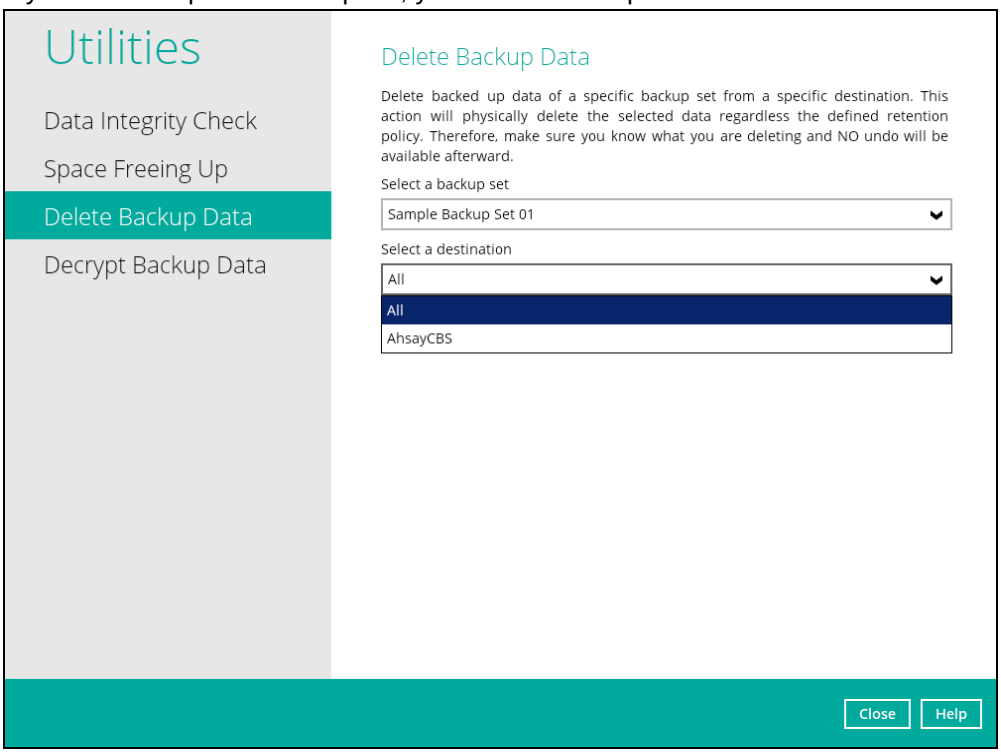
If you select **All** backup sets, then there is no need to select a destination.



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.

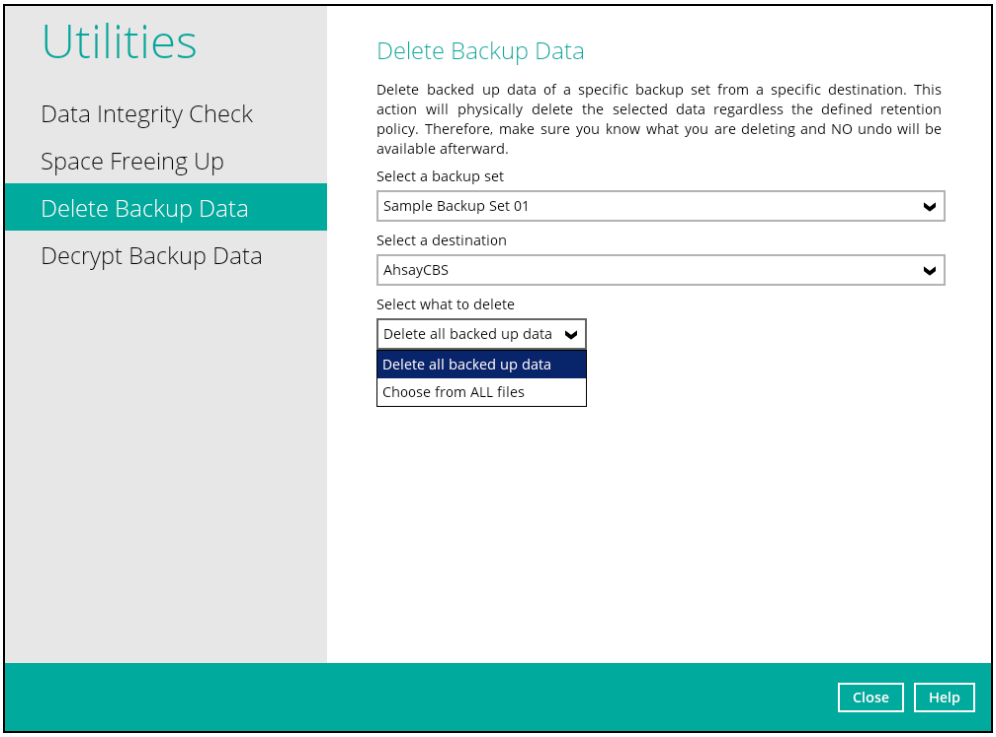


If you select a specific backup set, you will have an option to choose a destination.



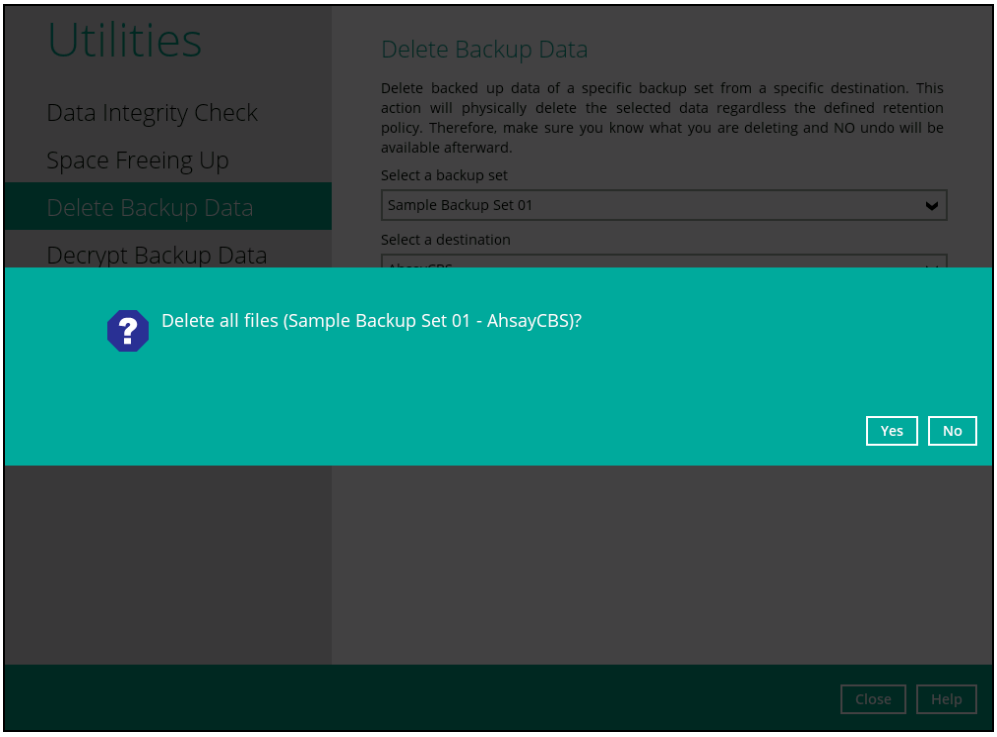
If you select a specific destination, there are two (2) available options for the type of files you wish to delete.

- Delete all backed up data
- Choose from ALL files



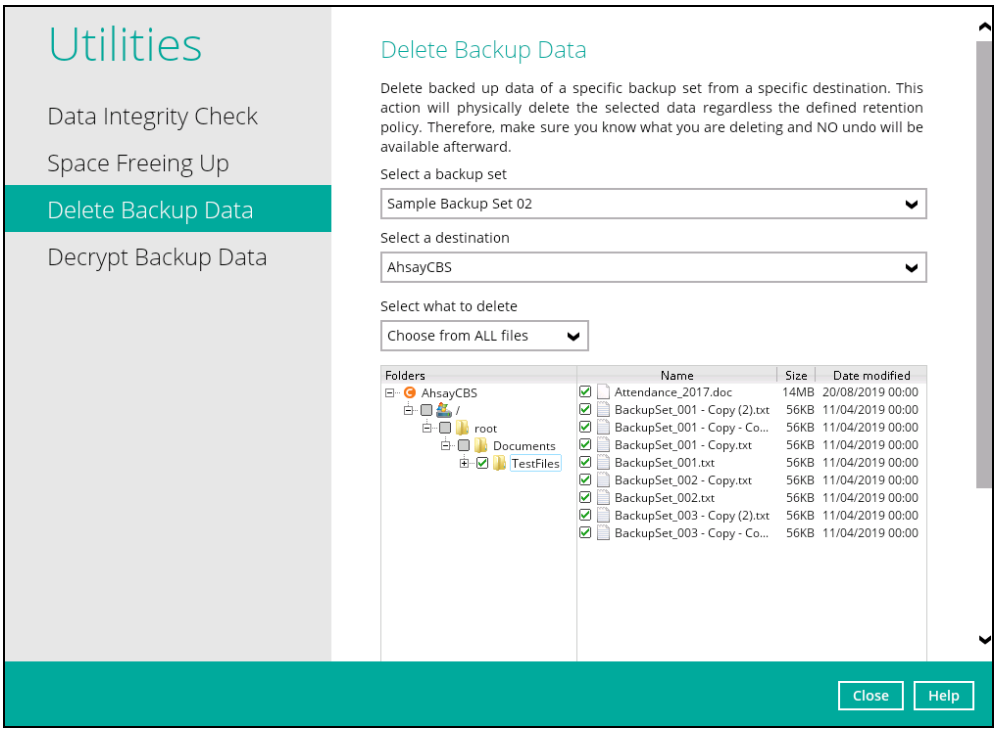
Delete all backed up data

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.

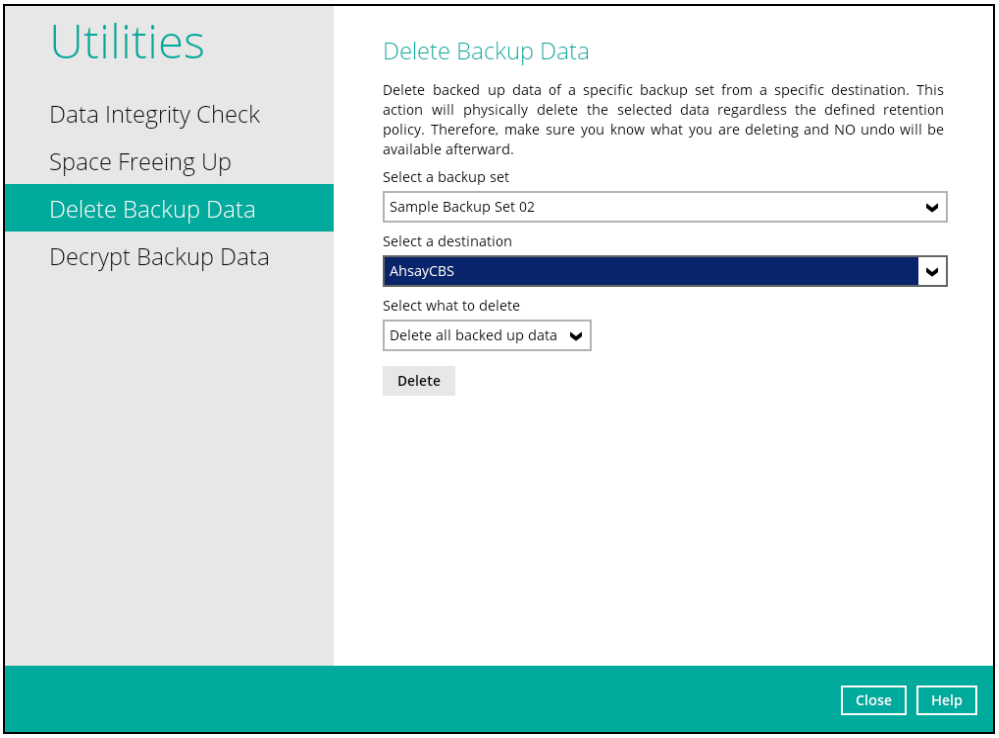


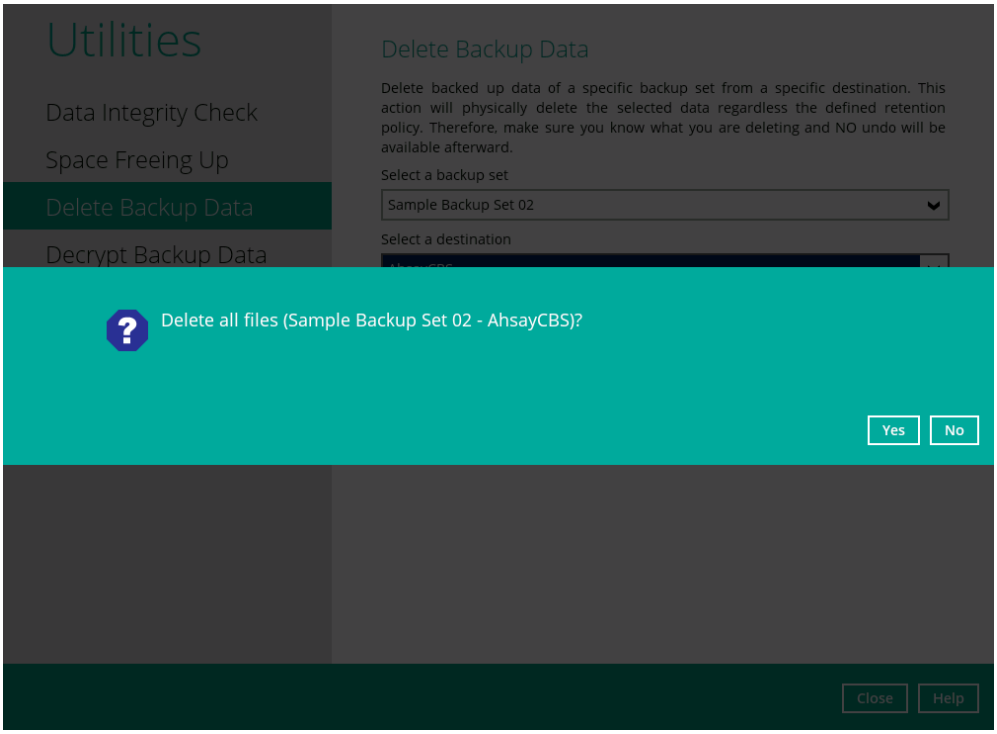
Choose from ALL files

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

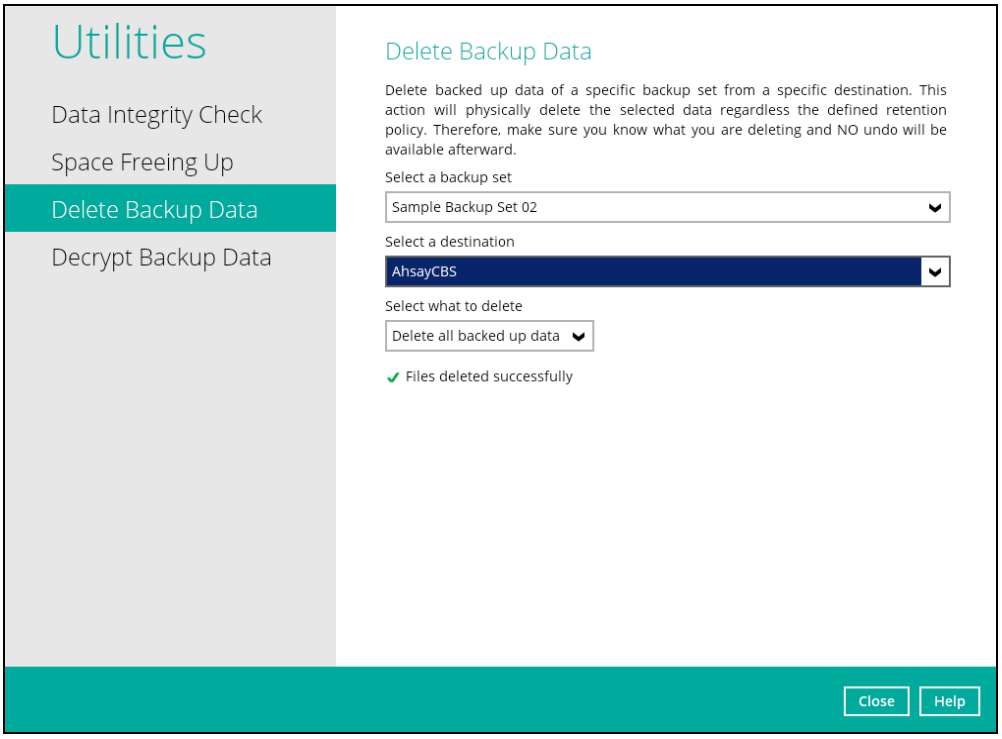


3. Click the [Delete] button, then click [Yes] to start the deletion of files.





4. Files are successfully deleted.

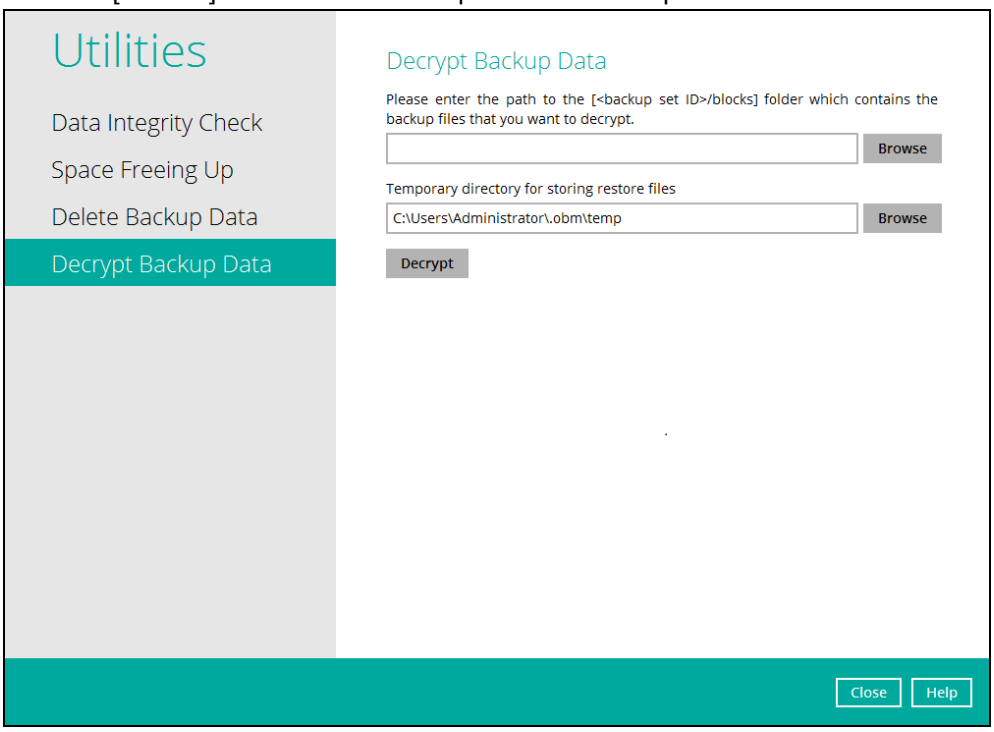


10.9.4 Decrypt Backup Data

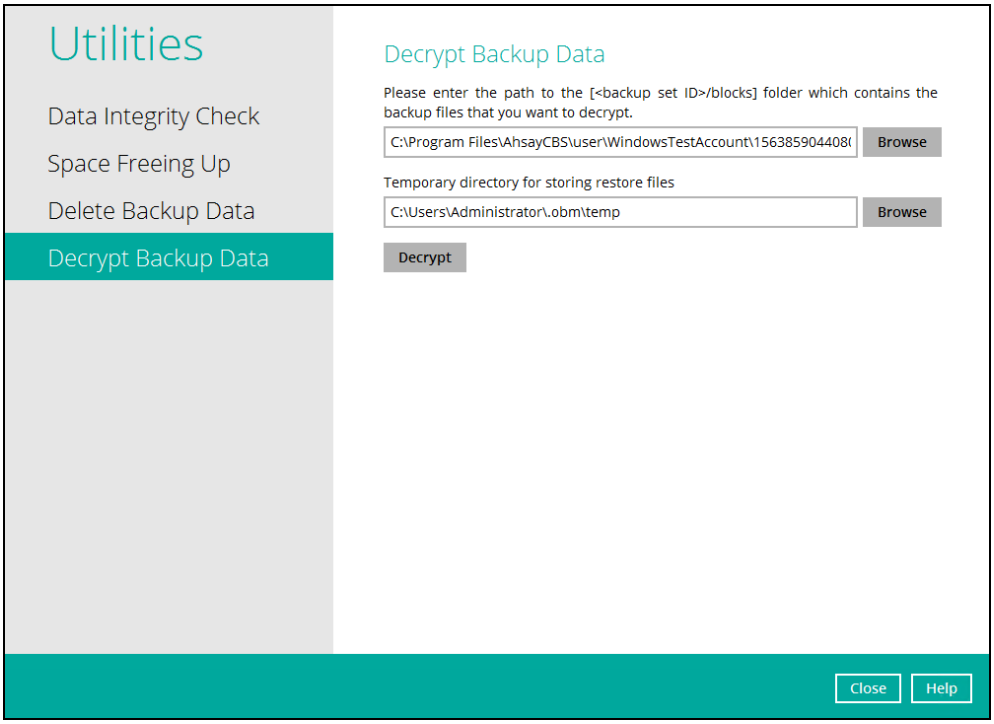
This feature is used to restore raw data by using the data encryption key that was set for the backup set.

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

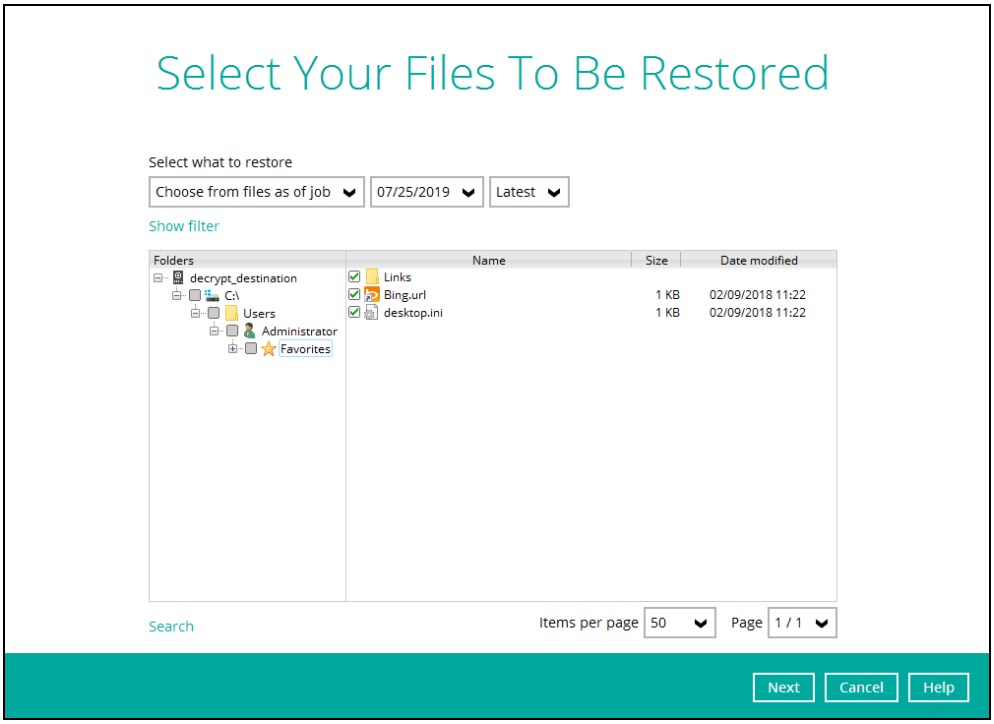
1. Click the [Browse] button to locate the path of the backup set ID / blocks folder.



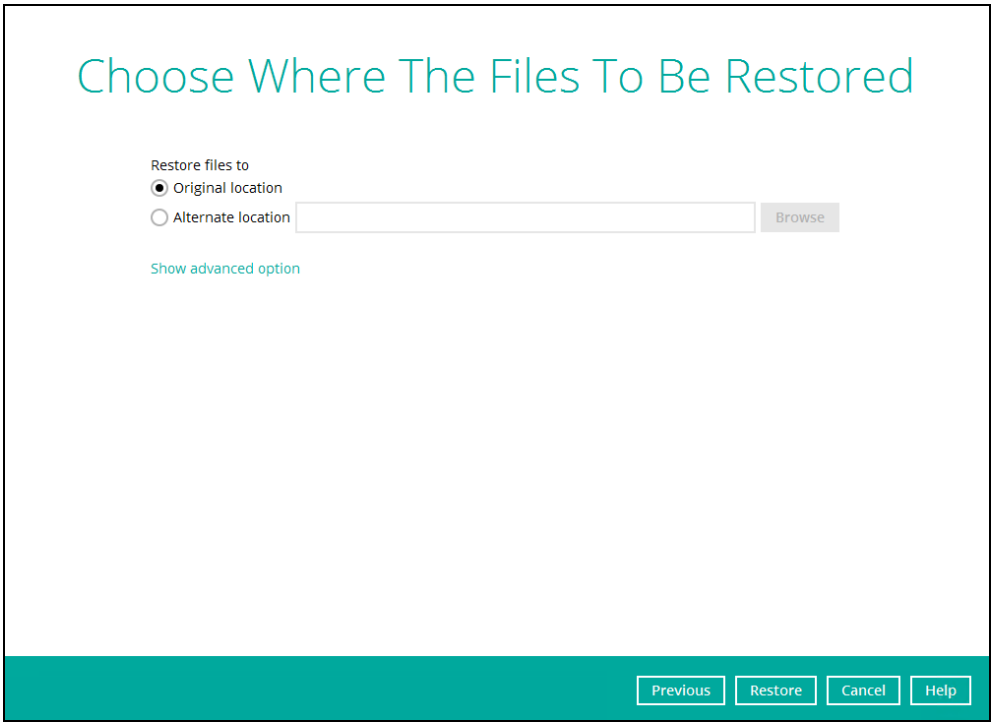
2. Click the [Browse] button to re-select the temporary folder for the decrypt process. Then click the [Decrypt] button to begin.



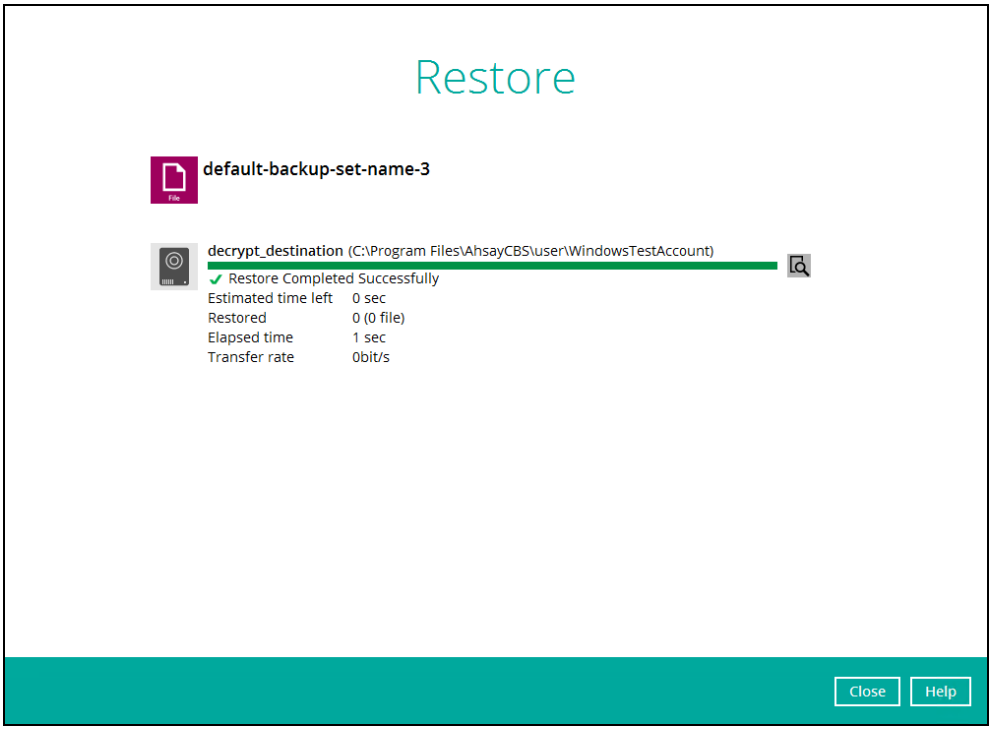
3. Select files to be decrypted.



4. Choose the location where the decrypted files will be restored to.

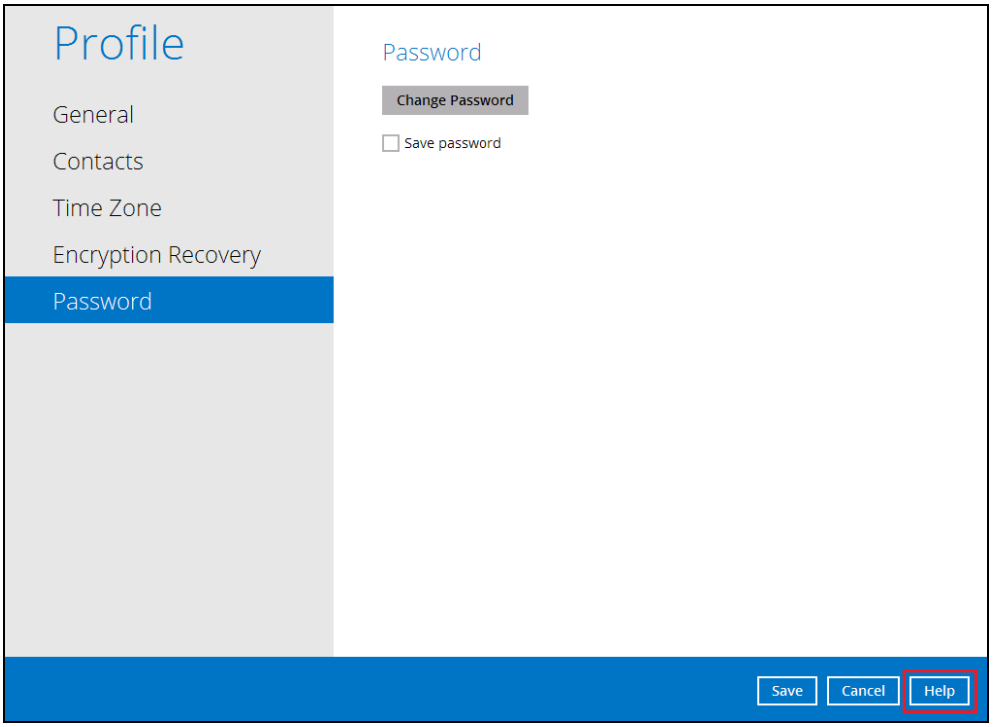


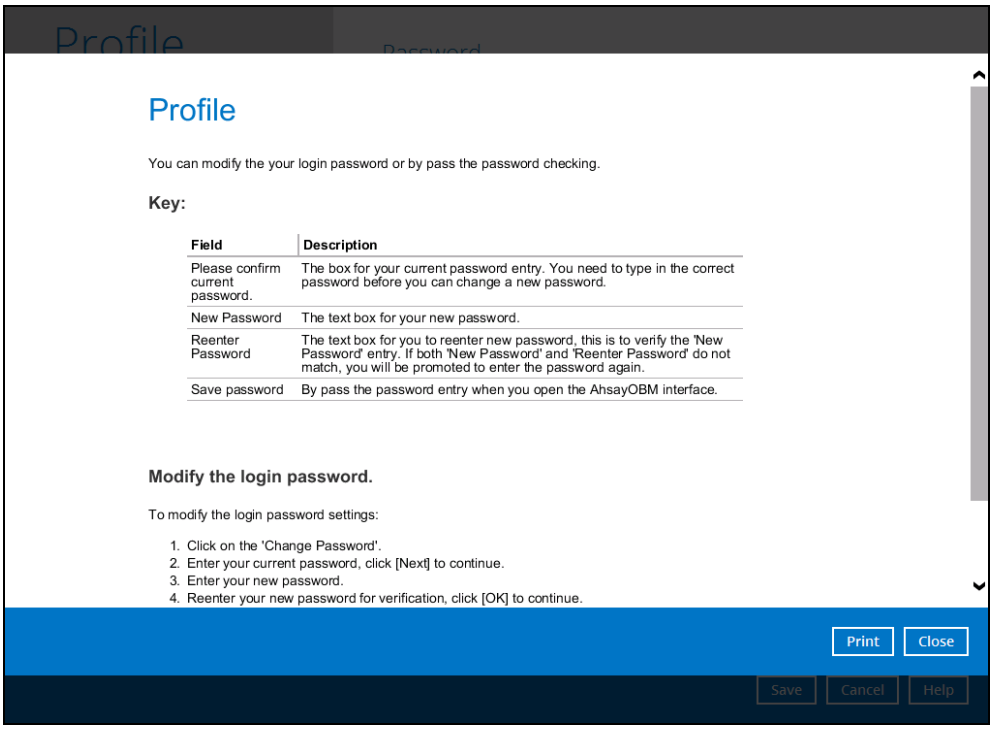
5. The status will be shown once completed.



10.10 Online Help

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

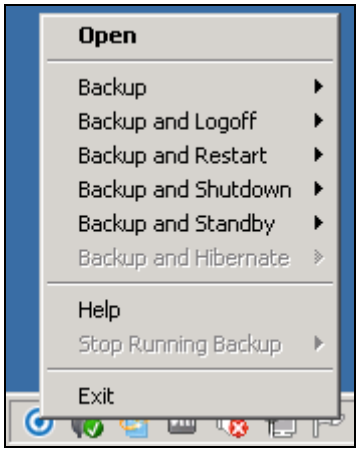




10.11 System Tray

If AhsayOBM is installed in the computer, you will see an AhsayOBM icon in the taskbar at the lower right corner of the screen.

When you right-click the AhsayOBM icon, a control menu will pop-up.

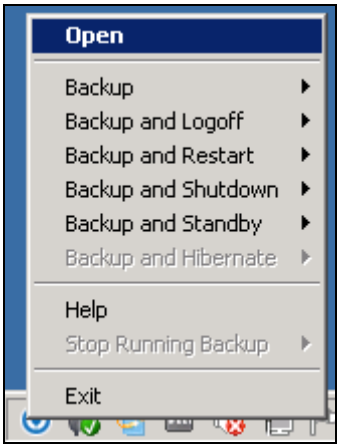


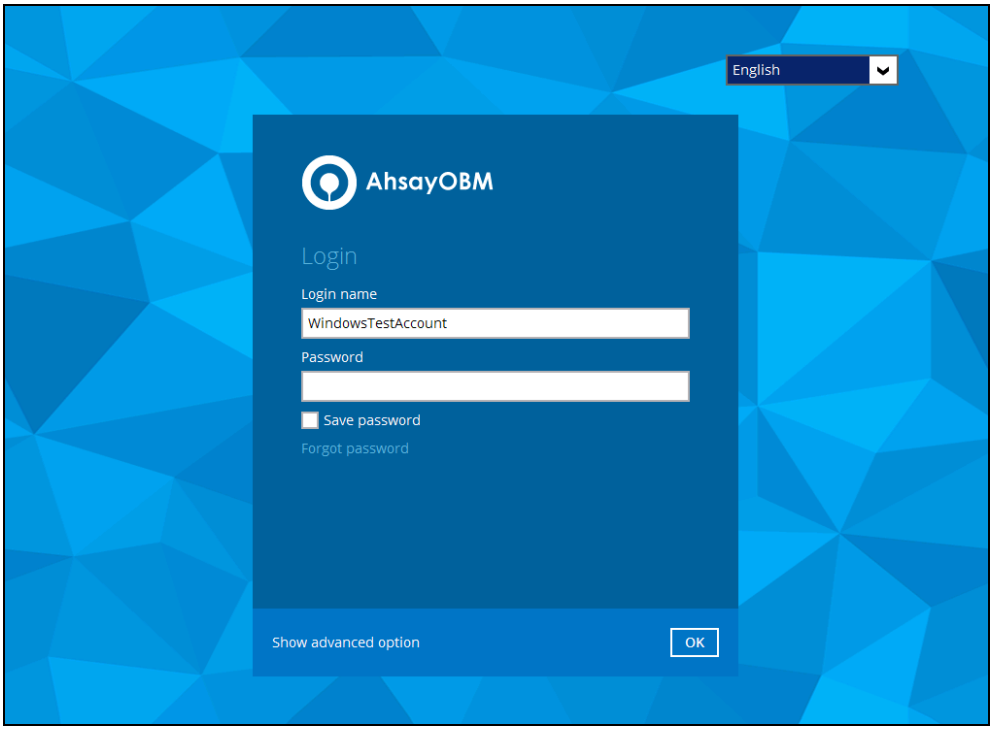
Ahsay OBM system tray has ten (10) controls:

- Open
- Backup
- Backup and Logoff
- Backup and Restart
- Backup and Shutdown
- Backup and Standby
- Backup and Hibernate
- Help
- Stop Running Backup
- Exit

Open

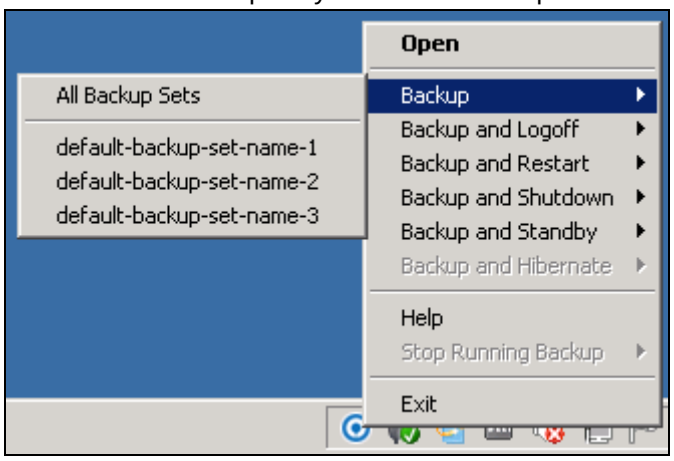
Select this option to open the AhsayOBM login screen.





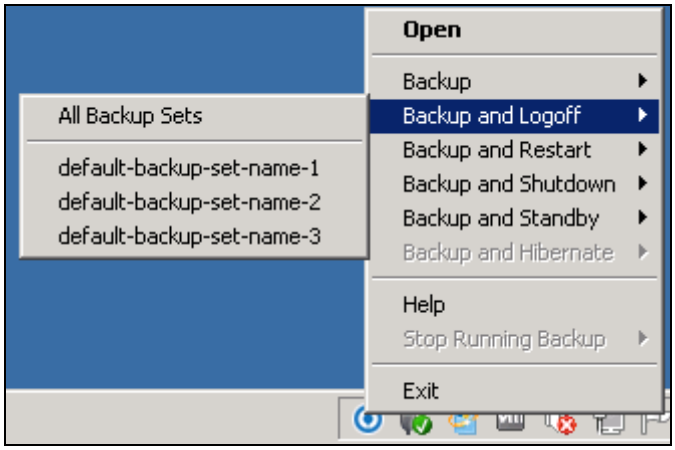
Backup

If you want to perform a backup without going to the interface, hover the mouse to this option and select the backup set you want to back up.



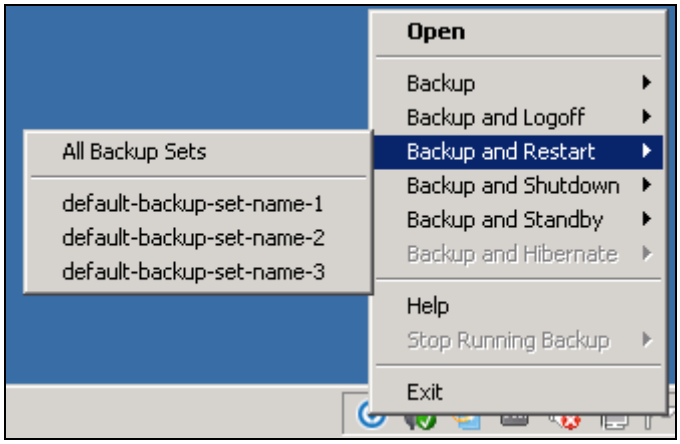
Backup and Logoff

Select this option if you want to logoff Windows after a manual backup job is done.



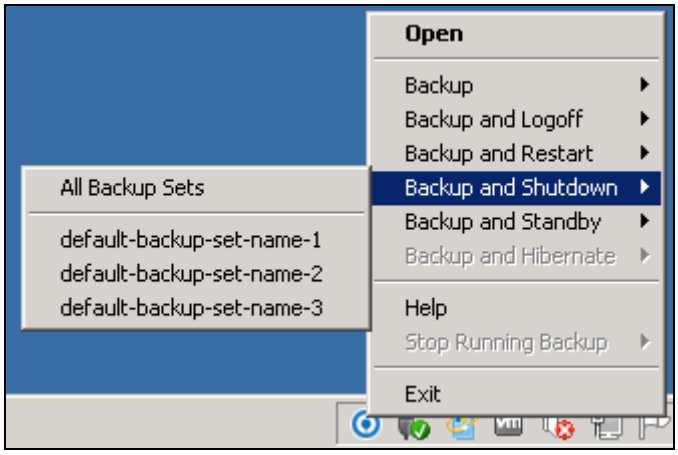
Backup and Restart

Choose this option if you want the machine to restart after a manual backup job is done.



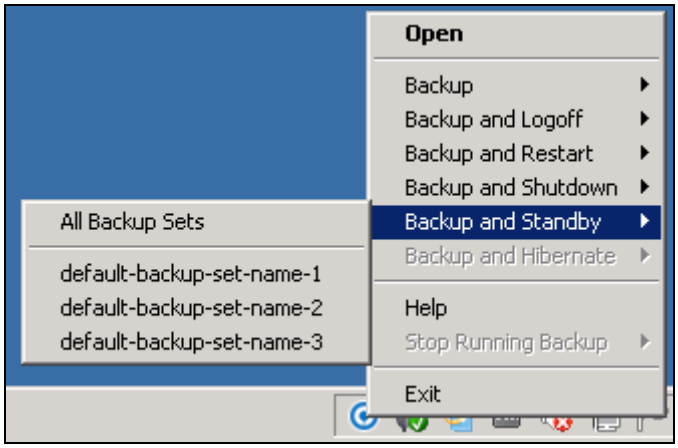
Backup and Shutdown

Choose this option if you want the machine to shut down after a manual backup job is done.



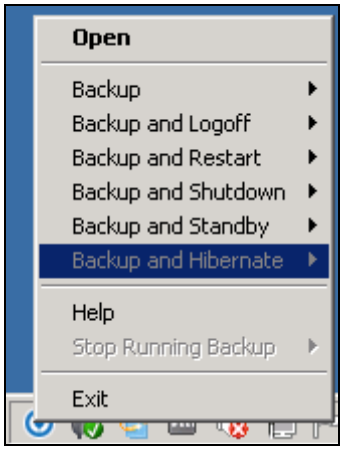
Backup and Standby

Choose this option if you want the machine to go on standby after a manual backup job is done.



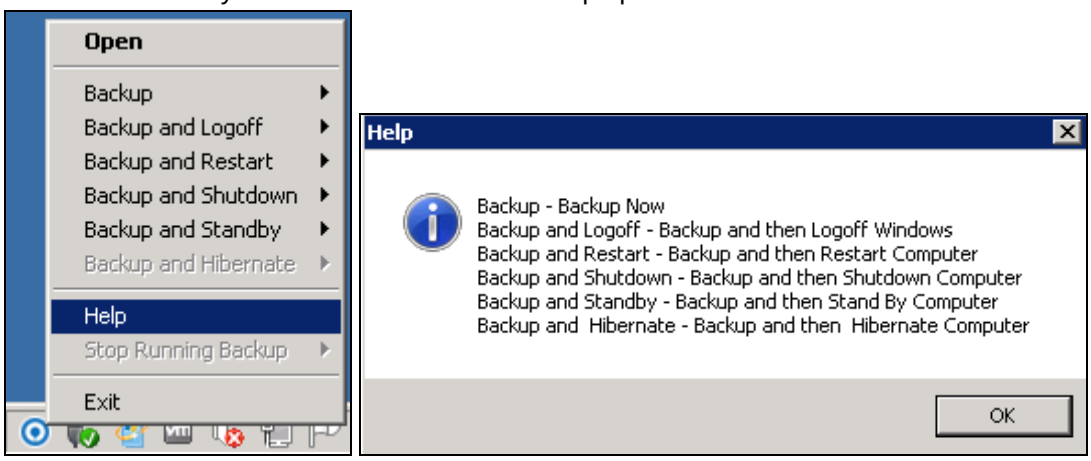
Backup and Hibernate

Choose this option if you want the machine to hibernate after a manual backup job is done. This will be disabled if hibernate mode is not available on the Windows version you are using.



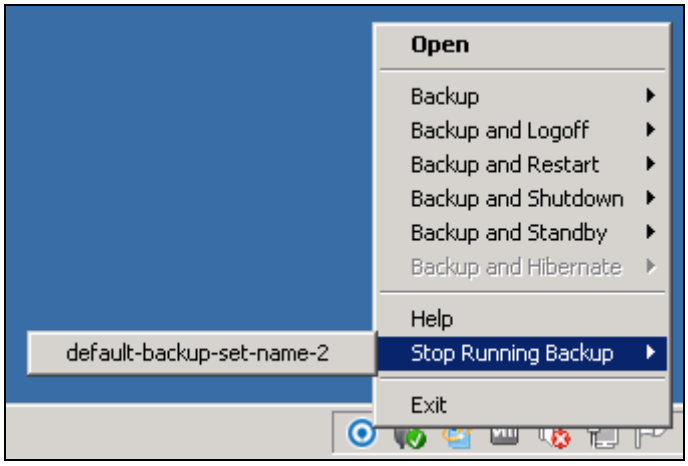
Help

This tab will show you the function of each backup option.

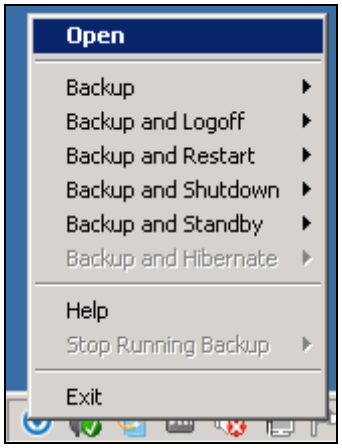


Stop Running Backup

Use this option if you wish to stop a running manual, continuous or scheduled backup.

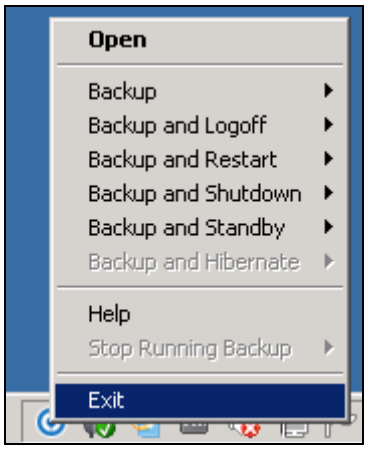


This option will be disabled if there is no backup job running.



Exit

Select this option if you want to close the application including the AhsayOBM icon at the taskbar.

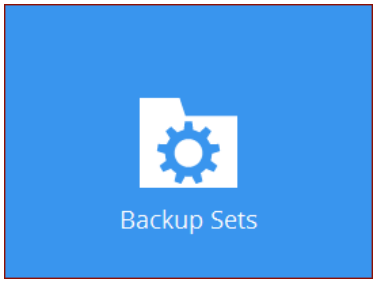


11 Create a Backup Set

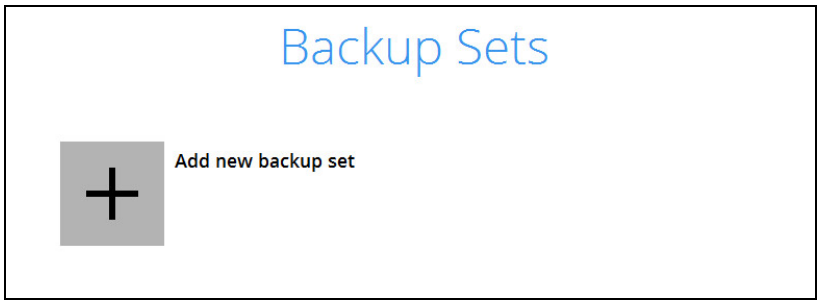
Starting with v8.3.4.0 and onwards, network drive support has been enhanced which will allow users to access different network drives not limited to Windows-based backup source. This enhancement will support:

- Network drives with different login credentials instead of limited to Windows User Authentication login or network drives without login credential.
- Network drives without the need for them to be setup first on Windows.
- Network drives as Backup Source (including filter), Backup Destination and Restore Location (Original or Alternate).

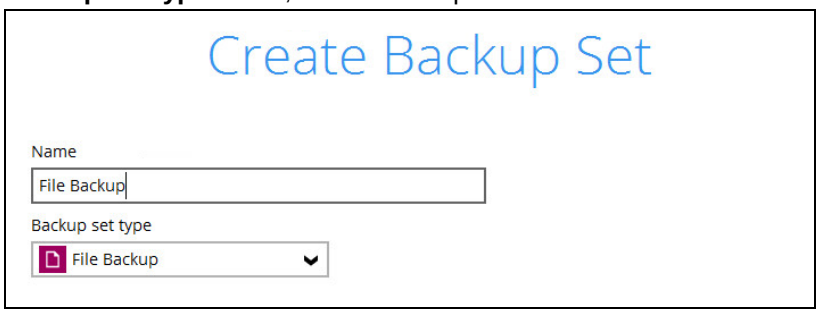
1. Click the **Backup Sets** icon on the AhsayOBM main interface.



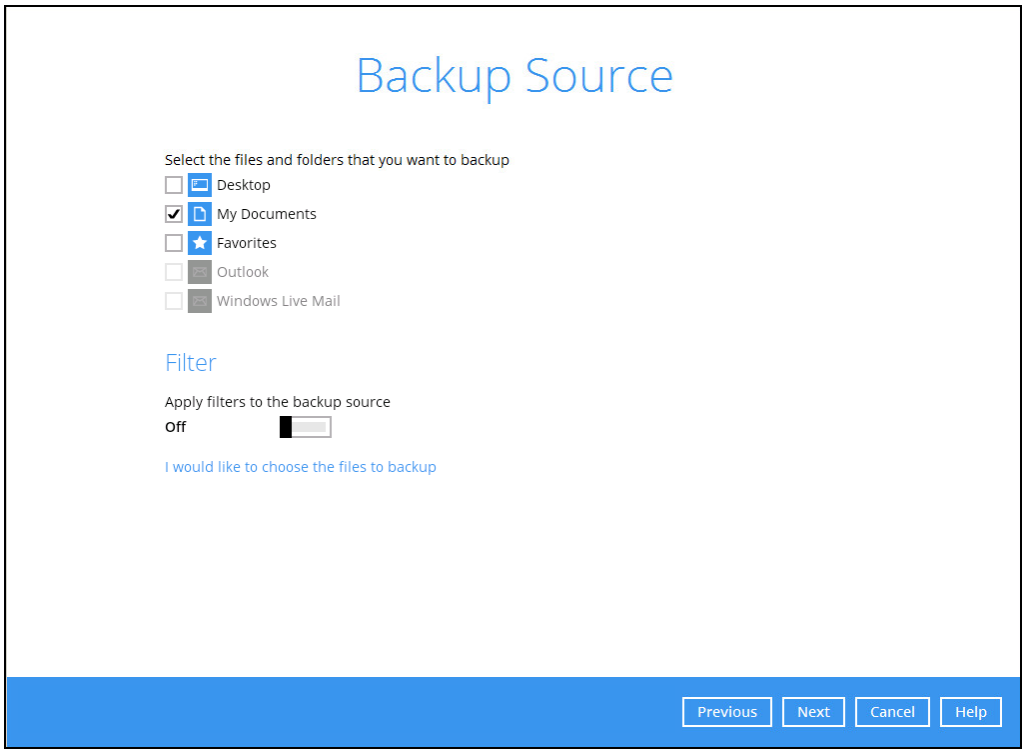
2. Create a new backup set by clicking the "**+**" icon next to **Add new backup set**.



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

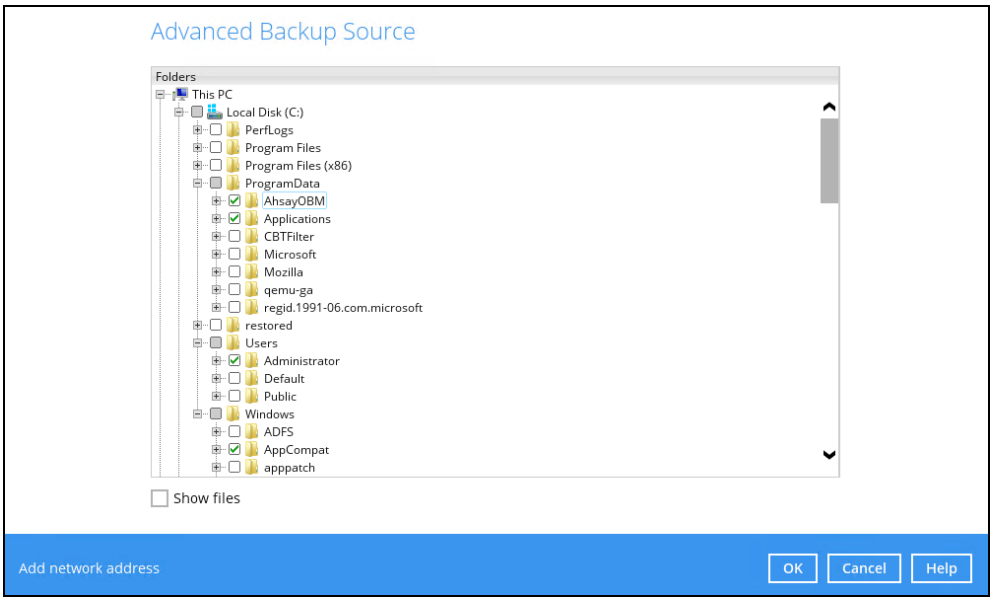


4. In the Backup Source window, select the files and folders for backup. Click **I would like to choose the files to backup** to select individual files for backup.

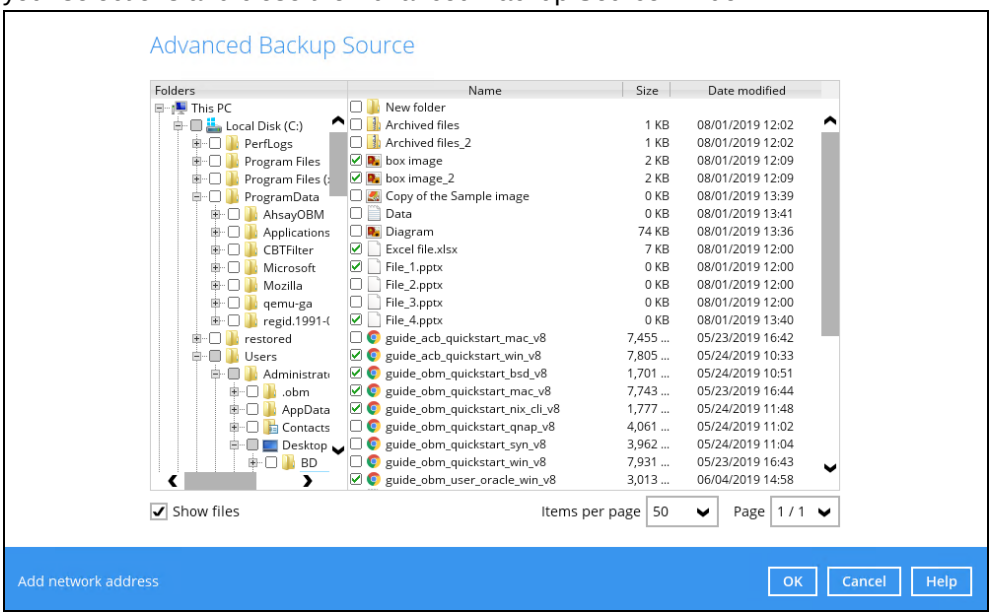


5. In the Advanced Backup Source window there are three (3) ways to select file(s) and folder(s) for back up:

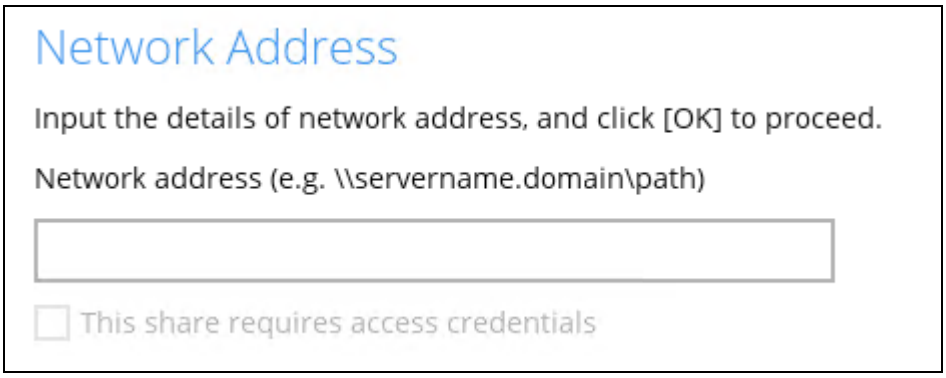
   i. Select folder(s) to back up all files in the folder(s). Click **OK** to save the selection and close the Advanced Backup Source window.



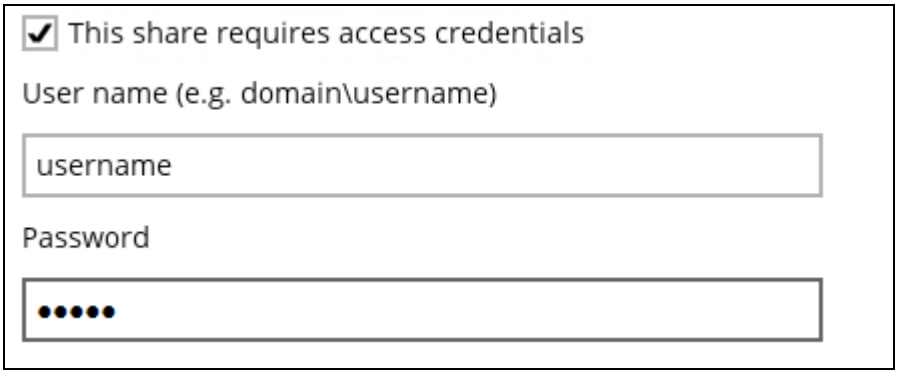
ii. Back up only individual file(s) instead of all files in the selected folder(s). Check the **Show files** checkbox at the bottom of the screen. A list of files will appear on the right-hand side. Select the checkbox(es) next to the file(s) to back up. Then, click **OK** to save your selections and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



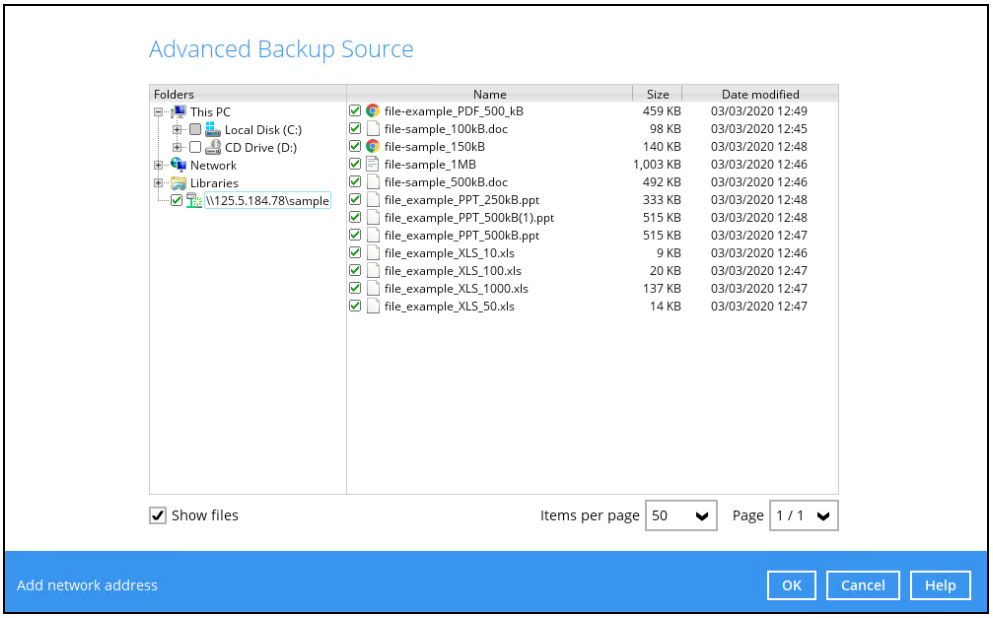
iii. Back up file(s) and/or folder(s) located in a network drive. Click the **Add network address** link at the botton of the screen. In the Network Address window, enter the network address.



Once a network address is entered, **This share requires access credentials** will be enabled. Check the box beside it if access credentials are required to backup and enter the User name and Password. Otherwise leave it unchecked and click **OK**.



The network drive will now be added and automatically selected. There is still an option to select only specific file(s) to back up by checking the **Show files** checkbox. Click **OK** to save your selections and close the Advanced Backup Source window.



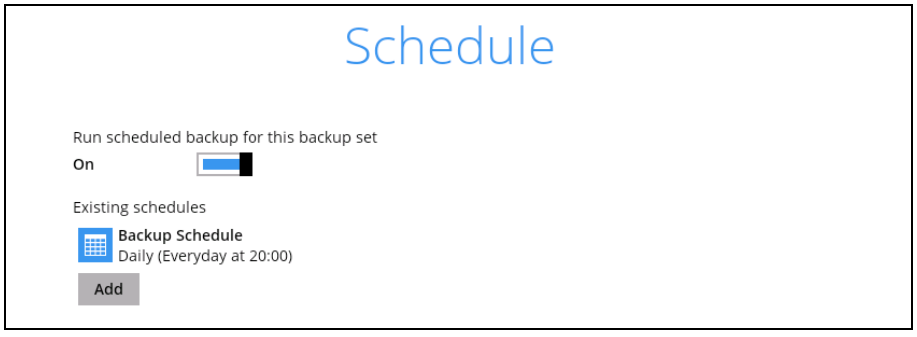
NOTE

Once a network drive is added, its network credentials may still be edited. For instructions on how to do this please refer to Appendix F: How to Manage non-Windows based Network Drives.

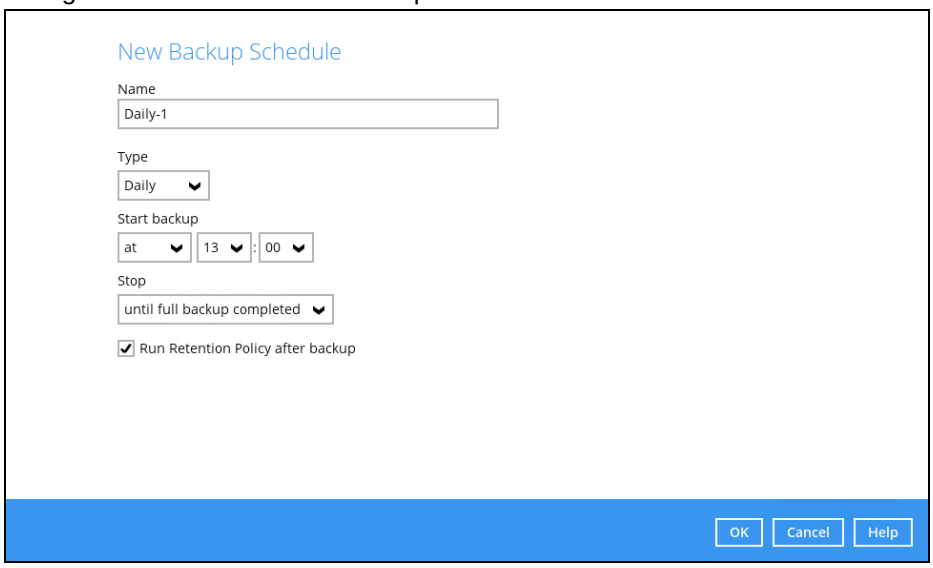
6. In the Backup Source window, click **Next** to proceed.

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

   - In the default backup schedule, there will be a scheduled backup that will be performed daily at 8pm. You can leave it as is or you can modify it by clicking on the existing backup schedule.

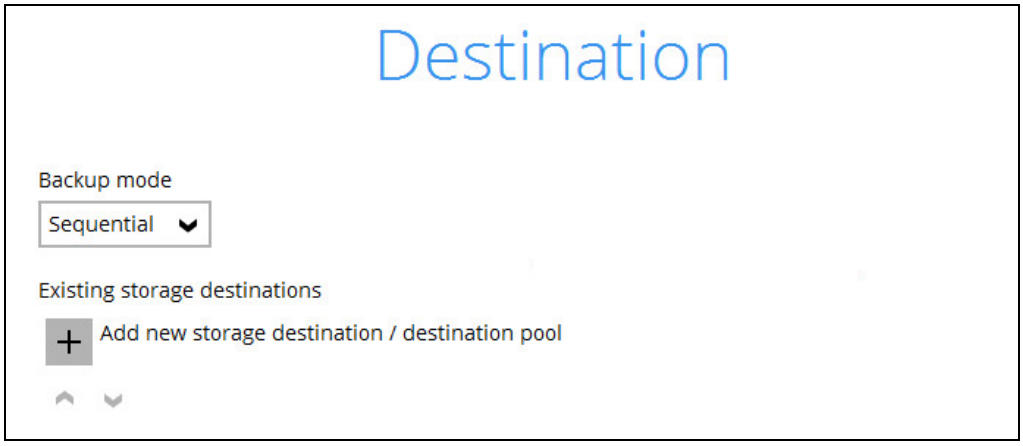


If you want to add another schedule, click Add. When the New Backup Schedule window appears, specify your backup schedule. Then, click **OK** to save your changes and close the New Backup Schedule window.



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

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

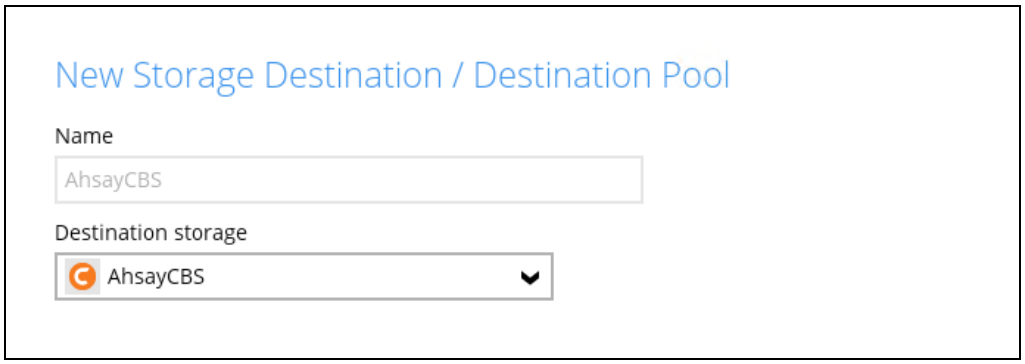


Select the appropriate option from the **Backup mode** dropdown menu.

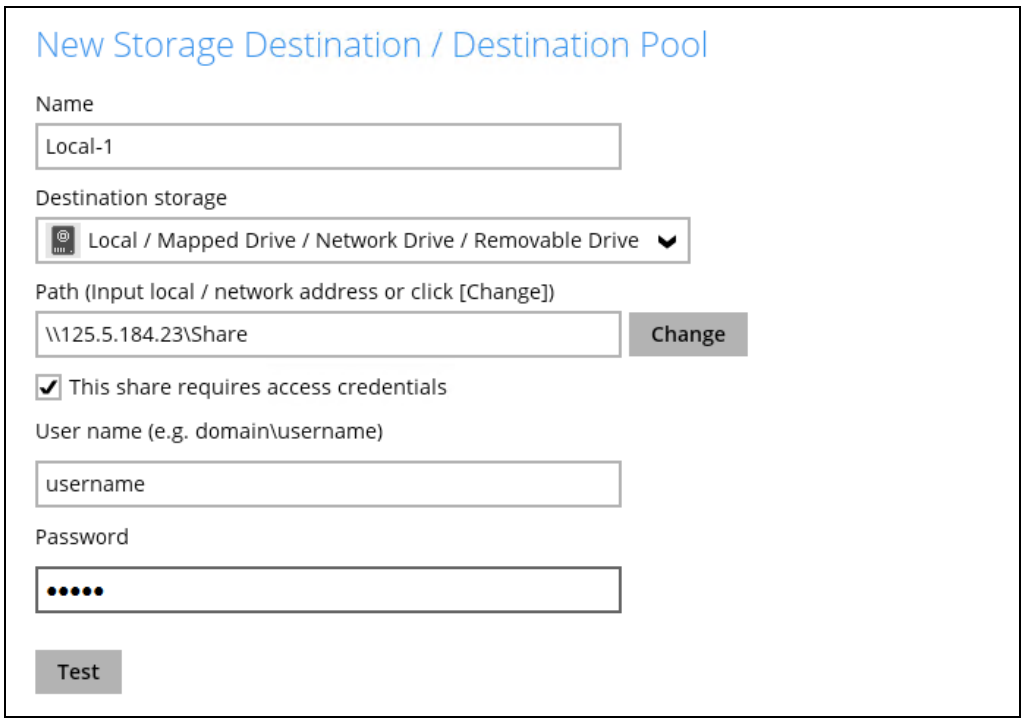
- **Sequential** (default value) – run backup jobs to each backup destination one by one
- **Concurrent** – run backup jobs to all backup destinations at the same time

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

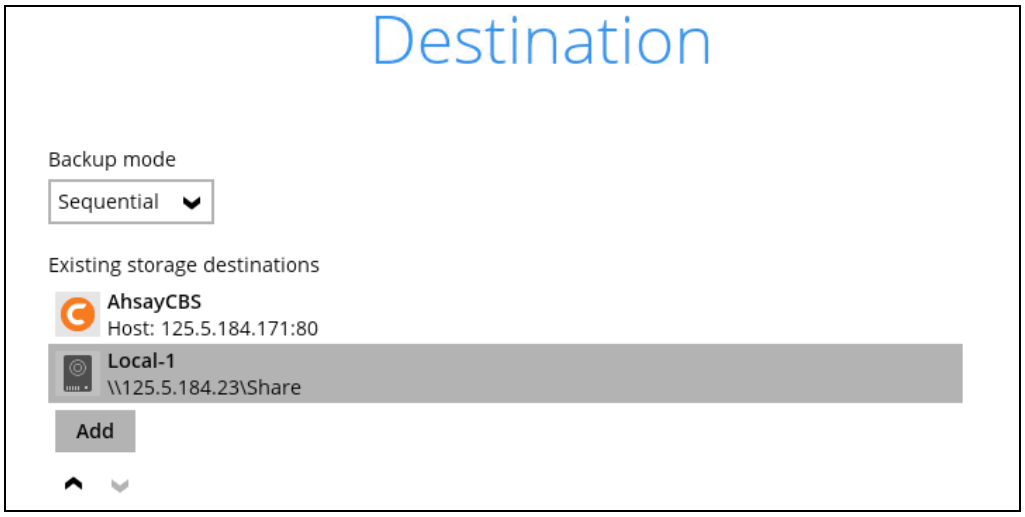
10. In the **New Storage Destination / Destination Pool** window, select the destination storage. Then, click **OK** to confirm your selection.



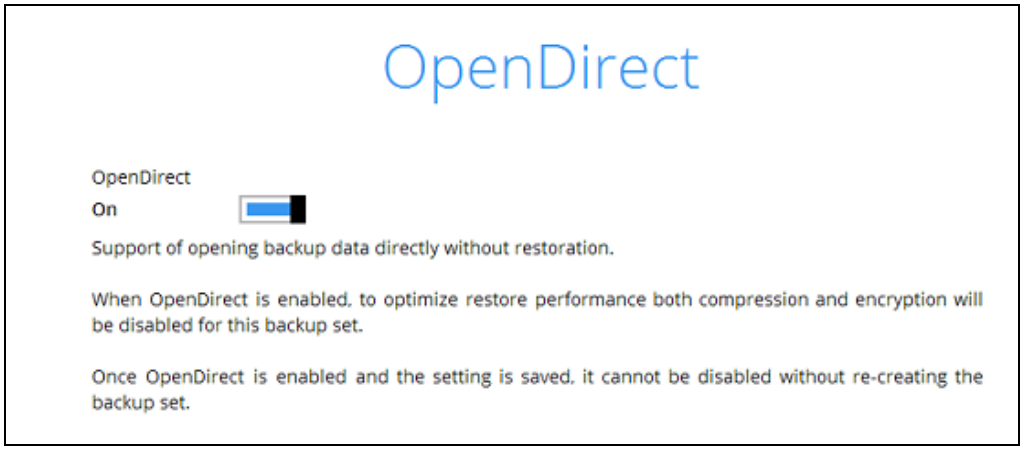
If **Local / Mapped Drive / Network Drive / Removable Drive** is selected, you need to specify the path by clicking **Change** to select the path or you can manually enter it. Once a network address is entered, **This share requires access credentials** check box will be enabled. Check the box beside it if access credentials are required to connect to the storage destination and enter the User name and Password. Otherwise, leave it unchecked and click **Test** to check the connection. Click **OK** to add the storage destination.



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



12. If you wish to enable the **OpenDirect Restore** feature, make sure you turn on the OpenDirect restore switch in this menu. Click **Next** to proceed.

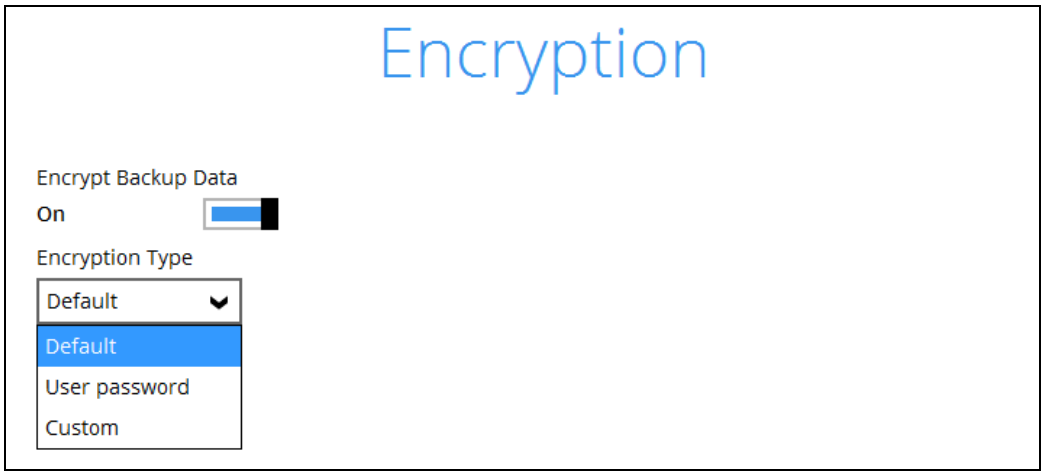


NOTES

1. Once the OpenDirect Restore feature is enabled and the backup set is saved, it is **NOT** possible to disable it afterwards, and vice versa. A new backup set will have to be created again if you wish to do so.
2. It is possible to enable both OpenDirect restore and Run Direct restore at the same time. However, AhsayOBM restore job will only allow either OpenDirect or Run Direct to run, but not to run concurrently.
3. OpenDirect restore requires an additional OpenDirect restore module license to work. Contact your backup service provider for further details.
4. OpenDirect restore might not be available, this depends on your backup service provider settings. Contact your backup service provider for more information.

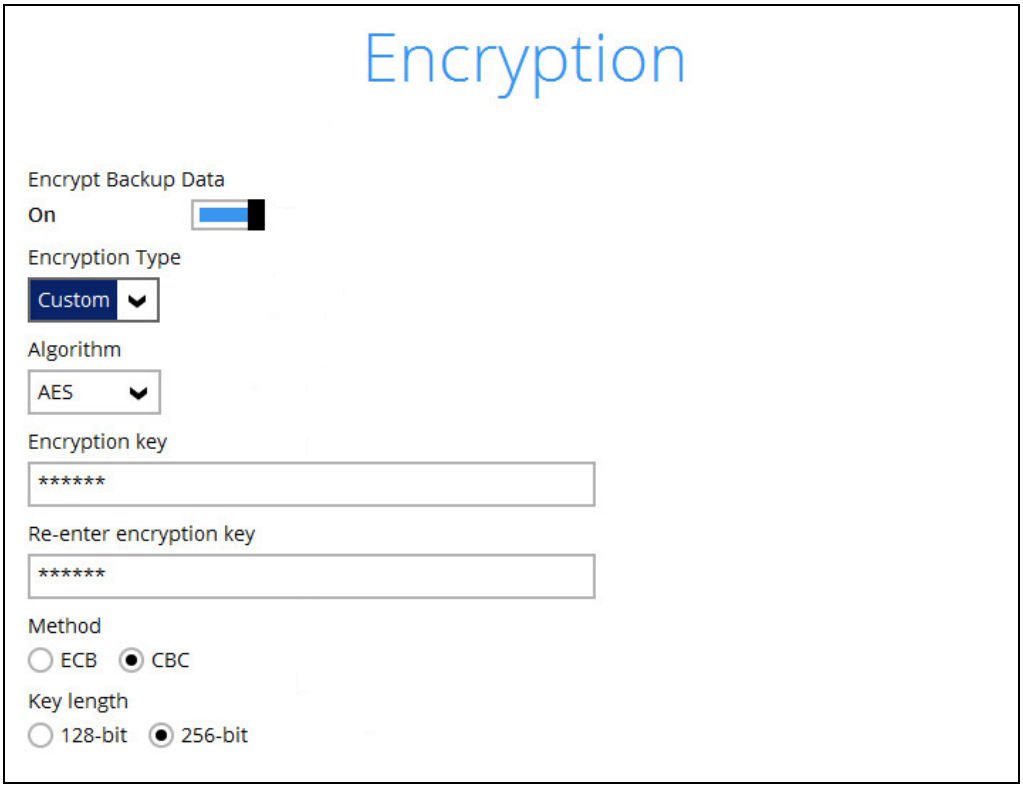
13. **IMPORTANT:** If you have enabled the OpenDirect Restore, backup data will not be compressed and encrypted to optimize restore performance, therefore you can skip to step 16.

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



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

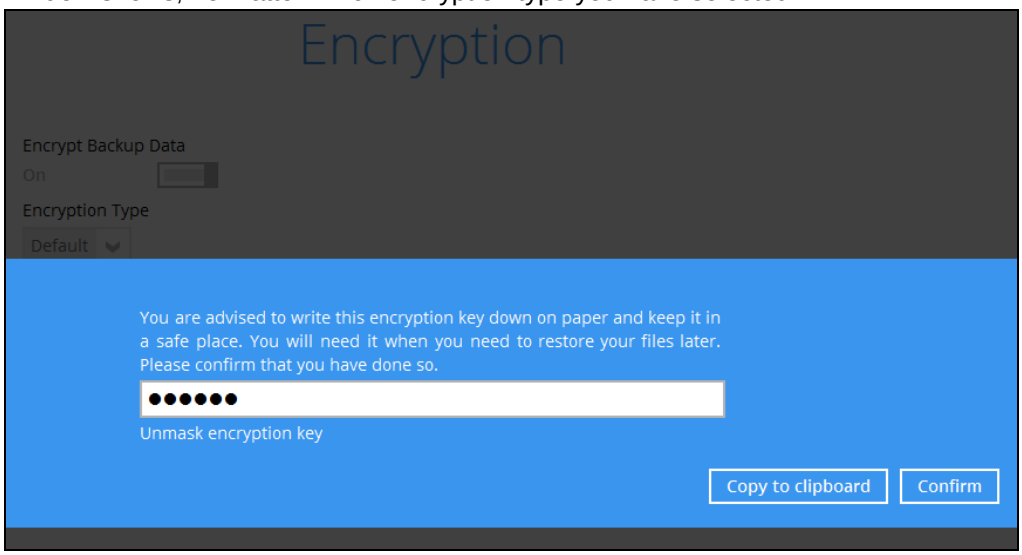
    - **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
    - **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM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



NOTE: For best practice on managing your encryption key, refer to the following Wiki article. http://wiki.ahsay.com/doku.php?id=public:8015_faq:best_practices_for_managing_encryption_key

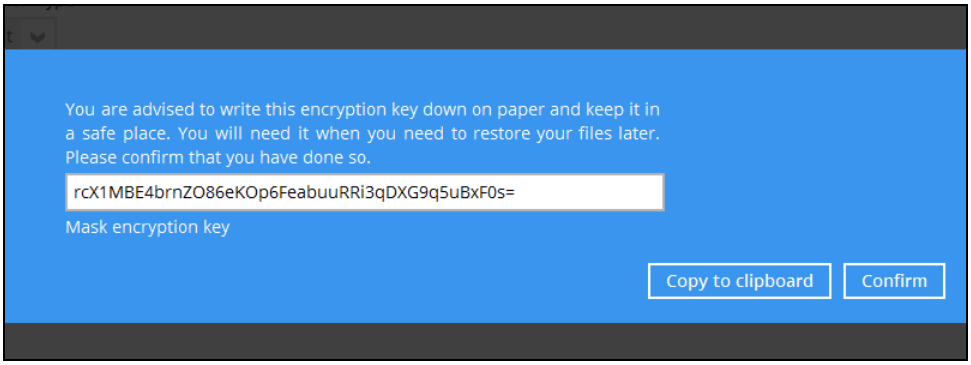
Click **Next** when you are done setting.

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



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

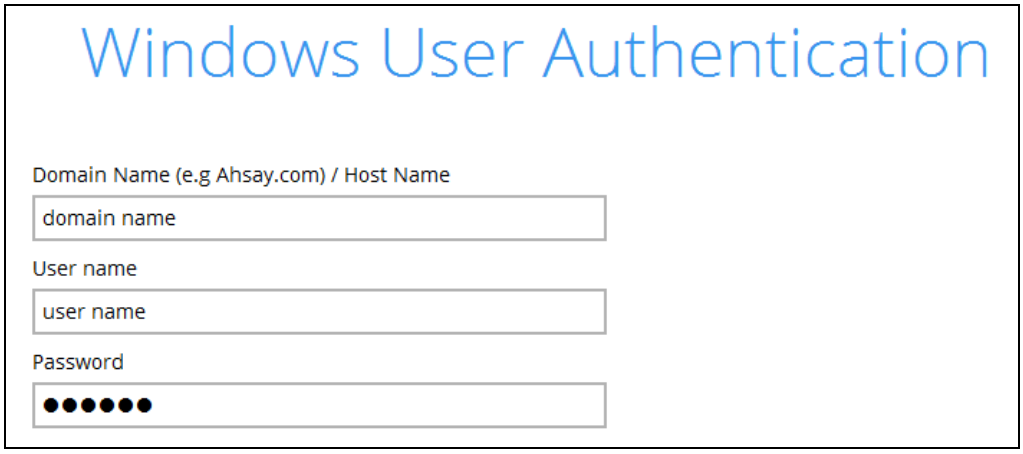
- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



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

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

15. The following screen prompts you to enter the Windows login credentials for user authentication if you have enabled the Schedule Backup feature in step 8.

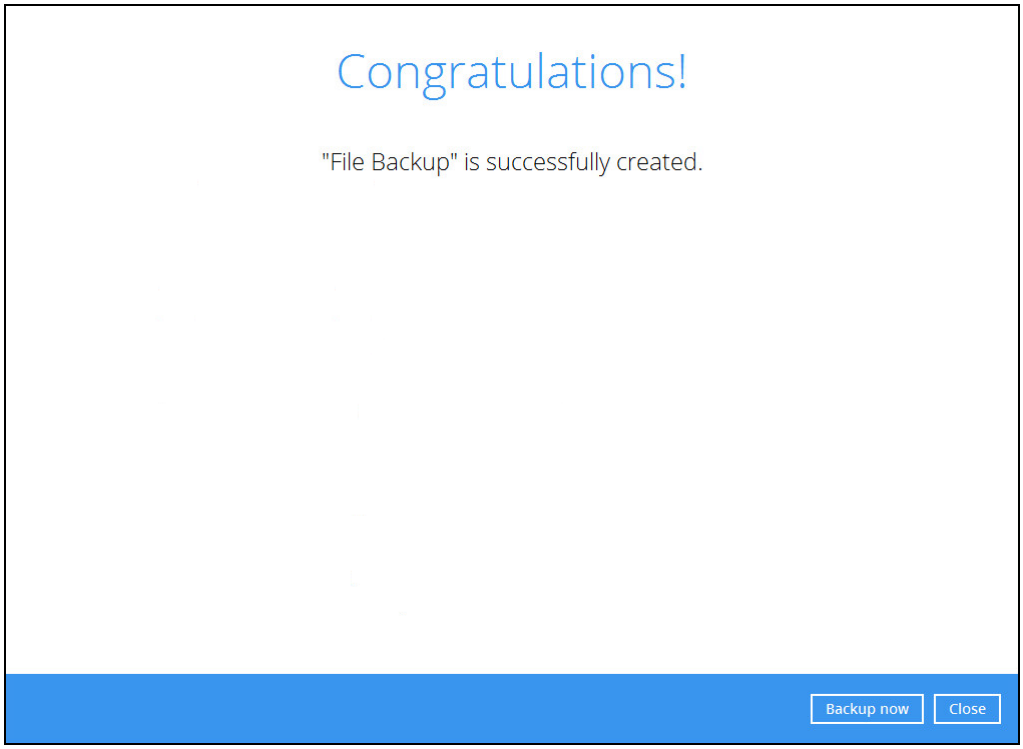


NOTE

If you have selected to back up individual folder(s) / file(s) on your local computer's drive in step 5, the Windows User Authentication request will be bypassed and therefore the screen shown above will not display even though the Schedule Backup feature has been turned on.

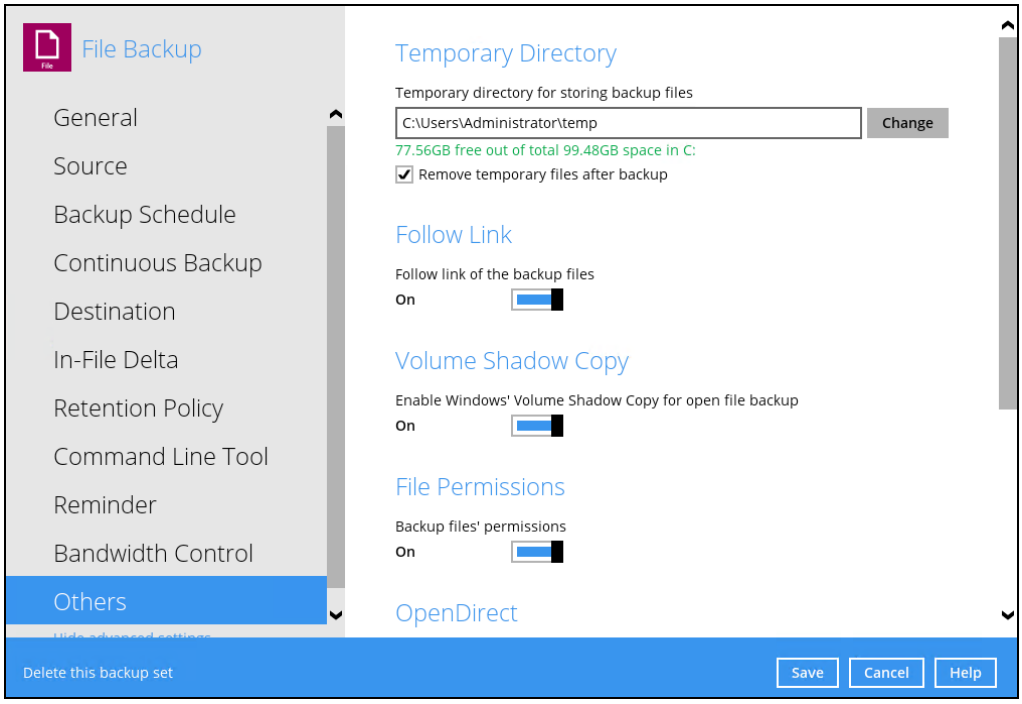
It is recommended to enter the information of user with Administrator privilege to support backup of network drives.

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. Based on Best Practices and Recommendations, it is highly recommended to change the **Temporary Directory**. Select another location with sufficient free disk space other than Drive C.

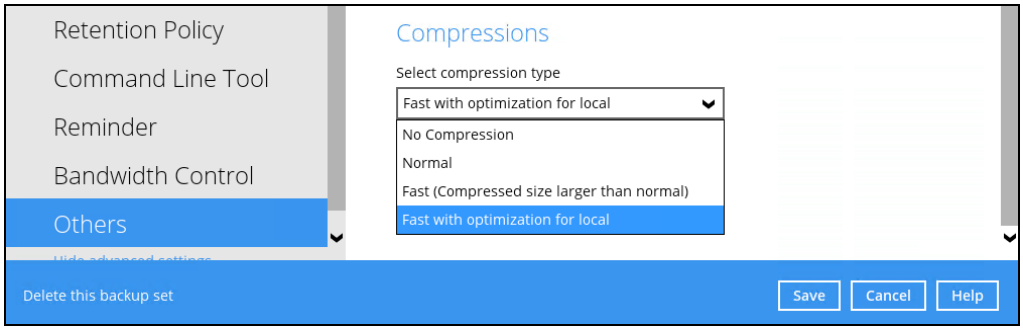
Go to **Others > Temporary Directory**. Click **Change** to browse for another location.



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

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

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



12 Overview on the 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)**

12.1 Periodic Data Integrity Check (PDIC) Process

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

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

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

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

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

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

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

2	**Wednesday**

In this example:

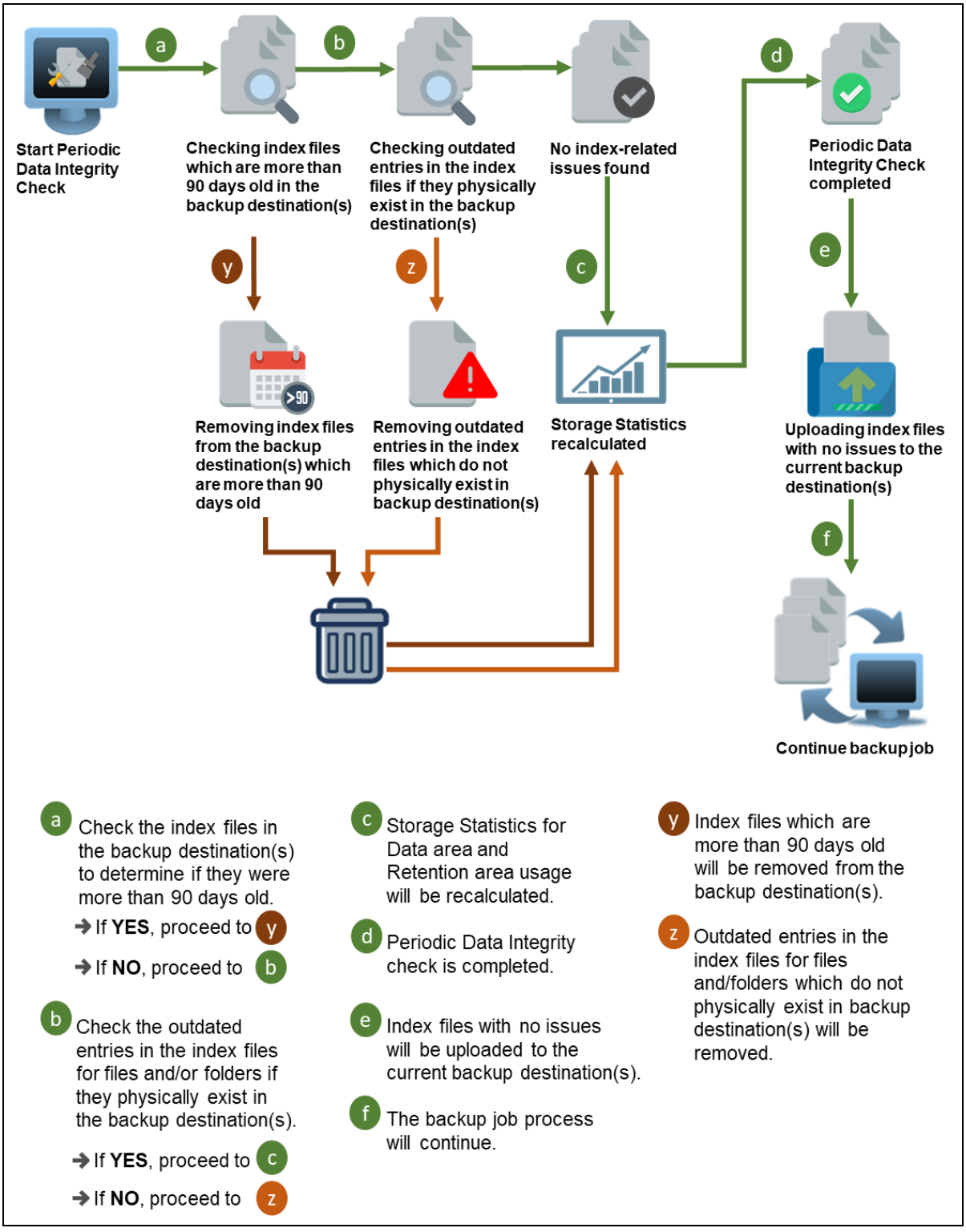
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTES

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

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

1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it detects that the previous PDIC job was run more than 7 days ago.
3. Every time a data integrity check (DIC) is run, the latest PDIC run date is reset, the next PDIC job will run after 7 days.
4. The PDIC job will not run if there are no files in both the data and retention areas. For example: a newly created backup set with no backup job history or a backup set where all the data has been deleted using the Delete Backup Data feature.
5. The PDIC job will not run on a backup set that contains any data which still in v6 format. It will only run if all v6 data format on a backup set has undergone data migration to v8 block format.



a Check the index files in the backup destination(s) to determine if they were more than 90 days old.

➔ If **YES**, proceed to y

➔ If **NO**, proceed to b

b Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).

➔ If **YES**, proceed to c

➔ If **NO**, proceed to z

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

d Periodic Data Integrity check is completed.

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

f The backup job process will continue.

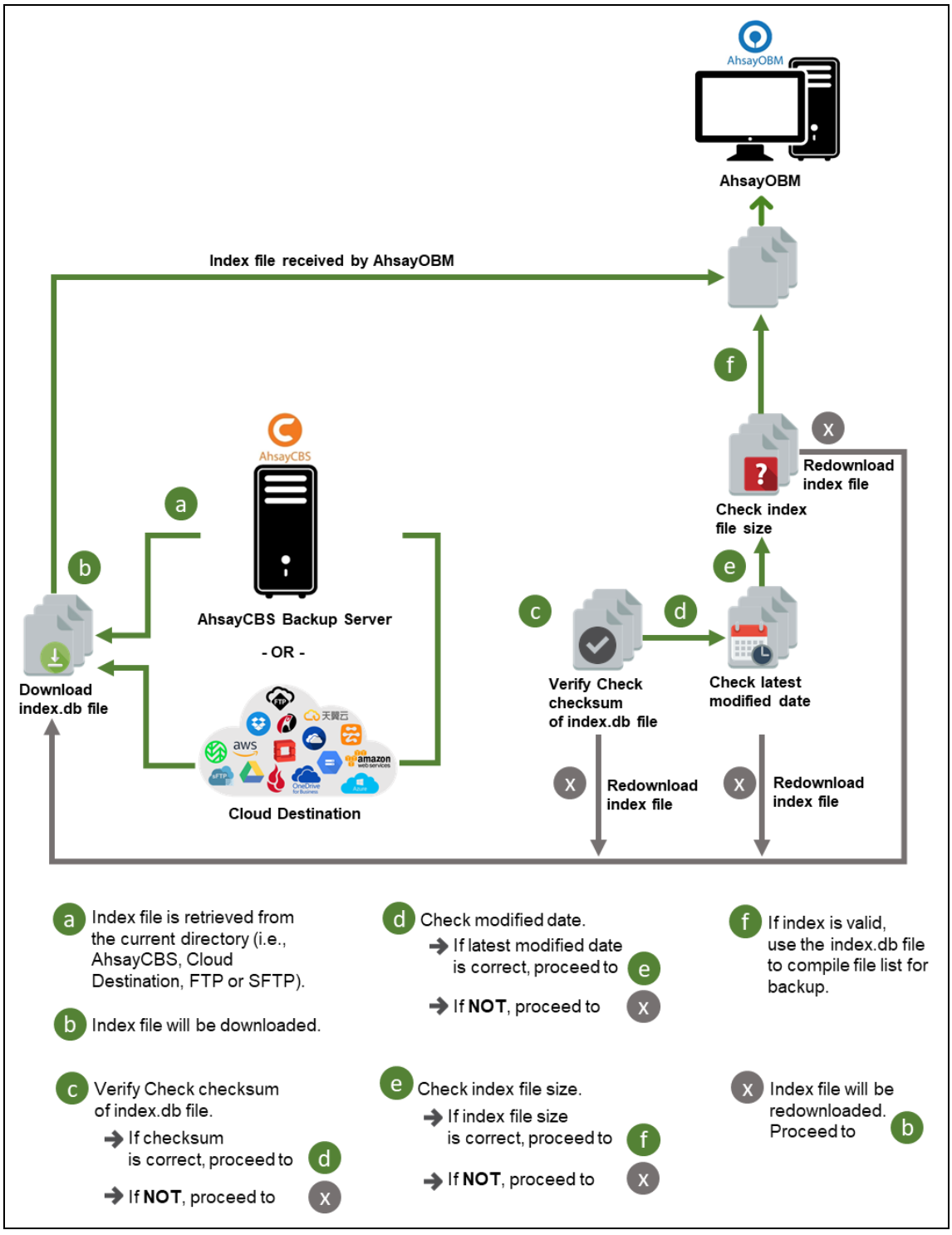
y Index files which are more than 90 days old will be removed from the backup destination(s).

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

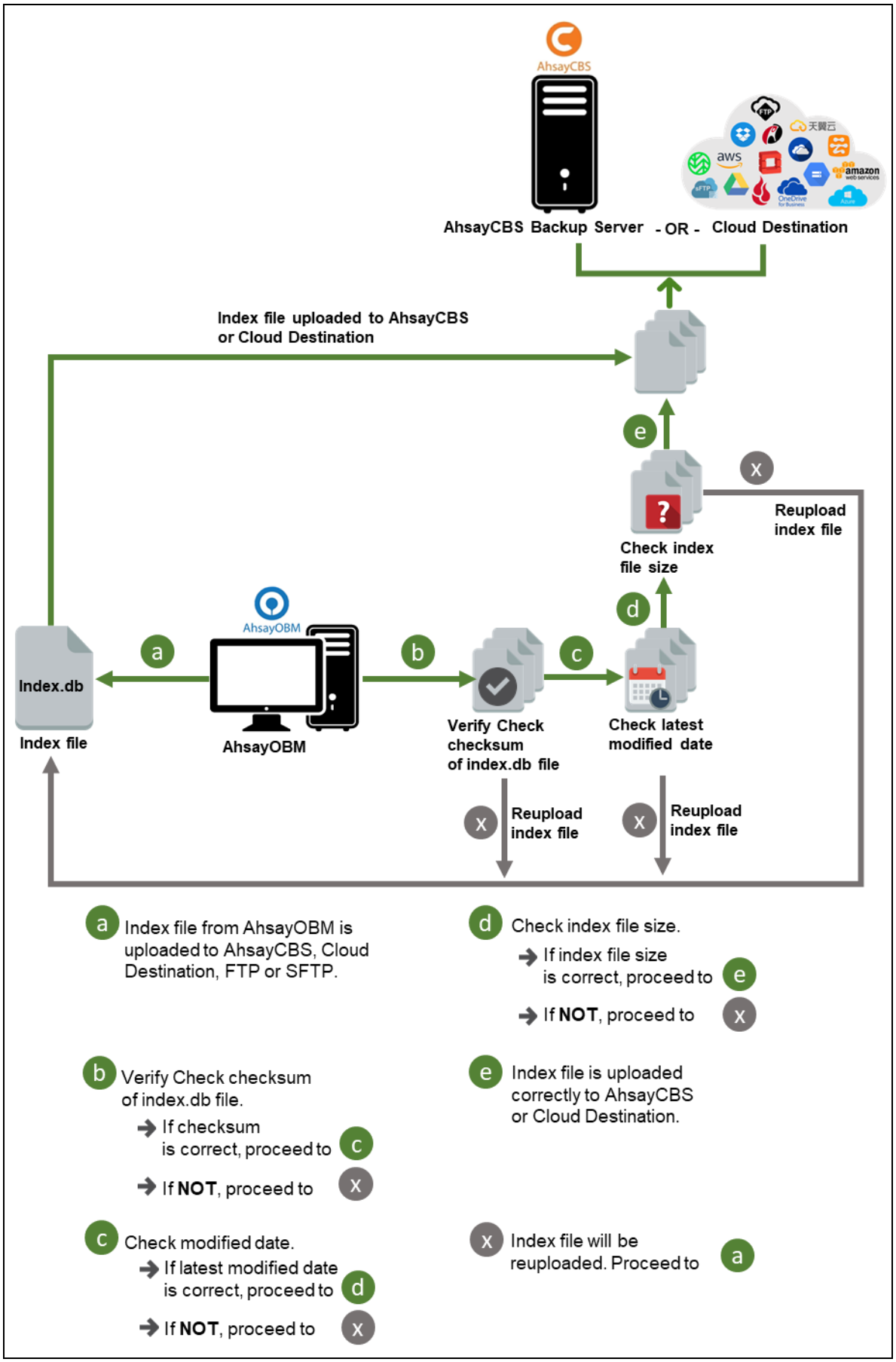
12.2 Backup Set Index Handling Process

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.

12.2.1 Start Backup Job

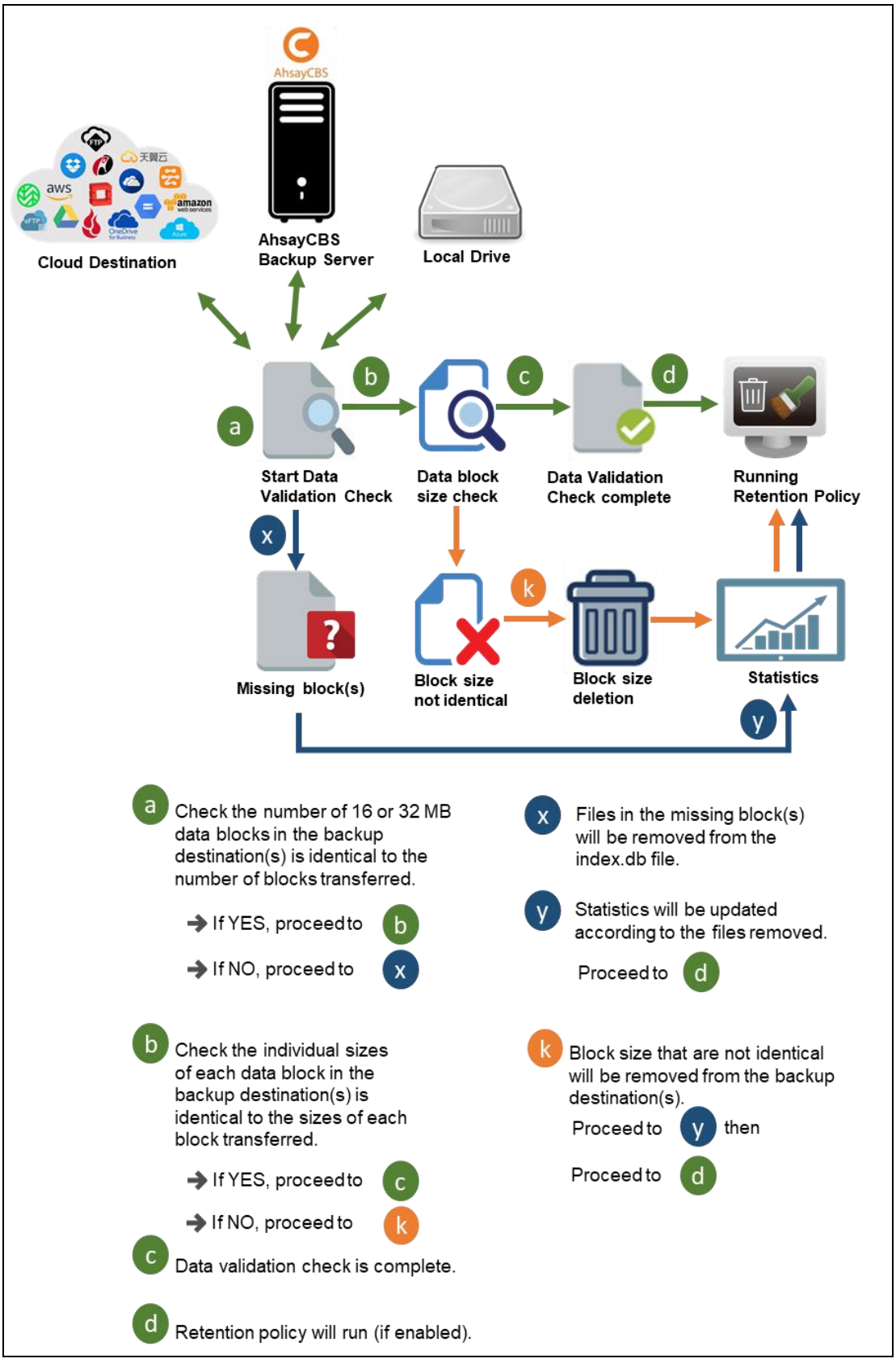


12.2.2 Completed Backup Job



12.3 Data Validation Check Process

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



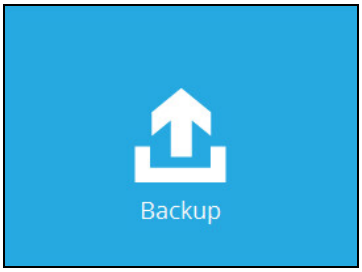
13 Run Backup Jobs

13.1 Login to AhsayOBM

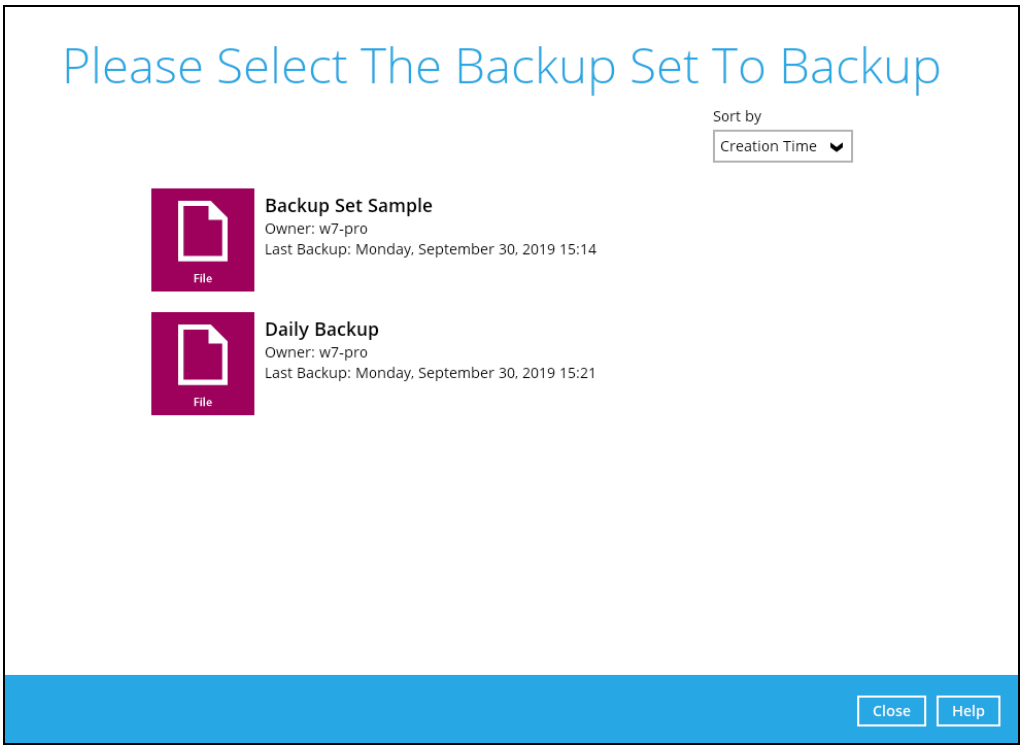
Login to the AhsayOBM application according to the instructions in Chapter 8 Logging in to AhsayOBM.

13.2 Start a Manual Backup

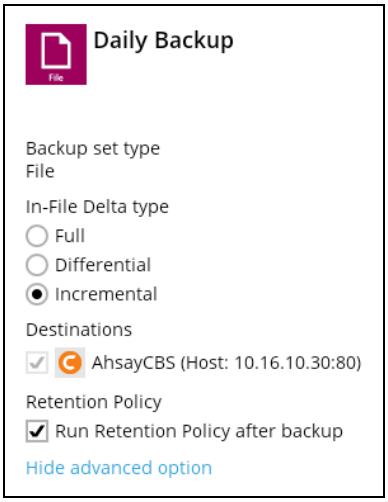
1. Click the **Backup** icon on the main interface of AhsayOBM.



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

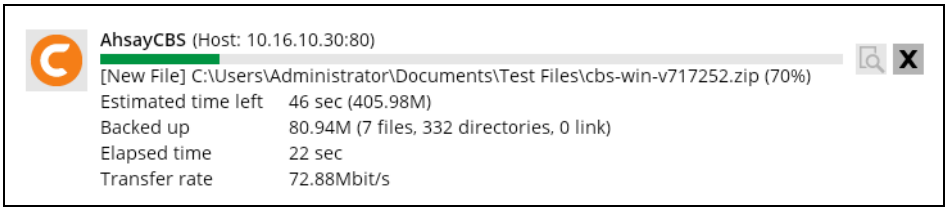


When advanced options are shown, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** in the Retention Policy section at the bottom. This will help you save hard disk quota in the long run. In the In-File Delta type section, the following three options are available:

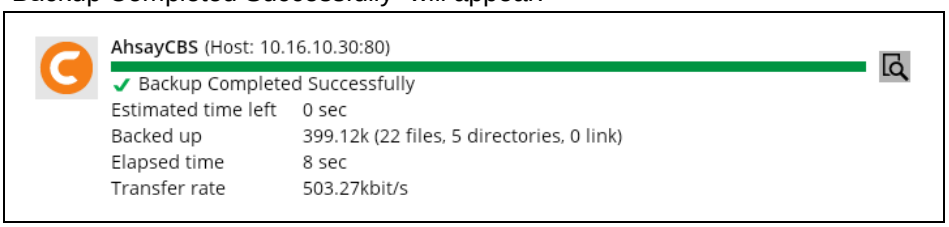


- **Full** – A full backup captures all the data that you want to protect. When you run a backup job for the first time, AhsayOBM will run a full backup regardless of the in-file delta setting.
- **Differential** – A differential backup captures only the changes made as compared with the last uploaded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

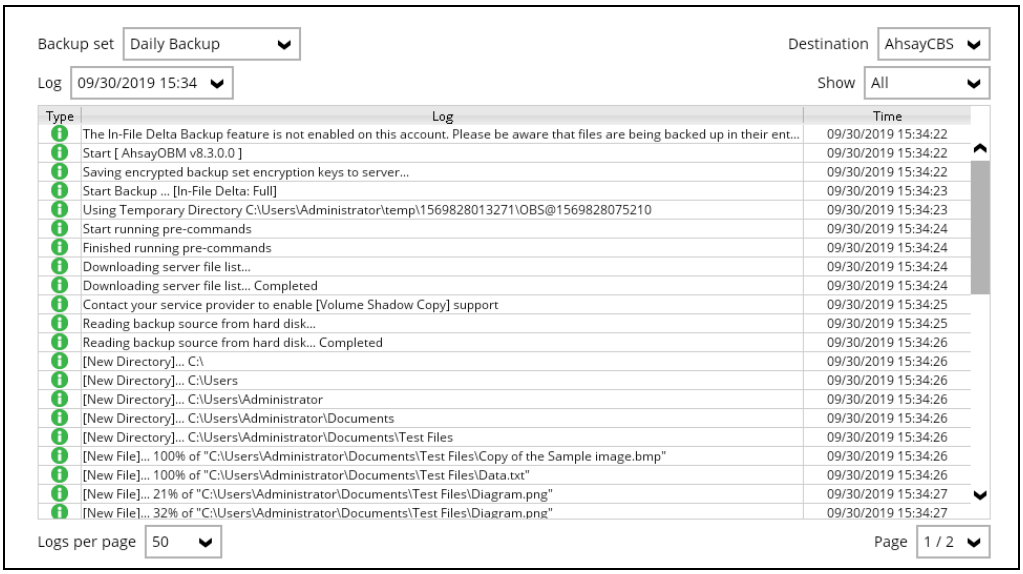
3. Click Backup to start the backup job. The status will be shown.



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



You can click the **View** icon on the right-hand side to check the log. A window will pop up to show the log. Click **Close** to exit the pop-up window.



14 Restore Data

14.1 Restore Method

There are two restore methods available, the traditional restore and OpenDirect restore. OpenDirect restore applies only to File backup sets with OpenDirect feature enabled.

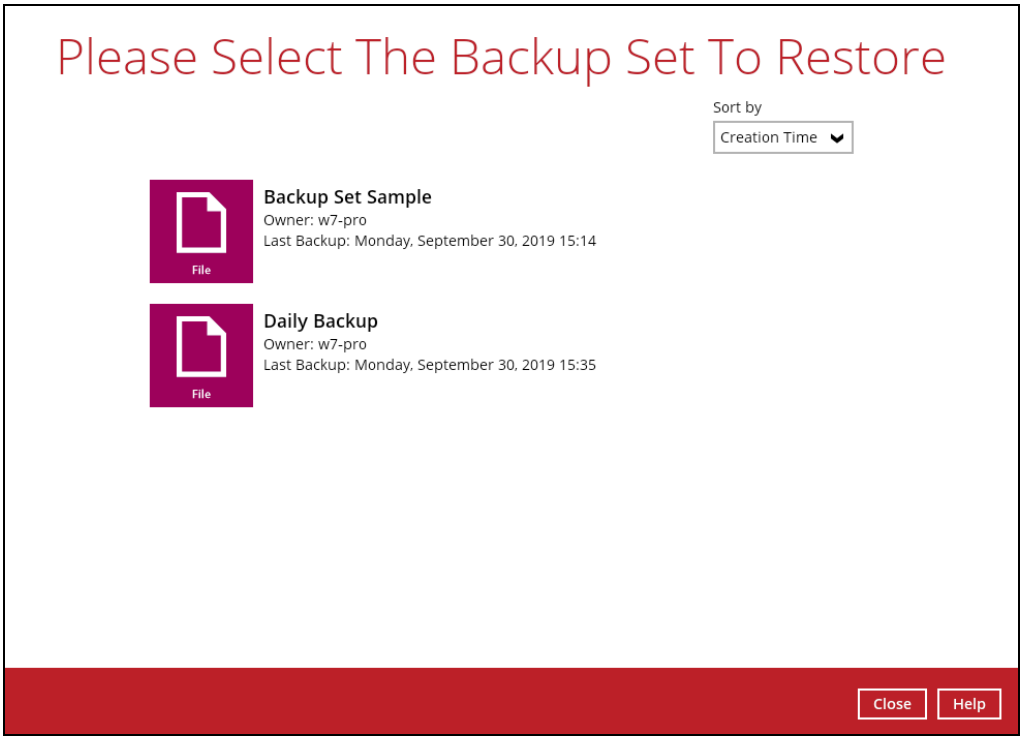
For more details on the differences of the two restore methods, refer to Benefits of using OpenDirect Restore.

14.1.1 Traditional Restore

1. Log in to the AhsayOBM application according to the instructions in section Chapter 8 Logging in to AhsayOBM.

2. Click the **Restore** icon on the AhsayOBM main interface.

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



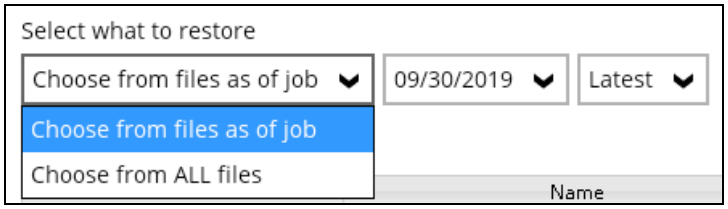
4. Select where you would like to restore your data from.

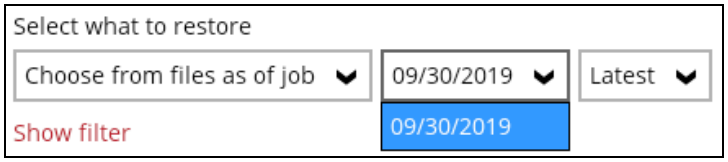
5. Select **Normal restore**.

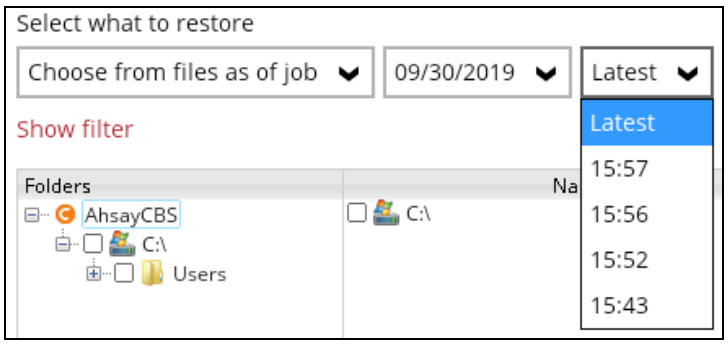
6. Select to restore files from a specific backup job, or from all files available, then select the files or folders that you would like to restore.

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

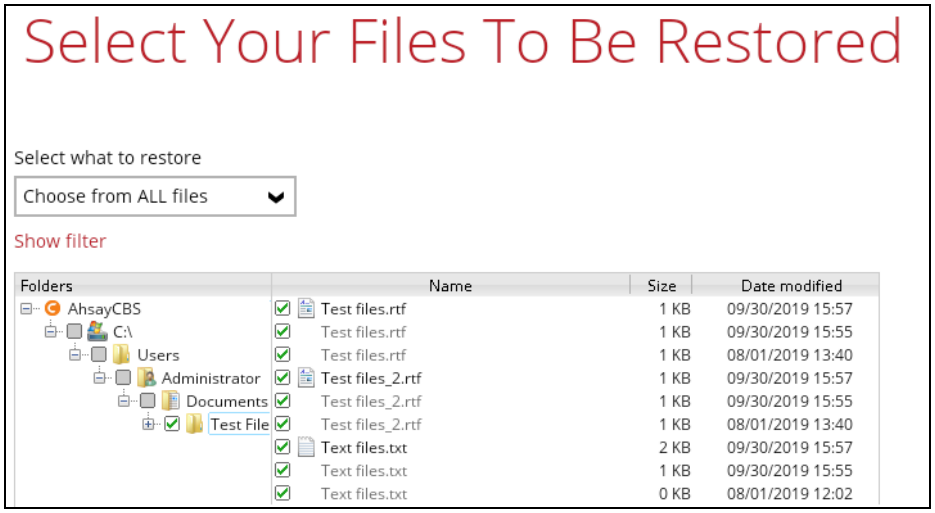
   Choose from files as of job – This option allows you to select a backup version from a specific date and time to restore.



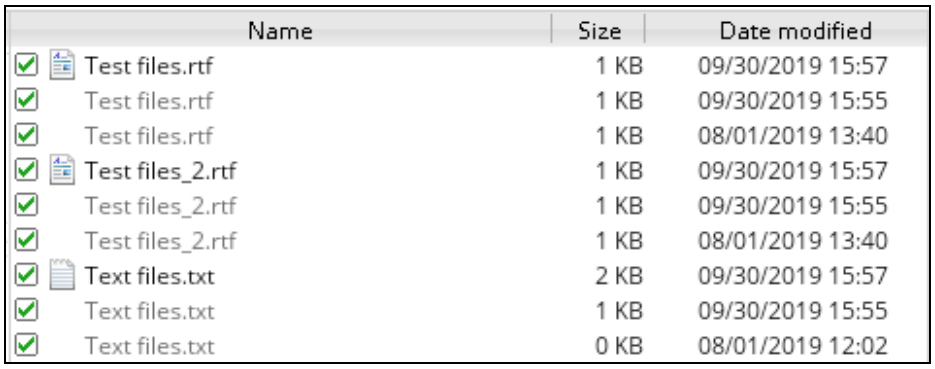




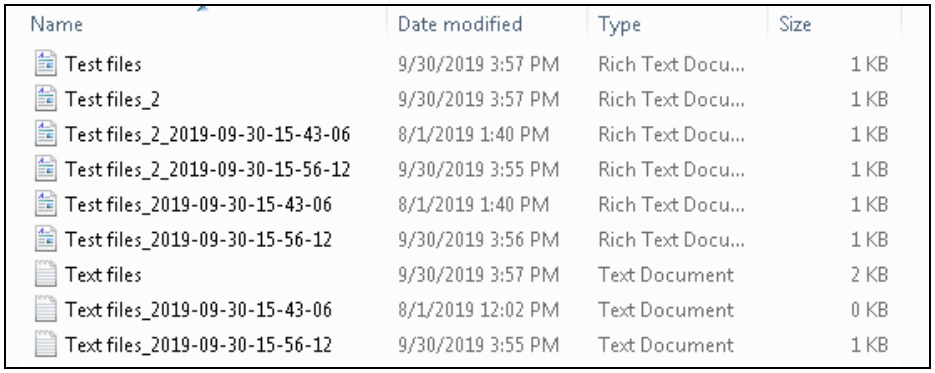
- **Choose from ALL files** – This option allows you to restore all the available backup versions for this backup set. Among all the available backup versions, you can even select only some of the backup versions of a file to restore.



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



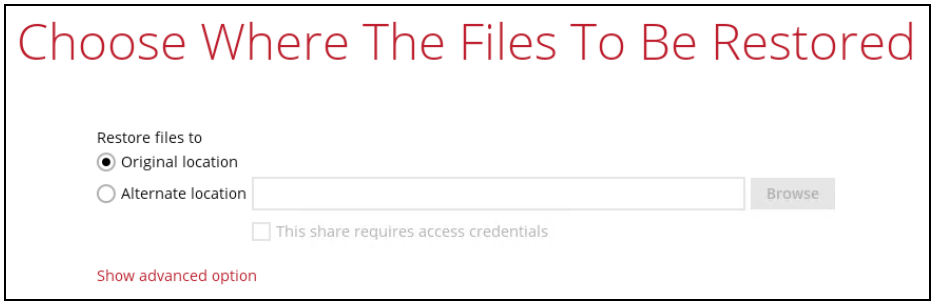
When the restore is done, you will see all the selected backup versions in the restore destination. The latest backup version has the file name as the original file, while the previous versions have the time stamps added to their file names for easy identification.



7. Click the **Show files** checkbox to select individual files for restoration. Click **Next** to proceed when you are done with the selections.

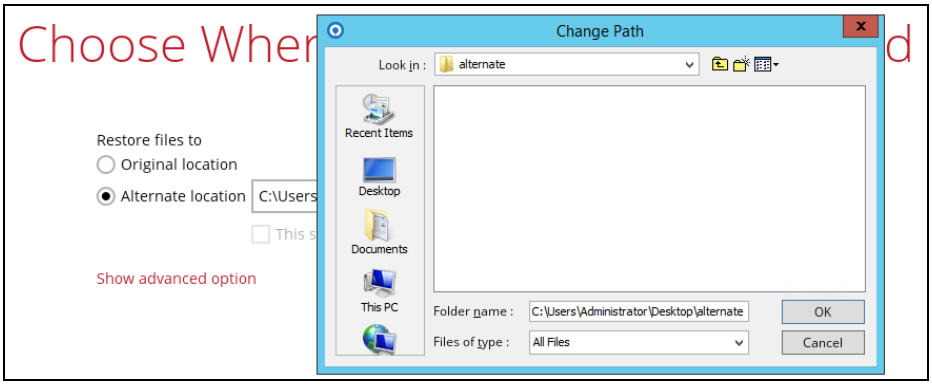
8. Select to restore the files to their **Original location**, or to an **Alternate location**. Then, click **Next** to proceed.

Original location – The backed up data will be restored to the computer running AhsayOBM under the same directory path as on the machine storing the backup source. For example, if the backup source files are stored under **Users/[User's Name]/Downloads** folder, the data will be restored to **Users/[User's Name]/Downloads** as well on the computer running AhsayOBM.

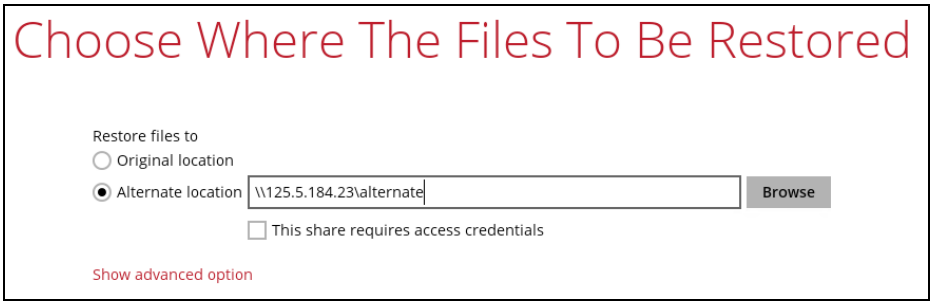


Alternate location – You can choose to restore the data to a location of your choice on the computer where AhsayOBM is running or to a network drive.

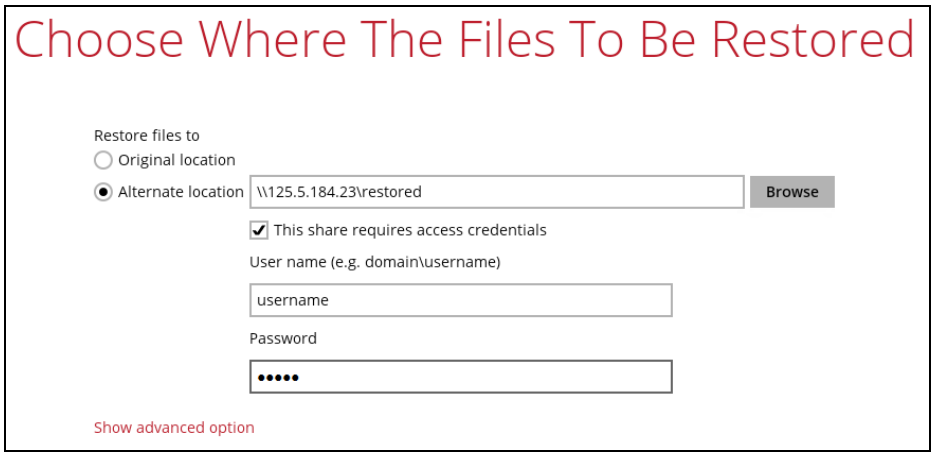
i. To restore to a location of your choice on the computer where AhsayOBM is running, click Browse. Select the location and click **OK**.



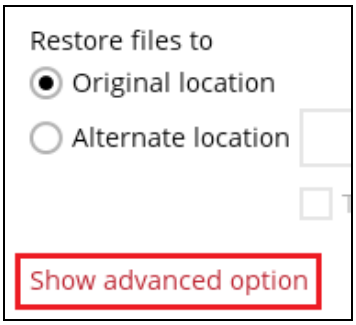
ii. To restore to a network drive, enter the network address where you want the backup files to be restored.

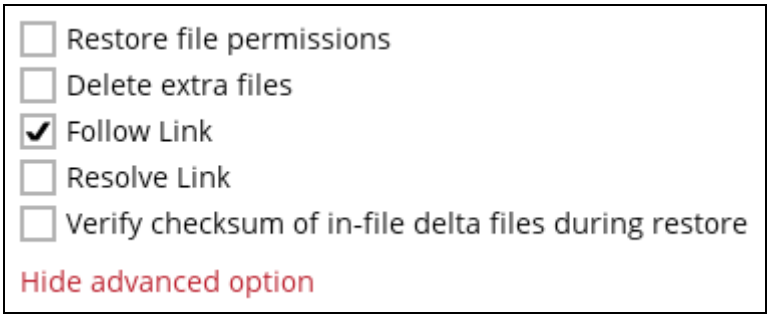


Check the box beside **This share requires access credentials** if the network drive was set up with password. Enter the User name and Password.



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





- **Restore file permissions**

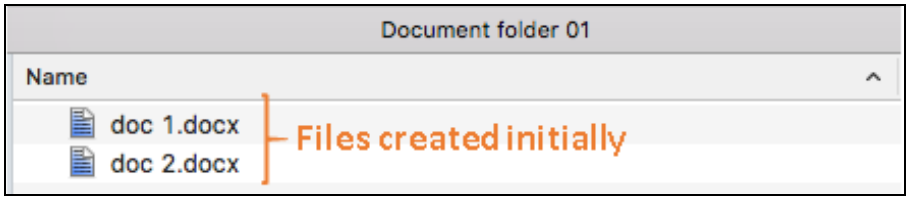
  Restore file permissions are disabled by default. When you perform a file restore on shared files or folders using a shared computer, it is recommended that you enable Restore file permissions by ticking the checkbox so that the files restored will not be fully accessible to everyone using the shared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

- **Delete extra files**

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

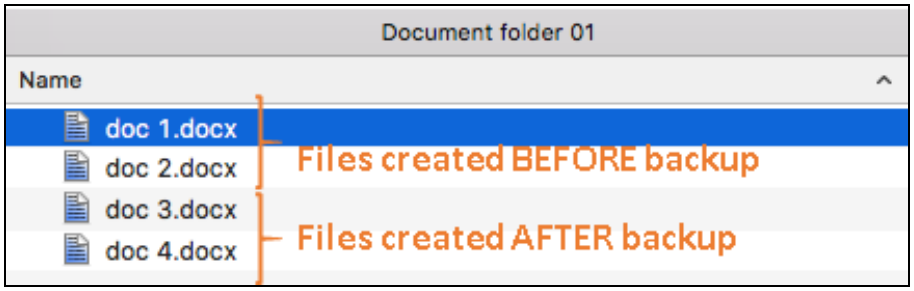
Example:

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



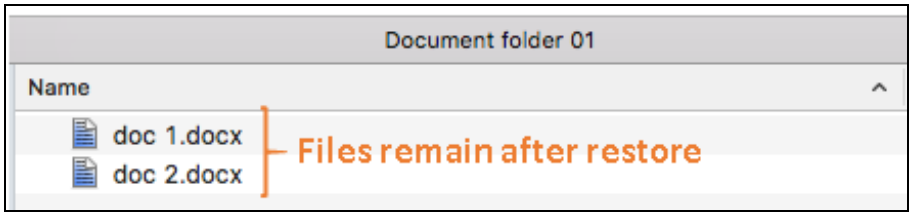
ii) A backup is performed for folder **Document folder 01**.

iii) Two new files are created, namely doc 3 & doc 4.



iv) A restore is performed for the **Document folder 01**, with **Delete extra files** option enabled.

v) Since doc 3 & doc 4 have never been backed up, therefore they will be deleted from **Document folder 01**, leaving only the two files that have been backed up.



WARNING

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

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

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

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

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

Follow Link	Restore to	Behavior
Enabled	**Original location**	Symbolic link or junction point is restored to the original backup location.

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

- **Resolve link (Only for restoring to Alternate Location)**

This option must be used in conjunction with the **Follow Link** option. When this option is enabled, the symbolic link, as well as the directories and files that the symbolic link links to will also be restored in the alternate location you have chosen. That means the symbolic link will point to the alternate location instead of the original location.

The table below summarizes the behaviors when a restore is performed with this option turned on and off.

Resolve Link	Behavior
Enabled	Symbolic link is restored to the alternate location specified, with its target directories and files also restored to the same location in their relative path. Target of the link is updated to the new relative path. In other word, the link now points to the new alternate location.
Disabled	Symbolic link is restored to the alternate location specified, with its target directories and files also restored to the same location in their relative path. However, target of the link is NOT updated to the new relative path. In other word, the link still points to the original location.

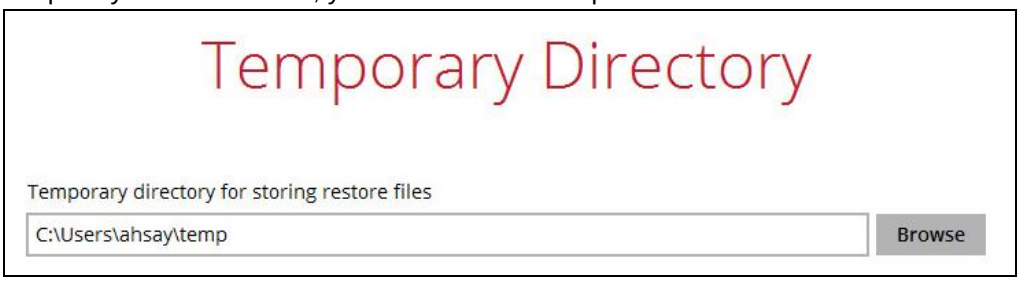
- **Verify checksum of in-file delta files during restore**

Verify checksum of in-file delta files during restore is disabled by default. 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.

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

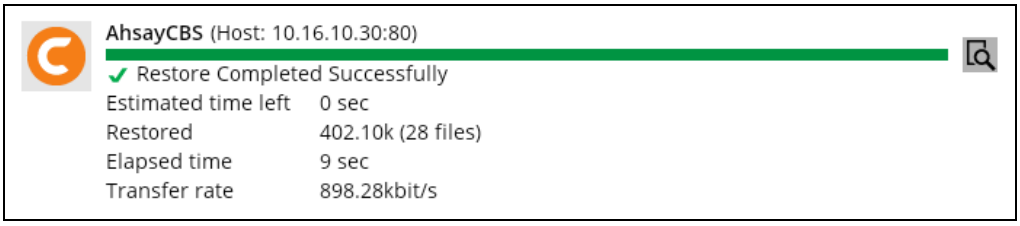
11. Select the temporary directory for storing temporary files, such as delta files, when they are being merged.

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

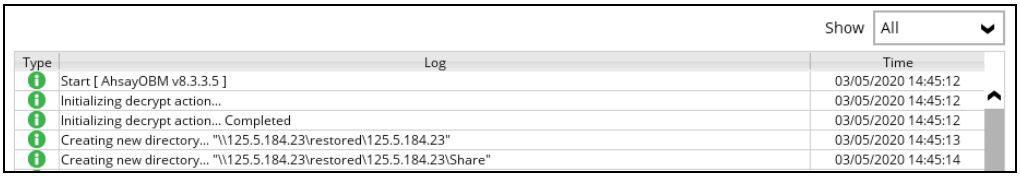


12. Click **Restore** to start the restore. The status will be shown.

13. When the restore is completed, the message "Restore Completed Successfully" will appear.



    You can click the **View** icon on the right-hand side to check the log. A window will pop up to show the log. Click **Close** to exit the pop-up window.



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

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

14.1.2 OpenDirect Restore

This restore method applies to backup sets created with OpenDirect restore enabled only.

IMPORTANT

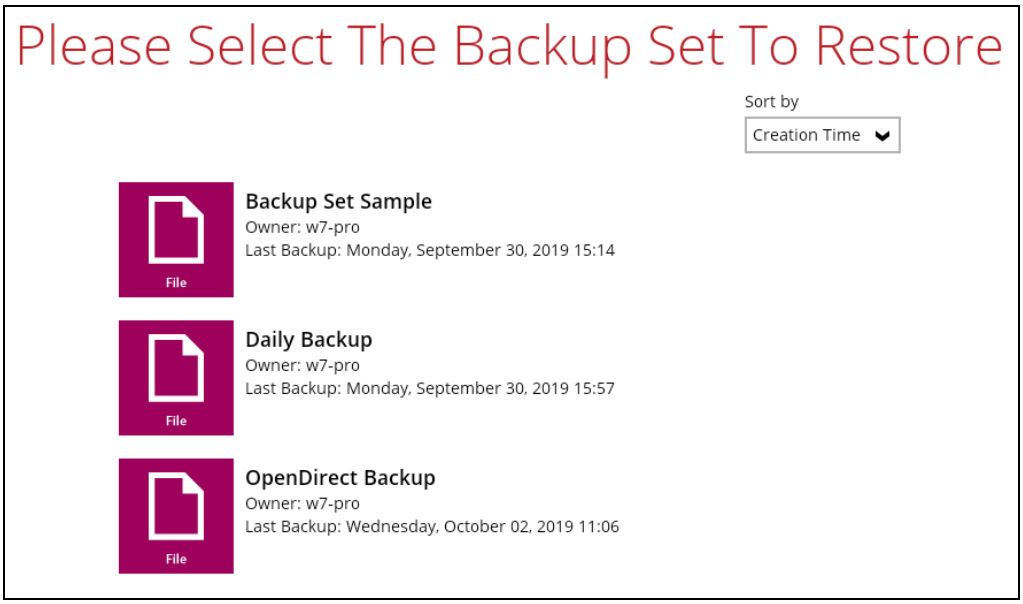
Before you proceed with the OpenDirect Restore, make sure the following dependencies are fulfilled. Failure to do so may cause the restore to fail.

- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
  https://www.microsoft.com/en-us/download/details.aspx?id=48145
- Update for Universal C Runtime in Windows
  https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows
- Microsoft Security Advisory 3033929 (for Windows 7 and Windows Server 2008 R2)
  https://technet.microsoft.com/en-us/library/security/3033929.aspx

1. Log in to the AhsayOBM application according to the instructions in section Login to AhsayOBM.

2. Click the **Restore** icon on the AhsayOBM main interface.

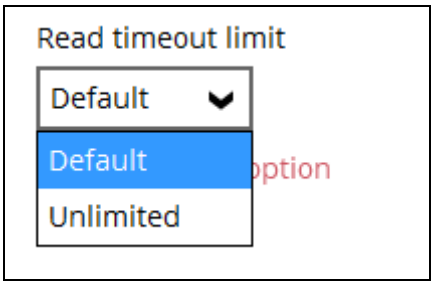
3. All the available backup sets for restore will be listed. Select the backup set that you would like to restore data from.



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

5. Select **Open backup data directly without restoration (OpenDirect).**

You may select the **Read timeout limit** by clicking Show advanced option.



This selection defines the duration when the OpenDirect restore session will be disconnected if there is no response from the mounted compressed or image file.

- **Default** – This setting should be suitable for compressed or image file located on a local, removable, or network drive. The time out value is15 seconds.
- **Unlimited** – the connection will not be time out when this is selected. This selection is recommended under the following usage:

  Backup destination is a cloud stroage.

  AhsayCBS over the Internet.

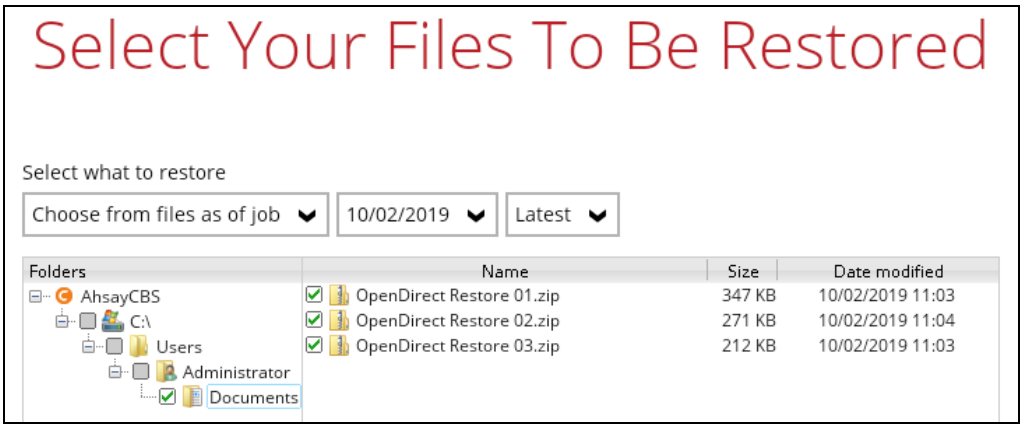
  A large compressed or image file with large incremental delta chain.

NOTE

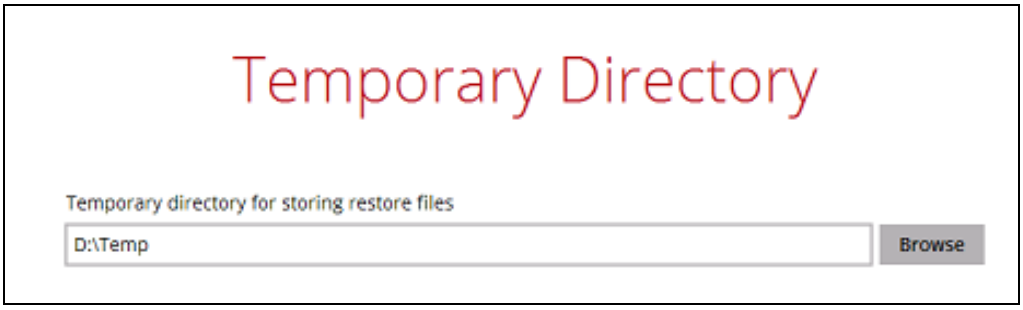
If in doubt or unsure about the compressed or image file size or network stability, it is recommended to use **Unlimited**.

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

6. 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.



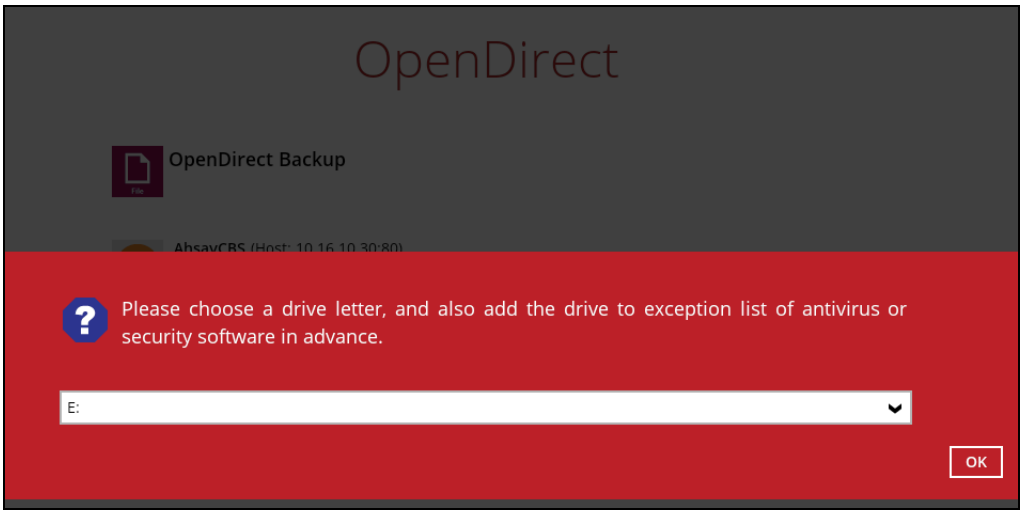
7. Select a temporary directory for storing restore files, then click Restore to start the OpenDirect restore.



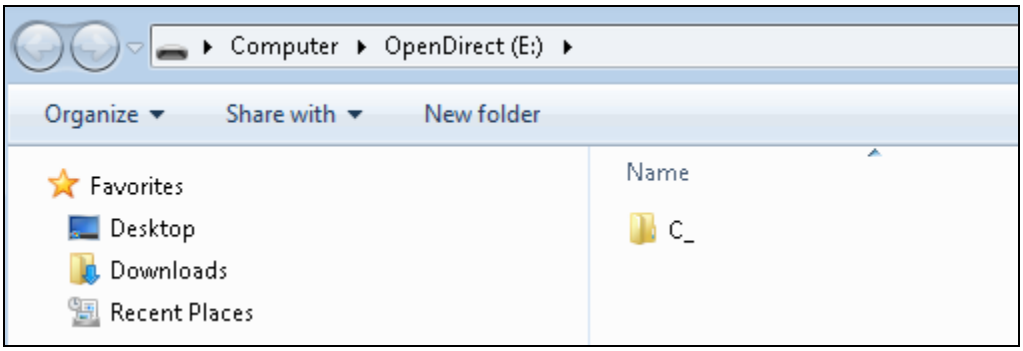
8. Click **Restore** to start the restore. The status will be shown.

9. The following screen shows when you perform OpenDirect restore for this backup set on this machine for the first time only. Make sure you click **Yes** to confirm mounting the file(s) on this machine. Clicking **No** will exit the restore process.

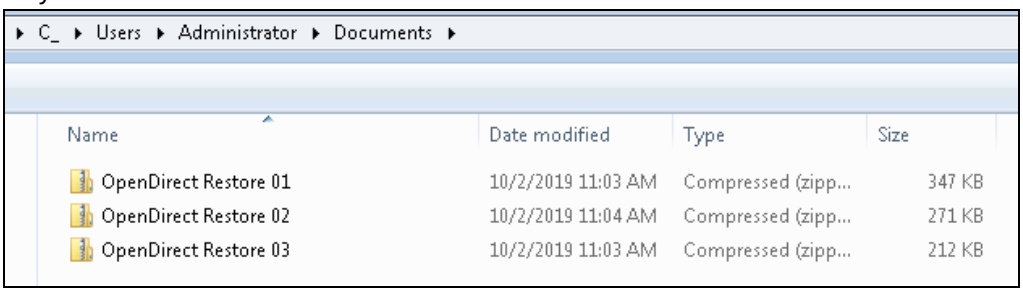
10. You will be prompted to select drive letter where you wish the mounted files to be mapped on your machine, click **OK** when you have finished selection.



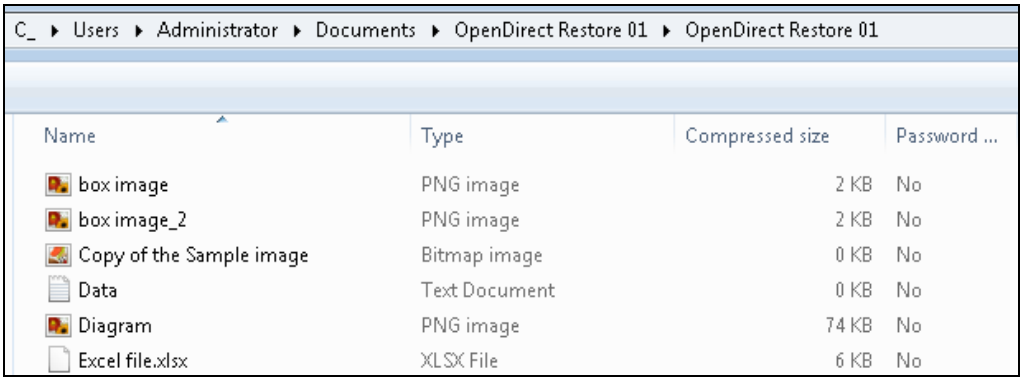
11. The selected drive letter will be mapped and prompted in the Windows Files Explorer with the files you wish to restore shown.



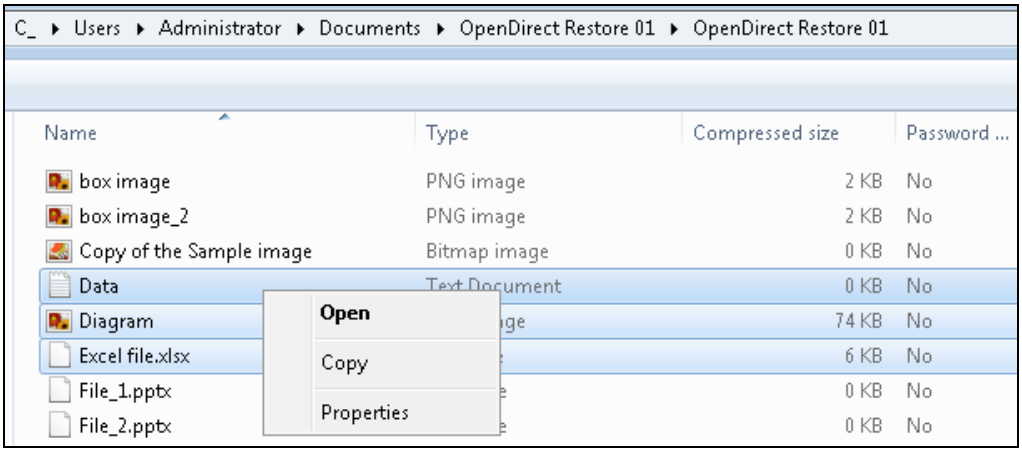
12. You can now click on the files to view them directly from here, which will be in read-only mode.



If it is a zipped file, you can directly click on it to see all the individual files inside.

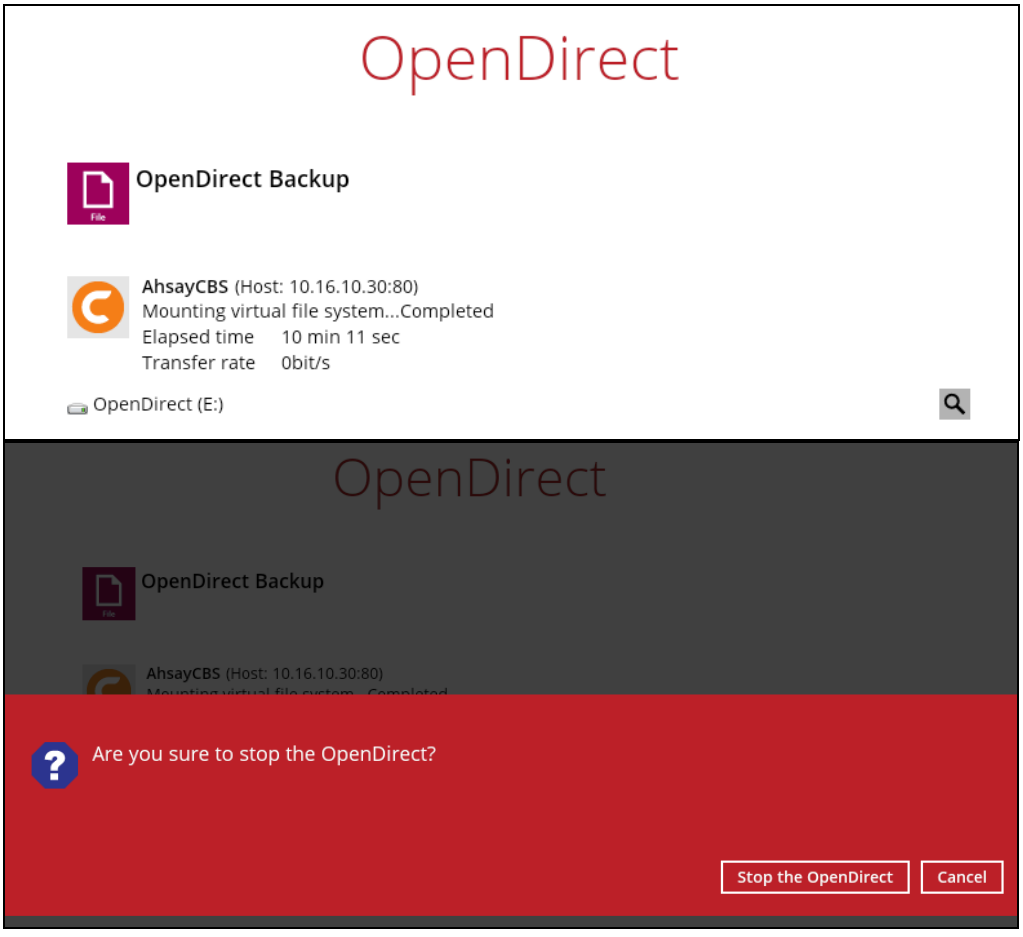


You may also copy individual file(s) you wish to restore toyour local machine.



13. The mounted drive letter cannot be ejected from the Windows File Explorer, it will only be closed when you exit AhsayOBM.

14. When you have finished restoring the necessary files, you can go back to AhsayOBM and click **Cancel** to exit the OpenDirect Restore.



IMPORTANT

1. As a result of the limitation of the virtual file system library, the mapped drive will only be unmounted from your machine when you exit AhsayOBM. In other words, each OpenDirect restore session on AhsayOBM can only mount and unmount once.

2. **OpenDirect restore** of file backup sets:

   - Will not show up on the **Restore Status** tab in **Live Activities** of the backup service provider AhsayCBS. **Restore Status** tab in **Live Activities** only applies to the restore performed directly through AhsayOBM.
   - Will not generate restore reports or report email on backup service provider AhsayCBS.
   - Will not generate restore log on AhsayOBM.

14.2 Restore Filter

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

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

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

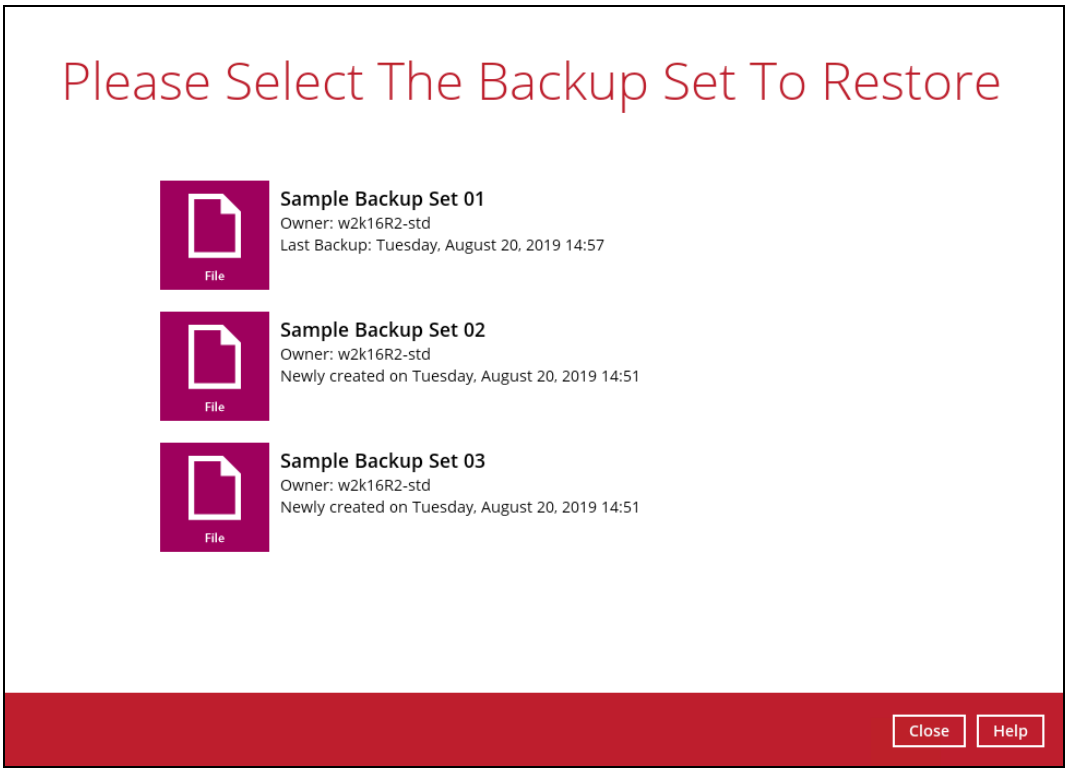
It also has the **Match Case** function, which serves as an additional accuracy when searching for any specific directories, files, folders, and mails.

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

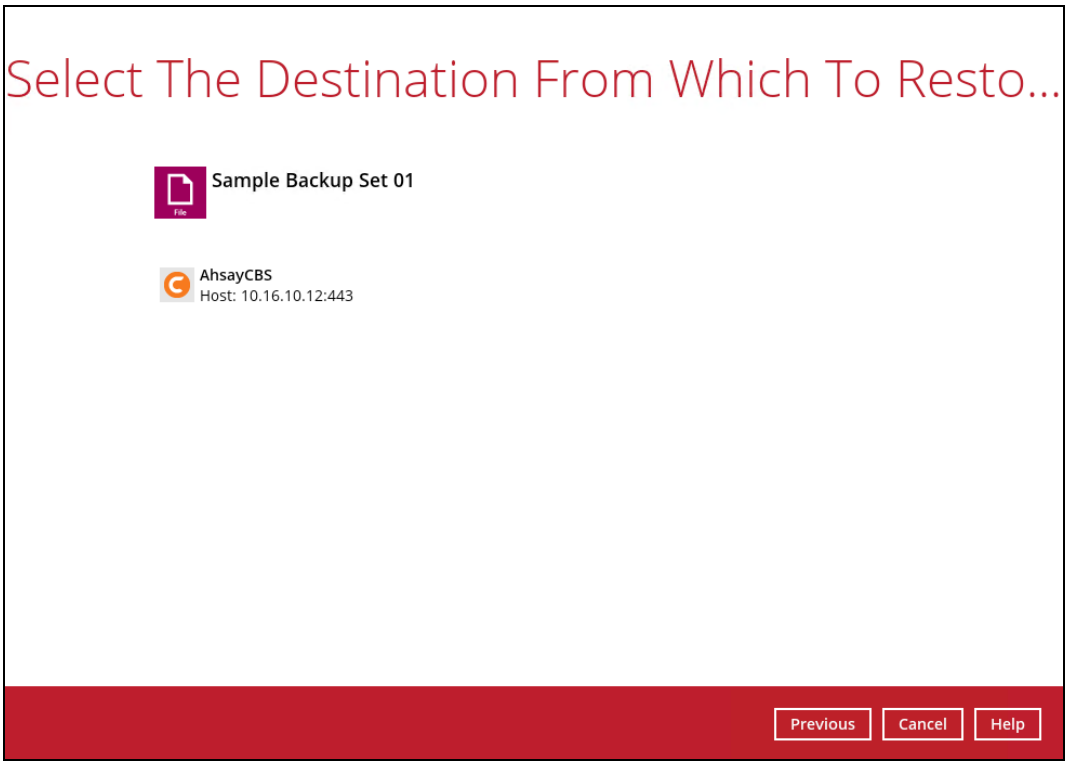
1 Log in to AhsayOBM according to the instructions in Chapter 8 Logging in to AhsayOBM.

2 Click the [Restore] icon on the main interface of AhsayOBM.

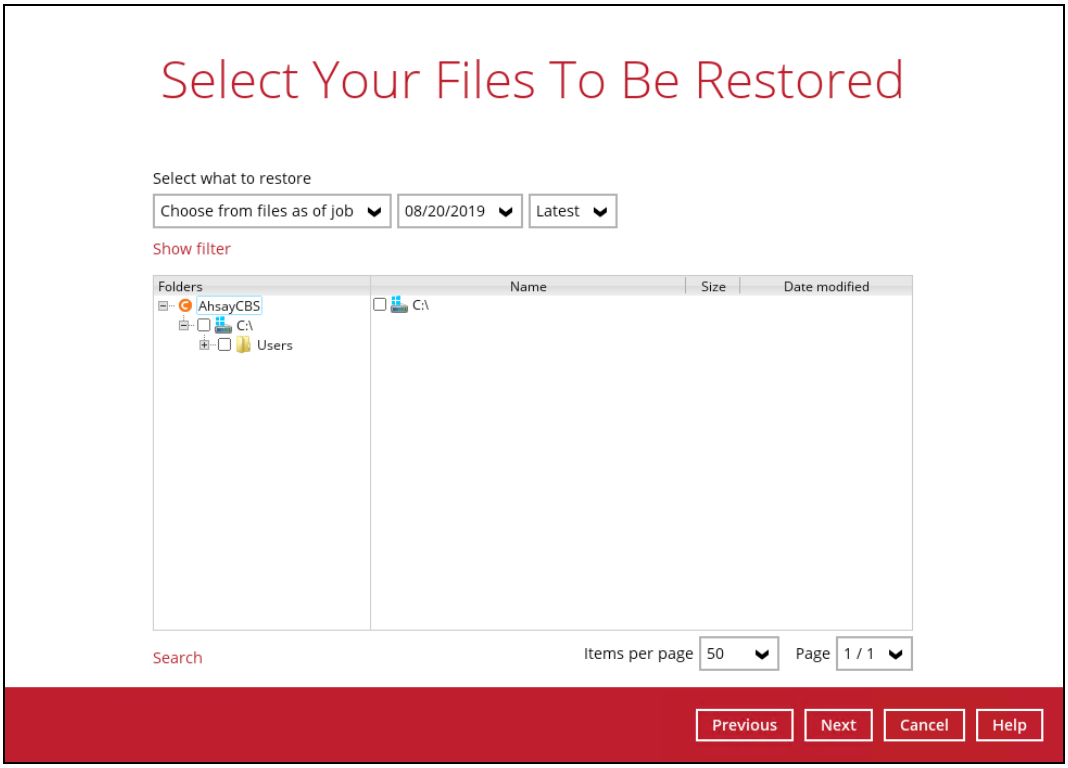
3 Select the backup set that you would like to restore.



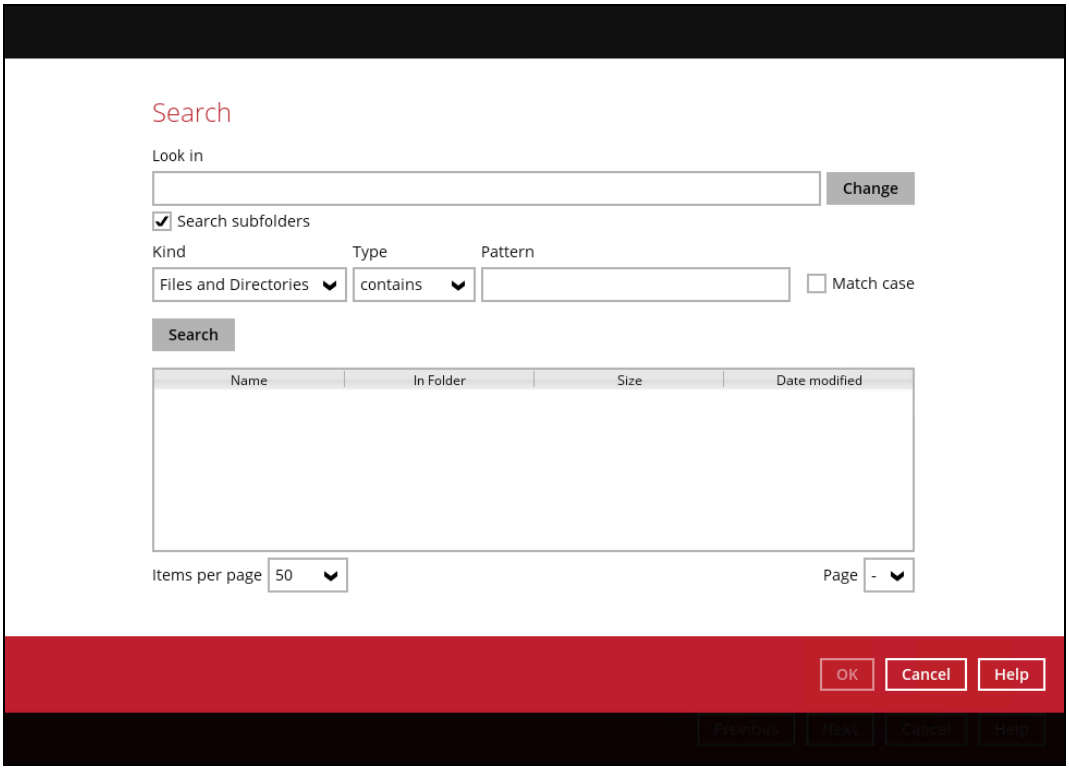
4 Select the backup destination that you would like to restore backed up items to.

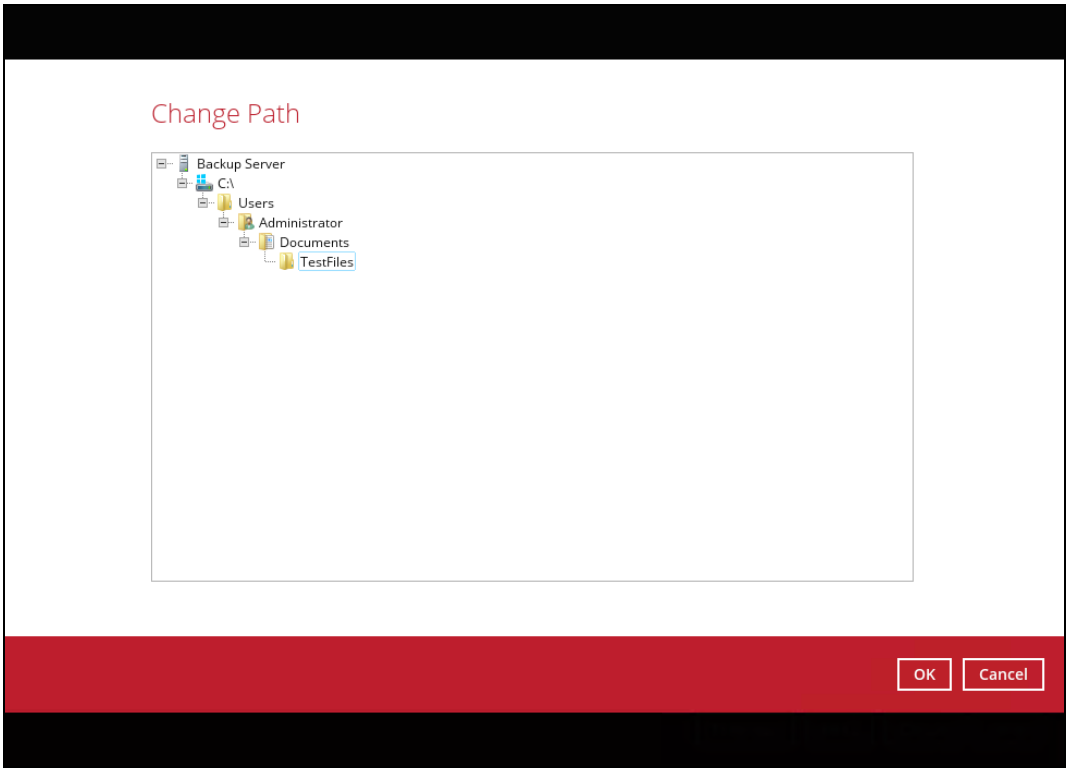


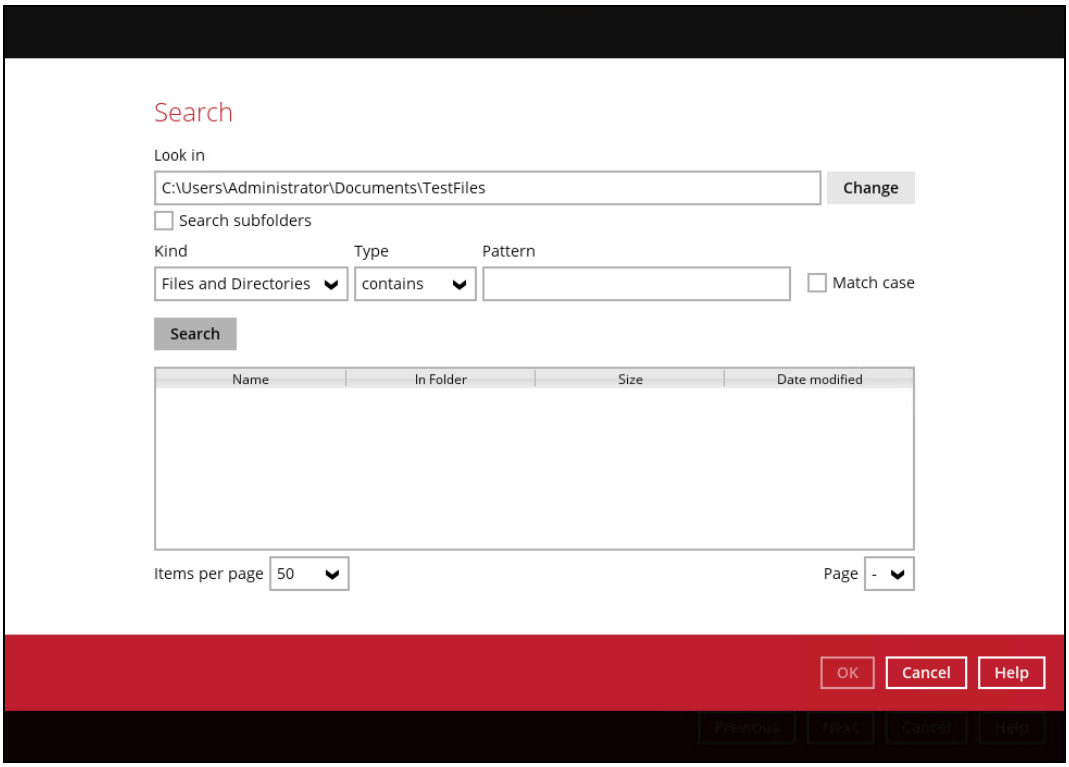
5 Click the [Search] located on the lower left side of the screen.



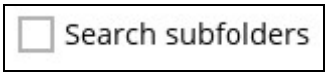
6 Click the [Change] button to change the path of the restore items from other location.

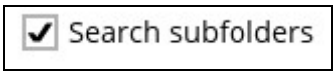



Change Path
Backup Server
C:\
Users
Administrator
Documents
TestFiles
OK
Cancel


Search
Look in
C:\Users\Administrator\Documents\TestFiles
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
Help

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





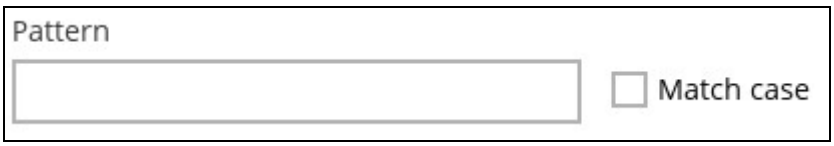
8 Select from the following Kind of files you want to search.

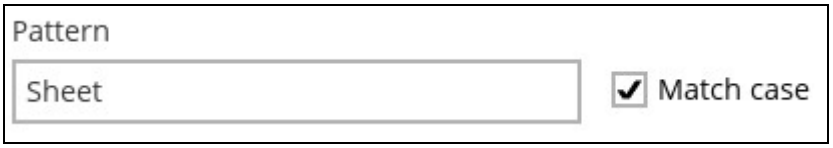
- Files and Directories
- Files only
- Directories

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.





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

12 Check all the items or check a specific item that you want and click the [OK] button to proceed and you will return to the restore main screen.

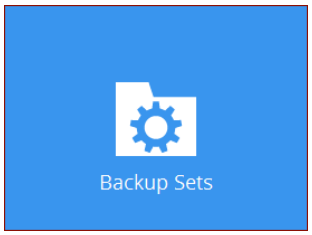
15 Mobile Backup and Restore to AhsayCBS and Predefined Destination

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

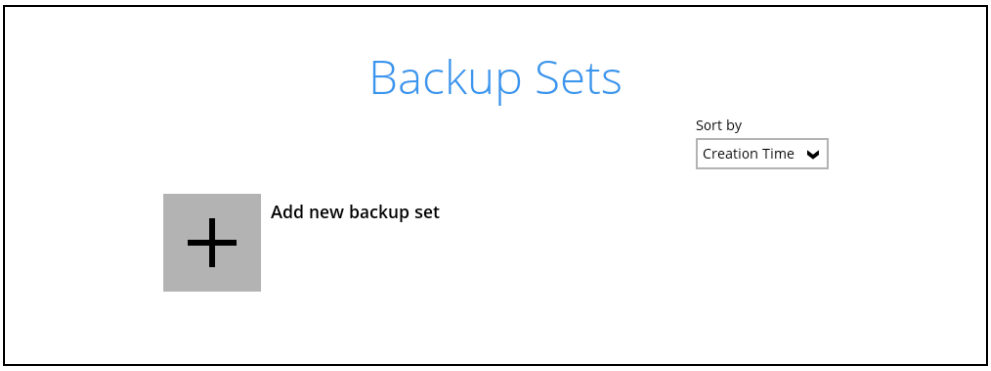
- Backup photos and videos from Ahsay Mobile app to AhsayOBM local destination. For more detailed information, check **Ahsay Mobile App User Guide for Android and iOS – Chapter 10**.
- Create a File Backup Set on AhsayOBM and follow these setup:
  - Backup source should be photos and videos backed up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

15.1 Create a File Backup Set

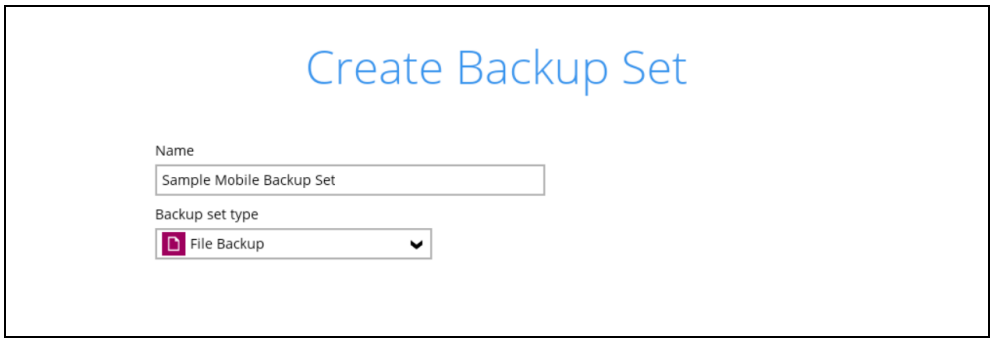
1. Click the **Backup Sets** icon on the main interface of AhsayOBM.



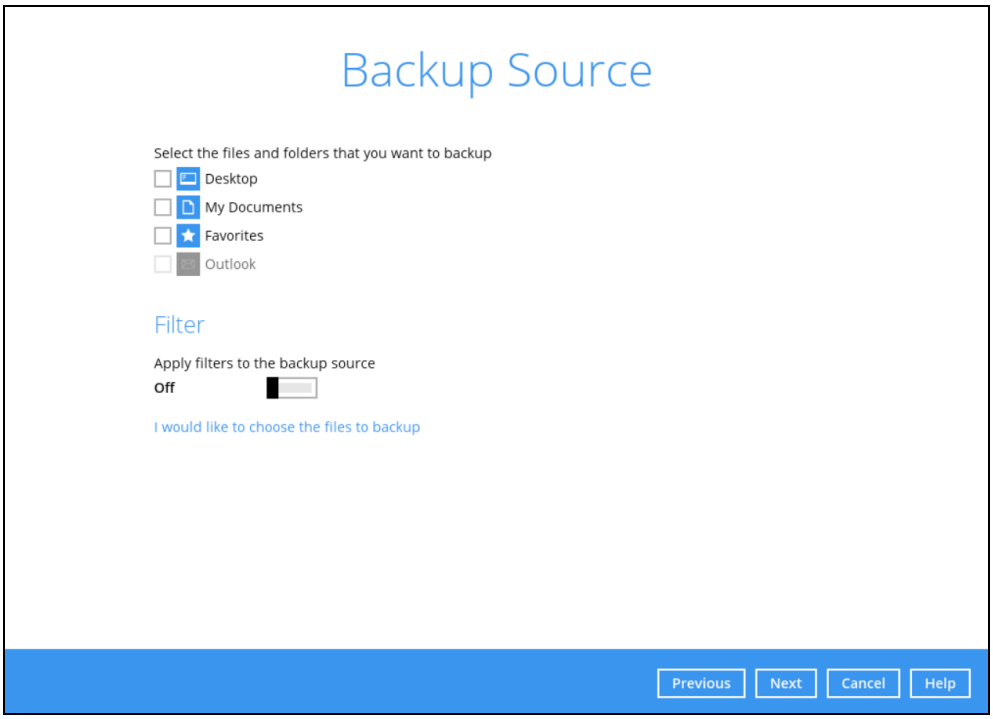
2. Create a new backup set by clicking + next to **Add new backup set**.



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

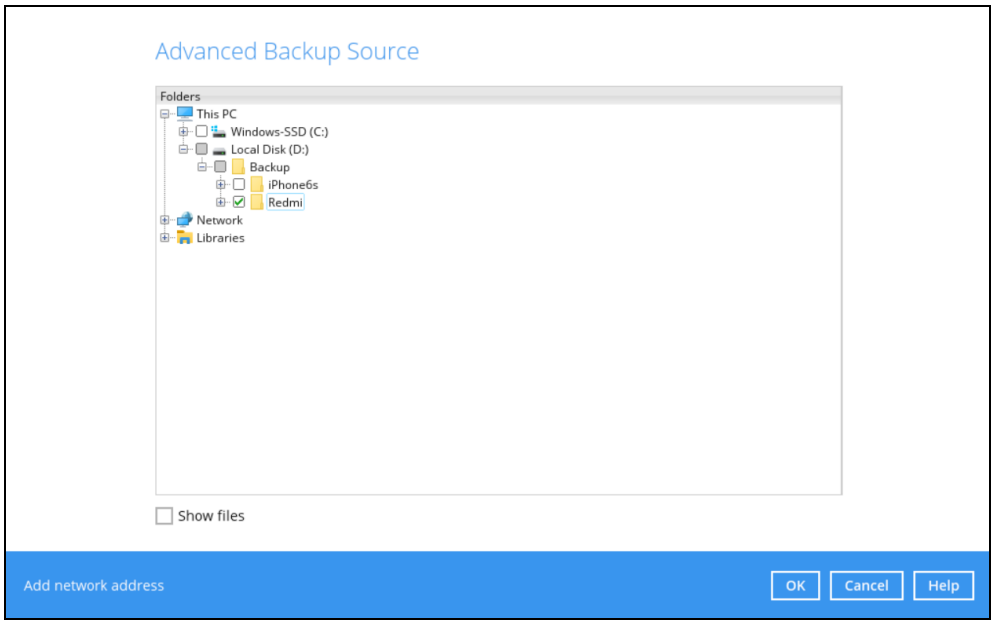


4. In the Backup Source window, select the mobile backup source for backup. Click **I would like to choose the files to backup**.

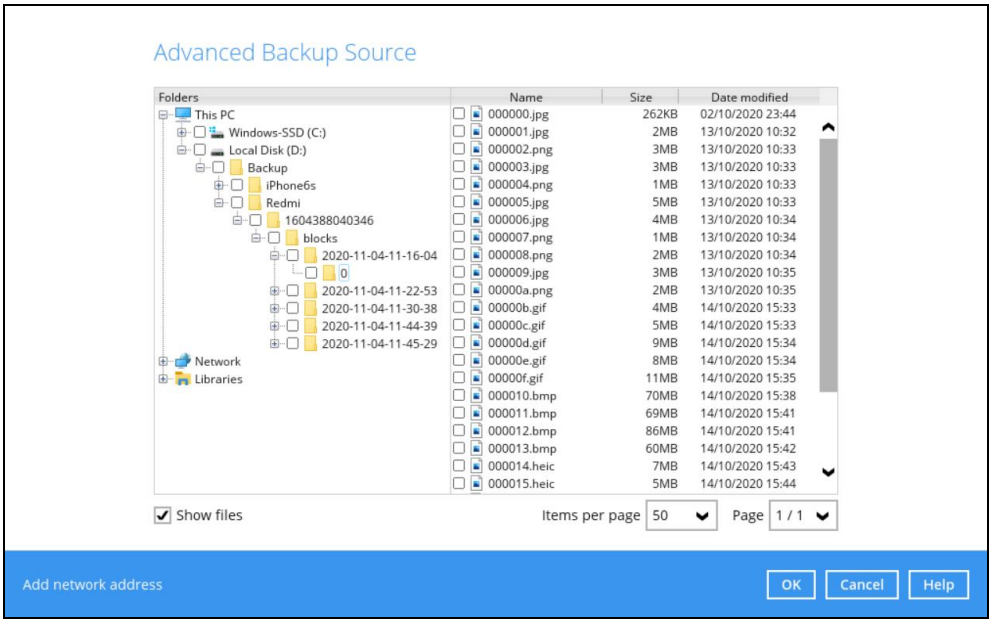


In the **Advanced Backup Source** window, select the mobile backup source.

In this example, Redmi folder is selected. The mobile backup source is in **Local Disk (D:)**.

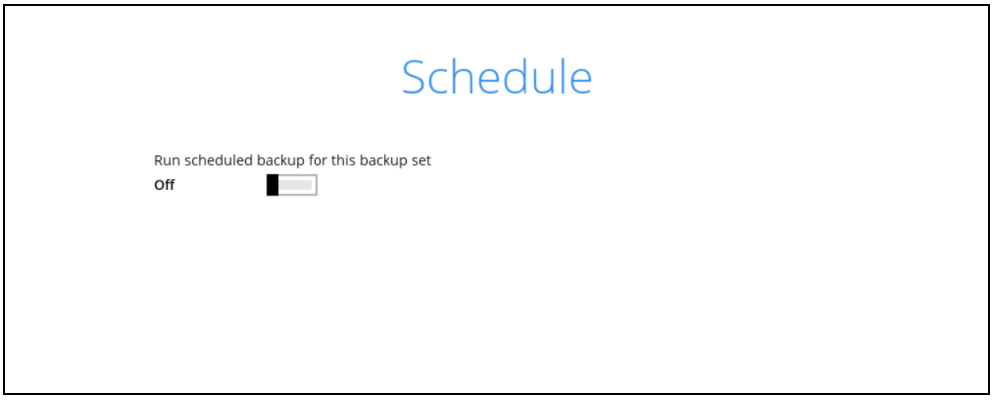


Alternatively, if you want to back up only specific files instead of all files in your selected folder(s), select the **Show files** checkbox at the bottom of the screen. A list of files will appear on the right-hand side. Select the checkbox(es) next to the file(s) to back up. Then, click **OK** to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

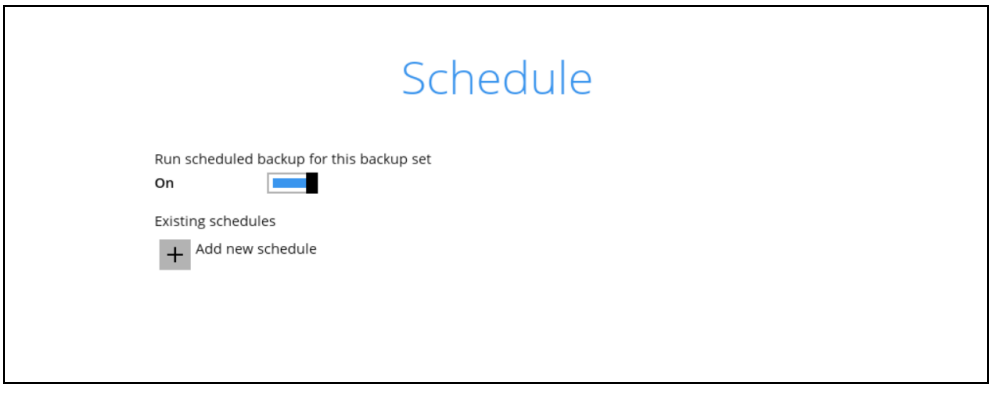


In the Backup Source window, click **Next** to proceed.

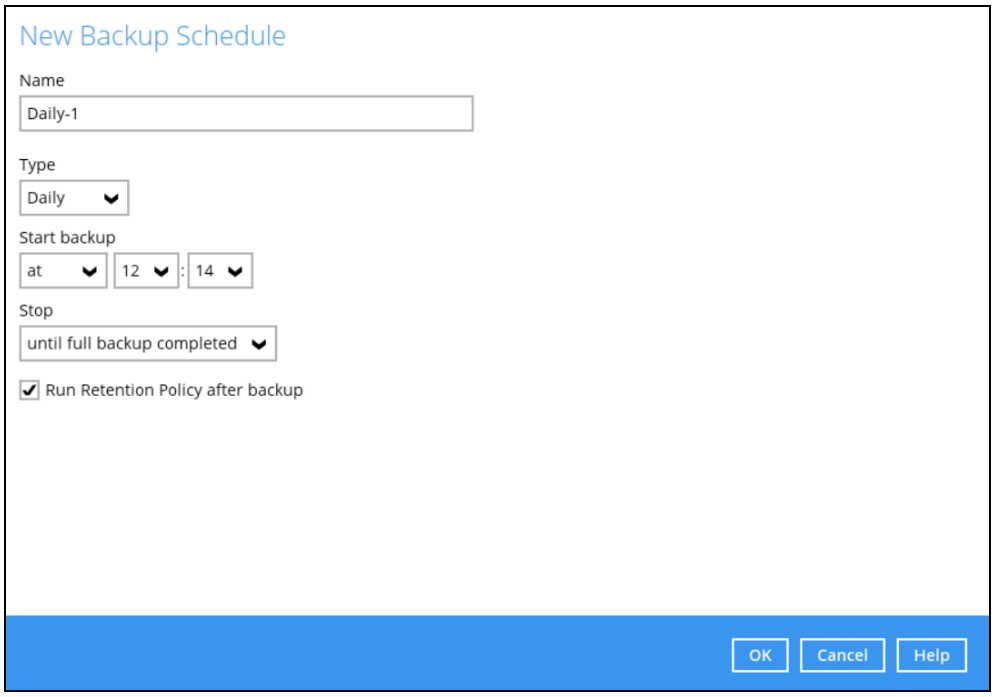
5. In the Schedule window, the Run scheduled backup for this backup set is **Off** by default. You can configure a backup schedule to automatically run a backup job at your specified time interval.



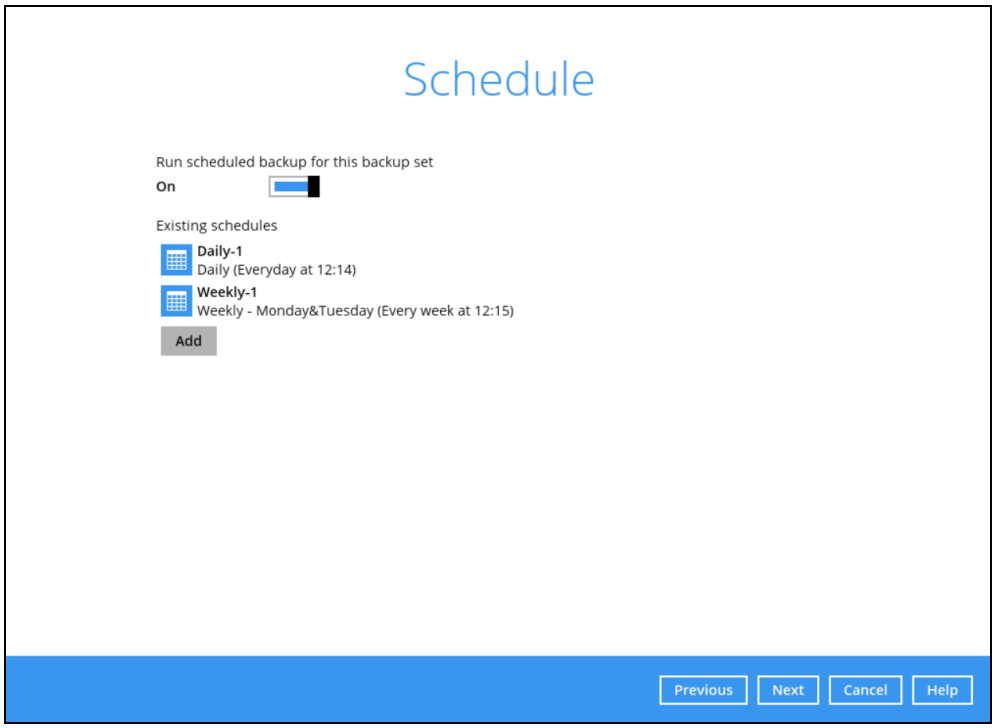
Swipe the switch to the right to enable the schedule then click **Add** to add a new schedule.



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

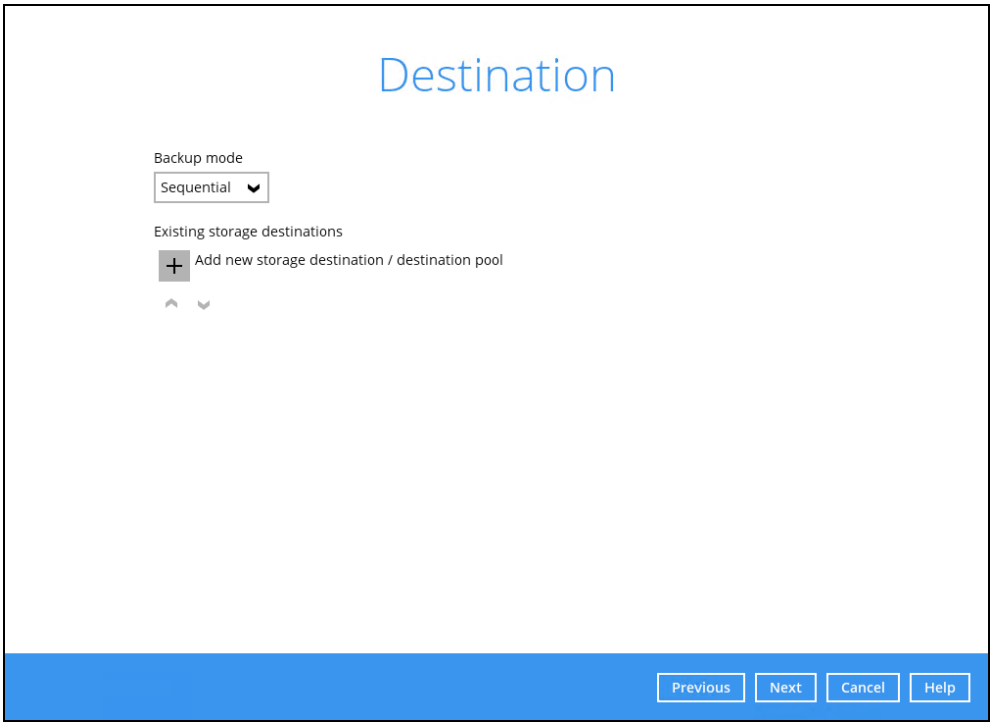


In case you have added a schedule, it will be shown in the Schedule window. Click **Next** to proceed when you are done setting.

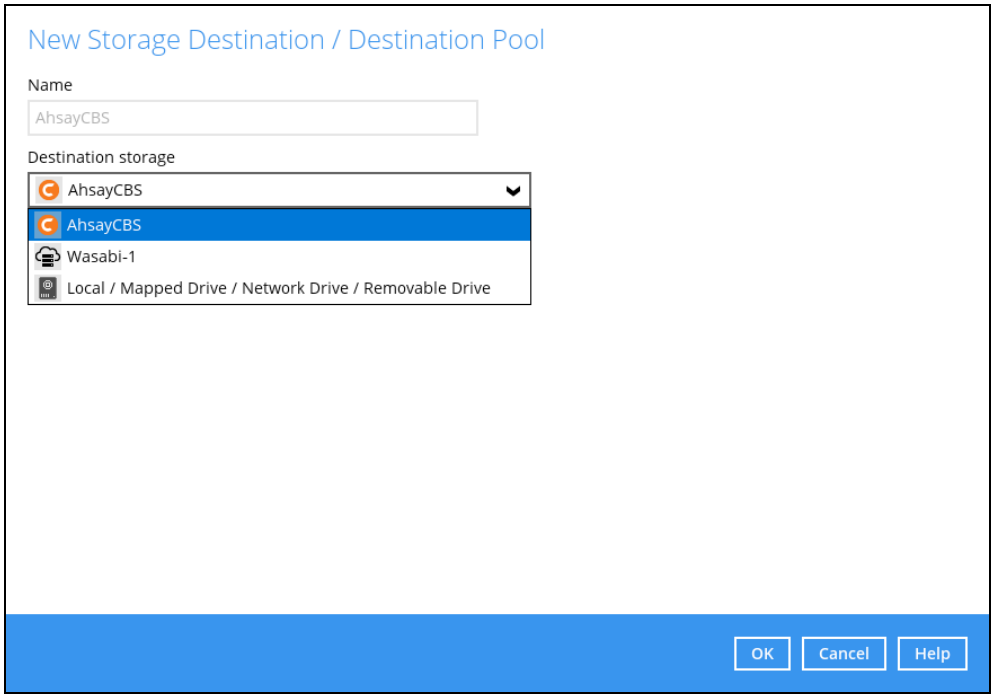


6. The **Destination** window will appear. Select the appropriate option from the **Backup mode** dropdown menu.
   - **Sequential** (default value) – run backup jobs to each backup destination one by one
   - **Concurrent** – run backup jobs to all backup destinations at the same time

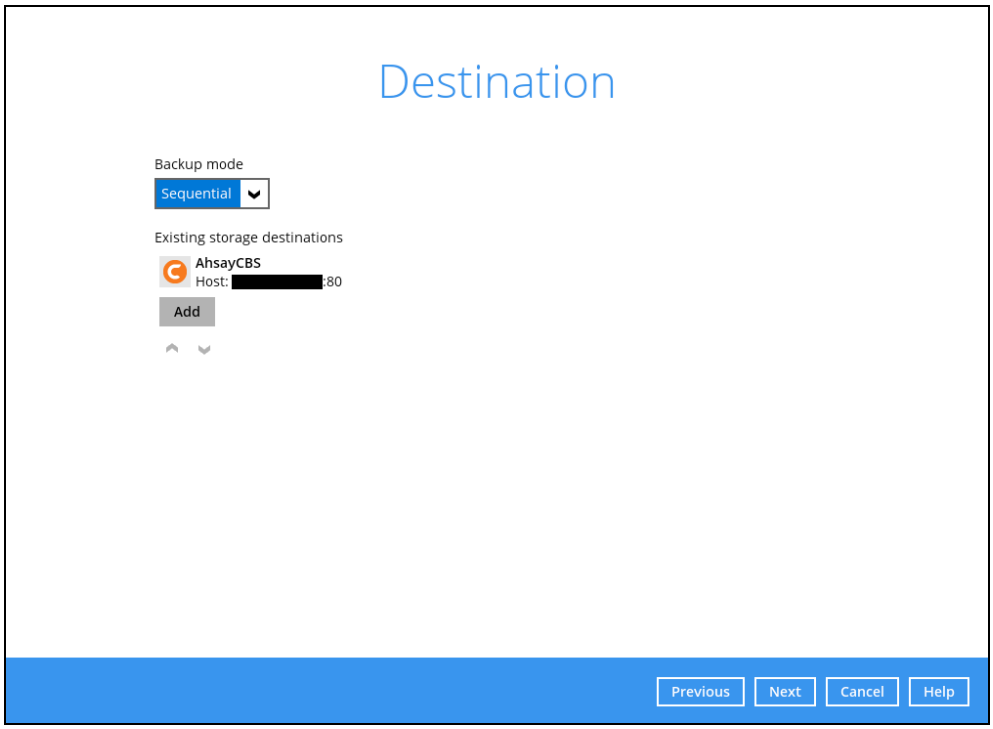
   To select a backup destination for the backup data storage, click + next to **Add new storage destination / destination pool**.



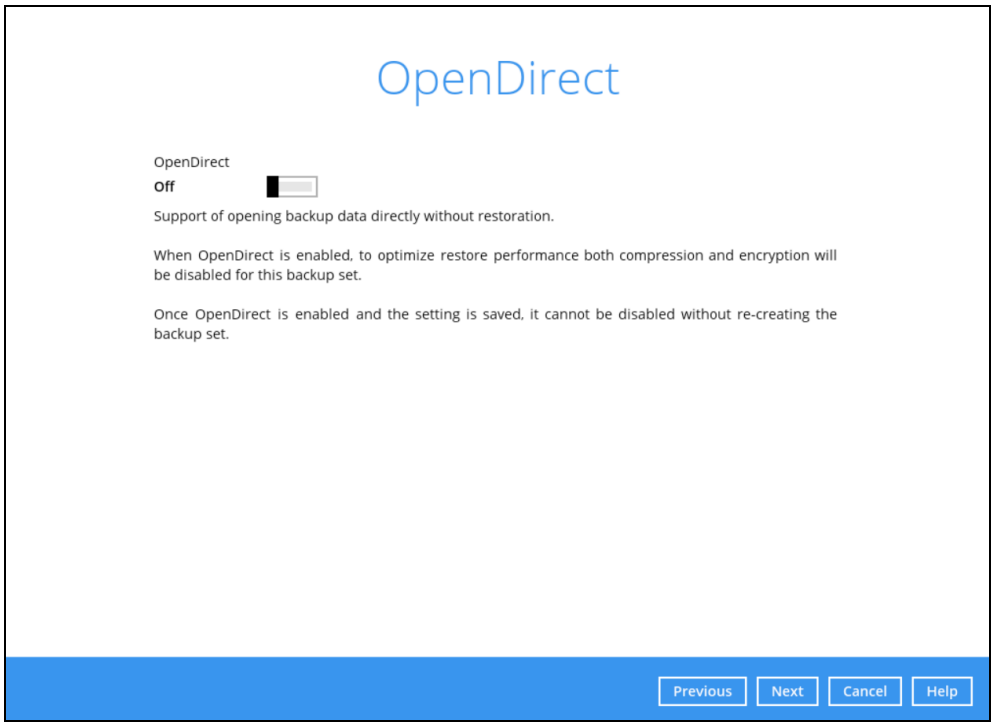
   In the New Storage Destination/Destination Pool window, select AhsayCBS or a Predefined destination. Then, click **OK** to confirm your selection.



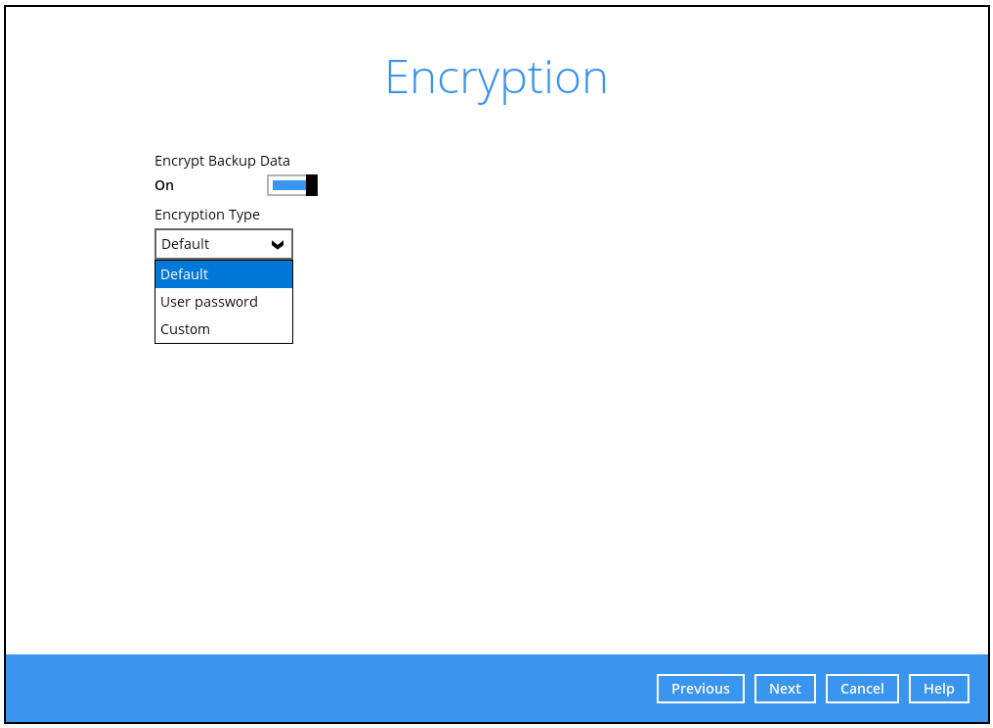
In the Destination window, your selected storage destination will be shown. Click **Next** to proceed.



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

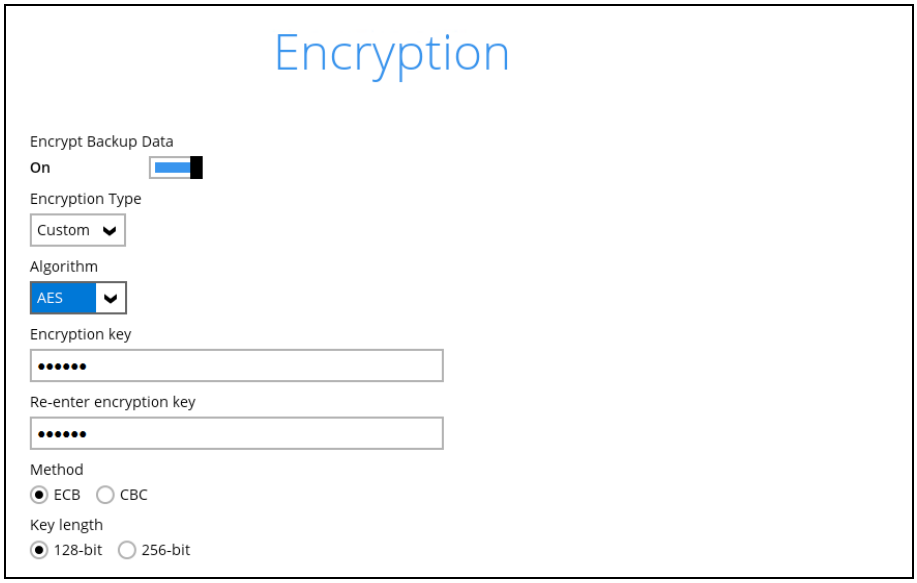


8. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection



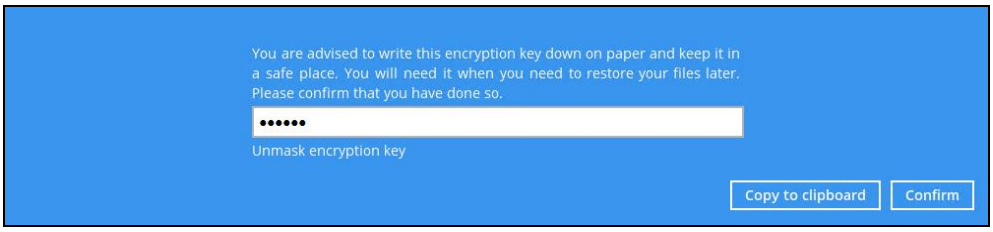
You can choose from one of the following three Encryption Type options:

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



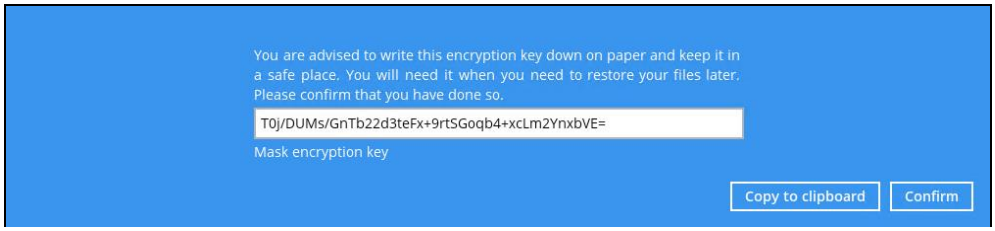
Click **Next** when you are done setting.

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



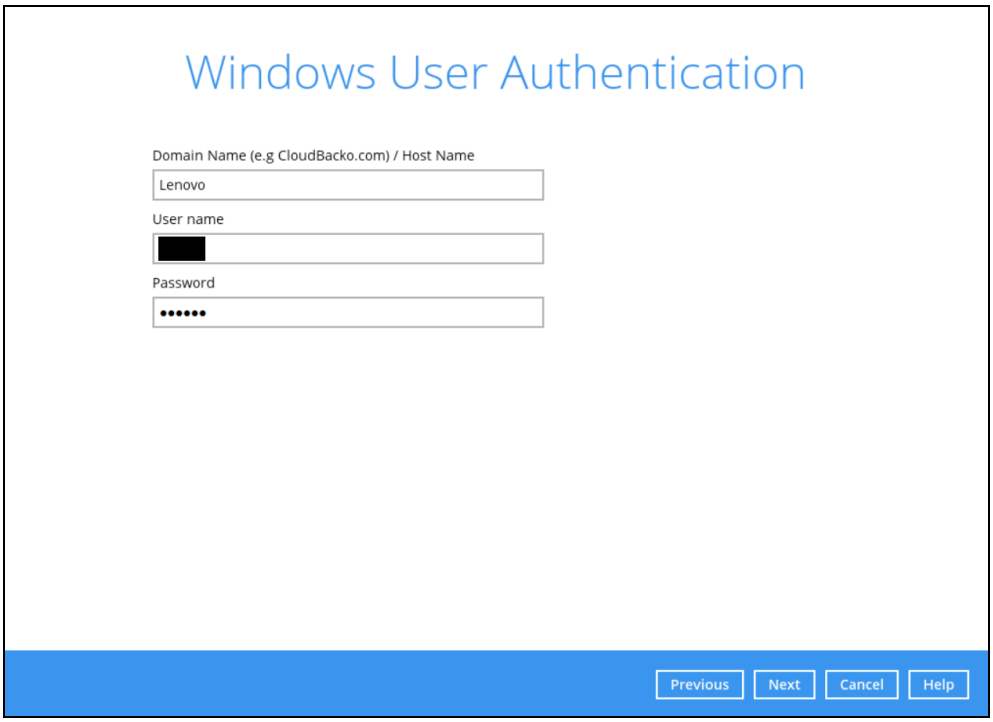
The pop-up window has the following three options to choose from:

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

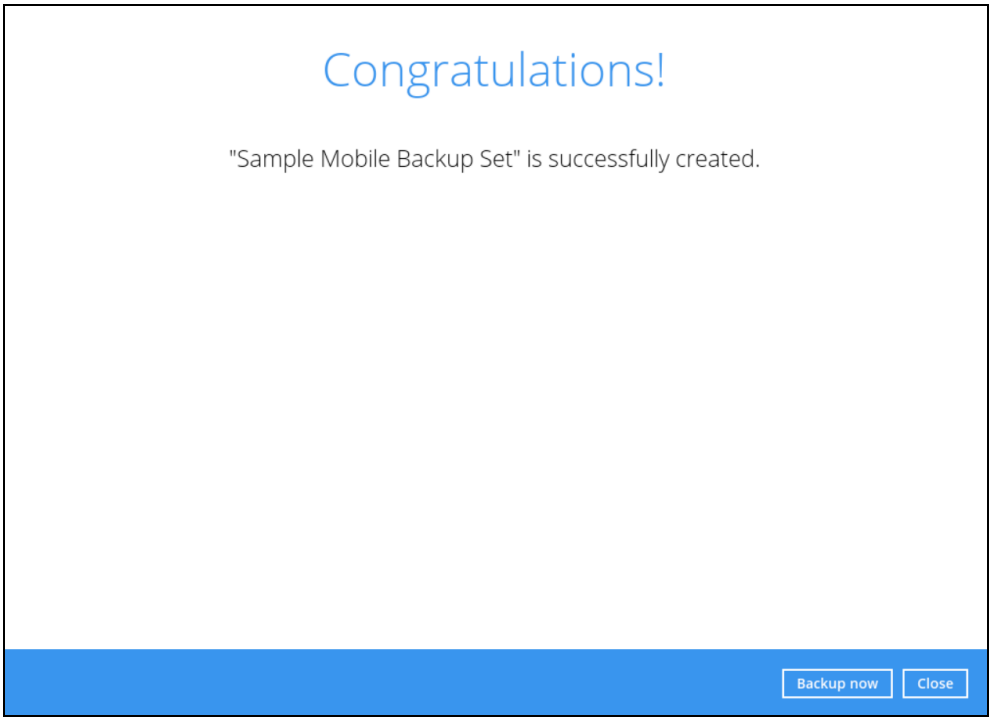


- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

10. The following screen prompts you to enter the Windows login credentials for user authentication if you have enabled the Schedule Backup feature in step 5.

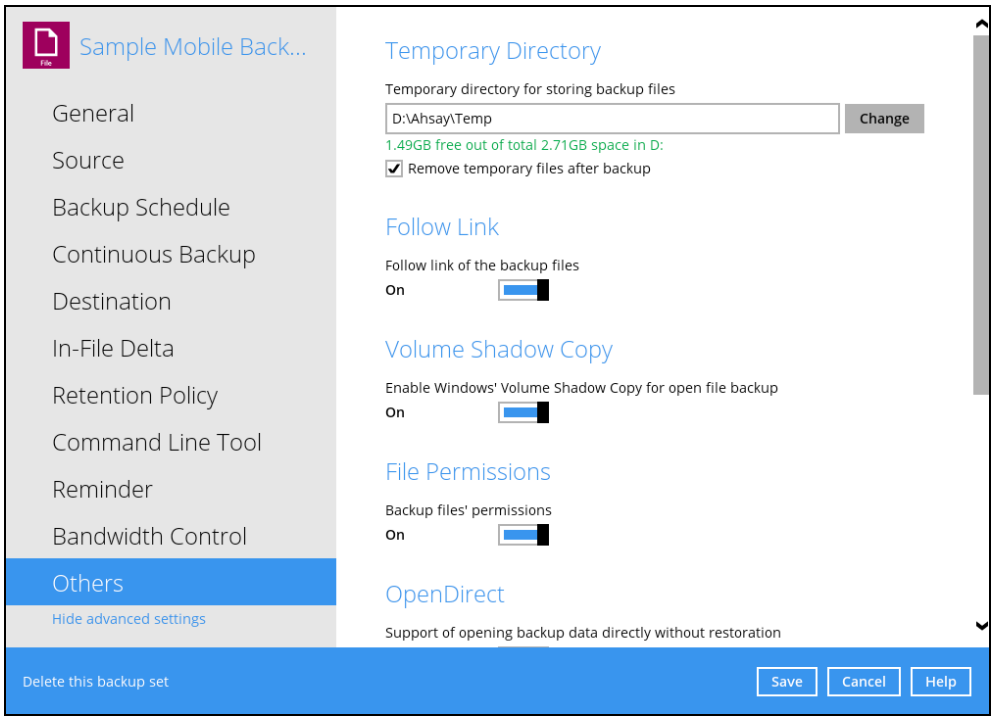


11. Upon successful creation of the backup set, the following screen will appear. You can click **Backup now** to back up your data or click **Close** to exit.



12. It is highly recommended to change the Temporary Directory. Select another location with sufficient free disk space other than **C:\Users\Ahsay\Temp**.

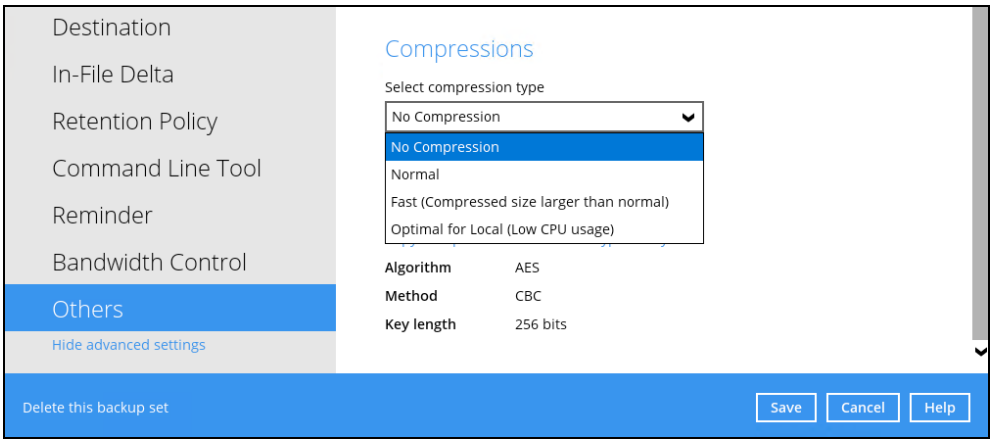
    Go to **Others** > **Temporary Directory**. Click **Change** to browse for another location.



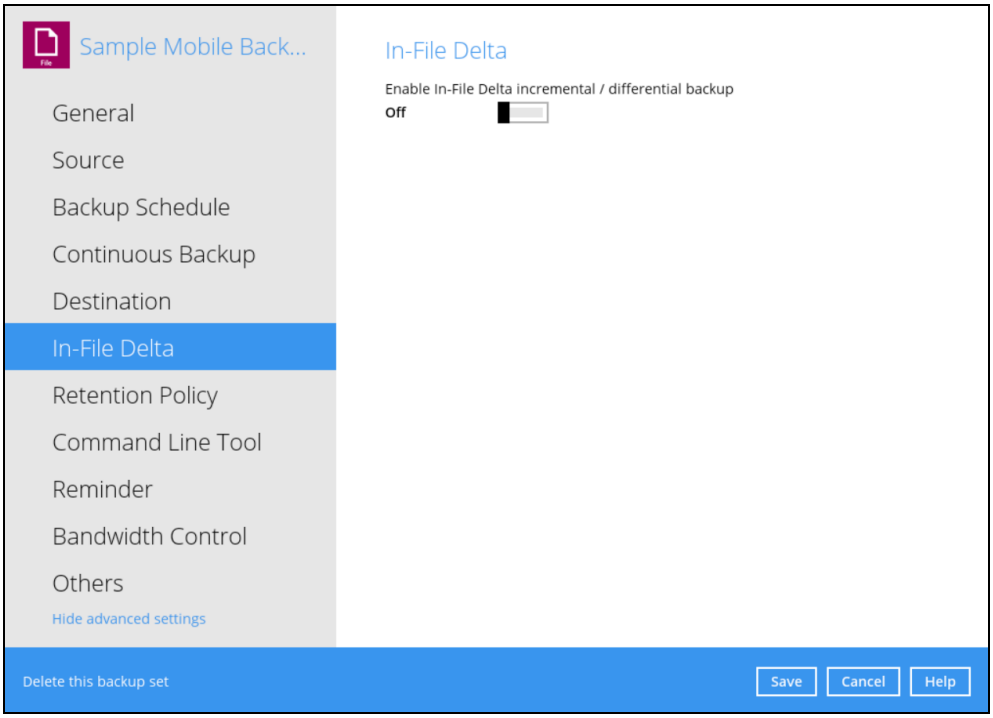
13. Optional: Select your preferred **Compression** type. By default, the compression is set Optimal for Local (Low CPU Usage) Go to **Others** > **Compressions**.

    Select from the following list:

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

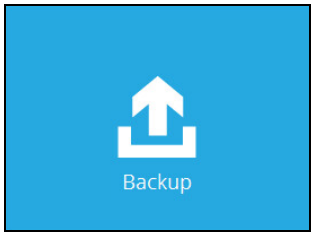


14. Optional: It is recommended to disable the **In-File Delta** as the files are relatively small, photos and videos are also not updated.

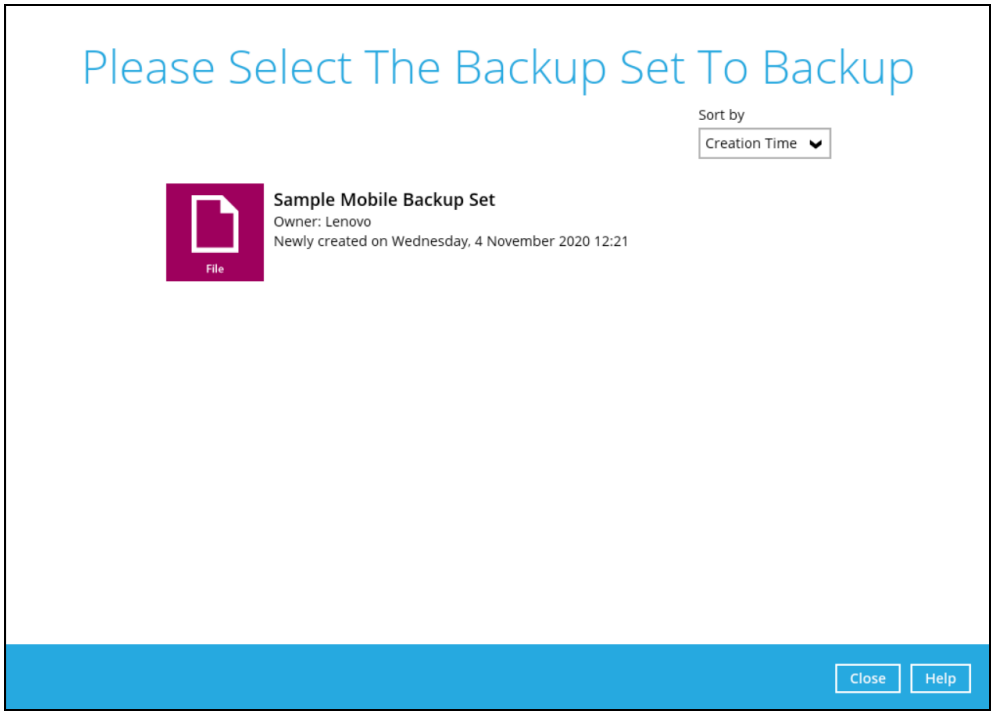


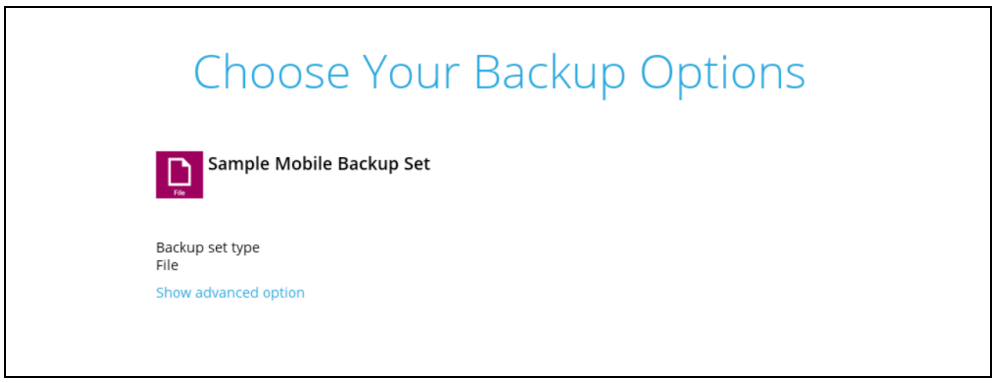
15.2 Run a Backup Job

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



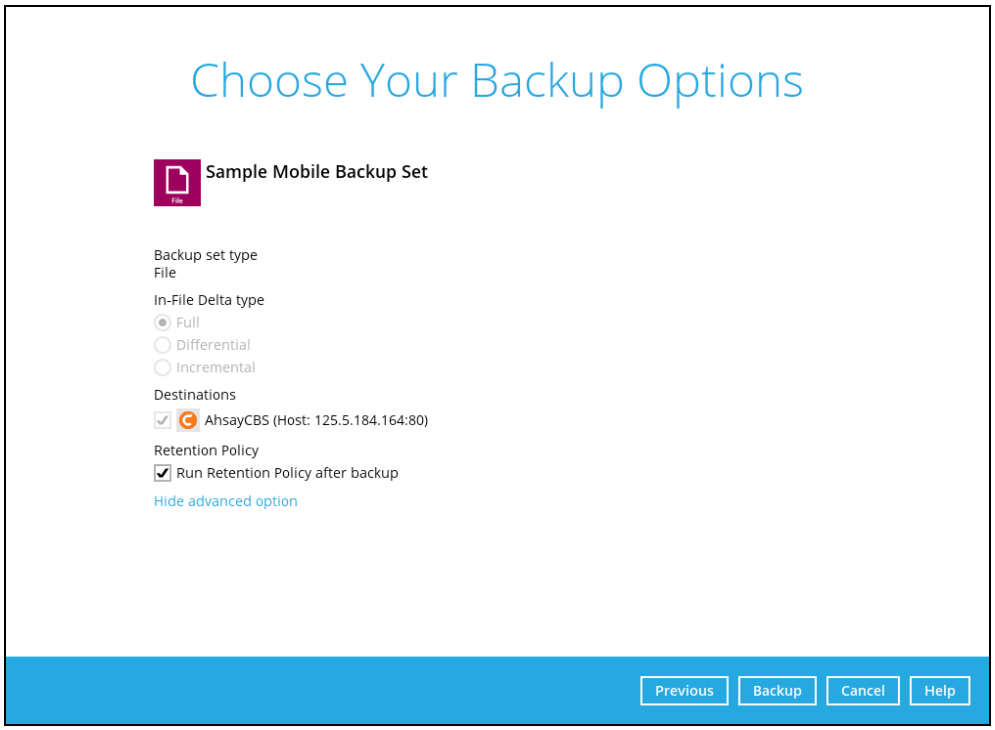
2. Select the backup set that you would like to start a backup job for. In case you want to modify the In-File Delta type, Destinations and Retention Policy settings, click **Show advanced option**.



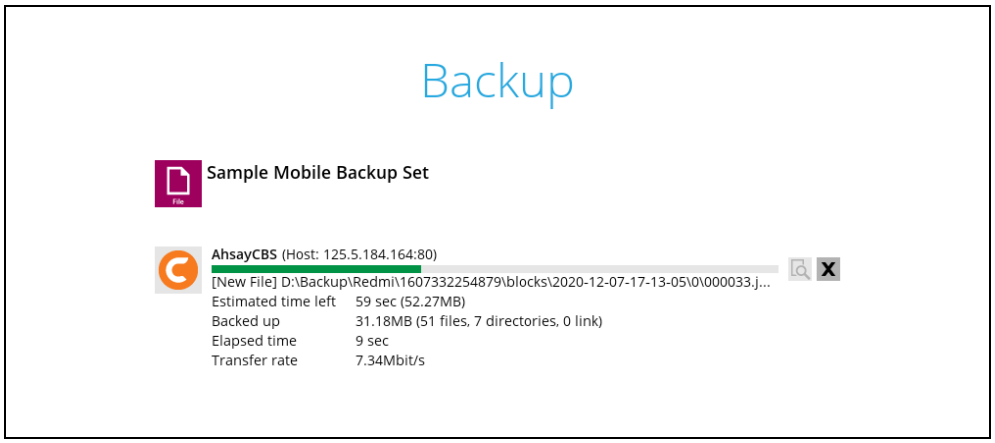


3. When advanced options are shown, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** in the Retention Policy section at the bottom.

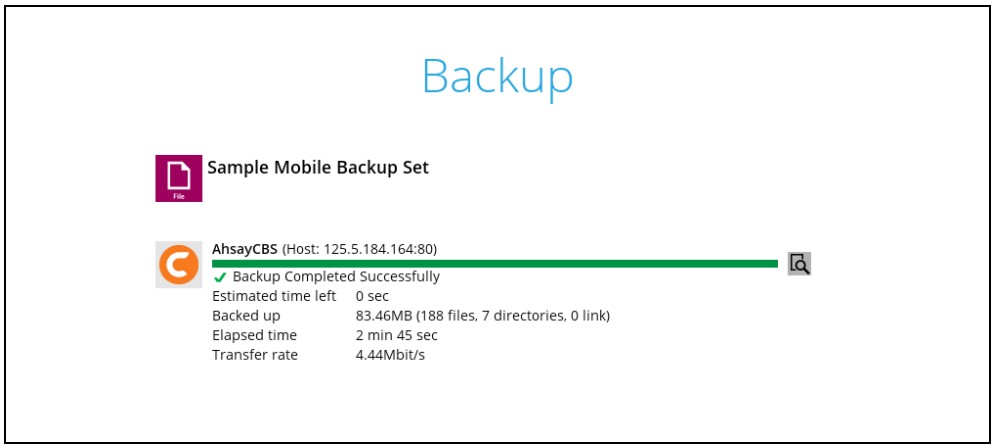
   This will help you save hard disk quota in the long run. In the In-File Delta type section, it is recommended to run in **Full** as a full backup captures all the data that you want to protect. When you run a backup job for the first time, AhsayOBM will run a full backup regardless of the in-file delta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



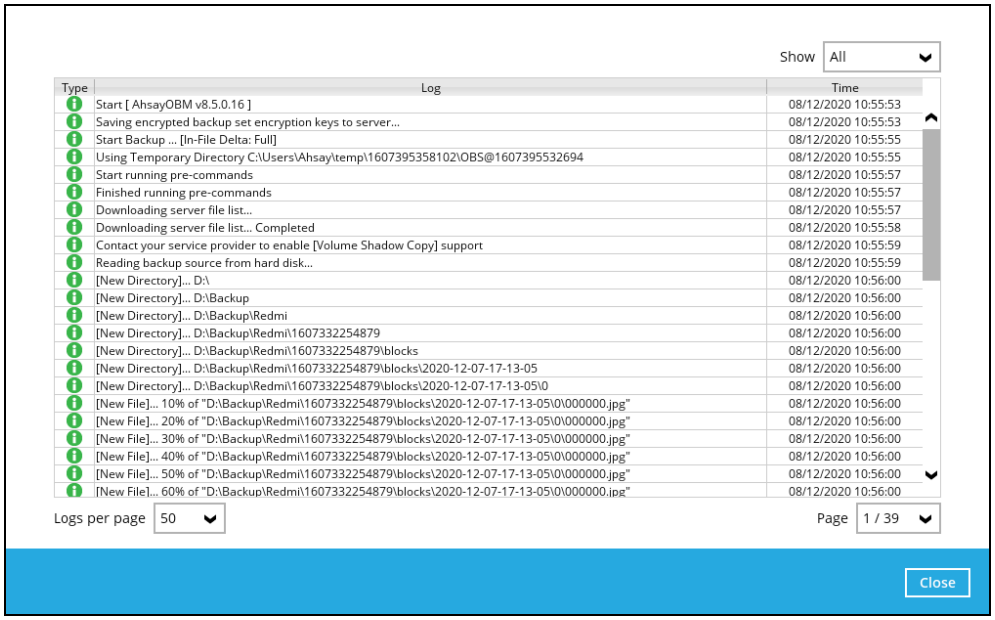
4. Click **Backup** to start the backup job. The status will be shown.



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



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



15.3 Restore Data

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

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

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

- Alternate location - data will be restored on an alternate location which can be setup anywhere in the AhsayOBM local machine. If you choose this option then restoring to your mobile device will have to be manually done. There are two (2) options available:

  - Option 1: Copy the restored data from alternate location to original location which is the **backup destination for your mobile device**. You can now use the Ahsay Mobile app to restore the photos and videos back to your mobile device.

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

    Examples:

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

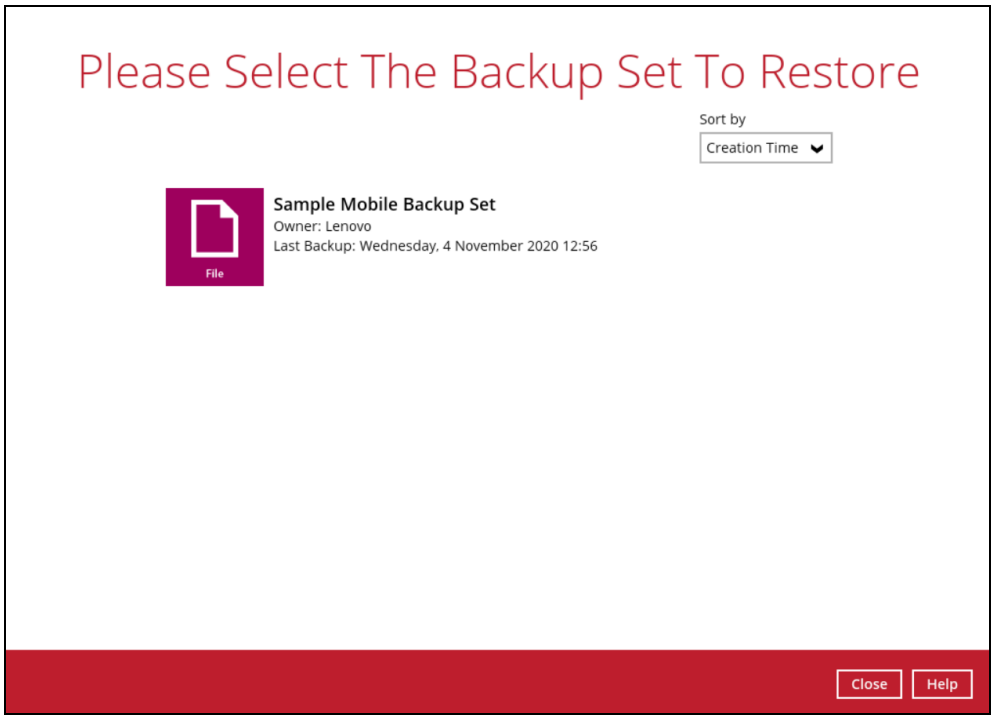
Restore to alternate location is not supported on another AhsayOBM machine. Options 1 and 2 must be on the original machine where the backups were performed.

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

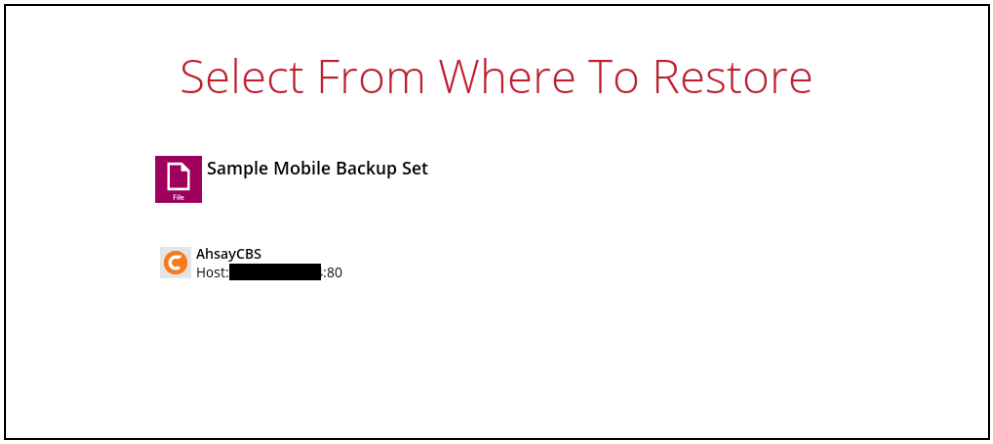
15.3.1 Original Location

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

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

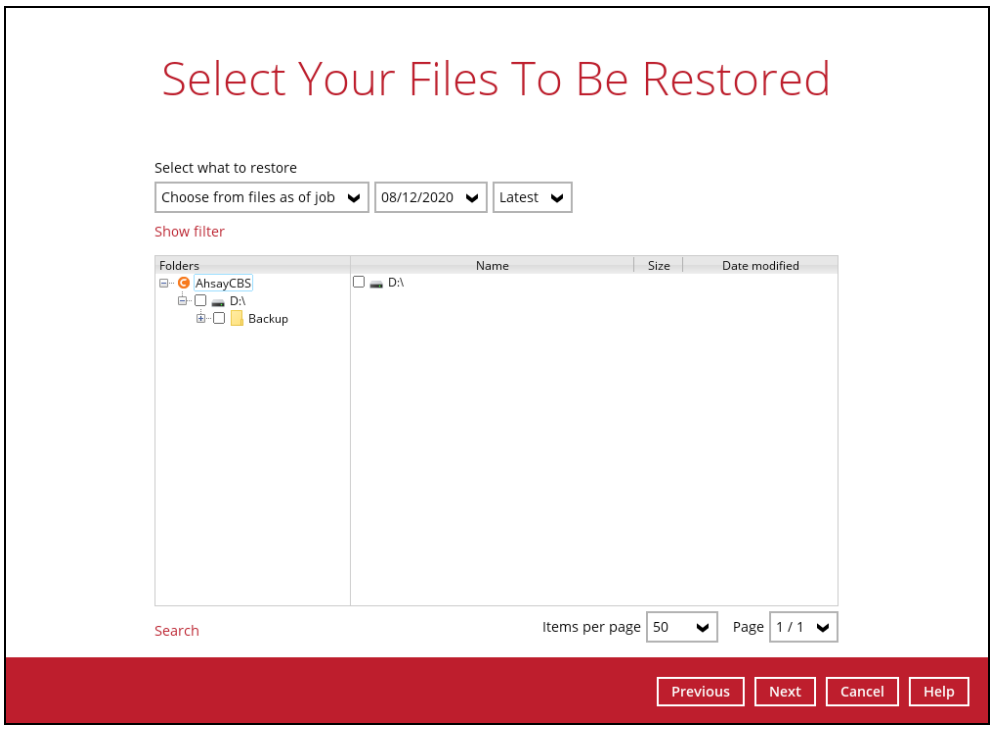


3. Select where you would like to restore your data from.

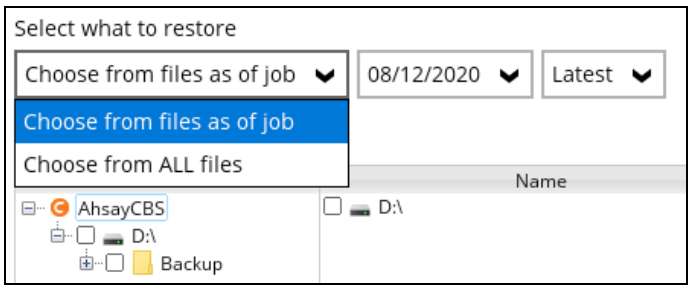


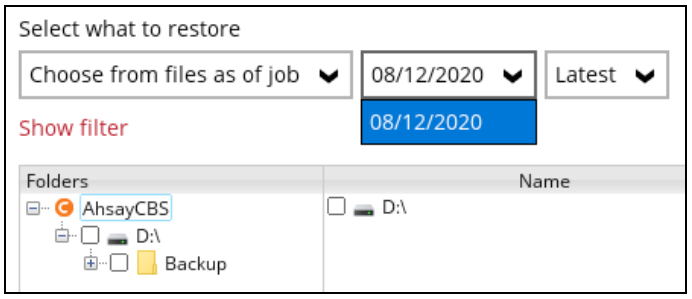
4. Select to restore files from a specific backup job, or from all files available. Then, select the files or folders that you would like to restore.

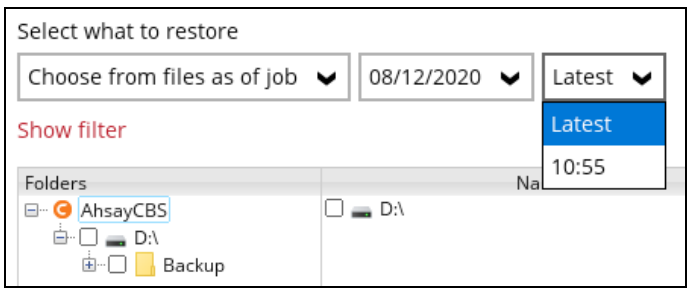
   There are two options from the **Select what to restore** dropdown menu:



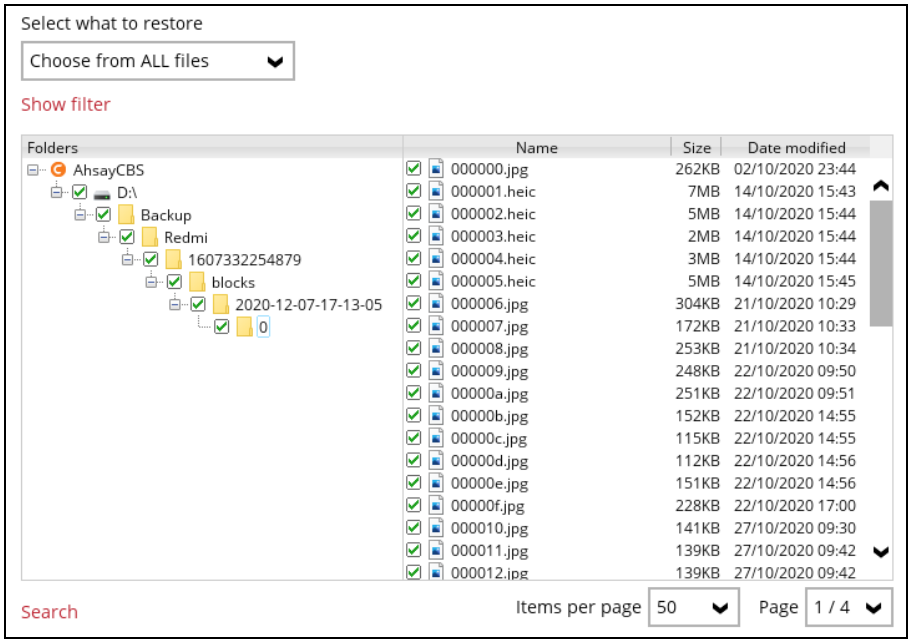
- **Choose from files as of job** – This option allows you to select a backup version from a specific date and time to restore.







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

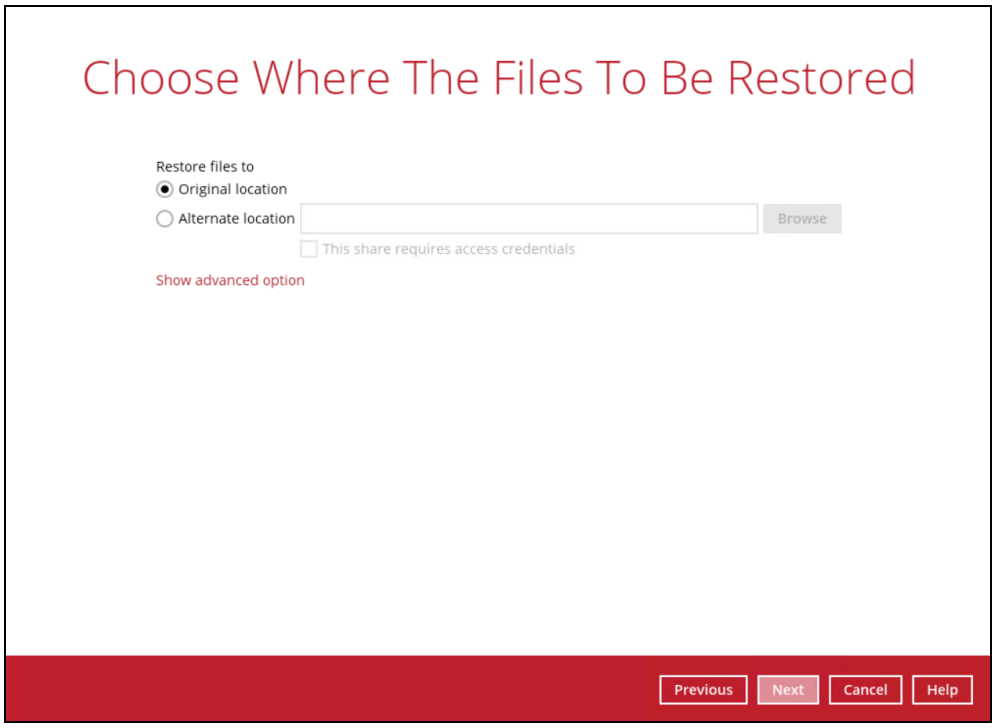


Click **Next** to proceed when you are done with the selections.

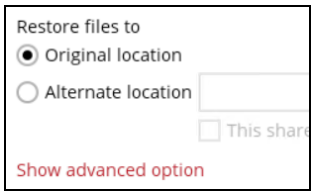
5. Select to restore the files to **Original location**. Then, click **Next** to proceed.

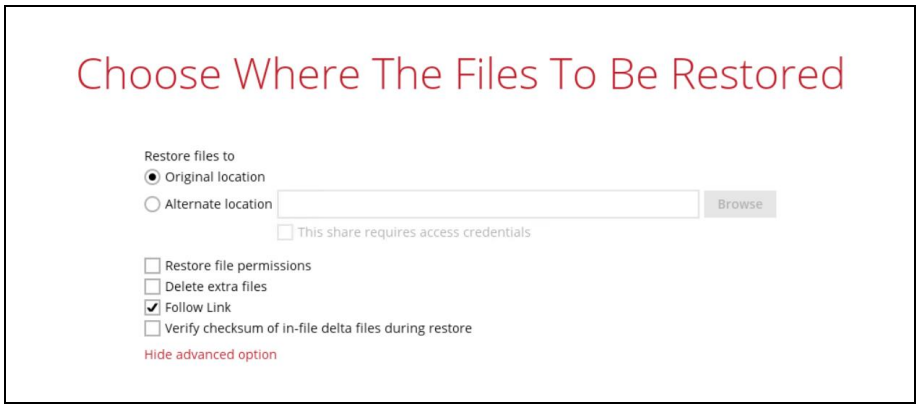
   The backed up data will be restored to the computer running the AhsayOBM under the same directory path as on the machine storing the backup source.

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



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





- **Restore file permissions**

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

- **Delete extra files**

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

  WARNING

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

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

- **Follow Link (Enabled by default)**
  When this option is enabled, not only the symbolic link or junction point will be restored, the directories and files that the symbolic link or junction point links to will also be restored.

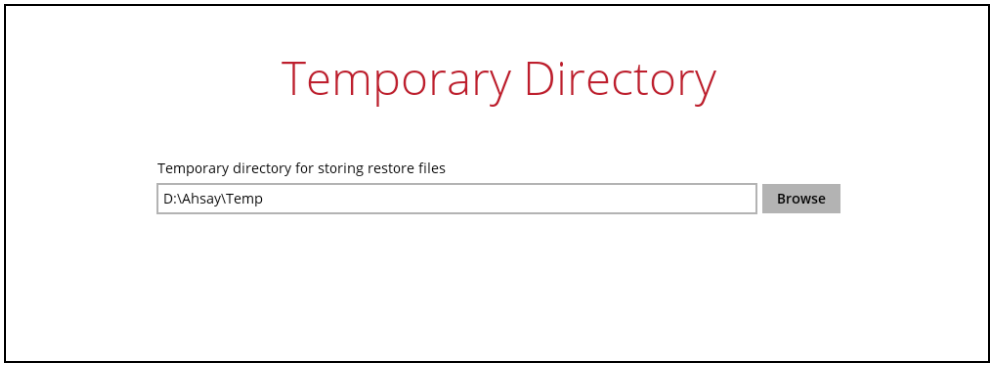
  The table below summarizes the behaviors when a restore is performed with different settings.

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

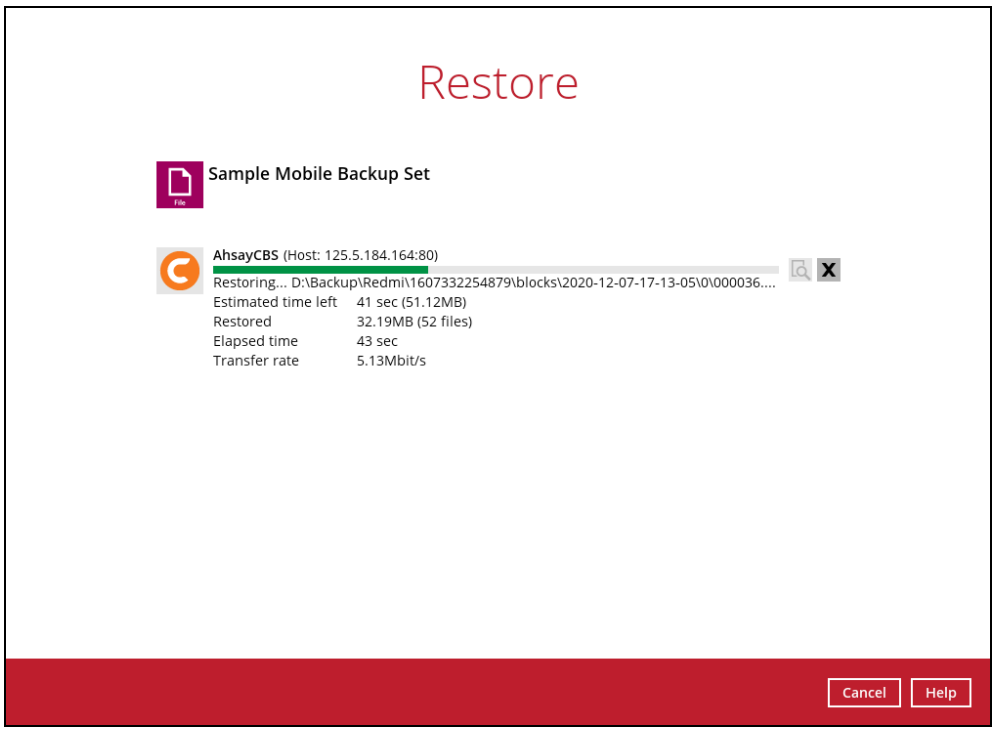
- **Verify checksum of in-file delta files during restore**
  Verify checksum of in-file delta files during restore is disabled by default. You can enable the feature by ticking the checkbox so that the checksum of in-file delta files will be verified. As the feature will make the restore process time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

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

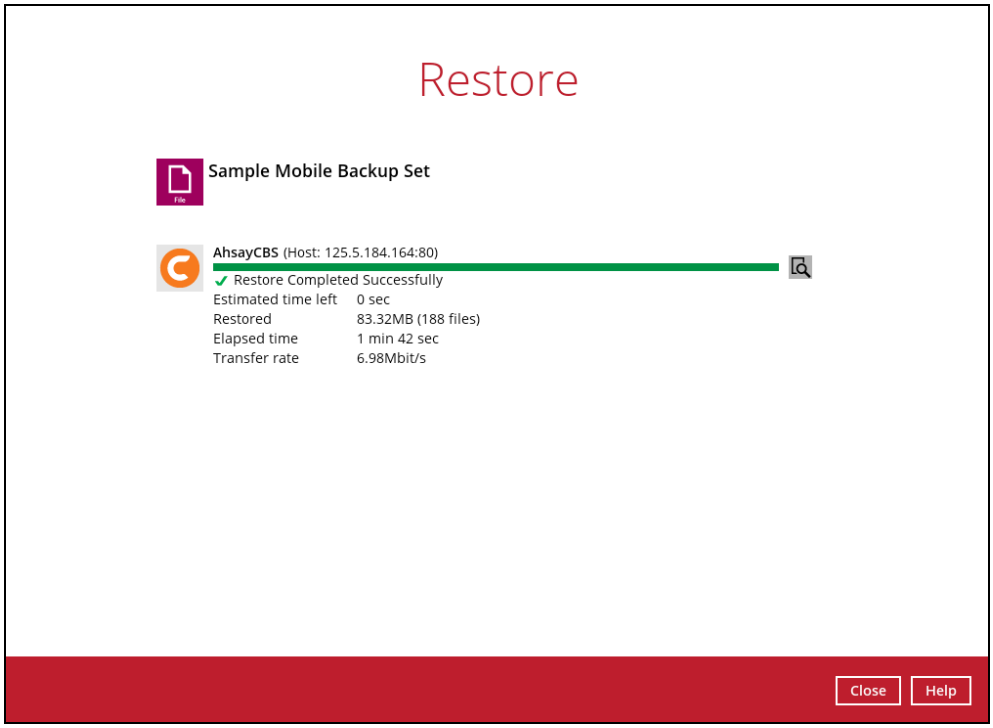
7. Select the temporary directory for storing temporary files, such as delta files, when they are being merged. By default, the temporary files are stored under the temp directory of the user profile directory. In case the same directory path does not exist in the computer you are running AhsayOBM, you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



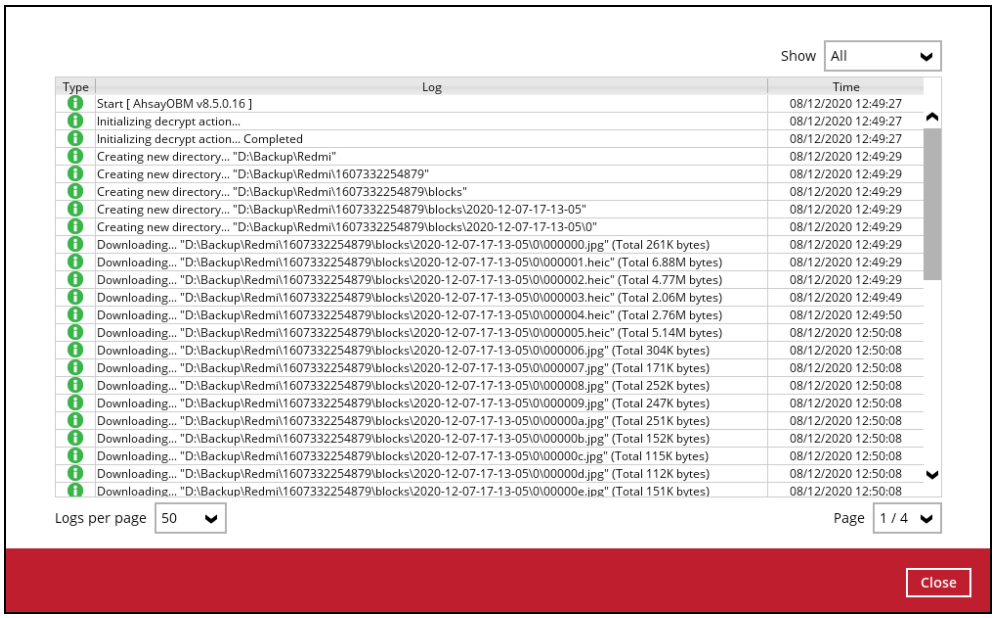
8. Click **Restore** to start the restore. The status will be shown.



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

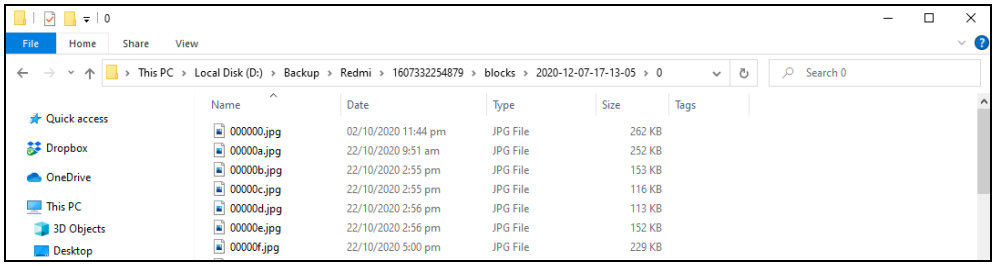


10. You can click the **View** icon on the right-hand side to check the log. A window will pop up to show the log. Close the pop-up window when you finish reading it.

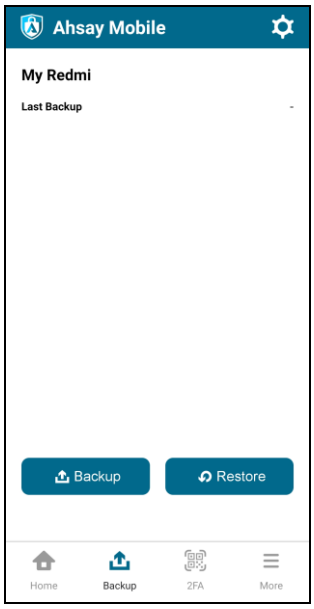


11. You can restore the restored data from the original location to your mobile device by using the Ahsay Mobile app.

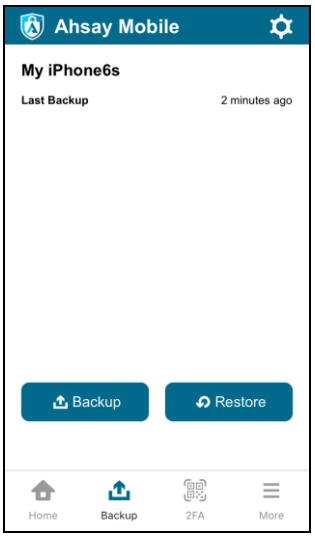
Original location: **D:\Backup\Redmi**



Android device



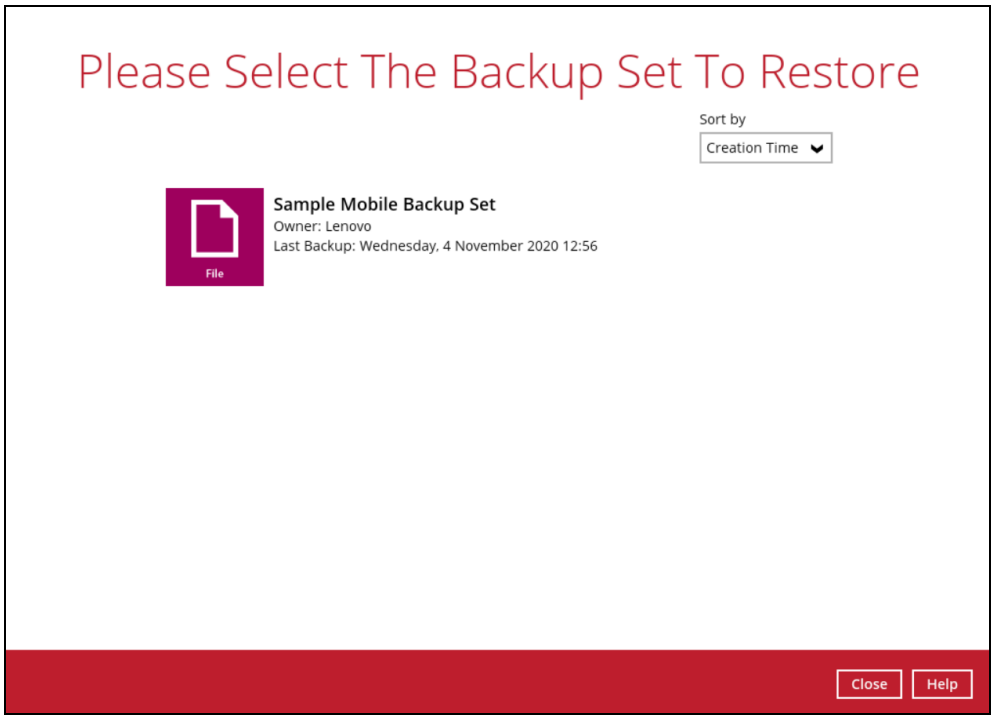
iOS device



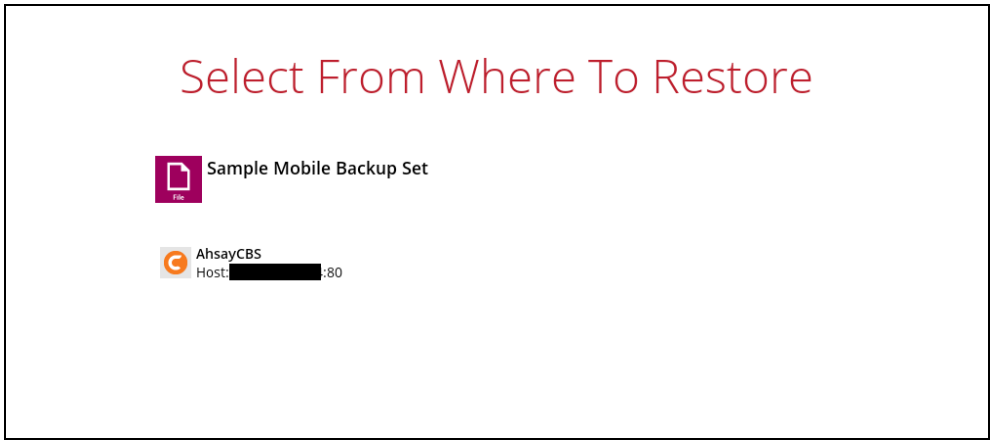
15.3.2 Alternate Location

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

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

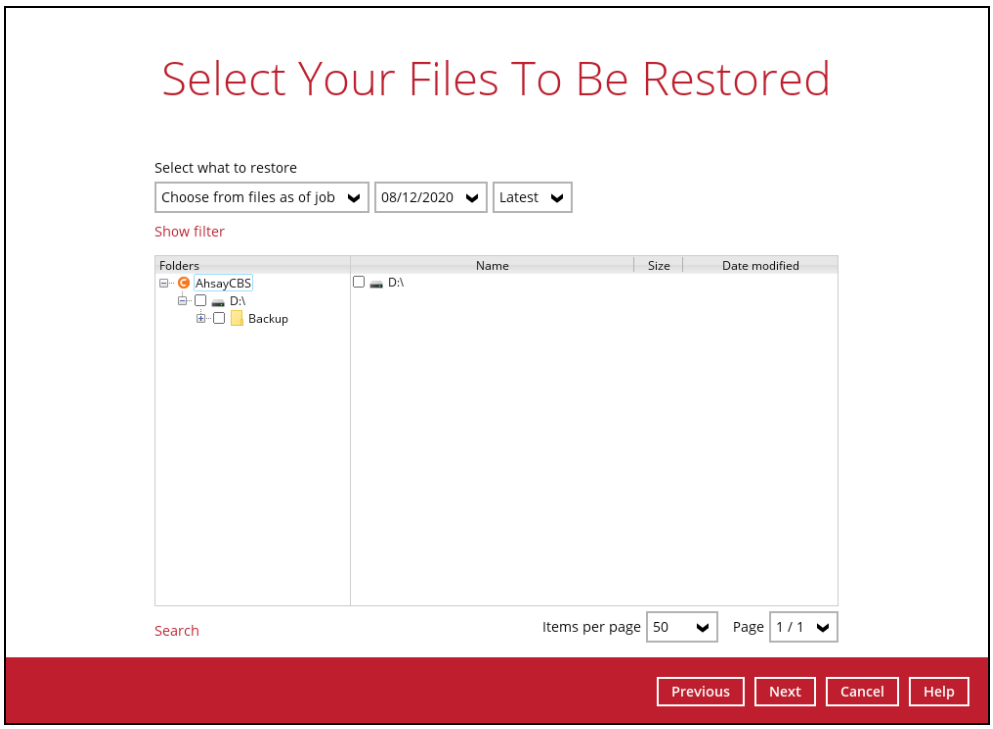


3. Select where you would like to restore your data from.

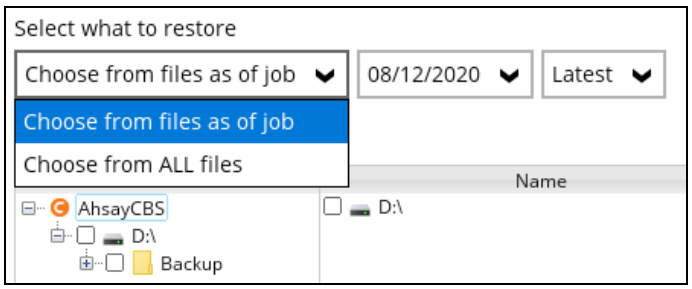


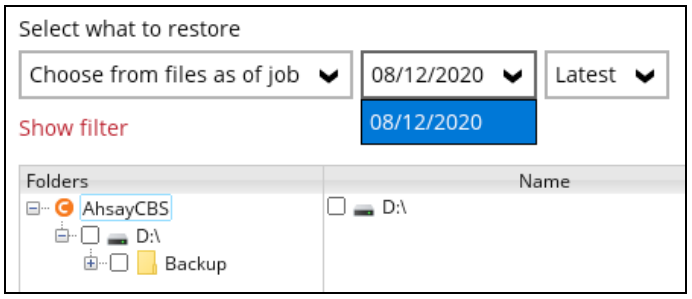
4. Select to restore files from a specific backup job, or from all files available. Then, select the files or folders that you would like to restore.

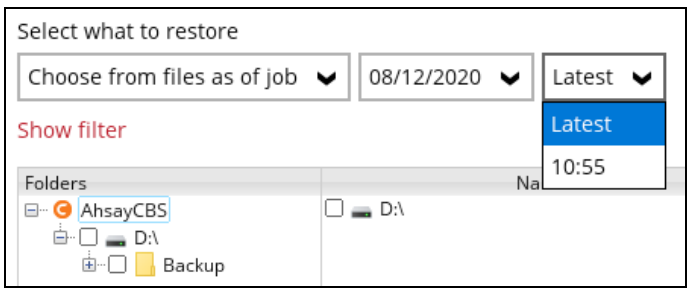
   There are two options from the **Select what to restore** dropdown menu:



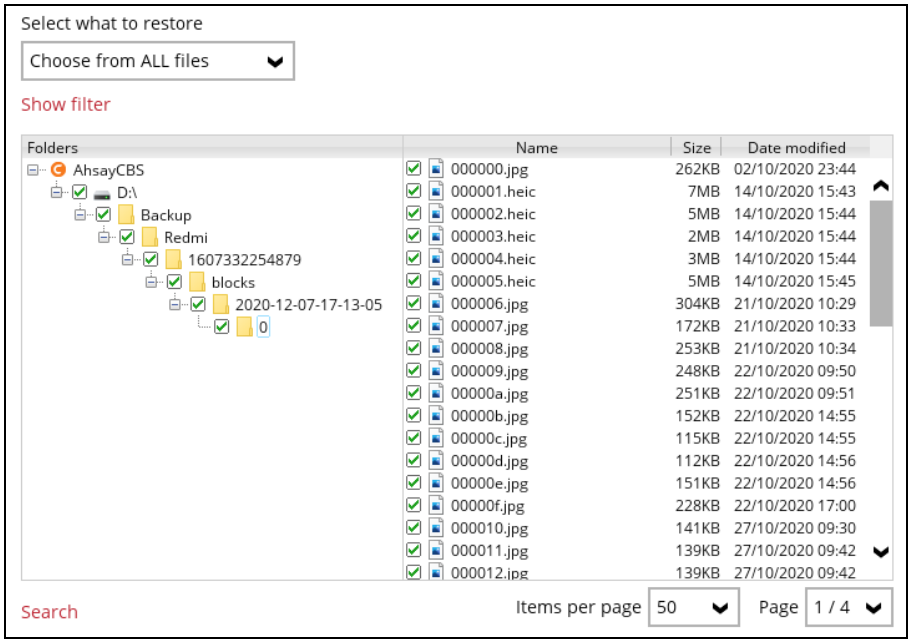
- **Choose from files as of job** – This option allows you to select a backup version from a specific date and time to restore.





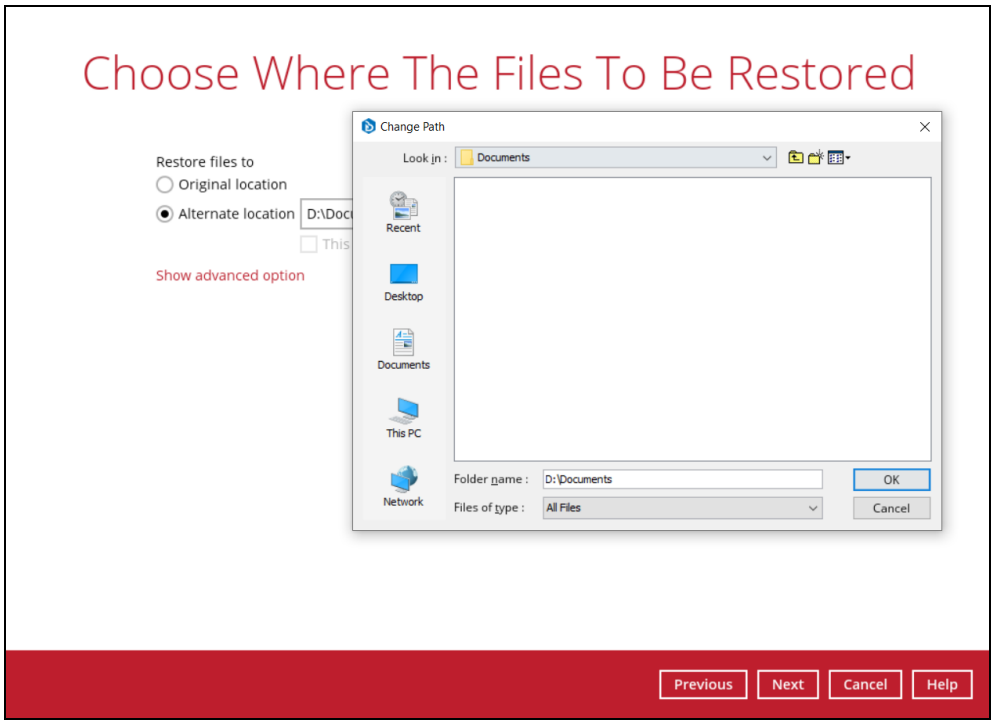


➢ **Choose from ALL files** – This option allows you to restore all files for this backup set.

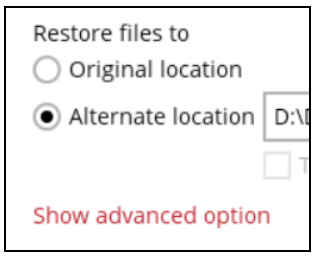


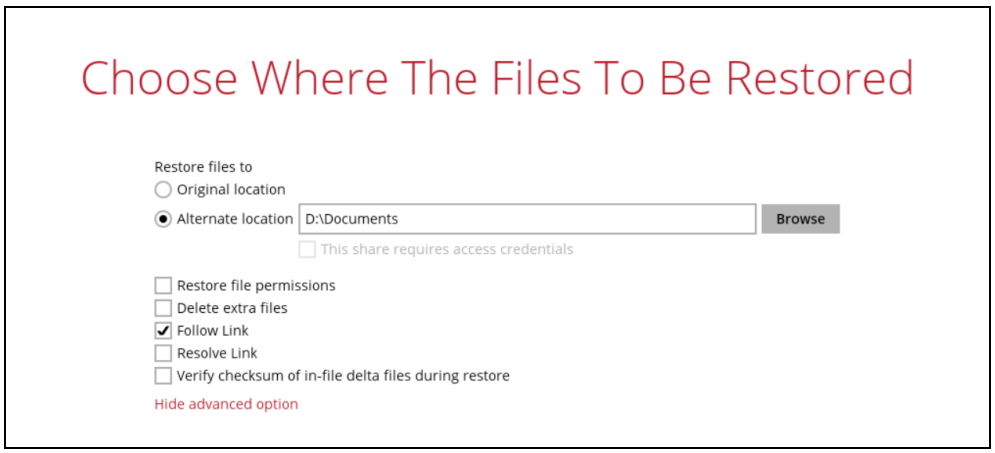
Click **Next** to proceed when you are done with the selections.

5. Select to restore the files to **Alternate location**. You can choose to restore the data to a location of your choice on the computer where AhsayOBM is running. Then, click **Next** to proceed.



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





- **Restore file permissions**

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

- **Delete extra files**

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

  WARNING

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

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

- **Follow Link (Enabled by default)**
  When this option is enabled, not only the symbolic link or junction point will be restored, the directories and files that the symbolic link or junction point links to will also be restored.

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

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

- **Resolve Link**

  This option must be used in conjunction with the Follow Link option. When this option is enabled, the symbolic link, as well as the directories and files that the symbolic link links to will also be restored in the alternate location you have chosen. That means the symbolic link will point to the alternate location instead of the original location.

  The table below summarizes the behaviors when a restore is performed with this option turned on and off.

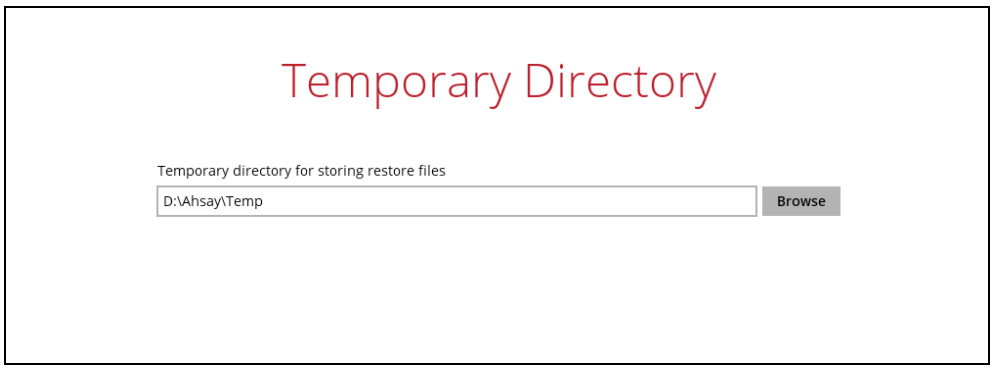
Resolve Link	Behavior
Enabled	Symbolic link is restored to the alternate location specified, with its target directories and files also restored to the same location in their relative path. Target of the link is updated to the new relative path. In other word, the link now points to the new alternate location.
Disabled	Symbolic link is restored to the alternate location specified, with its target directories and files also restored to the same location in their relative path. However, target of the link is NOT updated to the new relative path. In other word, the link still points to the original location.

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

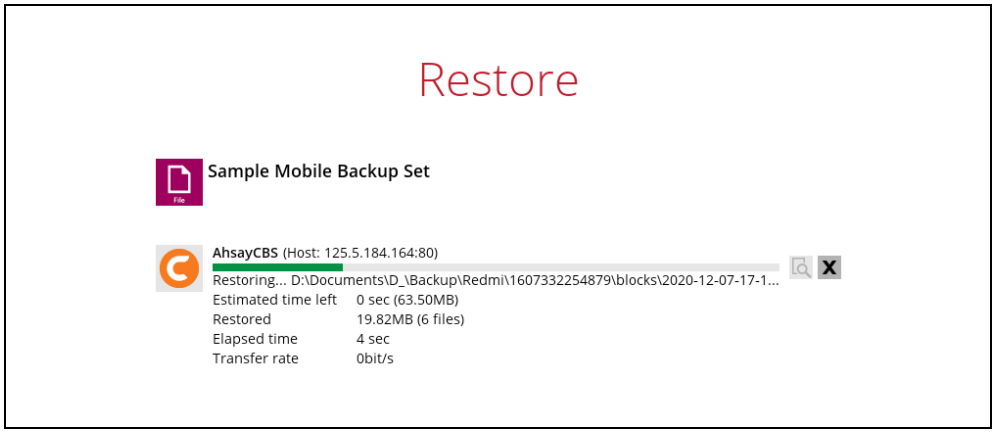
Verify checksum of in-file delta files during restore is disabled by default. You can enable the feature by ticking the checkbox so that the checksum of in-file delta files will be verified. As the feature will make the restore process time longer, it is recommended to enable the feature only if you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

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

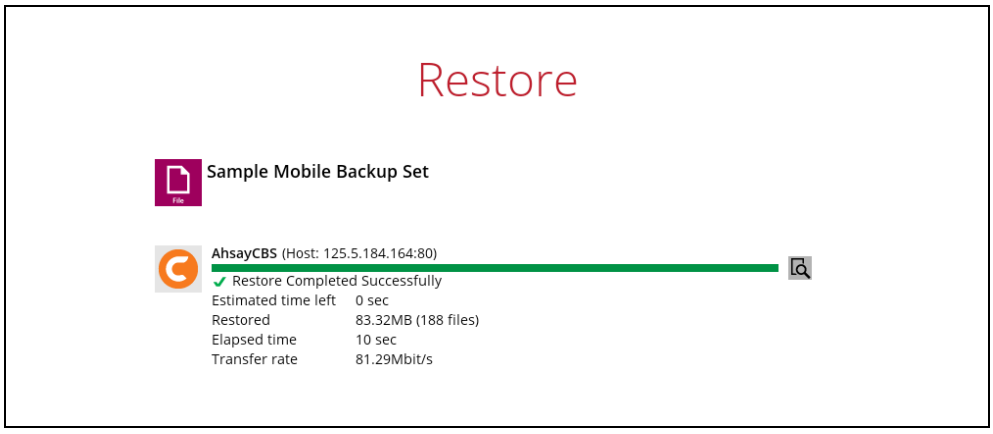
7. Select the temporary directory for storing temporary files, such as delta files, when they are being merged. By default, the temporary files are stored under the temp directory of the user profile directory. In case the same directory path does not exist in the computer you are running AhsayOBM, you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



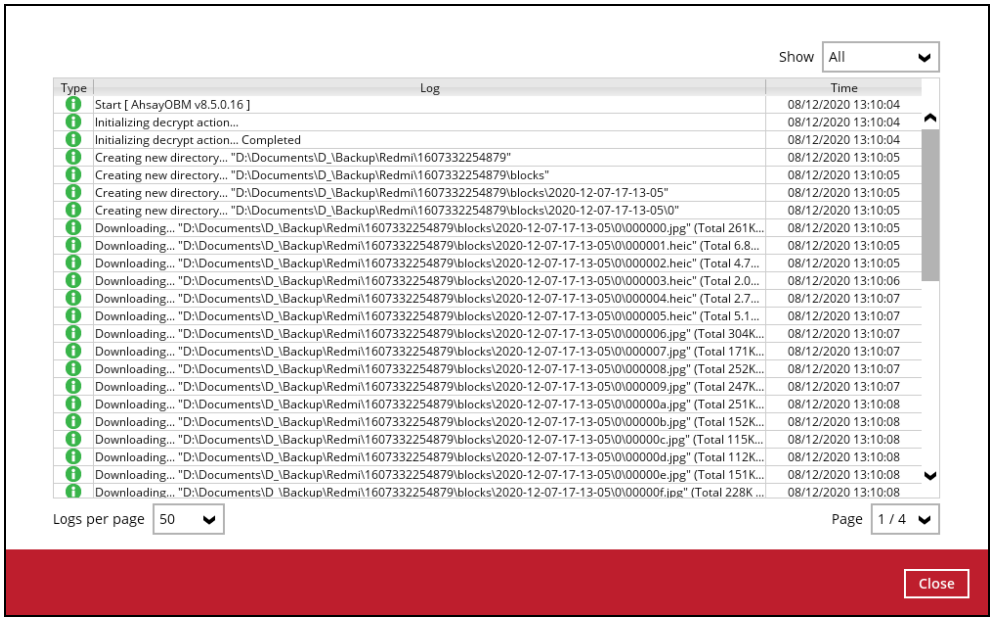
8. Click **Restore** to start the restore. The status will be shown.



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



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

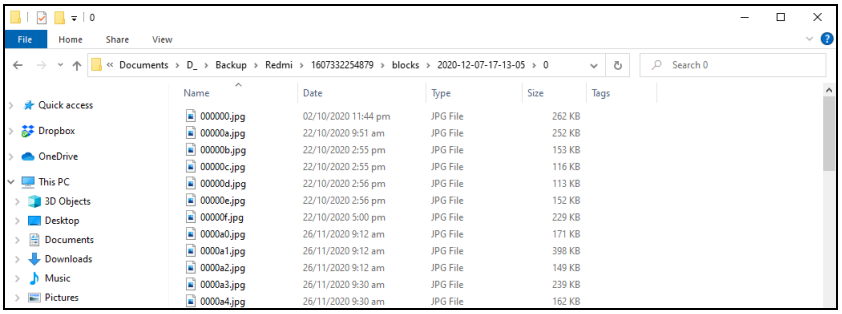


11. These are the steps to restore the restored data from the alternate location to your mobile device.

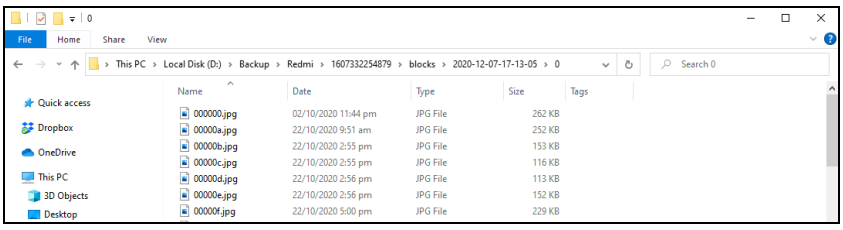
Option 1: Copy the restored data from alternate location to original location which is the **backup destination for your mobile device**.

Example:

Alternate location: **D:\Documents**



Original location: **D:\Backup**



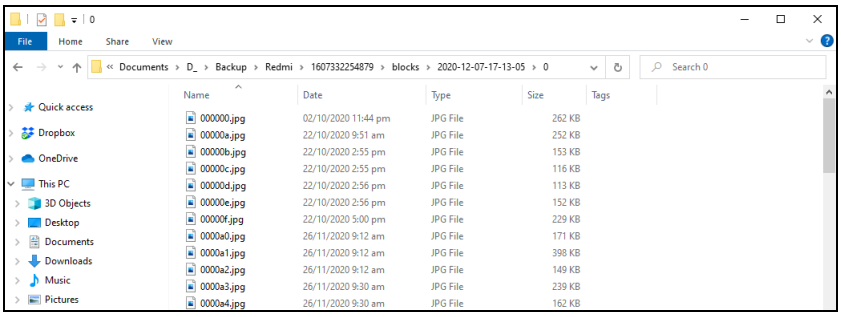
You can now use the Ahsay Mobile app to restore the photos and videos back to your mobile device.

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

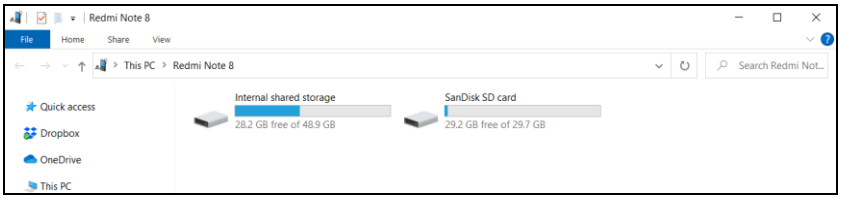
Examples:

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

  Alternate location: **D:\Documents**

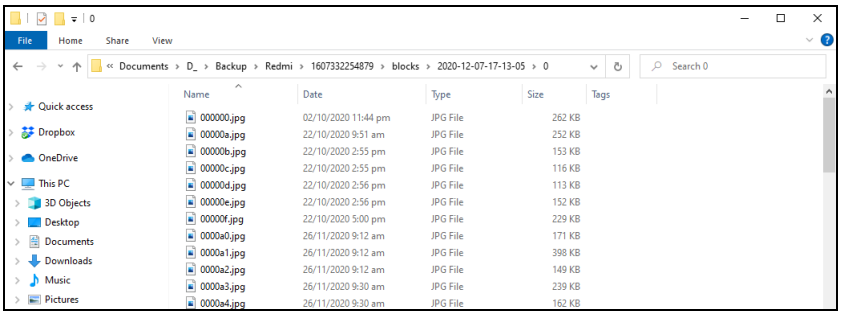


  Mobile device storage: Redmi Note 8 Internal storage and SD Card

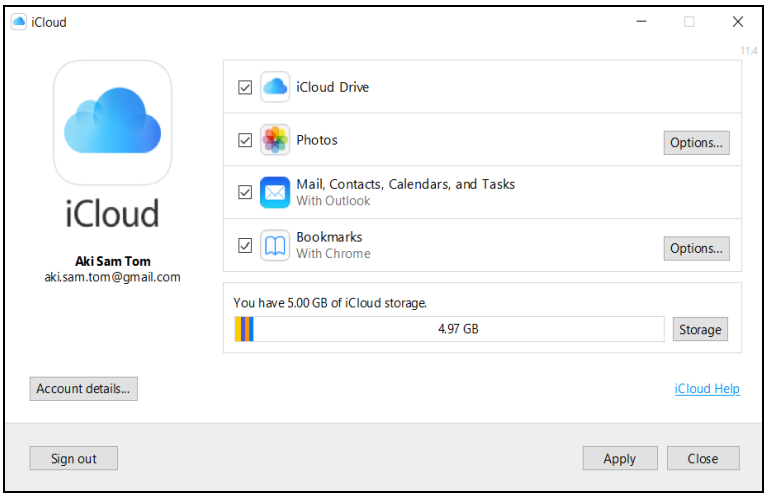


- For an iOS device, you need to transfer the restored data from the alternate location to iCloud.

  Alternate location: **D:\D_\Backup**



  Upload to iCloud using the iCloud app



16 Contact Ahsay

16.1 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/

16.2 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/

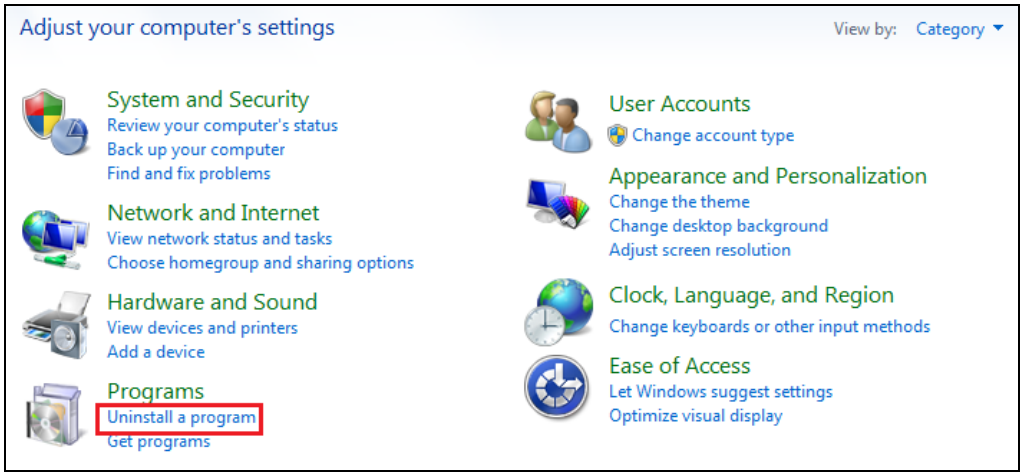
Please specify the specific document title as well as the change required/suggestion when contacting us.

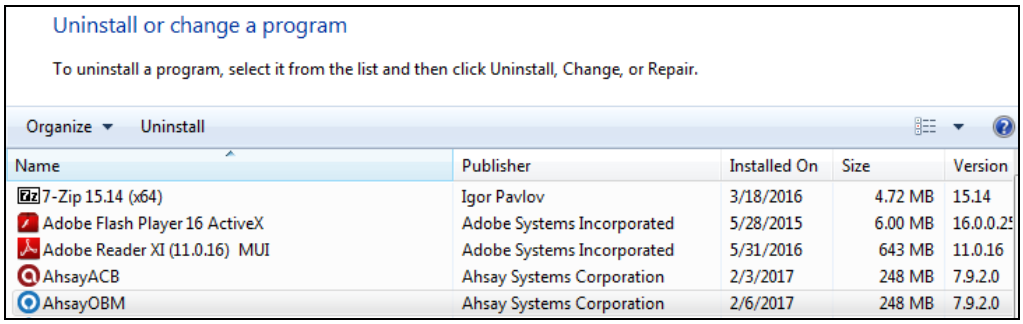
Appendix

Appendix A: Uninstall AhsayOBM

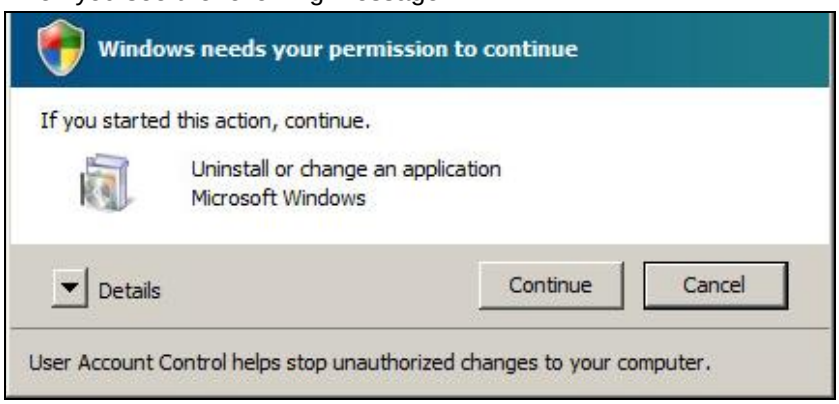
Follow the steps below to uninstall AhsayOBM from your Windows.

1. Go to **Control Panel** > **Programs and Features** > **Uninstall a program**, then look for AhsayOBM and double click on it.

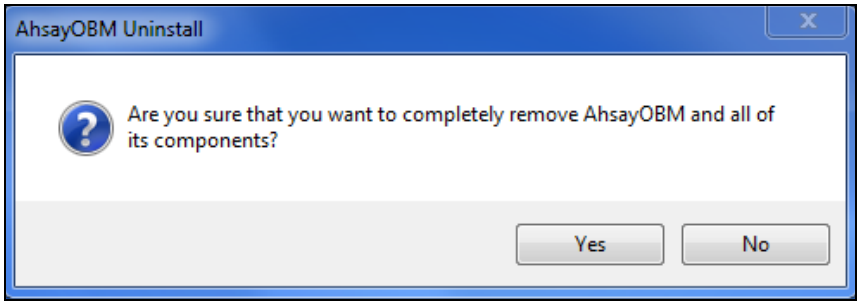




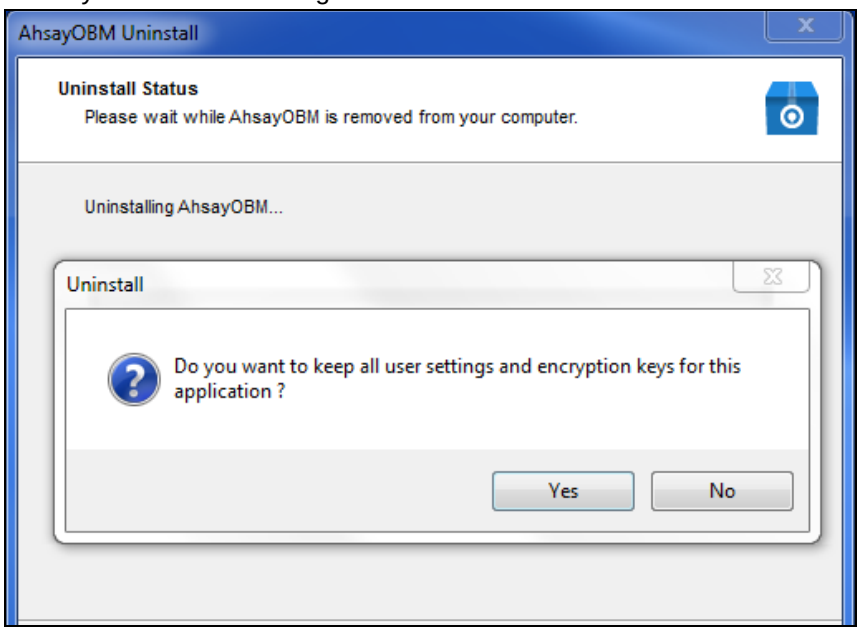
2. The following dialog box will appear only if User Account Control is enabled. Click **Continue** when you see the following message.



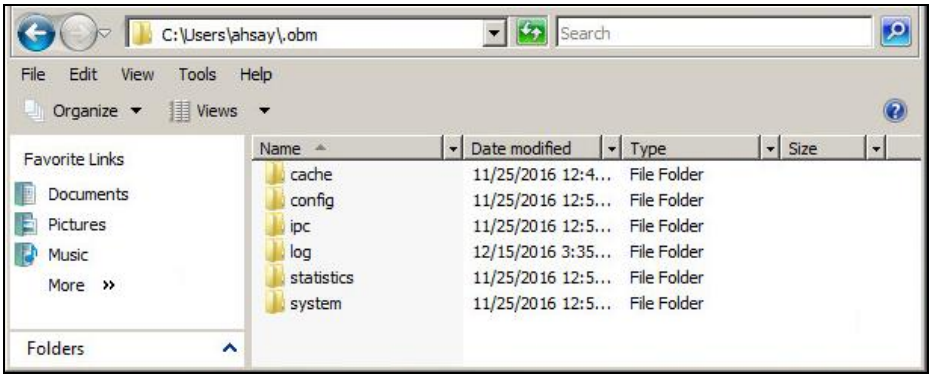
3. Click **Yes** to confirm and proceed with the uninstallation.



4. When you see the following screen:



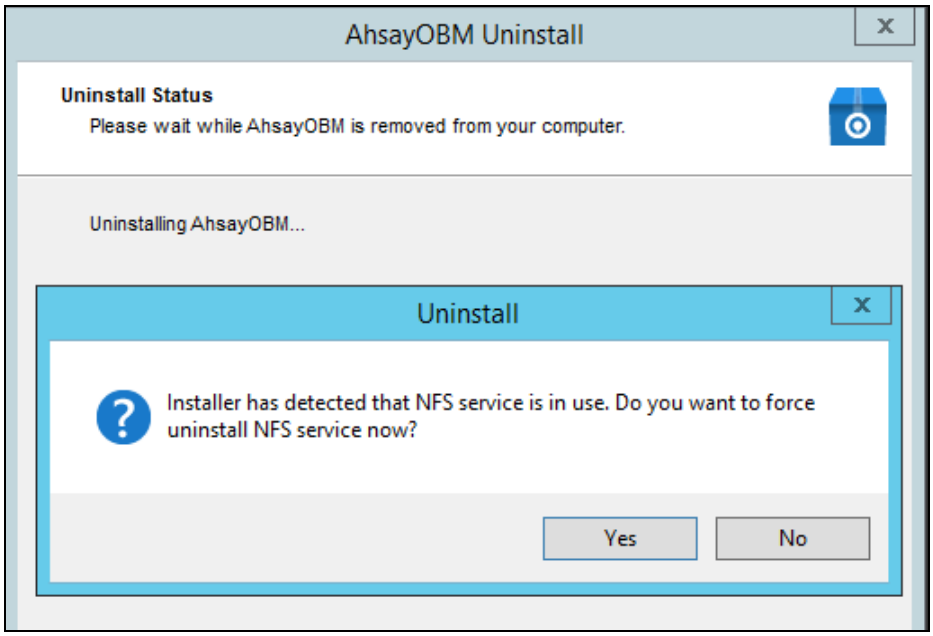
- Choose **Yes** to keep all user settings and the encryption keys associated with the users. If you are likely to install AhsayOBM on the same machine in the future again, the user settings, e.g., login details, backup sets and so forth will remain in **C:\Users\[username]\.obm** by default. The screen capture below shows the folders remain in the machine after uninstallation.



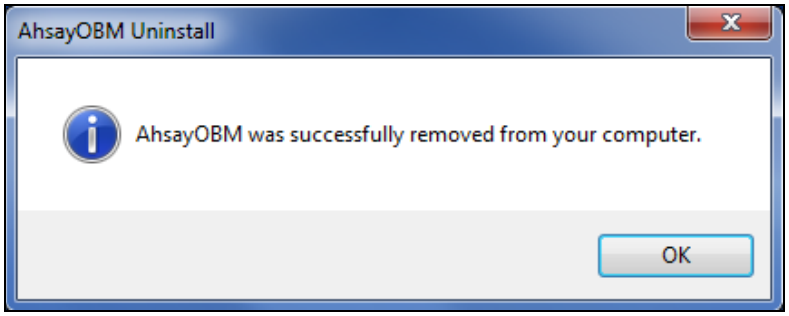
- Choose **No** to delete all user settings and encryption keys with this uninstallation. Please be reminded that the encryption keys are not retrievable once they have been deleted unless the encryption keys have been uploaded to AhsayCBS server, and therefore it will no longer be possible for backup user to recover their encryption key in case they do not have a separate written record.

If there is a Run Direct restore running at the time of the AhsayOBM uninstallation, the following screen prompts to alert you the NFS service is in use.

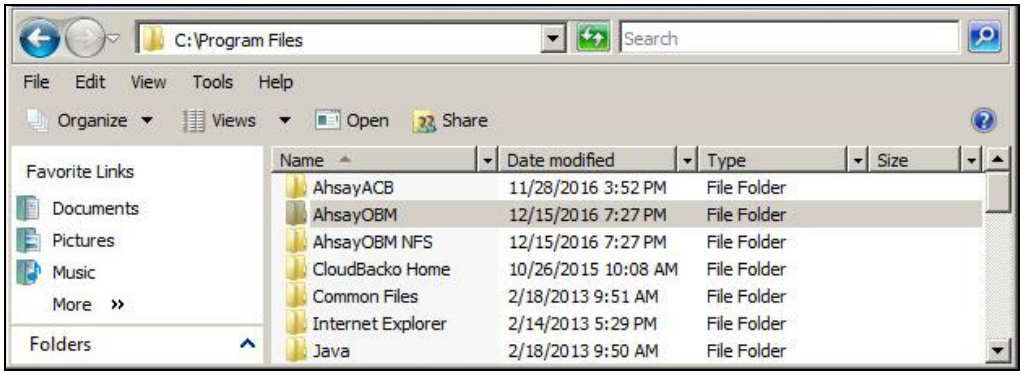
- Select **No** if you do not wish to force uninstall the NFS service. AhsayOBM will be uninstalled without affecting the NFS service, where the Run Direct restore will not be interrupted.
- Select **Yes** to force uninstall the NFS service. Both AhsayOBM and NFS service will be uninstalled from the machine. The VM running Run Direct restore and the datastore are both unmounted from the VMware server.



The following screen prompts when the uninstallation is completed.



(Optional) For a complete removal of all AhsayOBM-related files in your machine, please go to **C:\Program Files** and manually remove the **AhsayOBM** folder.

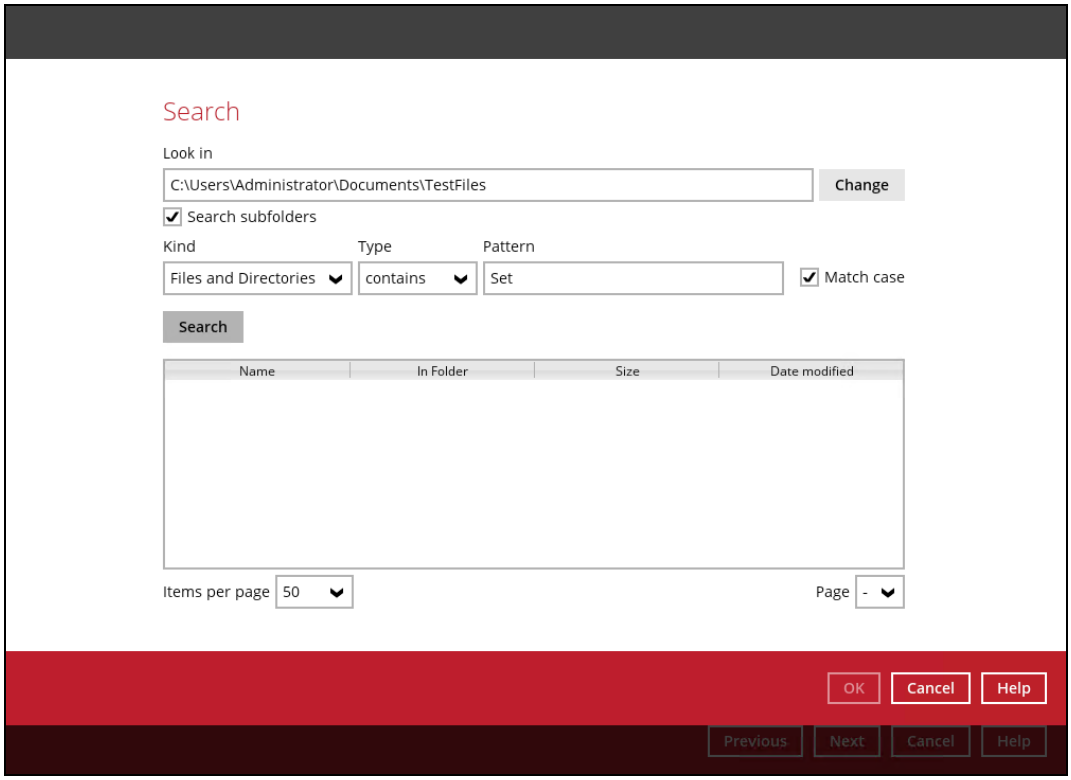


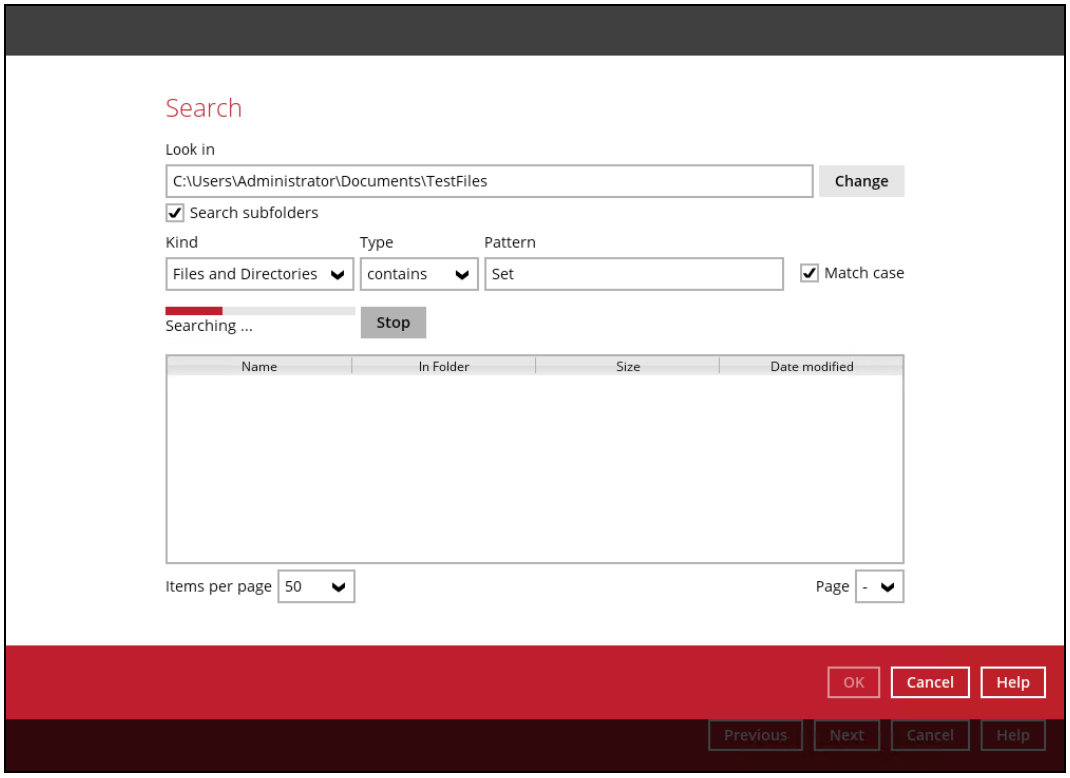
Appendix B: Example Scenarios for Restore Filter

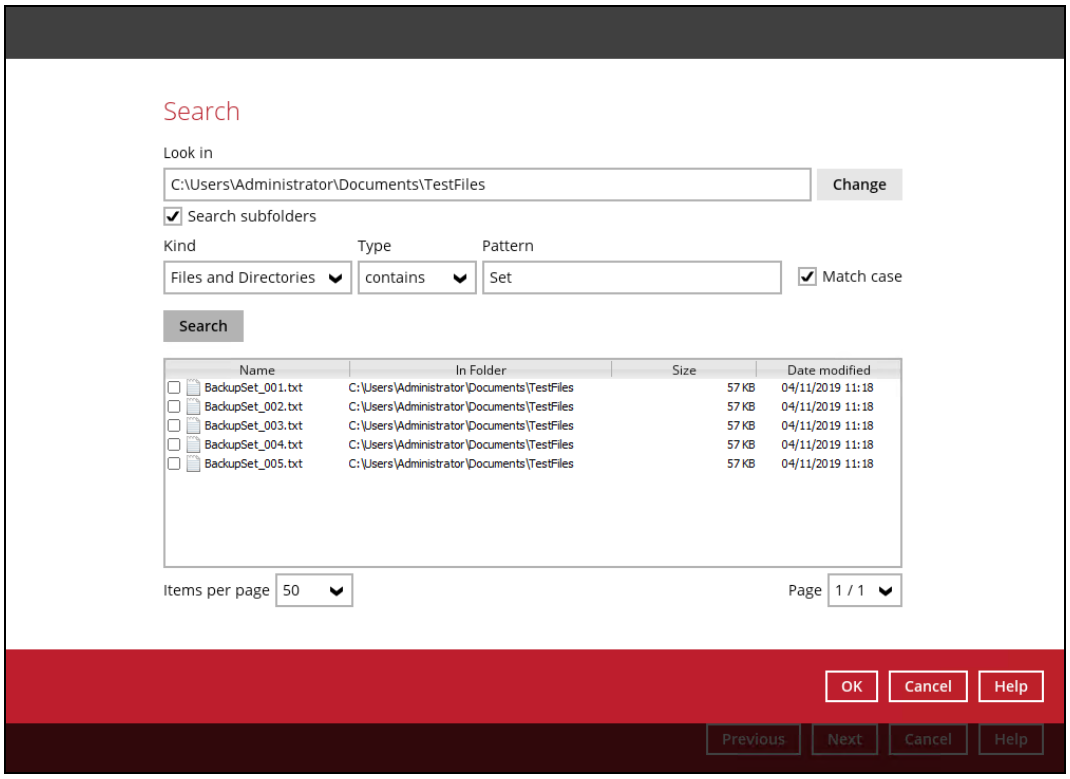
Example No.1: Restore filter setting from C:\Users\Administrator\Documents\TestFiles with filter type Contains

Location:	C:\Users\Administrator\Documents\TestFiles
Search subfolders:	True
Kind:	Files and Directories
Type:	Contains
Pattern:	Set
Match Case:	True

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







Explanation:

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

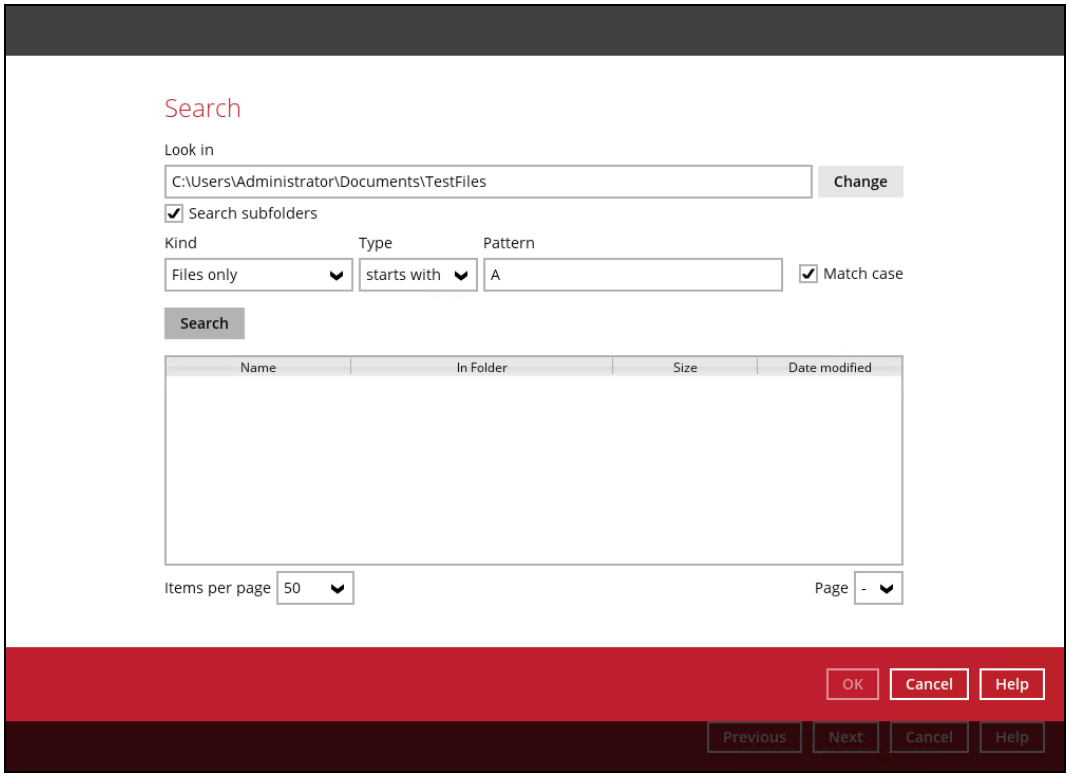
As you can see on the screen shot above, the result panel contains the Name of the file or directory, Directory which are indicated In-Folder column, Size, and Date Modified.

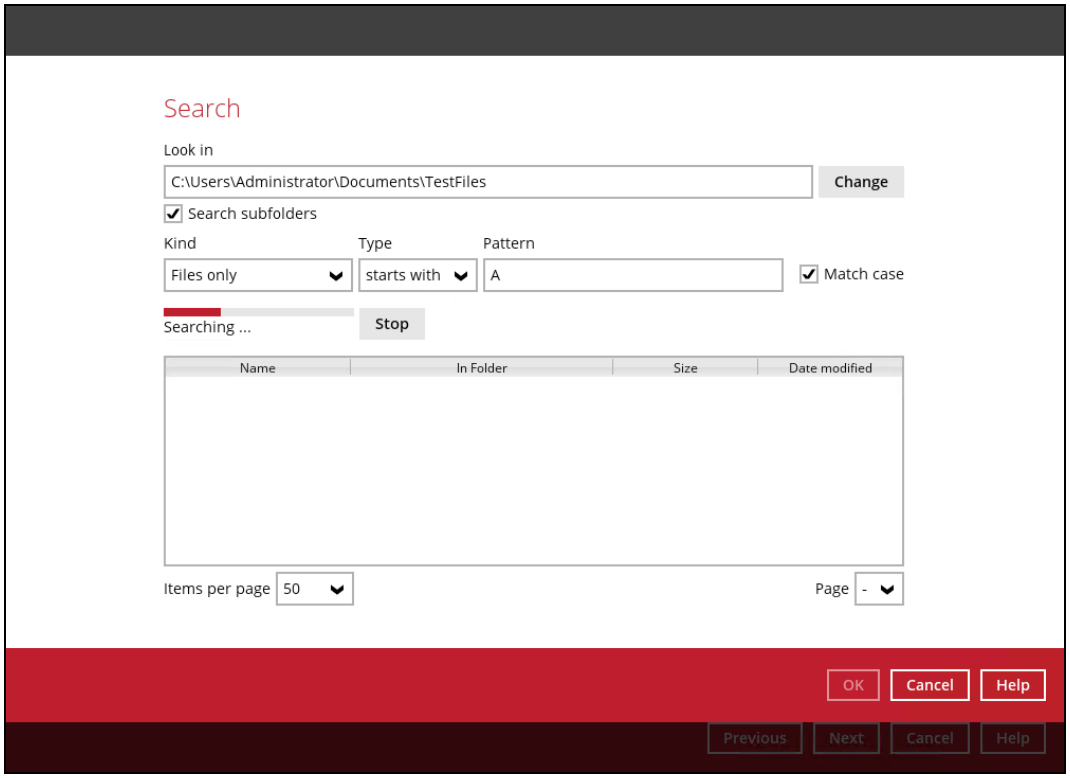
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in \TestFiles upon searching. And it will strictly search only the specified pattern and case which starts with 'Set'.

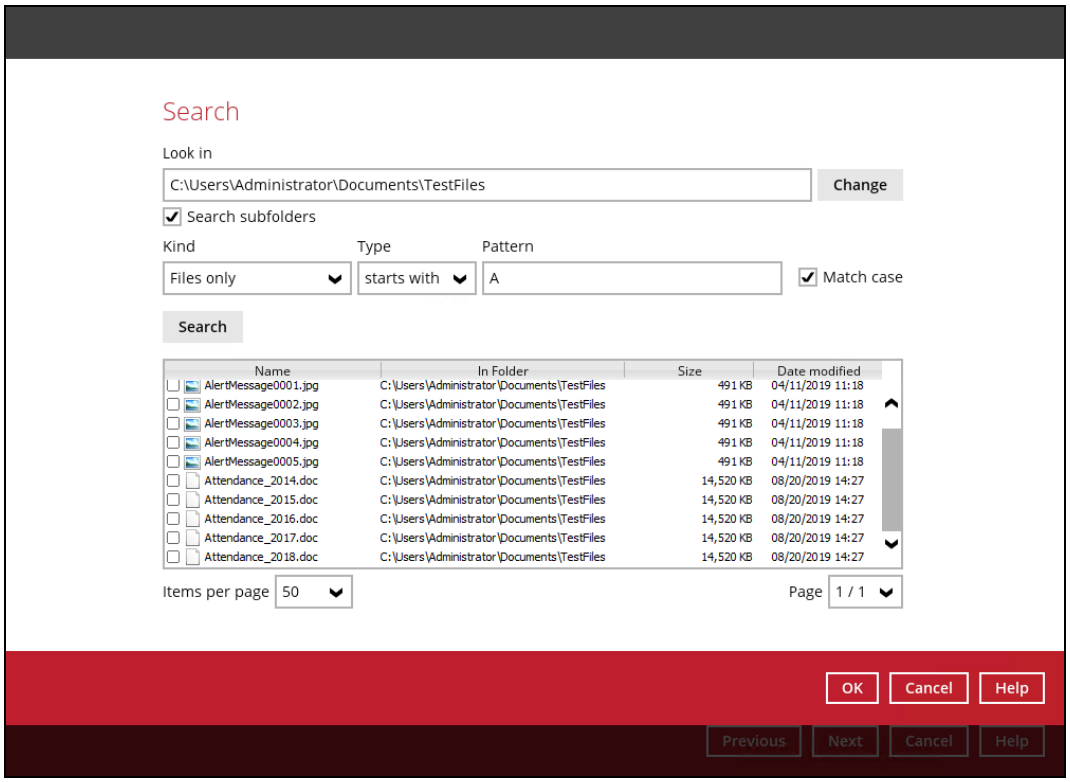
Example No.2: Restore filter setting from C:\Users\Administrator\Documents\TestFiles with filter type Starts With

Location:	C:\Users\Administrator\Documents\TestFiles
Search subfolders:	True
Kind:	Files
Type:	Starts With
Pattern:	A
Match Case:	True

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







Explanation:

All files and directories under C:\Users\Administrator\Documents\TestFiles that has the pattern that starts with 'A' with match case set to true will be included upon performing search.

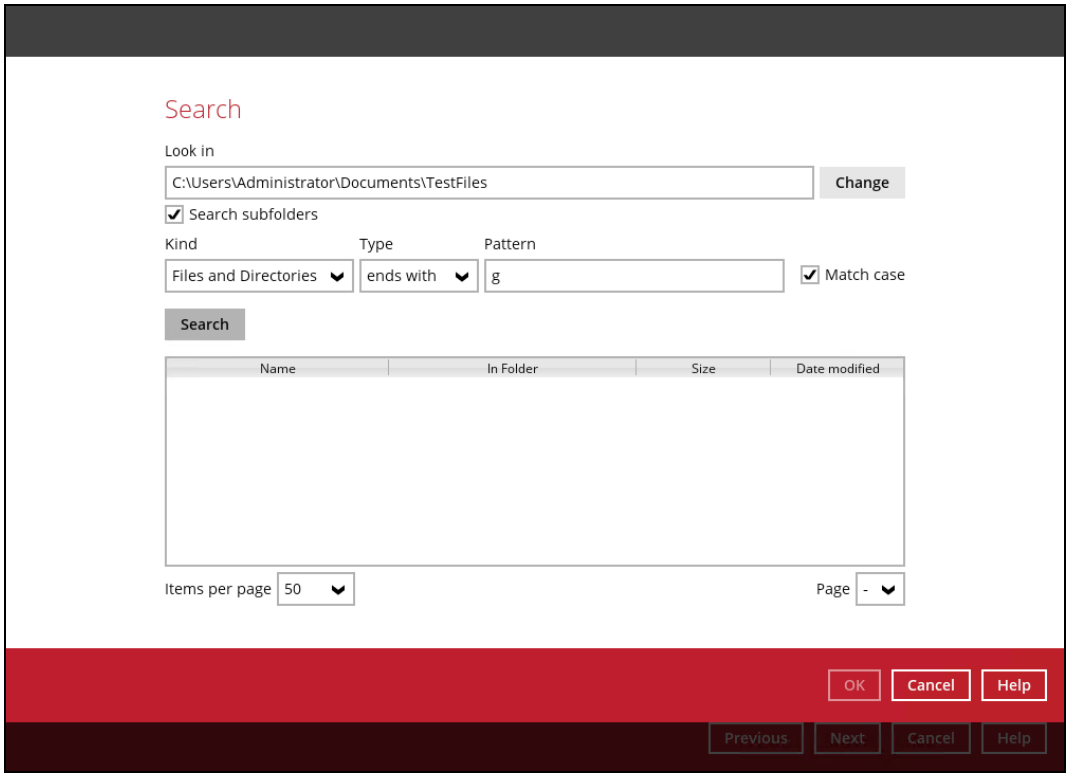
As you can see on the screen shot above, the result panel contains the Name of the file, Directory which are indicated In-Folder column, Size, and Date Modified.

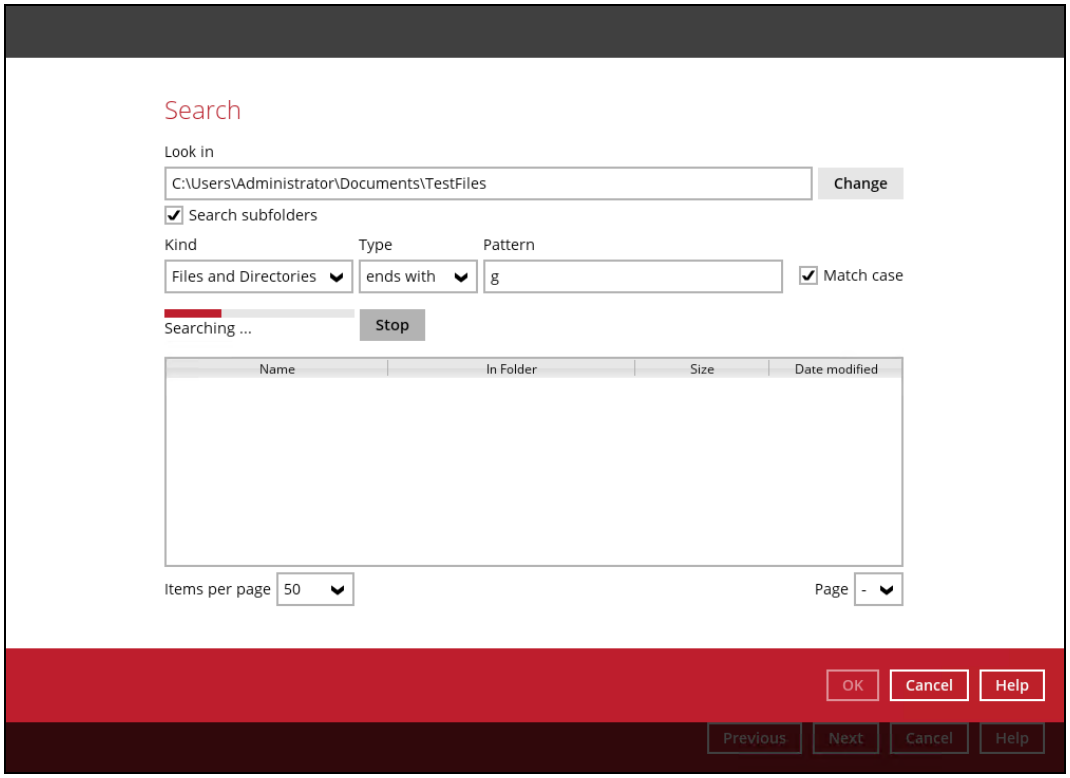
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in \TestFiles upon searching. And it will strictly search only the specified pattern and case which starts with 'A'.

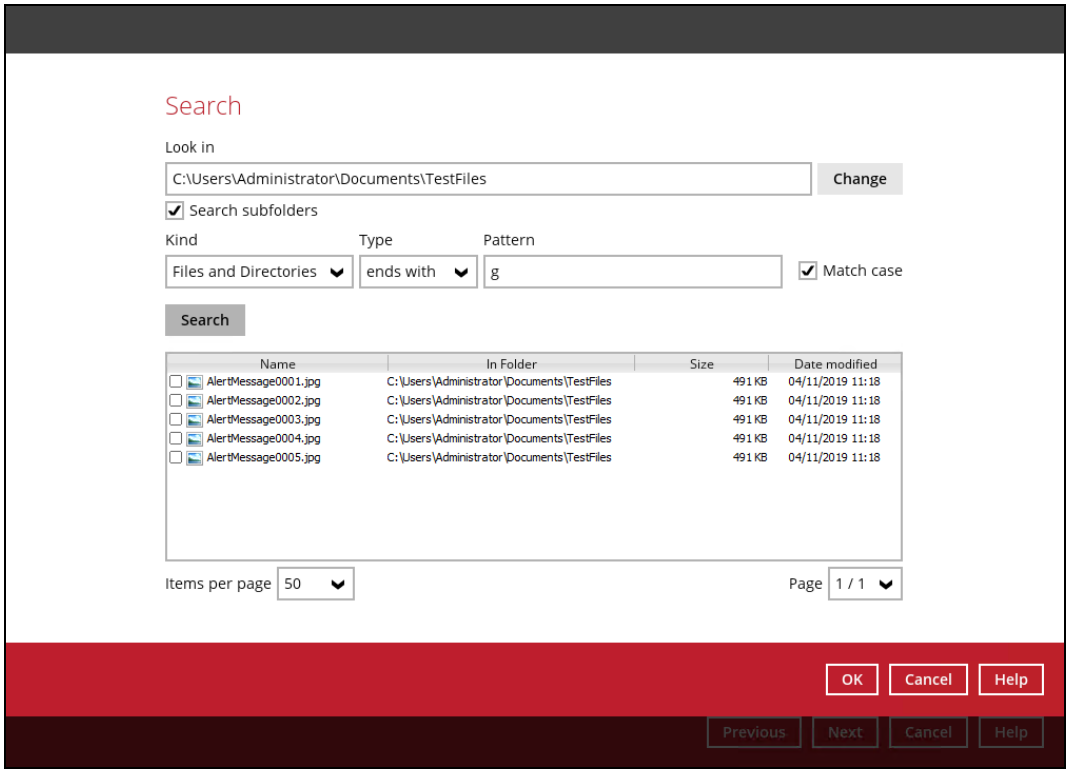
Example No.3: Restore filter setting from C:\Users\Administrator\Documents\TestFiles with filter type Ends With

Location:	C:\Users\Administrator\Documents\TestFiles
Search subfolders:	True
Kind:	Files and Directories
Type:	Ends With
Pattern:	g
Match Case:	True

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







Explanation:

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

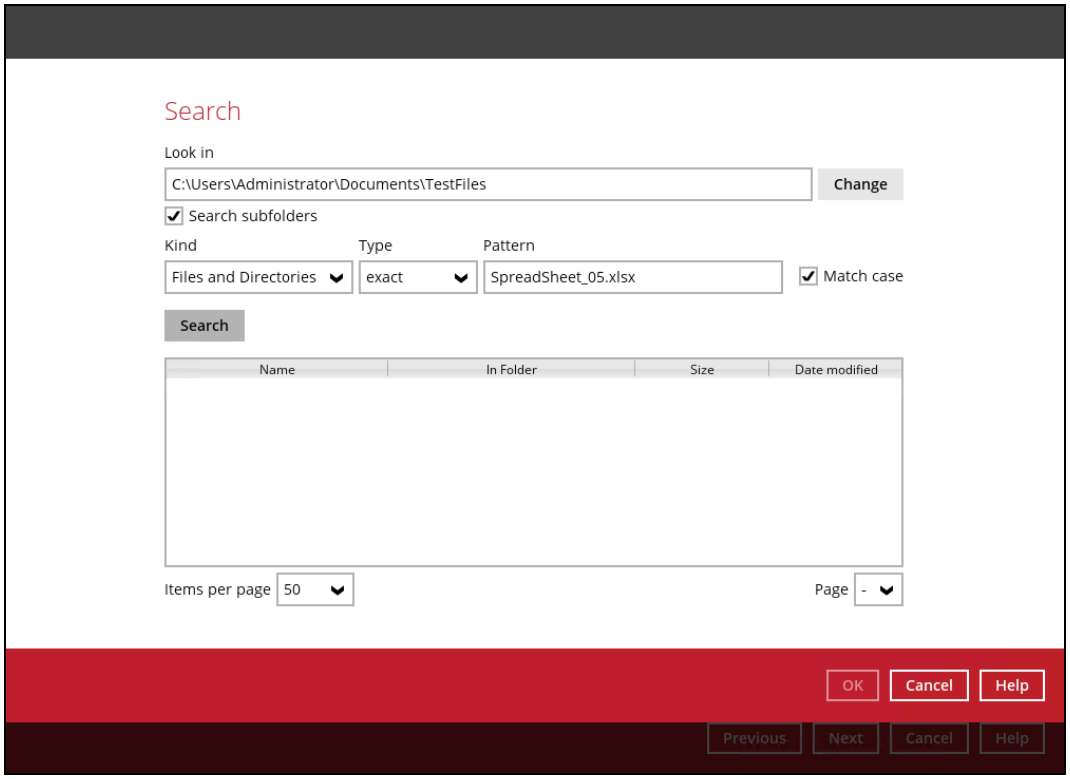
As you can see on the screen shot above, the result panel contains the Name of the files and directories, Directory which are indicated In-Folder column, Size, and Date Modified.

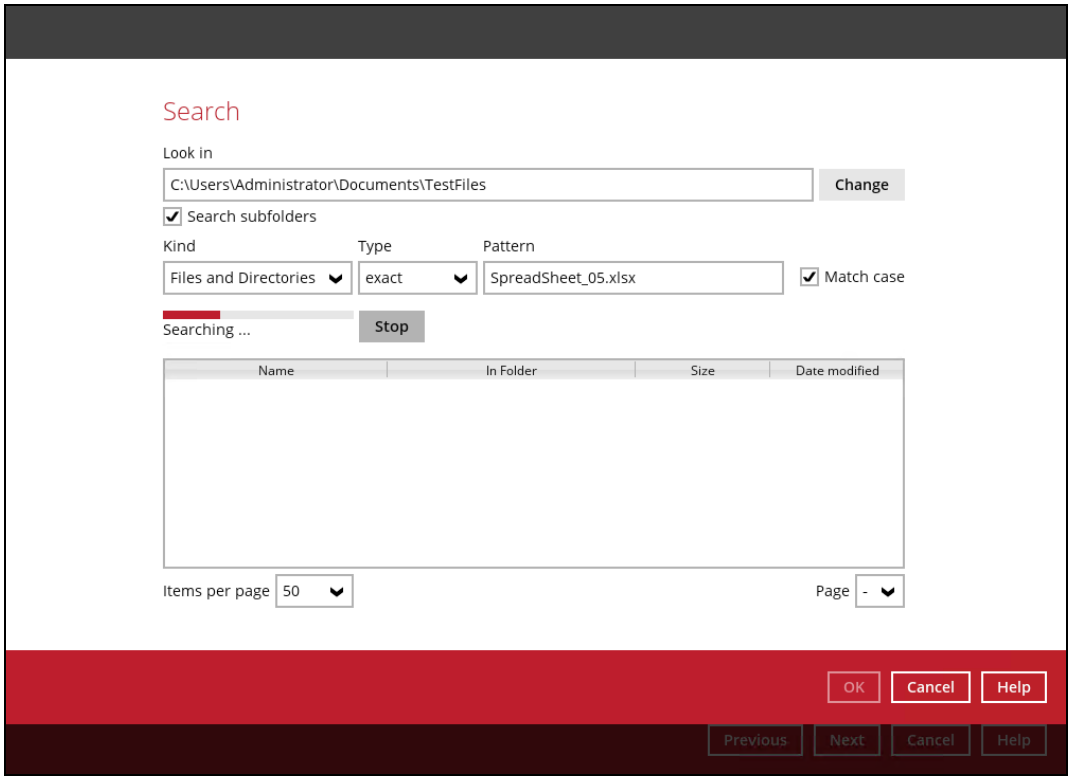
The restore filter setting includes the Search subfolder and Match case set to true. This means that the filter will include all available subfolders in \TestFiles upon searching. And it will strictly search only the specified pattern and case which starts with 'g'.

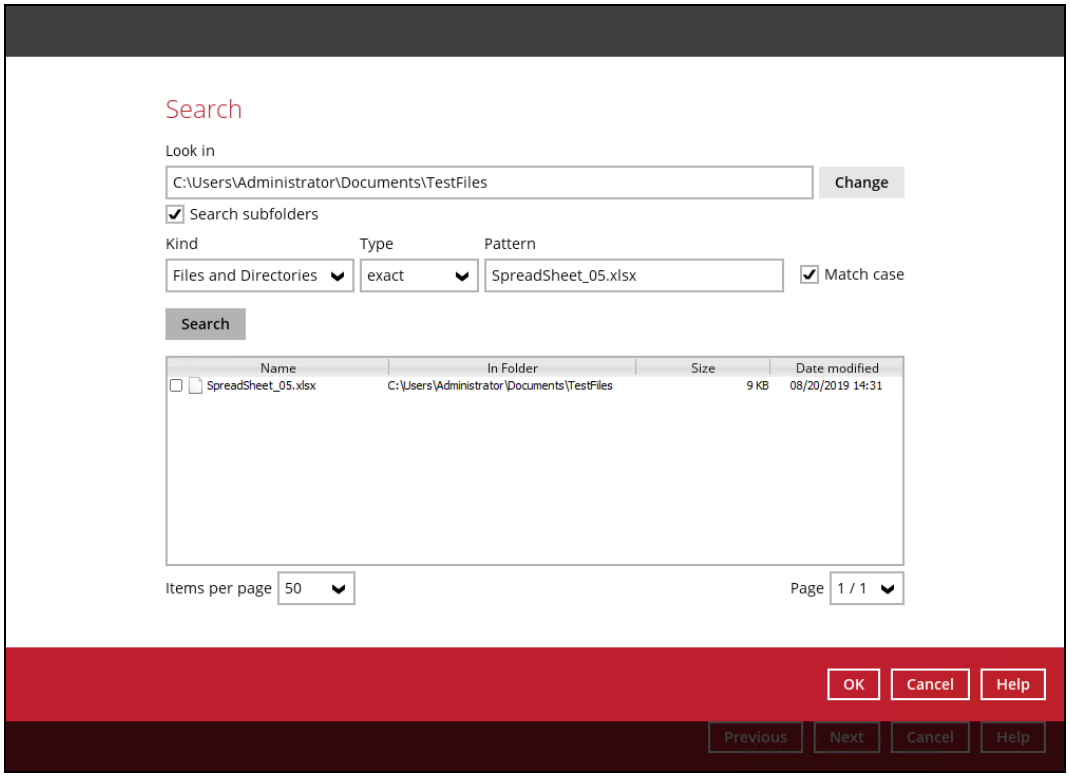
Example No.4: Restore filter setting from C:\Users\Administrator\Documents\TestFiles with filter type Exact

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

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







Explanation:

All files and directories under C:\Users\Administrator\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: Batch Files

Below is the list of batch files which can be used as an alternative way to run the AhsayOBM.

- RunCB.bat
- RunConfigurator.bat
- ListBackupSet.bat
- RunBackupSet.bat
- ListBackupJob.bat
- Restore.bat
- Decrypt.bat
- RunDataIntegrityCheck.bat

RunCB.bat

This allows the user to open the AhsayOBM without clicking the AhsayOBM icon.

On the command prompt (cmd), export the batch file to a text editor using the following script.

```
C:\Program Files\AhsayOBM\bin>notepad RunCB.bat

C:\Program Files\AhsayOBM\bin>
```

Configure the following parameters:

- **SETTING_HOME** – this is the directory to your setting home. If not set, the directory will be "C:\Users\USER\.obm" by default.

  e.g. *SET SETTING_HOME="C:\Users\John\.obm"*

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

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

```
@ECHO OFF
REM ############################  RunCB.bat  ##########################
REM # You can use this batch to run the backup client application
REM ##################################################################
REM ###################  Start: User Defined Section  ################
REM ----------------------------  SETTING_HOME  ----------------------
REM | Directory to your setting home. Default to
REM | "C:\Users\USER\.obm" when not set.
REM | e.g. SET SETTING_HOME="C:\Users\John\.obm"
REM ------------------------------------------------------------------
SET SETTING_HOME=""
REM ----------------------------  DEBUG_MODE  ----------------------
REM | Enable/Disable debug mode
REM | e.g. SET DEBUG_MODE="--debug"
REM |  or  SET DEBUG_MODE=""
REM ------------------------------------------------------------------
SET DEBUG_MODE=""
```

```
REM ####################  END: User Defined Section  ###################
SET EXE_DIR=%CD%
SET APP_HOME=..
SET JAVA_HOME=%APP_HOME%\jvm
SET JAVA_EXE=%JAVA_HOME%\bin\bJW.exe
SET JAVA_LIB_PATH=-Djava.library.path=%APP_HOME%\bin
SET PATH=%JAVA_HOME%\bin;%PATH%
IF "%PROCESSOR_ARCHITECTURE%"=="x86" (
  SET "DEP_LIB_PATH=X86"
  SET JAVA_OPTS=-Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
 ) ELSE (
  SET "DEP_LIB_PATH=X64"
   SET JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
)
SET PATH=%APP_HOME%\bin\%DEP_LIB_PATH%;%JAVA_HOME%\bin;%PATH%
 SET CLASSPATH=%APP_HOME%\bin;%APP_HOME%\bin\cb.jar
REM ########################################################################
ECHO -
ECHO APP_HOME=%APP_HOME%
ECHO SETTING_HOME=%SETTING_HOME%
ECHO JAVA_HOME=%JAVA_HOME%
ECHO JAVA_EXE=%JAVA_EXE%
ECHO JAVA_OPTS=%JAVA_OPTS%
ECHO JAVA_LIB_PATH=%JAVA_LIB_PATH%
ECHO PATH=%PATH%
ECHO CLASSPATH=%CLASSPATH%
ECHO -
@ECHO ON
%JAVA_EXE% %JAVA_LIB_PATH% -cp %CLASSPATH% %JAVA_OPTS% Gui %DEBUG_MODE%
%APP_HOME% %SETTING_HOME%
@ECHO OFF
CD "%EXE_DIR%"
IF "%APP_HOME%"==".." PAUSE
@ECHO ON
```

Once the parameters are configured, save the changes, and close the text editor. Proceed back to *cmd* and enter *RunCB.bat*.

```
C:\Program Files\AhsayOBM\bin>RunCB.bat

-

APP_HOME=..

SETTING_HOME=""

JAVA_HOME=..\jvm

JAVA_EXE=..\jvm\bin\bJW.exe

JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
```

```
JAVA_LIB_PATH=-Djava.library.path=..\bin
PATH=..\bin\X64;..\jvm\bin;..\jvm\bin;C:\Program Files (x86)\Common
Files\ Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\
System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program
Files\Microsoft SQL Server\Client SDK\ODBC\110\Tools\Binn\;C:\Program
Files (x86)\Microsoft SQL Server\120\Tools\Binn\;C:\Program
Files\Microsoft SQL Server\120\DTS\Binn\;C:\Program
Files\PuTTY\CLASSPATH=..\bin;..\bin\cb.jar
-

C:\Program Files\AhsayOBM\bin>..\jvm\bin\bJW.exe -
Djava.library.path=..\bin -cp ..\bin;..\bin\cb.jar -Xms128m -Xmx2048m -
XX:MaxDirectMemorySize=1024m-Dsun.java 2d.noddraw -Dsun.nio. PageAlignDi
rectMemory=true Gui "" .. ""
```

If the debug mode is ENABLED, more technical information will be displayed for troubleshooting purposes.

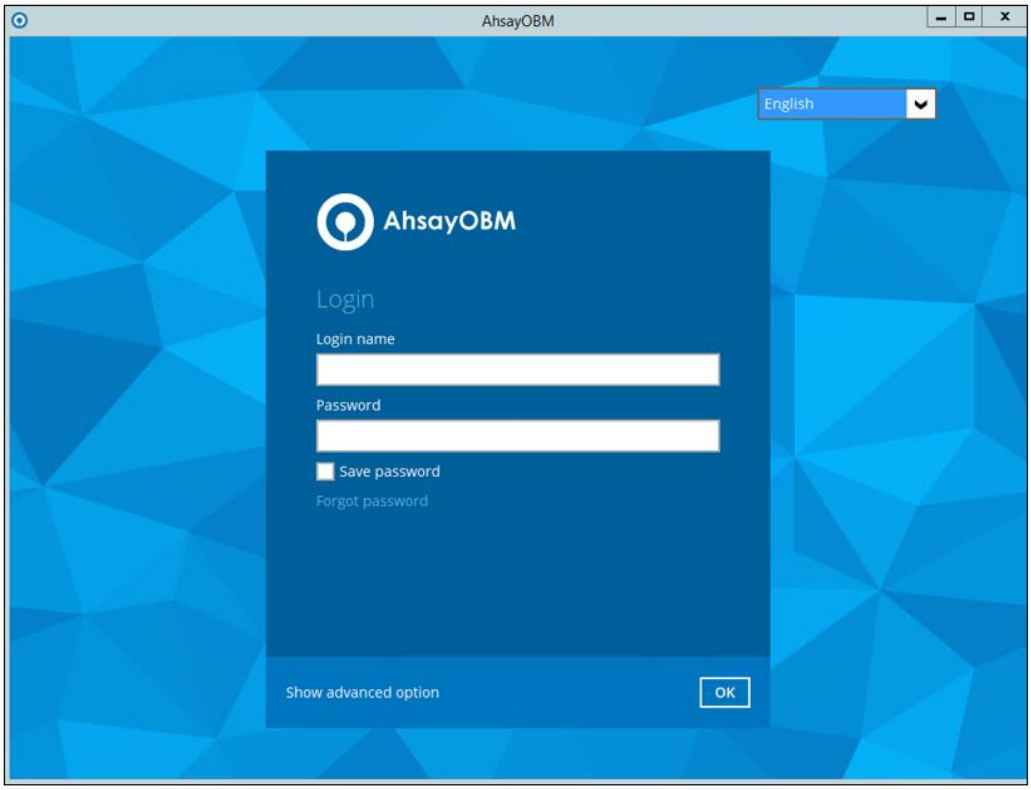
```
C:\Program Files\AhsayOBM\bin>RunCB.bat
-
APP_HOME=..

SETTING_HOME=""

JAVA_HOME=..\jvm

JAVA_EXE=..\jvm\bin\bJW.exe

JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -Dsun.java2d.
noddraw -Dsun.nio.PageAlignDirectMemory=true

JAVA_LIB_PATH=-Djava.library.path=..\bin PATH=..\bin\X64;..\jvm\bin;..
\jvm\bin;C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:
\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows
\System32\WindowsPowerShell\v1.0\;C:\Program Files\Microsoft SQL
Server\ClientSDK\ODBC\110\Tools\Binn\;C:\Program Files (x86)\Microsoft
SQL Server\120\Tools\Binn\;C:\Program Files\Microsoft SQL
Server\120\Tools\Binn\;C:\Program Files\Microsoft SQL
Server\120\DTS\Binn\;C:\Program Files\PuTTY\CLASSPATH=..\bin;..
\bin\cb.jar
-
C:\Program Files\AhsayOBM\bin>..\jvm\bin\bJW.exe -
Djava.library.path=..\bin -cp..\bin;..\bin\cb.jar -Xms128m -Xmx2048m -
XX:MaxDirectMemorySize=1024m -Dsun.java2d.noddraw -
Dsun.nio.PageAlignDirectMemory=true Gui "--debug" .. ""
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/asm-3.1.jar to
classpath ...OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/bcmail-jdk15on-
1.51.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/bcpkix-jdk15on-
1.51.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/bcprov-jdk15on-
151.jar to classpath ... OK
```

```
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/cab-parser-2.9.jar
to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/cab-parser-dorkbox-
util-1.1.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/cabinet-maker-
1.0.0.1.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/commons-codec-
1.6.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/commons-io-2.5.jar
to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/commons-logging-
1.1.3.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/commons-net-3.3.jar
to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/dom4j-1.6.1.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/dropbox-core-sdk-
1.7.5.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/dropbox-core-sdk-
3.0.3.1.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/dropbox-core-sdk-
3.0.3.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/fluent-hc-4.3.5.jar
to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/forms-1.3.0.jar to
classpath... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/google-api-client-
1.19.1.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/google-api-client-
jackson2-1.19.1.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/google-api-services-
drive-v2-rev158-1.19.1.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/google-http-client-
1.19.0.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/google-http-client-
jackson2-1.19.0.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/google-oauth-client-
1.19.0.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/httpclient-4.3.5.jar
to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/httpclient-cache-
4.3.5.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/httpcore-4.3.2.jar
to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/httpmime-4.3.5.jar
to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jackson-annotations-
2.2.3.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jackson-annotations-
2.7.4.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jackson-core-
2.2.3.jar to classpath ... OK
```

```
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jackson-core-
2.7.4.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jackson-core-asl-
1.9.13.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jackson-databind-
2.2.3.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jackson-databind-
2.7.4.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jackson-jaxrs-
1.9.2.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jackson-mapper-asl-
1.9.13.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jackson-xc-1.9.2.jar
to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/java-xmlbuilder-
0.4.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/javax.mail.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jcifs-1.3.18.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jdokan-20170627.jar
to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jdom-1.1.3.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jersey-apache-
client4-1.18.1.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jersey-bundle-
1.18.1.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jersey-multipart-
1.18.1.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jettison-1.1.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jsch-0.1.50.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jsch-0.1.54.1.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/json_simple-1.1.jar
to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/jsr305-1.3.9.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/log4j-1.2.17.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/microsoft-
windowsazure-api-0.4.6.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/microsoft-
windowsazure-storage-sdk-1.0.0.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/microsoft-
windowsazure-storage-sdk-6.0.0.1.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/microsoft-
windowsazure-storage-sdk-6.0.0.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/mysql-connector-
java-5.0.8-bin.jar to classpath ... OK
```

```
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/mysql-connector-
java-5.1.46-bin.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/ojdbc6.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/org.json-
20150730.jar to classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/servlet-api.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/sinetfactory.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/bin/../bin/yavijava.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/jvm/lib/charsets.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/jvm/lib/jce.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/jvm/lib/jfxswt.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/jvm/lib/jsse.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/jvm/lib/management-agent.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/jvm/lib/resources.jar to
classpath ... OK
Adding file:/C:/Program%20Files/AhsayOBM/jvm/lib/rt.jar to classpath ...
OK
```

Eventually, the AhsayOBM login screen will be displayed.



RunConfigurator.bat

This allows the user to run the AhsayOBM through *cmd*. Export the batch file to a text editor using the following script.

```
C:\Program Files\AhsayOBM\bin>notepad RunConfigurator.bat

C:\Program Files\AhsayOBM\bin>
```

Configure the following parameters:

- **SETTING_HOME** – this is the directory to your setting home. If not set, the directory will be "C:\Users\USER\.obm" by default.

  e.g. *SET SETTING_HOME="C:\Users\John\.obm"*

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

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

```
@ECHO OFF
REM ##############################  RunOBC.bat ##########################
REM # You can use this batch to run the backup client application
REM ###################################################################
####################  Start: User Defined Section  ####################
REM ------------------------------  SETTING_HOME  ----------------------
REM | Directory to your setting home. Default to
REM | "C:\Users\USER\.obm" when not set.
REM | e.g. SET SETTING_HOME="C:\Users\John\.obm"
REM -------------------------------------------------------------------
SET SETTING_HOME=""
REM ------------------------------  DEBUG_MODE  ----------------------
REM | Enable/Disable debug mode
REM | e.g. SET DEBUG_MODE="--debug"
REM |  or  SET DEBUG_MODE=""
REM -------------------------------------------------------------------
SET DEBUG_MODE=""
REM ####################  END: User Defined Section  ###################
SET APP_HOME=..
SET JAVA_HOME=%APP_HOME%\jvm
SET JAVA_EXE=%JAVA_HOME%\bin\bJW.exe
SET JAVA_OPTS=-Xms128m -Xmx768m -Dsun.java2d.noddraw -
Dsun.nio.PageAlignDirectMemory=true
SET JAVA_LIB_PATH=-Djava.library.path=%APP_HOME%\bin
SET PATH=%JAVA_HOME%\bin;%PATH%
IF "%PROCESSOR_ARCHITECTURE%"=="x86" (
  SET "DEP_LIB_PATH=X86"
) ELSE (
  SET "DEP_LIB_PATH=X64"
)
SET PATH=%APP_HOME%\bin\%DEP_LIB_PATH%;%JAVA_HOME%\bin;%PATH%
SET CLASSPATH=%APP_HOME%\bin;%APP_HOME%\bin\cb.jar
REM ###################################################################
```

```
ECHO -
ECHO APP_HOME=%APP_HOME%
ECHO SETTING_HOME=%SETTING_HOME%
ECHO JAVA_HOME=%JAVA_HOME%
ECHO JAVA_EXE=%JAVA_EXE%
ECHO JAVA_OPTS=%JAVA_OPTS%
ECHO JAVA_LIB_PATH=%JAVA_LIB_PATH%
ECHO PATH=%PATH%
ECHO CLASSPATH=%CLASSPATH%
ECHO -
@ECHO ON
%JAVA_EXE% %JAVA_LIB_PATH% -cp %CLASSPATH% %JAVA_OPTS% Gui --config
%DEBUG_MODE% %APP_HOME% %SETTING_HOME%
@ECHO OFF
CD "%APP_HOME%"
IF "%APP_HOME%"==".." PAUSE
@ECHO ON
```

Save the changes and close the text editor. Proceed back to *cmd* and enter *RunConfigurator.bat*. The AhsayOBM login menu will be displayed.

```
C:\Program Files\AhsayOBM\bin>RunConfigurator.bat

-

APP_HOME=..

SETTING_HOME=""

JAVA_HOME=..\jvm

JAVA_EXE=..\jvm\bin\bJW.exe

JAVA_OPTS=-Xms128m -Xmx768m -Dsun.java2d.noddraw -
Dsun.nio.PageAlignDirectMemory=true

JAVA_LIB_PATH=-Djava.library.path=..\bin
PATH=..\bin\X64;..\jvm\bin;..\jvm\bin;C:\Program Files (x86)\Common
Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\Sys
tem32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program
Files\Microsoft SQL Server\Client SDK\ODBC\110\Tools\Binn\;C:\Program
Files (x86)\Microsoft SQL Server\120\Tools\Binn\;C:\Program
Files\Microsoft SQL Server\120\Tools\Binn\;C:\Program Files\Microsoft
SQL Server\120\DTS\Binn\;C:\Program
Files\PuTTY\CLASSPATH=..\bin;..\bin\cb.jar

-

C:\Program Files\AhsayOBM\bin>..\jvm\bin\bJW.exe -
Djava.library.path=..\bin -cp..\bin;..\bin\cb.jar -Xms128m -Xmx768m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true Gui --config
"" .. ""

Config file found
```

```
Login Menu

----------
   (1). Login
   (2). Change Network Settings
   (3). Forgot Password
   (4). Quit
----------

Your Choice:
```

If you want to modify the network settings before logging in, select option **(2)** from the login menu.

```
Login Menu

----------

   (1). Login
   (2). Change Network Settings
   (3). Forgot Password
   (4). Quit
----------

Your Choice: 2

Network Setting

---------------
   (1). Backup Server URL [127.0.0.1]
   (2). Port [-1]
   (3). Protocol [http]
   (4). Proxy Setting [Not in Use]
   (5). Save and Return
   (6). Discard and Return
---------------

Your Choice:
```

Otherwise, select option **(1)**. Input your login name and password to log in. After a successful login, the AhsayOBM main menu will be displayed.

```
Login Menu

----------
   (1). Login
   (2). Change Network Settings
   (3). Forgot Password
   (4). Quit
----------

Your Choice: 1

Login Name : Win_OBM

Password : ********************

Please wait while verifying user account with server...
```

```
Your profile has been downloaded and updated.

Main Menu

---------
  (1). List Backup Sets
  (2). Delete Backup Set
  (3). Export Backup Set Settings to XML
  (4). Import Backup Set Settings from XML
  (5). Generate new Backup Set Settings Template
  (6). Change Language [English]
  (7). Update Profile Settings
  (8). Quit
---------
Your Choice:
```

If the password is forgotten, choose **(3)** on the login menu and input your login name. A link will be sent to the email you provided in the AhsayCBS server to reset the user account password.

```
Login Menu
----------
  (1). Login
  (2). Change Network Settings
  (3). Forgot Password
  (4). Quit
----------
Your Choice: 3

Login Name : Win_OBM
```

Select option **(4)** to exit the AhsayOBM.

```
Login Menu
----------
  (1). Login
  (2). Change Network Settings
  (3). Forgot Password
  (4). Quit
----------

Your Choice: 4

Exit Configurator Utility

Press any key to continue . . .
```

ListBackupSet.bat

This allows the user to see the list of existing backup set/s under the backup account. Enter *ListBackupSet.bat* to display the list of available backup sets with their backup set ID.

```
C:\Program Files\AhsayOBM\bin>ListBackupSet.bat

-

APP_HOME=..

SETTING_HOME=

JAVA_HOME=..\jvm

JAVA_EXE=..\jvm\bin\bJW.exe

JAVA_OPTS=-Xms128m -Xmx768m -Dsun.java2d.noddraw -
Dsun.nio.PageAlignDirectMemory=true

JAVA_LIB_PATH=-Djava.library.path=..\bin PATH=..\jvm\bin;C:\Program
Files (x86)\Common Files\Oracle\Java\javapath;C:\Windows\system32;C:
\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell
\v1.0\;C:\Program Files\Microsoft SQL Server\Client
SDK\ODBC\110\Tools\Binn\;C:\Program Files (x86)\Microsoft SQL
Server\120\Tools\Binn\;C:\Program Files\Microsoft SQL Server\120\
Tools\Binn\;C:\Program Files\Microsoft SQL Server\120\DTS
\Binn\;C:\Program Files\PuTTY\CLASSPATH=..\bin;..\bin\cb.jar

-

Listing all backup sets under this backup account ...

C:\Program Files\AhsayOBM\bin>..\jvm\bin\bJW.exe -
Djava.library.path=..\bin -cp..\bin;..\bin\cb.jar -Xms128m -Xmx768m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
ListBackupSet ..

BackupSet Name= Data Backup, ID= 1562897045523

BackupSet Name= File Backup, ID= 1561974801639

C:\Program Files\AhsayOBM\bin>PAUSE

Press any key to continue . . .
```

RunBackupSet.bat

This allows the user to run a backup. Export the batch file to a text editor using the following script.

```
C:\Program Files\AhsayOBM\bin>notepad RunBackupSet.bat

C:\Program Files\AhsayOBM\bin>
```

Make sure that the following parameters are set accordingly:

- **BACKUP_SET** – this is the backup set which you would like to run. There are two (2) options to specify the backup set; using the *backup set name* or the *backup set ID*. If the backup set name is not in English, use the backup set ID.

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

  You can leave this parameter blank if you only have one (1) backup set.

  e.g. *SET BACKUP_SET=""*

  If having multiple backup sets, you must specify which backup set you would like to be run.

- **BACKUP_DESTS** – this is the destination(s) of the backup set which you will run. There are two (2) options to specify the destination; using the *destination name* or the *destination ID*. If the destination is not in English, use the destination ID.

  e.g. *SET BACKUP_DEST="Local-1"*
  or *SET BACKUP_DEST="1119083740107"*

  Multiple destinations can be specified in a comma-separated format or you can indicate "ALL" to run a backup for all destinations.

  e.g. *SET BACKUP_DESTS="Destination-1,Destination-2"*
  or *SET BACKUP_DESTS="ALL"*

- **BACKUP_TYPE** – this is the backup set type. This does not need to be changed if backing up a file backup set.

  Options available: FILE/DATABASE/DIFFERENTIAL/LOG

  e.g. *SET BACKUP_TYPE="FILE"* for file backup
  or *SET BACKUP_TYPE="DATABASE"* for Full database backup
  or *SET BACKUP_TYPE="DIFFERENTIAL"* for Differential database backup
  or *SET BACKUP_TYPE="LOG"* for Log database backup

  For MSExchange 2010 BackupSet:

  e.g. *SET BACKUP_TYPE="DATABASE"* for Full database backup
  or *SET BACKUP_TYPE="DIFFERENTIAL"* for Differential database backup
  or *SET BACKUP_TYPE="LOG"* for Incremental database backup
  or *SET BACKUP_TYPE="COPY"* for Copy database backup

- **SETTING_HOME** – this is the directory to your setting home. If not set, the directory will be "C:\Users\USER\.obm" by default.

  e.g. *SET SETTING_HOME="C:\Users\John\.obm"*

- **DELTA_MODE** – this is used to set the In-File Delta mode when running a backup.

  e.g. *SET DELTA_MODE="I"* for Incremental In-file delta backup
  or *SET DELTA_MODE="D"* for Differential In-file delta backup
  or *SET DELTA_MODE="F"* for Full File backup
  or *SET DELTA_MODE=""* for using backup set in-file delta setting

- **CLEANUP_MODE** – same as the retention policy job and space freeing up, this parameter is used to remove obsolete files from your backup destinations after a backup has been run.

  Options available: ENABLE-CLEANUP/DISABLE-CLEANUP

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

- **DEBUG_MODE** – this parameter is used to enable or disable the debug mode when there is a backup job running.

  Options available: ENABLE-DEBUG/DISABLE-DEBUG

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

```
@ECHO OFF
REM ##################  RunBackupSet.bat  ##############################
REM # You can use this batch to run any of your backup sets from the
REM # command line. Just customize the "User Defined Section" below with
REM # your values for your backup action.
REM ###################################################################
REM ###################  START: User Defined Section #################
REM ------------------------------  BACKUP_SET  ----------------------
REM | The name or ID of the backup set that you want to run.
REM | If backup set name is not in English, please use ID instead.
REM | e.g. SET BACKUP_SET="1119083740107"
REM |  or  SET BACKUP_SET="FileBackupSet-1"
REM |
REM | You can leave this parameter blank if you have only 1 backup set.
REM -------------------------------------------------------------------
SET BACKUP_SET=""
REM ------------------------------  BACKUP_DESTS  --------------------
REM | The list of name or ID of the backup destinations that you want to
REM | run. If backup destination name is not in English, please use ID
REM | instead.
REM | e.g. SET BACKUP_DESTS="1740107119083"
REM |  or  SET BACKUP_DESTS="Destination-1,Destination-2"
REM |  or  SET BACKUP_DESTS="ALL"
REM |
REM | You can specify multiple destinations in comma-separated format,
REM | or use "ALL" to run backup for all destinations.
REM -------------------------------------------------------------------
SET BACKUP_DESTS="ALL"
REM ------------------------------  BACKUP_TYPE  ---------------------
REM | Set backup type. You don't need to change this if you are backing
```

```
REM |up a file back set.
REM | Options available: FILE/DATABASE/DIFFERENTIAL/LOG
REM | e.g. SET BACKUP_TYPE="FILE"          for file backup
REM |  or  SET BACKUP_TYPE="DATABASE"      for Full database backup
REM |  or  SET BACKUP_TYPE="DIFFERENTIAL"  for Differential database
REM |backup or  SET BACKUP_TYPE="LOG"     for Log database backup
REM |
REM | For MSExchange 2010 BackupSet
REM | e.g. SET BACKUP_TYPE="DATABASE"      for Full database backup
REM |  or  SET BACKUP_TYPE="DIFFERENTIAL"  for Differential database
REM |backup
REM |  or  SET BACKUP_TYPE="LOG"           for Incremental database
REM |backup or  SET BACKUP_TYPE="COPY"          for Copy database
REM |backup
REM ----------------------------------------------------------------
SET BACKUP_TYPE="FILE"
REM ----------------------------  SETTING_HOME  ----------------------
REM | Directory to your setting home. Default to
REM | "C:\Users\USER\.obm" when not set.
REM | e.g. SET SETTING_HOME="C:\Users\John\.obm"
REM ----------------------------------------------------------------
SET SETTING_HOME=""
REM ------------------------------  DELTA_MODE  ----------------------
REM | Set In-File Delta mode.
REM | Options available: Incremental/Differential/Full (I/D/F)
REM | e.g. SET DELTA_MODE="I"   for Incremental In-file delta backup
REM |  or  SET DELTA_MODE="D"   for Differential In-file delta backup
REM |  or  SET DELTA_MODE="F"   for Full File backup
REM |  or  SET DELTA_MODE=""    for using backup set in-file delta
REM |setting
REM ----------------------------------------------------------------
SET DELTA_MODE=""
REM ------------------------------  CLEANUP_MODE  ----------------------
REM | You can enable Cleanup mode to remove obsolete files from your
REM |backup destinations after backup.
REM | Options available: ENABLE-CLEANUP/DISABLE-CLEANUP
REM | e.g. SET CLEANUP_MODE="ENABLE-CLEANUP"
REM | or  SET CLEANUP_MODE="DISABLE-CLEANUP"
REM ----------------------------------------------------------------
SET CLEANUP_MODE="DISABLE-CLEANUP"
REM ------------------------------  DEBUG_MODE  ----------------------
REM | Set Debug mode.
REM | Options available: ENABLE-DEBUG/DISABLE-DEBUG
REM | e.g. SET DEBUG_MODE="ENABLE-DEBUG"
REM |  or  SET DEBUG_MODE="DISABLE-DEBUG"
REM ----------------------------------------------------------------
SET DEBUG_MODE="DISABLE-DEBUG"
REM ####################  END: User Defined Section ####################
SET APP_HOME=..
SET JAVA_HOME=%APP_HOME%\jvm
SET JAVA_EXE=%JAVA_HOME%\bin\bJW.exe
SET JAVA_LIB_PATH=-Djava.library.path=%APP_HOME%\bin
SET PATH=%JAVA_HOME%\bin;%PATH%
```

```
SET CLASSPATH=%APP_HOME%\bin;%APP_HOME%\bin\cb.jar
IF "%PROCESSOR_ARCHITECTURE%"=="x86" (
  SET "DEP_LIB_PATH=X86"
  SET JAVA_OPTS=-Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
) ELSE (
  SET "DEP_LIB_PATH=X64"
  SET JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
)
SET PATH=%CD%\%APP_HOME%\bin\%DEP_LIB_PATH%;%PATH%
REM ################################################################
ECHO -
ECHO APP_HOME=%APP_HOME%
ECHO SETTING_HOME=%SETTING_HOME%
ECHO JAVA_HOME=%JAVA_HOME%
ECHO JAVA_EXE=%JAVA_EXE%
ECHO JAVA_OPTS=%JAVA_OPTS%
ECHO JAVA_LIB_PATH=%JAVA_LIB_PATH%
ECHO PATH=%PATH%
ECHO CLASSPATH=%CLASSPATH%
ECHO -
ECHO Running Backup Set - '%BACKUP_SET%' ...
@ECHO ON
%JAVA_EXE% %JAVA_LIB_PATH% -cp %CLASSPATH% %JAVA_OPTS% RunBackupSet
%APP_HOME% %BACKUP_SET% %BACKUP_DESTS% %BACKUP_TYPE% %SETTING_HOME%
%DELTA_MODE% %CLEANUP_MODE% %DEBUG_MODE%
@ECHO OFF
CD %APP_HOME%
IF "%APP_HOME%"==".." PAUSE
@ECHO ON
```

NOTE

If some parameters are not configured, the backup job will run with the default backup settings.

Save the changes and close the text editor. Proceed back to *cmd* and enter *RunBackupSet.bat*.

```
C:\Program Files\AhsayOBM\bin>RunBackupSet.bat
-
APP_HOME=..
SETTING_HOME=""

JAVA_HOME=..\jvm
JAVA_EXE=..\jvm\bin\bJW.exe
JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true

JAVA_LIB_PATH=-Djava.library.path=..\bin PATH=C:\Program
Files\AhsayOBM\bin\..\bin\X64;..\jvm\bin;C:\Program Files (x86)\Common
Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\
System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program
Files\Microsoft SQL Server\Client SDK\ODBC\110\Tools\Binn\;C:\Program
Files (x86)\Microsoft SQL Server\120\Tools\Binn\;C:\Program
```

```
Files\Microsoft SQL Server\120\Tools\Binn\;C:\Program Files\Microsoft
SQL Server\120\DTS\Binn\;C:\Program
Files\PuTTY\CLASSPATH=..\bin;..\bin\cb.jar
-
Running Backup Set - '""' ...
C:\Program Files\AhsayOBM\bin>..\jvm\bin\bJW.exe -
Djava.library.path=..\bin -cp ..\bin;..\bin\cb.jar -Xms128m -Xmx2048m -
XX:MaxDirectMemorySize=1024m -Dsun.java2d.noddraw -
Dsun.nio.PageAlignDirectMemory=true RunBackupSet .. "" "ALL" "FILE" ""
"" "DISABLE-CLEANUP" "DISABLE-DEBUG"
[2019/07/12 12:50:20] [info] [-] Start [ AhsayOBM v8.2.1.18 ]
[2019/07/12 12:50:20] [info] [-] Saving encrypted backup set encryption
keys to server...
[2019/07/12 12:50:22] [info] [1562897364604] Start Backup ... [In-File
Delta: Incremental]
[2019/07/12 12:50:22] [info] [1562897364604] Using Temporary Directory
C:\Users\Administrator\temp\1562897045523\OBS@1562897364604
[2019/07/12 12:50:22] [info] [-] Start running pre-commands
[2019/07/12 12:50:22] [info] [-] Finished running pre-commands
[2019/07/12 12:50:22] [info] [1562897364604] Downloading server file
list...
[2019/07/12 12:50:22] [info] [1562897364604] Downloading server file
list... Completed
[2019/07/12 12:50:23] [info] [1562897364604] Reading backup source from
hard disk...
[2019/07/12 12:50:25] [info] [1562897364604] Getting all files which
have been moved...
[2019/07/12 12:50:25] [info] [1562897364604] Getting all files which
have been moved... Completed
[2019/07/12 12:50:25] [info] [1562897364604] Reading backup source from
hard disk... Completed
[2019/07/12 12:50:25] [info] [1562897364604] Total New Files = 0
[2019/07/12 12:50:25] [info] [1562897364604] Total New Directories = 0
[2019/07/12 12:50:25] [info] [1562897364604] Total New Links = 0
[2019/07/12 12:50:25] [info] [1562897364604] Total Updated Files = 0
[2019/07/12 12:50:25] [info] [1562897364604] Total Attributes Changed
Files = 0
[2019/07/12 12:50:25] [info] [1562897364604] Total Deleted Files = 0
[2019/07/12 12:50:25] [info] [1562897364604] Total Deleted Directories =
0
[2019/07/12 12:50:25] [info] [1562897364604] Total Deleted Links = 0
[2019/07/12 12:50:25] [info] [1562897364604] Total Moved Files = 0
[2019/07/12 12:50:26] [info] [1562897364604] Saving encrypted backup
file index to 1562897045523/blocks at destination AhsayCBS...
[2019/07/12 12:50:26] [info] [1562897364604] Saving encrypted backup
file index to 1562897045523/blocks/2019-07-12-12-50-20 at destination
AhsayCBS...
[2019/07/12 12:50:27] [info] [-] Start running post-commands
[2019/07/12 12:50:27] [info] [-] Finished running post-commands
[2019/07/12 12:50:27] [info] [1562897364604] Deleting temporary file
C:\Users\Administrator\temp\1562897045523\OBS@1562897364604
```

```
[2019/07/12 12:50:27] [info] [1562897364604] Backup Completed
Successfully

Press any key to continue . . .
```

ListBackupJob.bat

This allows the user to display the list of backup jobs under a specific backup set. Enter the following script to export the batch file to a text editor.

```
C:\Program Files\AhsayOBM\bin>notepad ListBackupJob.bat

C:\Program Files\AhsayOBM\bin>
```

Configure the following parameters:

- **BACKUP_SET** – this is the backup set which you would like to be displayed. There are two (2) ways to specify the backup set; using the *backup set name* or the *backup set ID*. If the backup set name is not in English, use the backup set ID.

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

  You can leave this parameter blank if you only have one (1) backup set.

  e.g. *SET BACKUP_SET=""*

- **BACKUP_DEST** – this is the destination of the backup set which you would like to be displayed. There are two (2) ways to specify the backup destination; using the *destination name* or the *destination ID*. If the destination is not in English, use the destination ID.

  e.g. *SET BACKUP_DEST="Local-1"*
  or *SET BACKUP_DEST="1119083740107"*

  You can leave this parameter blank if you only have one (1) backup destination.

  e.g. *SET BACKUP_DEST=""*

```
@ECHO OFF
REM ##################  ListBackupJob.bat  ##############################
REM # You can use this batch to list all backup jobs which ran under   #
REM # this backup set.                                                  #
REM ####################################################################
REM ####################  Start: User Defined Section  #################
REM ------------------------------  BACKUP_SET  ----------------------
REM | The name or ID of the backup set that you want to run
REM | If backup set name is not in English, please use BackupSetID
REM | e.g. SET BACKUP_SET="1119083740107"
REM |  or  SET BACKUP_SET="FileBackupSet-1"
REM |
REM | You can leave this parameter blank if you have only 1 backup set.
REM --------------------------------------------------------------------
SET BACKUP_SET="File Backup"
REM ------------------------------  BACKUP_DEST  ---------------------
REM | The name or ID of the destination that you want to list
REM | If destination name is not in English, please use DestinationID
REM | e.g. SET BACKUP_DEST="1119083740107"
REM |  or  SET BACKUP_DEST="CBS"
REM |
```

```
REM | You can leave this parameter blank if you have only 1 destination.
REM ------------------------------------------------------------------
SET BACKUP_DEST=""
REM ####################  END: User Defined Section ####################
REM ##################################################################
REM #                  SCRIPT                        USAGE
REM ##################################################################
REM # Input Arguments will overwrite the above settings
REM # defined in 'User Defined Section'.
IF NOT %1.==. SET BACKUP_SET=%1
IF NOT %2.==. SET BACKUP_DEST=%2
REM ##################################################################
SET APP_HOME=..
SET SETTING_HOME=
SET JAVA_HOME=%APP_HOME%\jvm
SET JAVA_EXE=%JAVA_HOME%\bin\bJW.exe
SET JAVA_OPTS=-Xms128m -Xmx768m -Dsun.java2d.noddraw -
Dsun.nio.PageAlignDire
ctMemory=true
SET JAVA_LIB_PATH=-Djava.library.path=%APP_HOME%\bin
SET PATH=%JAVA_HOME%\bin;%PATH%
SET CLASSPATH=%APP_HOME%\bin;%APP_HOME%\bin\cb.jar
REM ##################################################################
ECHO -
ECHO APP_HOME=%APP_HOME%
ECHO SETTING_HOME=%SETTING_HOME%
ECHO JAVA_HOME=%JAVA_HOME%
ECHO JAVA_EXE=%JAVA_EXE%
ECHO JAVA_OPTS=%JAVA_OPTS%
ECHO JAVA_LIB_PATH=%JAVA_LIB_PATH%
ECHO PATH=%PATH%
ECHO CLASSPATH=%CLASSPATH%
ECHO -
ECHO Listing all backup jobs for Backup Set - '%BACKUP_SET%' ...
@ECHO ON
%JAVA_EXE% %JAVA_LIB_PATH% -cp %CLASSPATH% %JAVA_OPTS% ListBackupJob --
app-home=%APP_HOME% --backup-set=%BACKUP_SET% --backup-
dest=%BACKUP_DEST% --setting-home=%SETTING_HOME%
PAUSE
```

NOTE

You can only select one (1) backup set and one (1) destination at a time.

Save the changes and close the text editor. Proceed back to *cmd* and enter *ListBackupJob.bat*. The list of backup jobs under the specified backup set will be displayed.

```
C:\Program Files\AhsayOBM\bin>ListBackupJob.bat

-

APP_HOME=..
```

```
SETTING_HOME=

JAVA_HOME=..\jvm

JAVA_EXE=..\jvm\bin\bJW.exe

JAVA_OPTS=-Xms128m -Xmx768m -Dsun.java2d.noddraw -
Dsun.nio.PageAlignDirectMemory=true

JAVA_LIB_PATH=-Djava.library.path=..\bin PATH=..\jvm\bin;C:\Program
Files (x86)\Common Files\Oracle\Java\javapath;C:\Windows\system32;C:
\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell
\v1.0\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\110\Tools
\Binn\;C:\Program Files (x86)\Microsoft SQL
Server\120\Tools\Binn\;C:\Program Files\Microsoft SQL
Server\120\Tools\Binn\;C:\Program Files\Microsoft SQL
Server\120\DTS\Binn\;C:\Program
Files\PuTTY\CLASSPATH=..\bin;..\bin\cb.jar

-

Listing all backup jobs for Backup Set - '"File Backup"' ...

C:\Program Files\AhsayOBM\bin>..\jvm\bin\bJW.exe -
Djava.library.path=..\bin -cp..\bin;..\bin\cb.jar -Xms128m -Xmx768m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true ListBackupJob -
-app-home=.. --backup-set="File Backup" --backup-dest="" --setting-home=

File Backup [1562220462692]

2019-07-05-11-31-41

2019-07-04-20-00-00

2019-07-04-14-08-13

C:\Program Files\AhsayOBM\bin>PAUSE

Press any key to continue . . .
```

Restore.bat

This allows the user to restore backed up data. Enter the following script to export the batch file to a text editor.

```
C:\Program Files\AhsayOBM\bin>notepad Restore.bat

C:\Program Files\AhsayOBM\bin>
```

Configure the following parameters:

- **BACKUP_SET** – this is the backup set which you would like to restore. If the backup set name is not in English, use the backup set ID.

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

- **DESTINATION** – this is the destination where you want to restore the backed up data from. If the destination is not in English, use the destination ID.

  e.g. *SET DESTINATION="Local-1"*
  or *SET DESTINATION="1119083740107"*

  You can leave this parameter blank if you only have one (1) backup destination.

  e.g. *SET DESTINATION=""*

- **RESTORE_TO** – this is the location where the files will be restored.

  e.g. *SET RESTORE_TO=" C:\Temp"*

- **RESTORE_FROM** – this is the selected file or directory on the backup server which you would like to restore.

  e.g. *SET RESTORE_FROM="* C:\Users*"*

- **POINT_IN_TIME** – this is the point-in-time snapshot (of a successful backup) that you want to restore from the backup server. Use "Current" for the latest backup snapshot. You can retrieve the point in time by using the *ListBackupJob.bat*.

  e.g. *SET POINT_IN_TIME="2006-10-04-12-57-13"*
  or *SET POINT_IN_TIME="Current"*

- **RESTORE_PERMISSION** – set this to “Y” if you want to restore file permissions. Otherwise, indicate “N” if you do NOT want to restore file permissions.

  e.g. *SET RESTORE_PERMISSION="N"*

- **SKIP_INVALID_KEY** – set this to “Y” if you want to skip restore file with an invalid key. Set this to "N" if you want to prompt user to input the correct key.

  e.g. *SET SKIP_INVALID_KEY="N"*

- **SYNC_OPTION** – set this to "Y" if you want to enable the sync option. Set this to "N" if you do NOT want to enable sync option. Leave this blank if you want to prompt user for a selection.

e.g. *SET SYNC_OPTION="N"*

- **REPLACE_EXISTING_FILE** – set to "--all" to replace all existing file(s) of the same filename. Set this to "--none" to skip all existing file(s) with the same filename. Leave this blank if you want to prompt user for a selection.

  e.g. *SET REPLACE_EXISTING_FILE="--all"*

- **SETTING_HOME** – this is the directory to your setting home. If not set, the directory will be "C:\Users\USER\.obm" by default.

  e.g. *SET SETTING_HOME="C:\Users\John\.obm"*

- **FILTER** – this parameter is used to filter the files that you want to restore.

  e.g. *SET FILTER="-Pattern=.txt-Type=exact-Target=toFile"*

- **TEMP_DIR** – this is the directory where you would like to store the restore files temporarily.

  e.g. *SET TEMP_DIR="C:\Temp"*

- **VERIFY_CHKSUM** – set this to "Y" if you want to verify the in-file delta file checksum during restore. Otherwise, set this to "N" if you do NOT want to verify the in-file delta file checksum during restore.

  e.g. *SET VERIFY_CHKSUM="N"*

```
@ECHO OFF
REM ##############################  Restore.bat  #######################
REM # You can use this batch file to restore backup files using command-
REM # line. Just customize the "User Define Section" below with values
REM # for your restore action.
REM ###################################################################
REM ###################  Start: User Defined Section  #################
REM ------------------------------  BACKUP_SET  -----------------------
REM | The name or ID of the backup set that you want to restore.
REM | If backup set name is not in English, please use ID instead.
REM | e.g. SET BACKUP_SET="1119083740107"
REM |  or  SET BACKUP_SET="FileBackupSet-1"
REM |
REM | You can leave this parameter blank if you have only 1 backup set.
REM ------------------------------------------------------------------
SET BACKUP_SET=""
REM ------------------------------  DESTINATION  -----------------------
REM | The name or ID of the backup destination that you want to restore
REM | from.
REM | If backup destination name is not in English, please use ID
REM | instead.
REM | e.g. SET DESTINATION="1740107119083"
REM |  or  SET DESTINATION="Destination-1"
REM |
REM | You can leave this parameter blank if you have only 1 destination.
REM ------------------------------------------------------------------
SET DESTINATION=""
```

```
REM ------------------------------  RESTORE_TO  -----------------------
REM | Directory to where you want files to be restored
REM | Use "\\\\" instead of "\\" when you specify a UNC path
REM | set to "" to restore files to original location
REM | e.g. SET RESTORE_TO="C:\Temp"
REM ------------------------------------------------------------------
SET RESTORE_TO="C:\Temp"
REM ------------------------------  RESTORE_FROM  ---------------------
REM | File/Directory on the backup server that you would like to restore
REM | e.g. SET RESTORE_FROM="C:\Data"
REM ------------------------------------------------------------------
SET RESTORE_FROM=" C:\Users\Administrator\Desktop\Data backup"
REM ------------------------------  POINT_IN_TIME  ---------------------
REM | The point-in-time snapshot (successful backup) that you want to
REM | restore from the backup server.
REM | Use "Current" for the latest backup
REM | snapshot e.g. SET POINT_IN_TIME="2006-10-04-12-57-13"
REM |  or  SET POINT_IN_TIME="Current"
REM |
REM | You can retrieve the point in time by using the ListBackupJob.bat
REM ------------------------------------------------------------------
SET POINT_IN_TIME="Current"
REM ---------------------------  RESTORE_PERMISSION  -------------------
REM | set to "Y" if you want to restore file permissions
REM | set to "N" if you do NOT want to restore file permissions
REM ------------------------------------------------------------------
SET RESTORE_PERMISSION="N"
REM ---------------------------  SKIP_INVALID_KEY  --------------------
REM | set to "Y" if you want to skip restore file with invalid key
REM | set to "N" if you want to prompt user to input a correct key
REM ------------------------------------------------------------------
SET SKIP_INVALID_KEY="N"
REM ------------------------------  SYNC_OPTION  ----------------------
REM | Delete extra files
REM | set to "Y" if you want to enable sync option
REM | set to "N" if you do NOT want to enable sync option
REM | set to "" to prompt for selection
REM ------------------------------------------------------------------
SET SYNC_OPTION="N"
REM -------------------------  REPLACE_EXISTING_FILE  ------------------
REM | set to "--all" to replace all existing file(s) of the same
REM |filename set to "--none" to skip all existing file(s) with the same
REM |filename set to "" to prompt for selection
REM ------------------------------------------------------------------
SET REPLACE_EXISTING_FILE="--all"
REM ------------------------------  SETTING_HOME  ---------------------
REM | Directory to your setting home. Default to
REM | "C:\Users\USER\.obm" when not set.
REM | e.g. SET SETTING_HOME="C:\Users\John\.obm"
REM ------------------------------------------------------------------
SET SETTING_HOME=""
REM OPTION:
REM --------------------------------  FILTER  -------------------------
```

```
REM | Filter out what files you want to restore
REM | -Pattern=xxx-Type=yyy-Target=zzz
REM | where xxx is the filter pattern,
REM |       yyy is the filter type, whice can be one of the following:
REM |           [exact | exactMatchCase | contains | containsMatchCase|
REM |            startWith | startWithMatchCase | endWith |
REM |endWithMatchCase]  |
REM |       zzz is the filter target, which can be one of the following:
REM |           [toFile | toFileDir | toDir]
REM |
REM | e.g. SET FILTER="-Pattern=.txt-Type=exact-Target=toFile"
REM ------------------------------------------------------------------
SET FILTER=""
REM -------------------------------  TEMP_DIR  ------------------------
REM | Directory to where you want to store restore files temporarily
REM | Use "\\\\" instead of "\\" when you specify a UNC path
REM | set to "" to use the temporary directory in the backup set
REM | e.g. SET TEMP_DIR="C:\Temp"
REM ------------------------------------------------------------------
SET TEMP_DIR=""
REM ----------------------------  VERIFY_CHKSUM  ----------------------
REM | set to "Y" if you want to verify in-file delta file checksum
REM | during restore
REM | set to "N" if you do NOT want to verify in-file delta file
REM | checksum during restore
REM ------------------------------------------------------------------
SET VERIFY_CHKSUM="N"
REM ####################  END: User Defined Section  ###################
SET APP_HOME=..
SET JAVA_HOME=%APP_HOME%\jvm
SET JAVA_EXE=%JAVA_HOME%\bin\bJW.exe
SET JAVA_LIB_PATH=-Djava.library.path=%APP_HOME%\bin
SET PATH=%JAVA_HOME%\bin;%PATH%
SET CLASSPATH=%APP_HOME%\bin;%APP_HOME%\bin\cb.jar
IF "%PROCESSOR_ARCHITECTURE%"=="x86" (
  SET "DEP_LIB_PATH=X86"
  SET JAVA_OPTS=-Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
) ELSE (
  SET "DEP_LIB_PATH=X64"
  SET JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
)
SET PATH=%CD%\%APP_HOME%\bin\%DEP_LIB_PATH%;%PATH%
REM ##################################################################
ECHO -
ECHO APP_HOME=%APP_HOME%
ECHO SETTING_HOME=%SETTING_HOME%
ECHO JAVA_HOME=%JAVA_HOME%
ECHO JAVA_EXE=%JAVA_EXE%
ECHO JAVA_OPTS=%JAVA_OPTS%
ECHO JAVA_LIB_PATH=%JAVA_LIB_PATH%
ECHO PATH=%PATH%
```

```
ECHO CLASSPATH=%CLASSPATH%
ECHO -
@ECHO ON
%JAVA_EXE% %JAVA_LIB_PATH% -cp %CLASSPATH% %JAVA_OPTS% Restore --
to=%RESTORE_TO% --from=%RESTORE_FROM% --backup-set=%BACKUP_SET% --
backup-dest=%DESTINATION% %REPLACE_EXISTING_FILE% --date=%POINT_IN_TIME%
--set-permission=%RESTORE_PERMISSION% --skip-invalid-
key=%SKIP_INVALID_KEY% --sync=%SYNC_OPTION% --filter=%FILTER% --temp-
dir=%TEMP_DIR% --verify-delta-file-chksum=%VERIFY_CHKSUM% --app-
home=%APP_HOME% --setting-home=%SETTING_HOME%
@ECHO OFF
CD %APP_HOME%
IF "%APP_HOME%"==".." PAUSE
@ECHO ON
```

NOTE

If some parameters are not set, the restore job will run with the default restore settings.

Save the changes and close the text editor. Proceed back to *cmd* and enter *Restore.bat*.

```
C:\Program Files\AhsayOBM\bin>Restore.bat

-

APP_HOME=..

SETTING_HOME=""

JAVA_HOME=..\jvm

JAVA_EXE=..\jvm\bin\bJW.exe

JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true

JAVA_LIB_PATH=-Djava.library.path=..\binPATH=C:\Program Files\AhsayOBM
\bin\..\bin\X64;..\jvm\bin;C:\Program Files (x86)\Common Files\Oracle\
Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;

C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files\Microsoft
SQL Server\Client SDK\ODBC\110\Tools\Binn\;C:\Program Files
(x86)\Microsoft SQL Server\120\Tools\Binn\;C:\Program Files\Microsoft
SQL Server\120\Tools\Binn\;C:\Program Files\Microsoft SQL
Server\120\DTS\Binn\;C:\Program Files\PuTTY\CLASSPATH=..
\bin;..\bin\cb.jar

-

C:\Program Files\AhsayOBM\bin>..\jvm\bin\bJW.exe -
Djava.library.path=..\bin -cp ..\bin;..\bin\cb.jar -Xms128m -Xmx2048m -
XX:MaxDirectMemorySize=1024m -Dsun.java2d.noddraw -
Dsun.nio.PageAlignDirectMemory=true Restore --to="C:\Temp" --
from="C:\Users\Administrator\Desktop\Data backup" --backup-set="" --
backup-dest="" "--all" --date="Current"--set-permission="N" --skip-
```

```
invalid-key="N" --sync="N" --filter="" --temp-dir="" --verify-delta-
file-chksum="N" --app-home=.. --setting-home=""

Filter Pattern not set, filter would not apply to restore

Temporary directory not set, use the temporary directory in the backup
set

[2019-07-12 11:52:03] Start [ AhsayOBM v8.2.1.18 ]

[2019-07-12 11:52:03] OS: Windows Server 2012 R2 (w2k16R2-std); CPU
Model: VMware-Intel(R) Xeon(R) CPU E5520 @ 2.27GHz,Intel(R) Xeon(R) CPU
E5520  @2.27GHz; Number of Processors: 4; Heap Size: 32.3MB (Current) /
1.8GB (Maximum); Physical Memory: 726.9MB (Free) / 4GB (Total)

[2019-07-12 11:52:03] start,Start [ AhsayOBM v8.2.1.18 ],0,0,0,,0,0

[2019-07-12 11:52:03] Initializing decrypt action...

[2019-07-12 11:52:03] Initializing decrypt action... Completed

[2019-07-12 11:52:04] Creating new directory... "C:\Temp\C_"

[2019-07-12 11:52:04] Creating new directory... "C:\Temp\C_\Users"

[2019-07-12 11:52:04] Creating new directory...
"C:\Temp\C_\Users\Administrator"

[2019-07-12 11:52:04] Creating new directory...
"C:\Temp\C_\Users\Administrator\Desktop"

[2019-07-12 11:52:04] Creating new directory...
"C:\Temp\C_\Users\Administrator\Desktop\Data backup"

[2019-07-12 11:52:04] Downloading...
"C:\Temp\C_\Users\Administrator\Desktop\Data backup\Sample file.txt"
(Total 0 bytes)

[2019-07-12 11:52:04] Downloading...
"C:\Temp\C_\Users\Administrator\Desktop\Data backup\Text File.txt"
(Total 0 bytes)

[2019-07-12 11:52:05] file,C:\Temp\C_\Users\Administrator\Desktop\Data
backup\Sample file.txt,0,0,1562897245044,,1562903525530,1562903525531

[2019-07-12 11:52:05] file,C:\Temp\C_\Users\Administrator\Desktop\Data
backup\Text File.txt,0,0,1562897254708,,1562903525531,1562903525531

[2019-07-12 11:52:06] Restore Completed Successfully

[2019-07-12 11:52:06] end,RESTORE_STOP_SUCCESS,0,0,0,,0,0

Press any key to continue . . .
```

Decrypt.bat

This allows the user to restore raw data. Enter the following script to export the batch file to a text editor.

```
C:\Program Files\AhsayOBM\bin>notepad Decrypt.bat

C:\Program Files\AhsayOBM\bin>
```

Configure the following parameters:

- **SOURCE_DIR** – this is the path of the folder which contains the backed up files that you want to decrypt.

  e.g. *SOURCE_DIR="C:\john\backupdata\1498444438340\blocks"*

- **ENCRYPT_KEY** – this is the encryption key that was set for the backup set. You can leave this parameter blank if the backed up data is not encrypted.
  e.g. *ENCRYPT_KEY="NjQAtHhBSyAVgfFkaFI="*
  e.g. *ENCRYPT_KEY=""*

- **DECRYPT_TO** – this is the specified directory where the decrypted files will be stored.

  e.g. *SET DECRYPT_TO=" C:\Temp"*

- **DECRYPT_FROM** – this is the file or directory on the backup data that you would like to decrypt.

  e.g. *SET DECRYPT_TO="C:\Data"*

- **POINT_IN_TIME** – this is the point-in-time snapshot (of a successful backup) that you want to decrypt from the backed up data. Use "Current" for the latest backup snapshot. The point-in-time should be one of the directory names under *SOURCE_DIR*.

  e.g. *SET POINT_IN_TIME="2006-10-04-12-57-13"*
  or *SET POINT_IN_TIME="Current"*

- **RESTORE_PERMISSION** – set this to "Y" if you want to restore file permissions. Otherwise, indicate “N” if you do NOT want to restore file permissions.

  e.g. *SET RESTORE_PERMISSION="N"*

- **SKIP_INVALID_KEY** – set this to "Y" if you want to skip decrypt file with invalid key. Set this set to "N" if you want to prompt user to input a correct key.

  e.g. *SKIP_INVALID_KEY="Y"*

- **SYNC_OPTION** – set this to "Y" if you want to enable sync option. Set this to "N" if you do NOT want to enable sync option. Leave this parameter blank if you want to prompt user for selection.

  e.g. *SET SYNC_OPTION="N"*

  e.g. *SET SYNC_OPTION=""*

- **REPLACE_EXISTING_FILE** – set this to "--all" if you want to replace all existing file(s) of the same filename. Set this to "--none" if you want to skip all existing file(s) with the same filename. Leave this parameter blank if you want to prompt user for selection.

  e.g. *SET REPLACE_EXISTING_FILE="--all"*
  e.g. *SET REPLACE_EXISTING_FILE="--none"*
  e.g. *SET REPLACE_EXISTING_FILE=""*

- **SETTING_HOME** – this is the directory to your setting home. This is where the log files will be placed. If not set, the directory will be "C:\Users\USER\.obm" by default.

  e.g. *SET SETTING_HOME="C:\Users\John\.obm"*

- **FILTER** – this parameter is used to filter the files that you want to decrypt.

  e.g. *SET FILTER="-Pattern=.txt-Type=exact-Target=toFile"*

- **TEMP_DIR** – this is the directory where you would like to store the decrypt files temporarily.

  e.g. *SET TEMP_DIR="C:\Temp"*

- **VERIFY_CHKSUM** – set this to "Y" if you want to verify the in-file delta file checksum during decrypt. Set this to "N" if you do NOT want to verify the in-file delta file checksum during decrypt.

  e.g. *SET VERIFY_CHKSUM="N"*

```
@ECHO OFF
REM ##############################  Decrypt.bat  ########################
REM # You can use this batch file to decrypt backup files using command-
REM # line. Just customize the "User Define Section" below with values
REM # for your decrypt action.
REM ###################################################################
REM ####################  Start: User Defined Section  ################
REM ------------------------------  SOURCE_DIR  -----------------------
REM | The path to the [<backup set ID>/blocks] folder which contains    |
REM | the backup files that you want to decrypt.
REM | This folder should be located under backup destination physically.
REM | e.g. SET SOURCE_DIR="C:\john\backupdata\1498444438340\blocks"
REM | where directory "C:\john\backupdata" is path of local destination
REM -------------------------------------------------------------------
SET SOURCE_DIR="C:\Program
Files\AhsayCBS\user\Win_OBM\1562897045523\blocks"
REM ------------------------------  ENCRYPT_KEY  ----------------------
REM | The encrypting key of the backup data.
REM | e.g. SET ENCRYPT_KEY="RU5DUllQVF9LRVk="
REM |
REM | You can leave this parameter blank if backup data is not
REM | encrypted.
REM -------------------------------------------------------------------
SET ENCRYPT_KEY=""
REM ------------------------------  DECRYPT_TO  -----------------------
REM | Directory to where you want files to be decrypted
REM | Use "\\\\" instead of "\\" when you specify a UNC path
REM | e.g. SET DECRYPT_TO="C:\Temp"
```

```
REM ------------------------------------------------------------------------
SET DECRYPT_TO="C:\Data"
REM ----------------------------  DECRYPT_FROM  ----------------------
REM | File/Directory on the backup data that you would like to decrypt
REM | e.g. SET DECRYPT_FROM="C:\Data"
REM ------------------------------------------------------------------------
SET DECRYPT_FROM="C:\Users\Administrator\Desktop\Data backup"
REM ----------------------------  POINT_IN_TIME  ----------------------
REM | The point-in-time snapshot (successful backup) that you want to
REM | decrypt from the backup data. Use "Current" for the latest backup
REM | snapshot
REM | e.g. SET POINT_IN_TIME="2006-10-04-12-57-13"
REM |  or  SET POINT_IN_TIME="Current"
REM |
REM | The point in time should be one of the directory name under
REM | SOURCE_DIR unless you want to decrypt latest backup snapshot.
REM ------------------------------------------------------------------------
SET POINT_IN_TIME="Current"
REM --------------------------  RESTORE_PERMISSION  -------------------
REM | set to "Y" if you want to restore file permissions
REM | set to "N" if you do NOT want to restore file permissions
REM ------------------------------------------------------------------------
SET RESTORE_PERMISSION="N"
REM ----------------------------  SKIP_INVALID_KEY  --------------------
REM | set to "Y" if you want to skip decrypt file with invalid key
REM | set to "N" if you want to prompt to input a correct key
REM ------------------------------------------------------------------------
SET SKIP_INVALID_KEY="Y"
REM ----------------------------  SYNC_OPTION  ----------------------
REM | Delete extra files
REM | set to "Y" if you want to enable sync option
REM | set to "N" if you do NOT want to enable sync option
REM | set to "" to prompt for selection
REM ------------------------------------------------------------------------
SET SYNC_OPTION="N"
REM -------------------------  REPLACE_EXISTING_FILE  -------------------
REM | set to "--all" to replace all existing file(s) of the same
REM | filename  set to "--none" to skip all existing file(s) with the
REM | same filename    set to "" to prompt for selection
REM ------------------------------------------------------------------------
SET REPLACE_EXISTING_FILE="--all"
REM ----------------------------  SETTING_HOME  ----------------------
REM | Directory to your setting home. Log files will be located inside.
REM | Default to "C:\Users\USER\.obm" when not set.
REM | e.g. SET SETTING_HOME="C:\Users\John\.obm"
REM ------------------------------------------------------------------------
SET SETTING_HOME="C:\Users\Administrator\.obm"
REM OPTION:
REM --------------------------------  FILTER  -------------------------
REM | Filter out what files you want to decrypt
REM | -Pattern=xxx-Type=yyy-Target=zzz
REM | where xxx is the filter pattern,
REM |       yyy is the filter type, whice can be one of the following:
```

```
REM |            [exact | exactMatchCase | contains | containsMatchCase|
REM |             startWith | startWithMatchCase | endWith |
REM |          endWithMatchCase]
REM |       zzz is the filter target, which can be one of the following:
REM |            [toFile | toFileDir | toDir]
REM |
REM | e.g. SET FILTER="-Pattern=.txt-Type=exact-Target=toFile"
REM ------------------------------------------------------------------
SET FILTER=""
REM ------------------------------  TEMP_DIR  -----------------------
REM | Directory to where you want to store decrypt files temporarily
REM | Use "\\\\" instead of "\\" when you specify a UNC path
REM | e.g. SET TEMP_DIR="C:\Temp"
REM ------------------------------------------------------------------
SET TEMP_DIR="C:\Temp"
REM ----------------------------  VERIFY_CHKSUM  ---------------------
REM | set to "Y" if you want to verify in-file delta file checksum
REM | during decrypt
REM | set to "N" if you do NOT want to verify in-file delta file
REM | checksum during decrypt
REM ------------------------------------------------------------------
SET VERIFY_CHKSUM="N"
REM ####################  END: User Defined Section  ###################
SET APP_HOME=..
SET JAVA_HOME=%APP_HOME%\jvm
SET JAVA_EXE=%JAVA_HOME%\bin\bJW.exe
SET JAVA_LIB_PATH=-Djava.library.path=%APP_HOME%\bin
SET PATH=%JAVA_HOME%\bin;%PATH%
SET CLASSPATH=%APP_HOME%\bin;%APP_HOME%\bin\cb.jar
IF "%PROCESSOR_ARCHITECTURE%"=="x86" (
  SET "DEP_LIB_PATH=X86"
  SET JAVA_OPTS=-Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
) ELSE (
  SET "DEP_LIB_PATH=X64"
  SET JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
)
SET PATH=%CD%\%APP_HOME%\bin\%DEP_LIB_PATH%;%PATH%
REM ##################################################################
ECHO -
ECHO APP_HOME=%APP_HOME%
ECHO SETTING_HOME=%SETTING_HOME%
ECHO JAVA_HOME=%JAVA_HOME%
ECHO JAVA_EXE=%JAVA_EXE%
ECHO JAVA_OPTS=%JAVA_OPTS%
ECHO JAVA_LIB_PATH=%JAVA_LIB_PATH%
ECHO PATH=%PATH%
ECHO CLASSPATH=%CLASSPATH%
ECHO -
@ECHO ON
%JAVA_EXE% %JAVA_LIB_PATH% -cp %CLASSPATH% %JAVA_OPTS% Decrypt --
to=%DECRYPT_TO% --from=%DECRYPT_FROM% --source-dir=%SOURCE_DIR% --
```

```
key=%ENCRYPT_KEY% %REPLACE_EXISTING_FILE% --date=%POINT_IN_TIME% --set-
permission=%RESTORE_PERMISSION% --skip-invalid-key=%SKIP_INVALID_KEY% --
sync=%SYNC_OPTION% --filter=%FILTER% --temp-dir=%TEMP_DIR% --verify-
delta-file-chksum=%VERIFY_CHKSUM% --app-home=%APP_HOME% --setting-
home=%SETTING_HOME%
@ECHO OFF
CD %APP_HOME%
IF "%APP_HOME%"==".." PAUSE
@ECHO ON
```

Save the changes and close the text editor. On the *cmd,* enter *Decrypt.bat*. When asked if you want to input the encrypting key, select '**1**' *(Yes)*. Enter the correct encryption key to continue.

```
C:\Program Files\AhsayOBM\bin>Decrypt.bat
-
APP_HOME=..
SETTING_HOME="C:\Users\Administrator\.obm"
JAVA_HOME=..\jvm
JAVA_EXE=..\jvm\bin\bJW.exe
JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true

JAVA_LIB_PATH=-Djava.library.path=..\bin PATH=C:\Program
Files\AhsayOBM\bin
\..\bin\X64;..\jvm\bin;C:\Program Files (x86)\Common
Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\
System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program
Files\Microsoft SQL Server\Client SDK\ODBC\110\Tools\Binn\;C:\Program
Files (x86)\Microsoft SQL Server\120\Tools\Binn\;C:\Program
Files\Microsoft SQL Server\120\Tools\Binn\;C:\Program Files\Microsoft
SQL Server\120\DTS\
Binn\;C:\Program Files\PuTTY\CLASSPATH=..\bin;..\bin\cb.jar
-
C:\Program Files\AhsayOBM\bin>..\jvm\bin\bJW.exe -
Djava.library.path=..\bin -cp ..\bin;..\bin\cb.jar -Xms128m -Xmx2048m -
XX:MaxDirectMemorySize=1024m -Dsun.java2d.noddraw -
Dsun.nio.PageAlignDirectMemory=true Decrypt --to="C:\Data" --
from="C:\Users\Administrator\Desktop\Data backup" --source-
dir="C:\Program Files\AhsayCBS\user\Win_OBM\1562897045523\blocks" --
key="" "--all" --date="Current" --set-permission="N" --skip-invalid-
key="Y" --sync="N" --filter="" --temp-dir="C:\Temp" --verify-delta-file-
chksum="N" --app-home=.. --setting-home="C:\Users\Administrator\.obm"

Filter Pattern not set, filter would not apply to decrypt
(C:\Program Files\Ahsay CBS\user\Win_OBM\1562897045523\blocks\index-
s0.j00.100.16be3f1a078.cgz)

Please input the Encrypting Key.
Want to input encrypting key?
1.YES    2.CANCEL  >>1
Enter Correct Encrypting Key:********************

[2019-07-12 10:27:23] Start [ AhsayOBM v8.2.1.18 ]
```

```
[2019-07-12 10:27:25] OS: Windows Server 2012 R2 (w2k16R2-std); CPU
Model: VMware-Intel(R) Xeon(R) CPU E5520 @ 2.27GHz,Intel(R) Xeon(R) CPU
E5520 @ 2.27GHz; Number of Processors: 4; Heap Size: 35.6MB (Current)
/ 1.8GB (Maximum); Physical Memory: 722.2MB (Free) / 4GB (Total)
[2019-07-12 10:27:25] start,Start [ AhsayOBM v8.2.1.18 ],0,0,0,,0,0
[2019-07-12 10:27:25] Initializing decrypt action...
[2019-07-12 10:27:25] Initializing decrypt action... Completed
[2019-07-12 10:27:26] Creating new directory... "C:\Data\C_"
[2019-07-12 10:27:26] Creating new directory... "C:\Data\C_\Users"
[2019-07-12 10:27:26] Creating new directory...
"C:\Data\C_\Users\Administrator"
[2019-07-12 10:27:26] Creating new directory...
"C:\Data\C_\Users\Administrator\Desktop"
[2019-07-12 10:27:26] Creating new directory...
"C:\Data\C_\Users\Administrator\Desktop\Data backup"
[2019-07-12 10:27:26] Downloading...
"C:\Data\C_\Users\Administrator\Desktop\Data backup\Sample file.txt"
(Total 0 bytes)
[2019-07-12 10:27:26] Downloading...
"C:\Data\C_\Users\Administrator\Desktop\Data backup\Text File.txt"
(Total 0 bytes)
[2019-07-12 10:27:27] file,C:\Data\C_\Users\Administrator\Desktop\Data
backup\Sample file.txt,0,0,1562897245044,,1562898447522,1562898447522
[2019-07-12 10:27:27] file,C:\Data\C_\Users\Administrator\Desktop\Data
backup\Text File.txt,0,0,1562897254708,,1562898447522,1562898447522

[2019-07-12 10:27:28] Restore Completed Successfully

[2019-07-12 10:27:28] end,RESTORE_STOP_SUCCESS,0,0,0,,0,0

Press any key to continue . . .
```

RunDataIntegrityCheck.bat

This allows the user to perform data integrity check to all available backup sets. Enter the following script to export the batch file to a text editor.

```
C:\Program Files\AhsayOBM\bin>notepad RunDataIntegrityCheck.bat

C:\Program Files\AhsayOBM\bin>
```

To perform a data integrity check, the following parameters must be set first:

- **SETTING_HOME** *(Optional)*– this is the directory to your setting home. This is where the log files will be located. If not set, the directory will be "C:\Users\USER\.obm" by default

  e.g. *SET SETTING_HOME="C:\Users\John\.obm"*

- **BACKUP_SET** – this is the backup set which you would like to run a data integrity check on. If the backup set name is not in English, use the backup set ID.

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

  You can leave this parameter blank if you only have one (1) backup set.

  e.g. *SET BACKUP_SET=""*

- **BACKUP_DEST** – this is the destination of the backup set which you will run a data integrity check on. If the destination is not in English, use the destination ID.

  e.g. *SET BACKUP_DEST="Destination-1"*
  or *SET BACKUP_DEST="1740107119083"*

  This parameter can be left blank if you have a single destination.

  e.g. *SET BACKUP_DEST=""*

  This parameter will be ignored if the *BACKUP_SET* is set to *"ALL".*

  e.g. *SET BACKUP_SET="ALL"*

- **CRC_MODE** – when enabled, a Cyclic Redundancy Check (CRC) will run during the data integrity check.

  e.g. *SET CRC_MODE="ENABLE-CRC"*
  SET CRC_MODE="DISABLE-CRC"

```
@ECHO OFF

REM ######################  RunDataIntegrityCheck.bat ################
REM # You can use this batch to run any of your backup sets from the
REM # command line. Just customize the "User Defined Section" below with
REM # your values for your backup action.
REM ##############################################################
REM ####################  START: User Defined Section  #############
REM ------------------------  SETTING_HOME (Optional)  -----------------
```

```
REM | Directory to your setting home. Default to
REM | "C:\Users\USER\.obm" when not set.
REM | e.g. SET SETTING_HOME="C:\Users\John\.obm"
REM ------------------------------------------------------------------
SET SETTING_HOME=""
REM ------------------------------  BACKUP_SET  ----------------------
REM | The name or ID of the backup set that you want to run.
REM | If backup set name is not in English, please use ID instead.
REM | e.g. SET BACKUP_SET="1119083740107"
REM |  or  SET BACKUP_SET="FileBackupSet-1"
REM | You can use "ALL" to run data integrity check for all backup sets.
REM | i.e. SET BACKUP_SET="ALL"
REM |
REM | You can leave this parameter blank if you have only 1 backup set.
REM ------------------------------------------------------------------
SET BACKUP_SET="Data Backup"
REM ----------------------------  BACKUP_DEST  ----------------------
REM | The name or ID of the backup destination that you want to run.
REM | If backup destination name is not in English, please use ID
REM | instead. e.g. SET BACKUP_DEST="1740107119083"
REM |  or  SET BACKUP_DEST="Destination-1"
REM | You can use "ALL" to run data integrity check for all
REM | destinations. i.e. SET BACKUP_DEST="ALL"
REM |
REM | You can leave this parameter blank if you have only 1 destination.
REM | Remark: This option is ignored if BACKUP_SET="ALL"
REM ------------------------------------------------------------------
SET BACKUP_DEST=""
REM -------------------------------  CRC_MODE  ----------------------
REM | You can run Cyclic Redundancy Check (CRC) during data integrity
REM | check
REM | Options available: ENABLE-CRC/DISABLE-CRC
REM | i.e. SET CRC_MODE="ENABLE-CRC"
REM |  or  SET CRC_MODE="DISABLE-CRC"
REM ------------------------------------------------------------------
SET CRC_MODE="DISABLE-CRC"
REM ######################  END: User Defined Section ################
SET APP_HOME=..
SET JAVA_HOME=%APP_HOME%\jvm
SET JAVA_EXE=%JAVA_HOME%\bin\bJW.exe
SET JAVA_LIB_PATH=-Djava.library.path=%APP_HOME%\bin
SET PATH=%JAVA_HOME%\bin;%PATH%
SET CLASSPATH=%APP_HOME%\bin;%APP_HOME%\bin\cb.jar
IF "%PROCESSOR_ARCHITECTURE%"=="x86" (
  SET "DEP_LIB_PATH=X86"
  SET JAVA_OPTS=-Xms128m -Xmx768m -XX:MaxDirectMemorySize=512m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
) ELSE (

  SET "DEP_LIB_PATH=X64"
  SET JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true
)
```

```
SET PATH=%CD%\%APP_HOME%\bin\%DEP_LIB_PATH%;%PATH%
REM ################################################################
ECHO -
ECHO APP_HOME=%APP_HOME%
ECHO SETTING_HOME=%SETTING_HOME%
ECHO JAVA_HOME=%JAVA_HOME%
ECHO JAVA_EXE=%JAVA_EXE%
ECHO JAVA_OPTS=%JAVA_OPTS%
ECHO JAVA_LIB_PATH=%JAVA_LIB_PATH%
ECHO PATH=%PATH%
ECHO CLASSPATH=%CLASSPATH%
ECHO -
ECHO Running data integrity check for backup set - '%BACKUP_SET%',
destination - '%BACKUP_DEST%' ...

@ECHO ON

%JAVA_EXE% %JAVA_LIB_PATH% -cp %CLASSPATH% %JAVA_OPTS%
RunDataIntegrityCheck %APP_HOME% %SETTING_HOME% %BACKUP_SET%
%BACKUP_DEST% %CRC_MODE% %REBUILD_MODE%
@ECHO OFF
CD %APP_HOME%
IF "%APP_HOME%"==".." PAUSE

@ECHO ON
```

Save the changes and close the text editor. Proceed back to *cmd* and enter the following script.

```
C:\Program Files\AhsayOBM\bin>RunDataIntegrityCheck.bat

-

APP_HOME=..

SETTING_HOME=""

JAVA_HOME=..\jvm

JAVA_EXE=..\jvm\bin\bJW.exe

JAVA_OPTS=-Xms128m -Xmx2048m -XX:MaxDirectMemorySize=1024m -
Dsun.java2d.noddraw -Dsun.nio.PageAlignDirectMemory=true

JAVA_LIB_PATH=-Djava.library.path=..\bin PATH=C:\Program Files\AhsayOBM
\bin\..\bin\X64;..\jvm\bin;C:\Program Files (x86)\Common Files\Oracle
\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C
:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files\Microsoft
SQL Server\Client SDK\ODBC\110\Tools\Binn\;C:\Program Files
(x86)\Microsoft SQL Server\120\Tools\Binn\;C:\Program Files\Microsoft
SQL Server\120\Tools\Binn\;C:\Program Files\Microsoft SQL
Server\120\DTS\Binn\;C:\Program
Files\PuTTY\CLASSPATH=..\bin;..\bin\cb.jar

-
```

```
Running data integrity check for backup set - '"Data Backup"',
destination - '""' ...

C:\Program Files\AhsayOBM\bin>..\jvm\bin\bJW.exe -
Djava.library.path=..\bin -cp ..\bin;..\bin\cb.jar -Xms128m -Xmx2048m -
XX:MaxDirectMemorySize=1024m -Dsun.java2d.noddraw -
Dsun.nio.PageAlignDirectMemory=true RunDataIntegrityCheck .. "" "Data
Backup" "" "DISABLE-CRC" "DISABLE-REBUILD"

[doInfo] Start [ AhsayOBM v8.2.1.18 ]

[doStart] Start data integrity check on backup set "Data
Backup(1562897045523)", "AhsayCBS(1562897364604)", crc disabled, rebuild
index disabled

[doDetail] Start processing data integrity check on backup set= "Data
Backup" destination= "AhsayCBS"

[doLogProgress] Start processing data integrity check on backup set=
"Data Backup" destination= "AhsayCBS"

[doLogProgress] Browsing "/files/1562897045523"

[doLogProgress] Browsing "1562897045523/blocks/2019-07-12-10-09-33"

[doLogProgress] Browsing "1562897045523/blocks/2019-07-12-10-09-33/0"

[doLogProgress] Processing Job "2019-07-12-10-09-33", ""

[doLogProgress] Processing Job "Current", ""

[doLogProgress] Processing Job "Current", "C:"

[doLogProgress] Processing Job "Current", "C:/Users"

[doLogProgress] Processing Job "Current", "C:/Users/Administrator"

[doLogProgress] Processing Job "Current",
"C:/Users/Administrator/Desktop"

[doLogProgress] Processing Job "Current",
"C:/Users/Administrator/Desktop/Data backup"

[doLogProgress] Checking dangling backup file index entries...

[doInfo] Existing statistics of backup set= "Data Backup" destination=
"AhsayCBS": Data area compressed size: 32B, Data area uncompressed size:
0B, Data area file count: 2, Retention area compressed size: 0B,
Retention area uncompressed size: 0B, Retention area file count: 0

[doInfo] Recalculated statistics of backup set= "Data Backup"
destination= "AhsayCBS": Data area compressed size: 32B, Data area
uncompressed size: 0B, Data area file count: 2, Retention area
compressed size: 0B, Retention area uncompressed size: 0B, Retention
area file count: 0
```

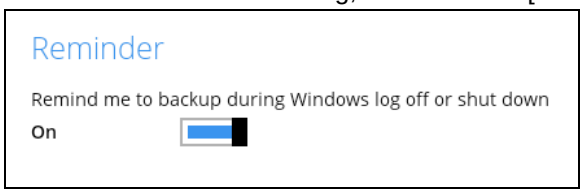
```
[doInfo] The statistics of backup set= "Data Backup" destination=
"AhsayCBS" is correct.

[doLogProgress] Saving encrypted backup file index to
1562897045523/blocks at destination AhsayCBS...

[doInfo] Saving encrypted backup file index to 1562897045523/blocks at
destination AhsayCBS...

[doDetail] Data integrity check on backup set= "Data Backup"
destination= "AhsayCBS" is completed

[doLogProgress] Data integrity check on backup set= "Data Backup"
destination= "AhsayCBS" is completed

[doEnd][INFO] Finished data integrity check on backup set "Data
Backup(1562897045523)", "AhsayCBS(1562897364604)", crc disabled, rebuild
index disabled

[doInfo] Completed data integrity check on backup set "Data
Backup(1562897045523)", "AhsayCBS(1562897364604)", crc disabled, rebuild
index disabled

Press any key to continue . . .
```

Appendix D: Example Scenarios for the Reminder

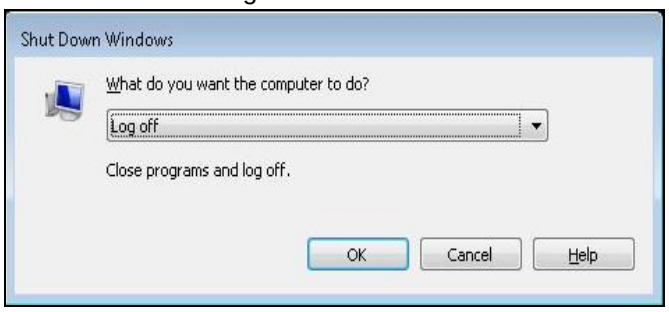
Windows Log Off

The following example shows when the user performs Windows Log off with the Reminder setting turned on.

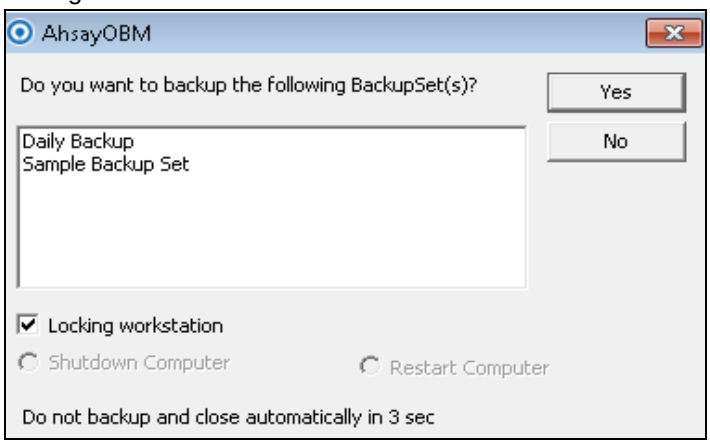
1. Turn on the Reminder setting, then click the [Save] button.



2. Perform Windows logoff.



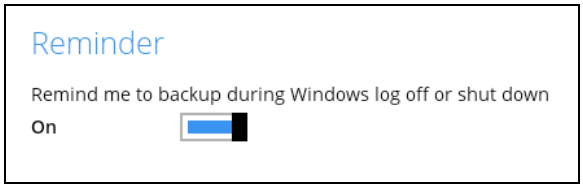
3. A dialog box will prompt the user to back up all the backup sets with enabled 'Reminder' setting.



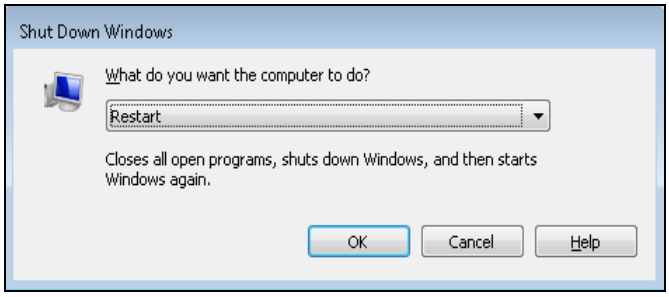
Windows Restart

The following example shows when the user performs Windows restart with the Reminder setting turned on.

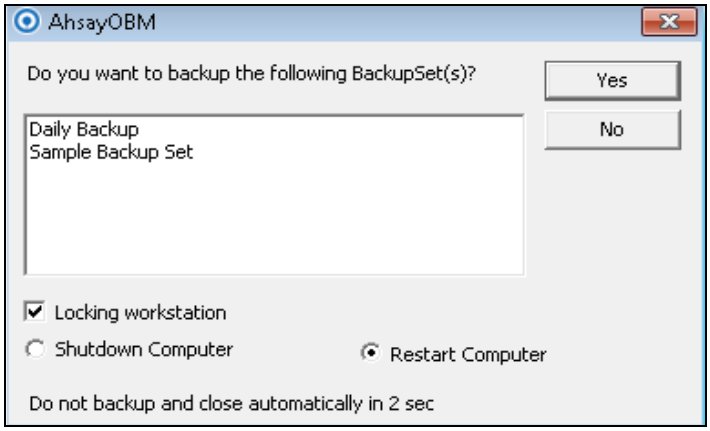
1. Turn on the Reminder setting, then click the [Save] button.



2. Perform Windows restart.



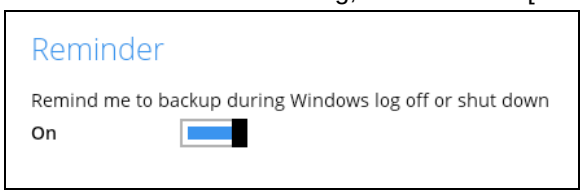
3. A dialog box will prompt the user to back up all the backup sets with enabled 'Reminder' setting.



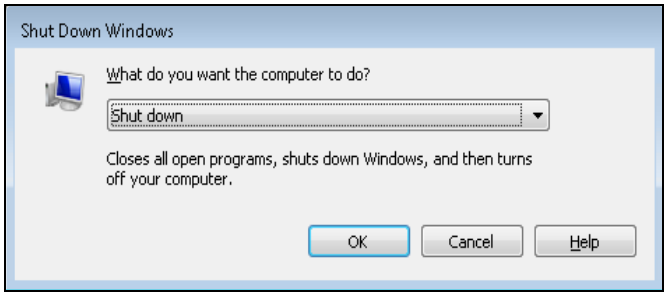
Windows Shutdown

The following example shows when the user performs Windows shutdown with the Reminder setting turned on.

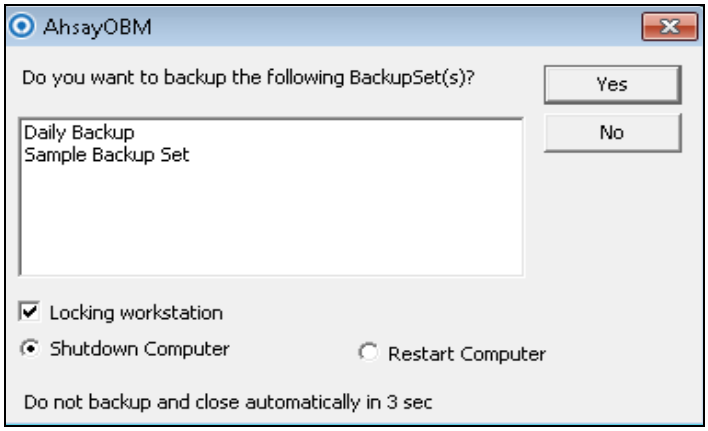
1. Turn on the Reminder setting, then click the [Save] button.



2. Perform Windows shutdown.



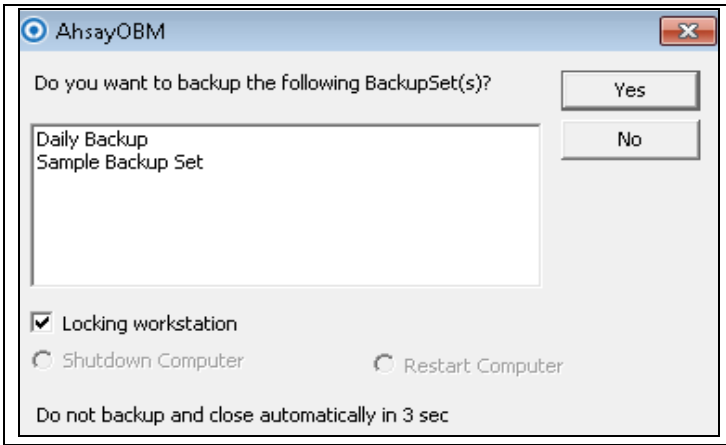
3. A dialog box will prompt the user to back up all the backup sets with enabled 'Reminder' setting.



Below is the list of example scenarios with complex settings:

Scenario 1 (Windows Log Off + Enabled Locking Workstation)

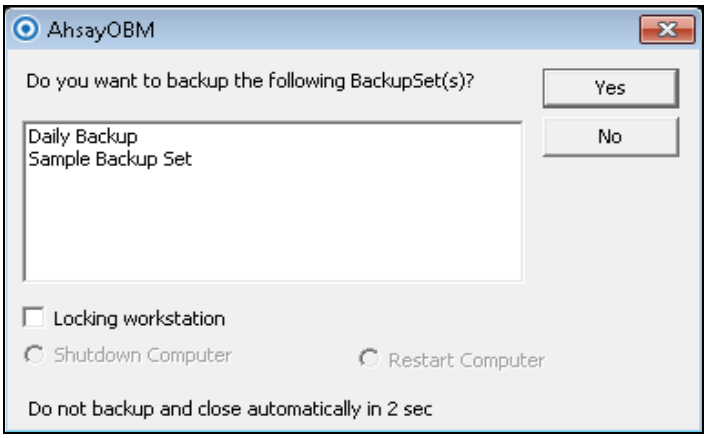
The following scenario shows when the user performs Windows logoff with the Reminder setting turned on, and Locking Workstation enabled.

<table>
<tr>
<td rowspan="2"> 
</td>
<td>[Yes] – If Yes is selected, then the Windows will be locked, and the displayed backup sets will start backing up in the background. Once all the backup jobs are completed, the machine will log off automatically even if Windows is still on lock.</td>
</tr>
<tr>
<td>[No] – If No is selected, then no backup job will run, and the machine will proceed to log off.</td>
</tr>
</table>

NOTE
The machine will log off after four (4) seconds if no action is selected.

Scenario 2 (Windows Log Off + Unselected Locking Workstation)

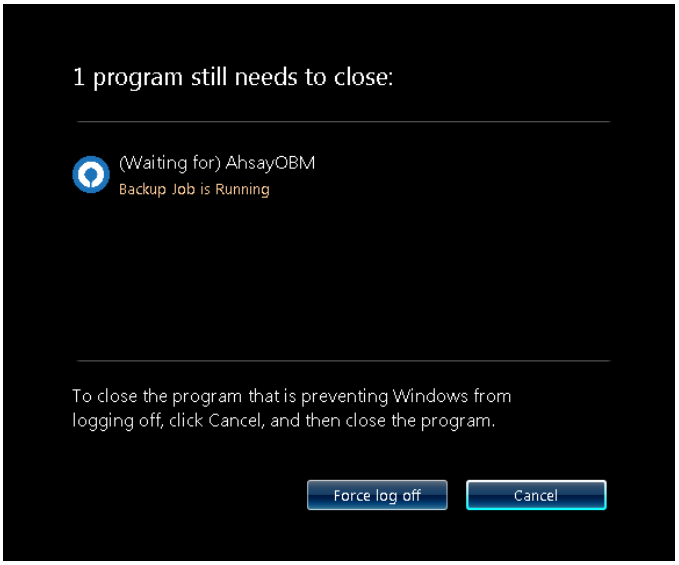
The following scenario shows when the user performs Windows logoff with the Reminder setting turned on, and Locking Workstation unselected.



[Yes] – If Yes is selected, an alert message will be displayed to inform the user that a backup job is still running which prevents Windows from logging off.

[No] – If No is selected, then no backup job will run, and the machine will proceed logging off.

Clicking the **[Yes]** button will result to the following screen:

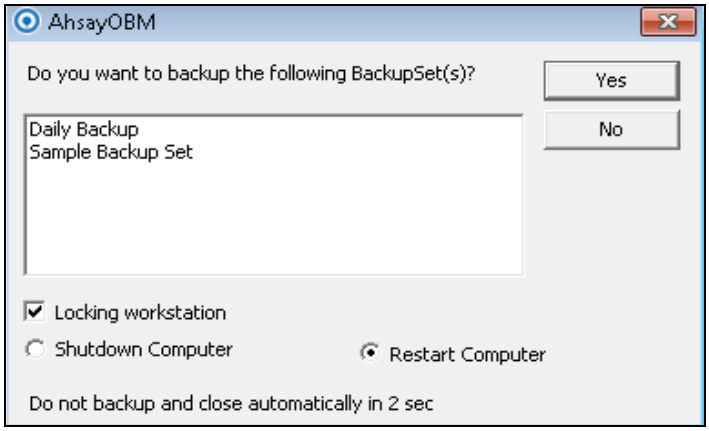


[Force log off] – If you choose to force log off the machine, the backup job will not push through, then the machine will log off immediately.

[Cancel] – If Cancel is selected, the backup job will run in the background. Once all the backup jobs are completed, the machine will log off automatically.

Scenario 3 (Windows Restart + Enabled Locking Workstation)

The following scenario shows when the user performs Windows restart with the Reminder setting turned on, and Locking Workstation enabled.



[Yes] – If Yes is selected, then the Windows will be locked, and the displayed backup sets will start backing up in the background. Once all the backup jobs are completed, the machine will restart automatically even if the Windows is still on lock.

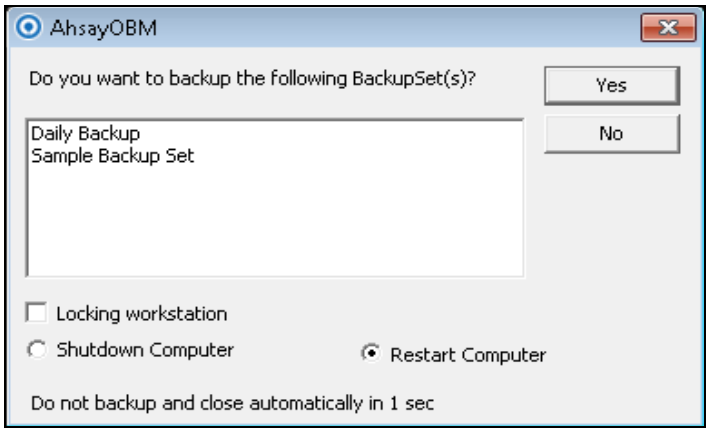
[No] – If No is selected, then no backup job will run, and the machine will restart immediately.

NOTE

1. You can select the 'Shutdown Computer' from the options in the dialog box, but the machine will still follow the action that you perform from the Windows, which is 'restart'. The machine will reboot once all the backup jobs are completed.
2. The machine will restart after four (4) seconds if no action is selected.

Scenario 4 (Windows Restart + Unselected Locking Workstation)

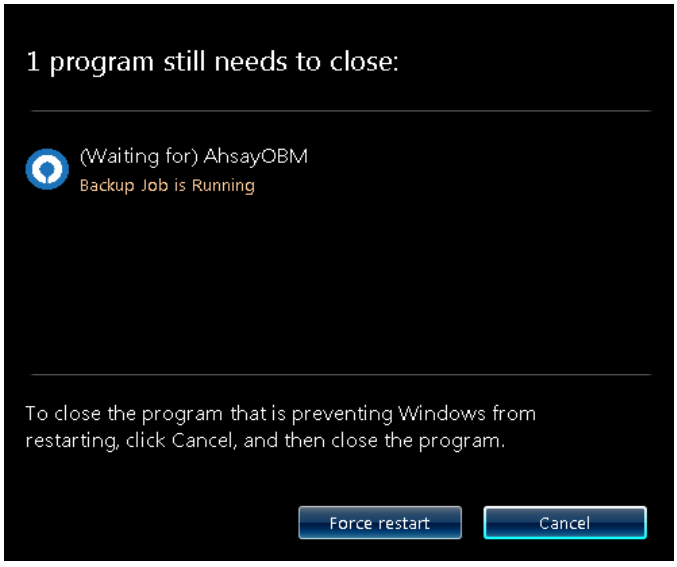
The following scenario shows when the user performs Windows restart with the Reminder setting turned on, and Locking Workstation unselected.



[Yes] – If Yes is selected, an alert message will be displayed to inform the user that a backup job is still running which prevents Windows from restarting.

[No] – If No is selected, then no backup job will run, and the machine will restart immediately.

Clicking the **[Yes]** button will result to the following screen:

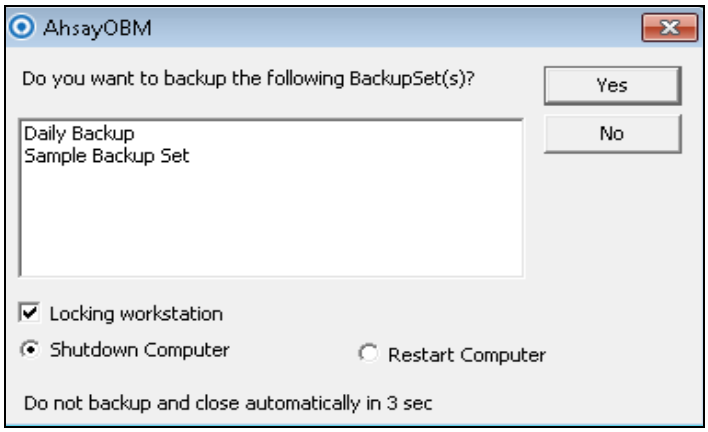


[Force restart] – If you choose to force restart the machine, the backup job will not push through, then the machine will restart immediately.

[Cancel] – If Cancel is selected, the backup job will run in the background. Once all the backup jobs are completed, the machine will restart automatically.

Scenario 5 (Windows Shutdown + Enabled Locking Workstation)

The following scenario shows when the user performs Windows shutdown with the Reminder setting turned on, and Locking Workstation enabled.



[Yes] – If Yes is selected, then the Windows will be locked, and the displayed backup sets will start backing up in the background. Once all the backup jobs are completed, the machine will shut down automatically even if the Windows is still on lock.

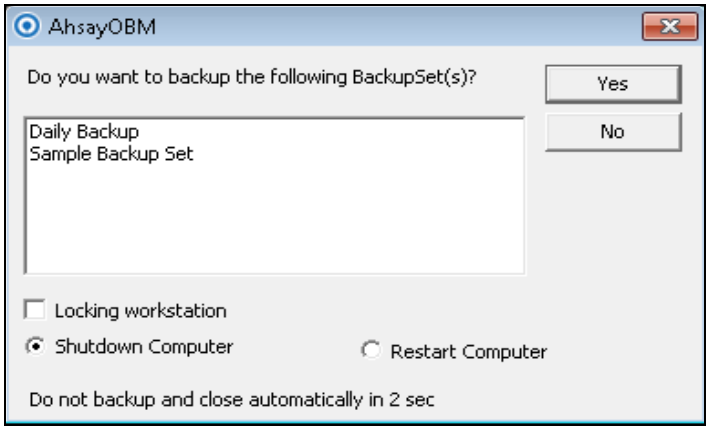
[No] – If No is selected, then no backup job will run, and the machine will shut down immediately.

NOTE

1. You can select the 'Restart Computer' from the options in the dialog box, but the machine will still follow the action that you perform from the Windows, which is 'shutdown'. The machine will shut down once all the backup jobs are completed.
2. The machine will shut down after four (4) seconds if no action is selected.

Scenario 6 (Windows Shutdown + Unselected Locking Workstation)

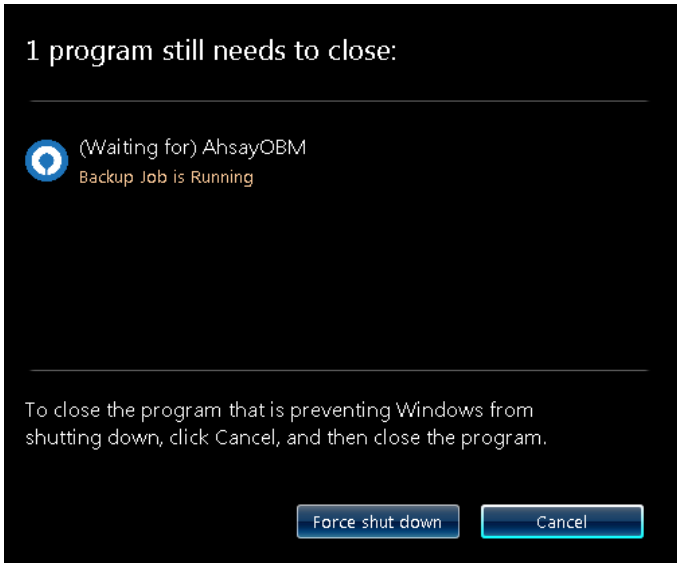
The following scenario shows when the user performs Windows shut down with the Reminder setting turned on, and Locking Workstation unselected.



[Yes] – If Yes is selected, an alert message will be displayed to inform the user that a backup job is still running which prevents Windows from shutting down.

[No] – If No is selected, then no backup job will run, and the machine will shut down immediately.

Clicking the **[Yes]** button will result to the following screen:



[Force shut down] – If you choose to force shutdown the machine, the backup job will not push through, then the machine will shut down immediately.

[Cancel] – If Cancel is selected, the backup job will run in the background. Once all the backup jobs are completed, the machine will shut down automatically.

Appendix E: 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:

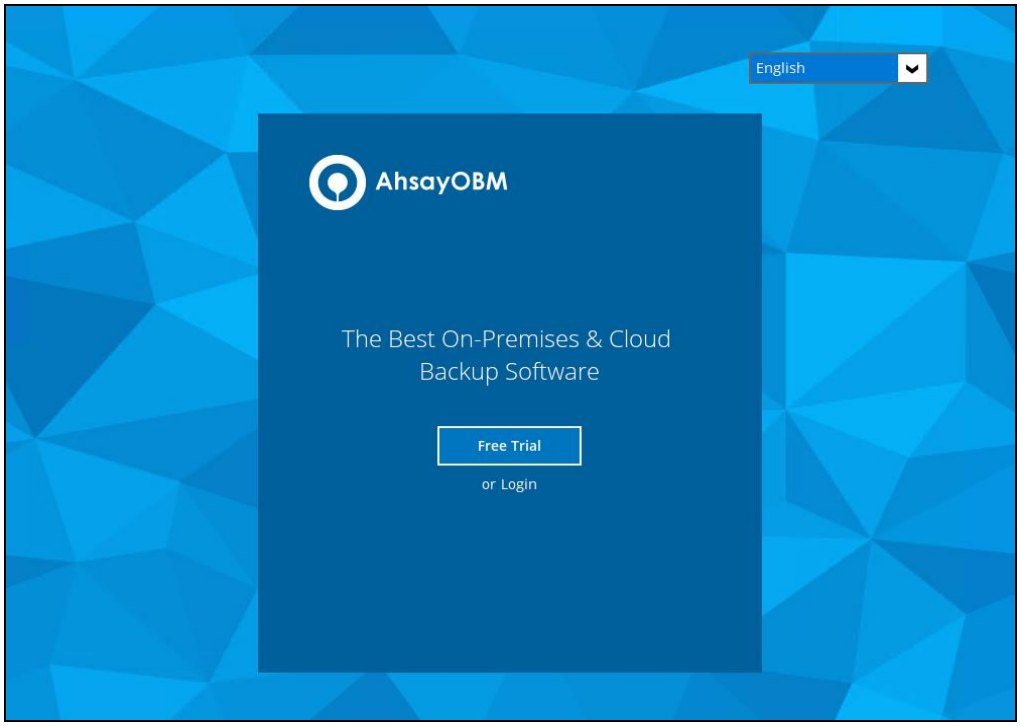
- The Free Trial registration option will only be displayed once when the user login for the first time. If you cannot create a free trial account kindly contact your backup service provider.
- Only alphanumeric characters and selected special characters, A to Z, 0 to 9, @, - and _, are allowed to be 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

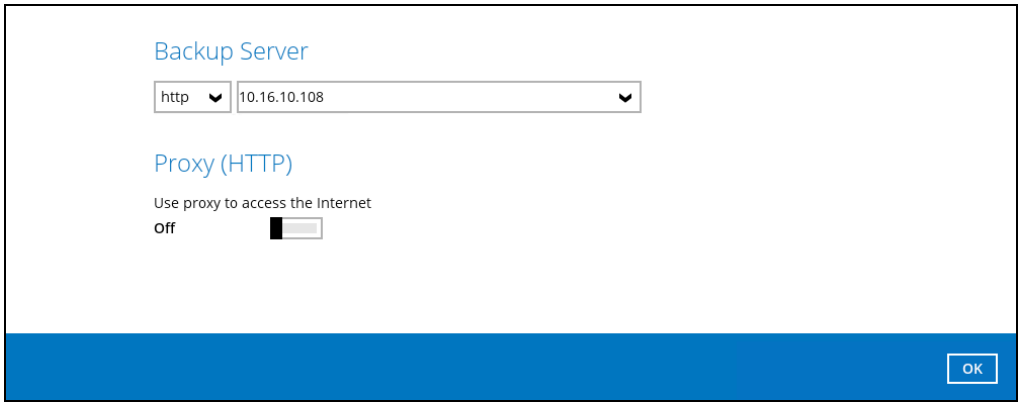
The Free Trial registration option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

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

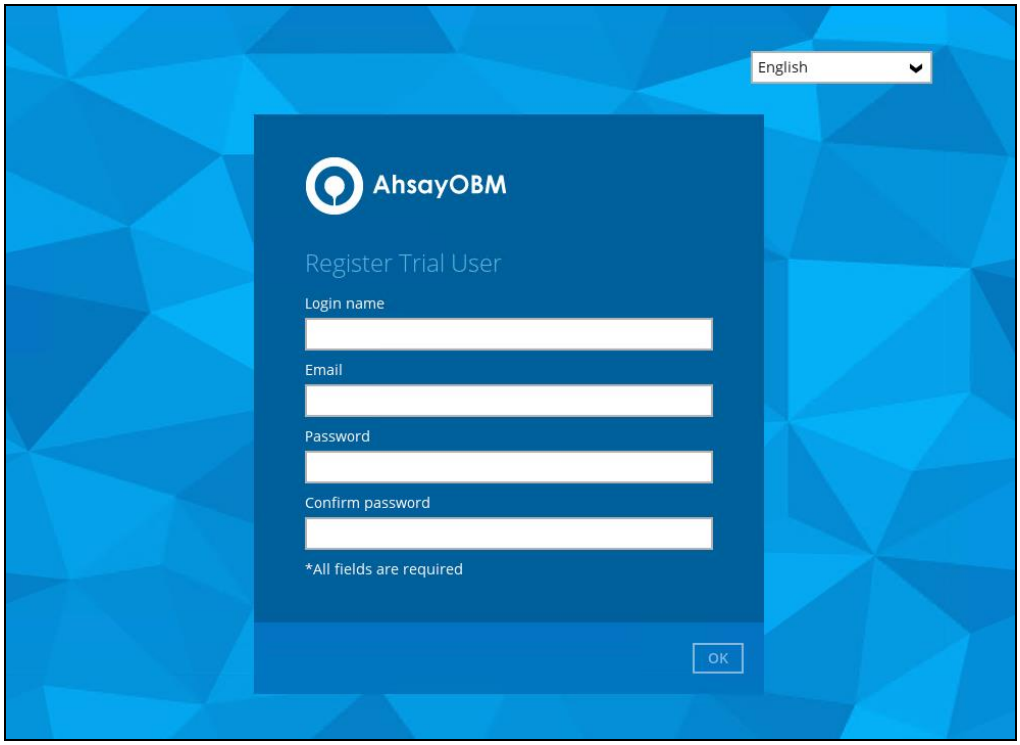
1. Click on **Free Trial**.



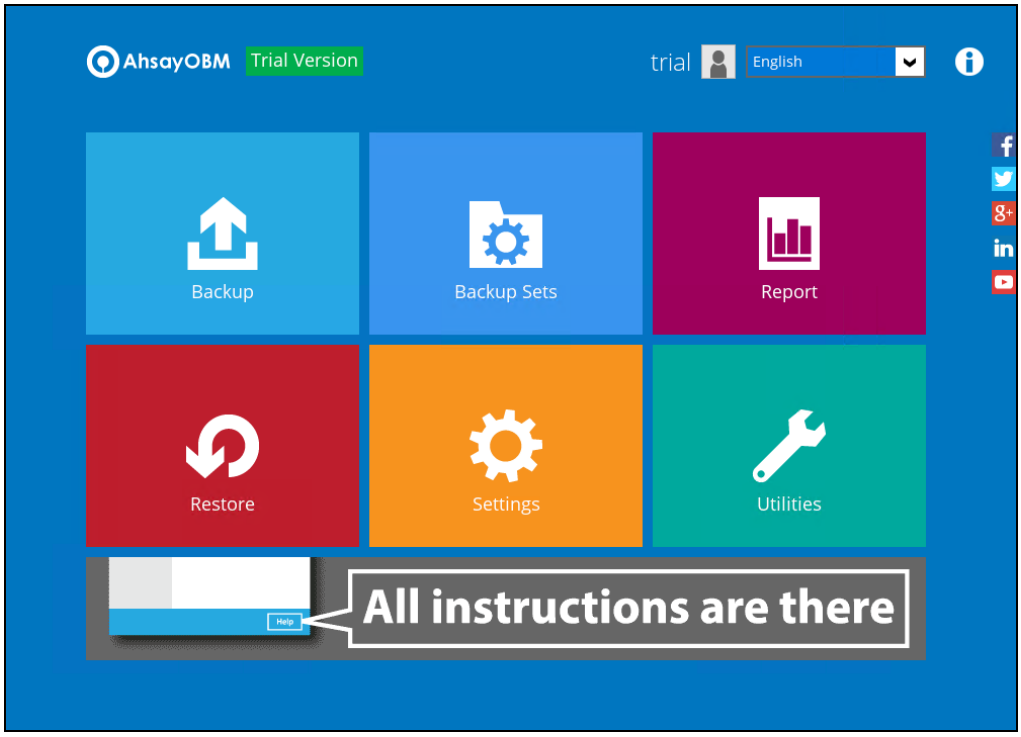
Configure your Backup Server settings.



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.



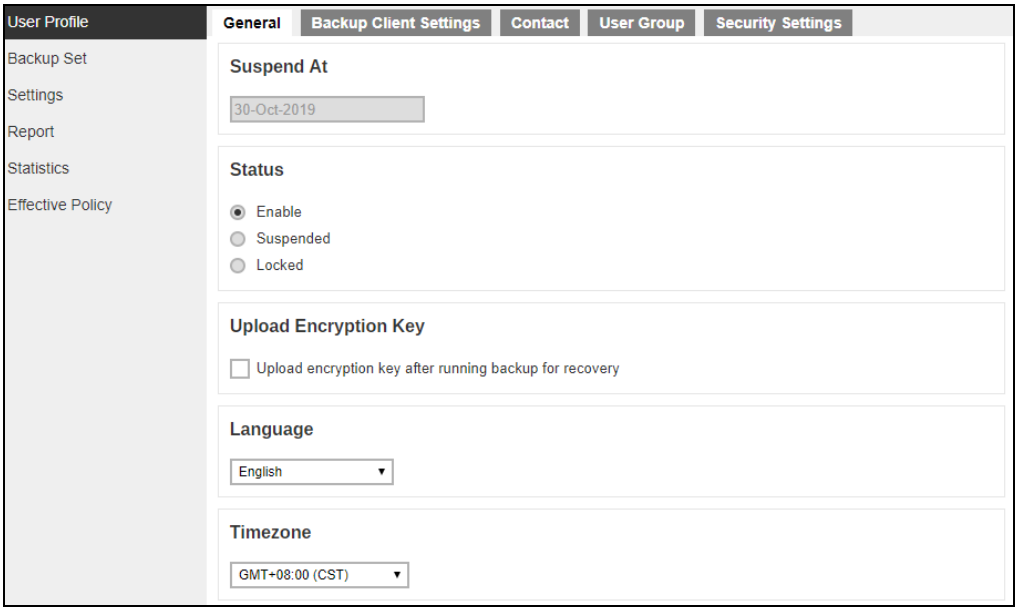
Once the trial account is created, this screen will be displayed.



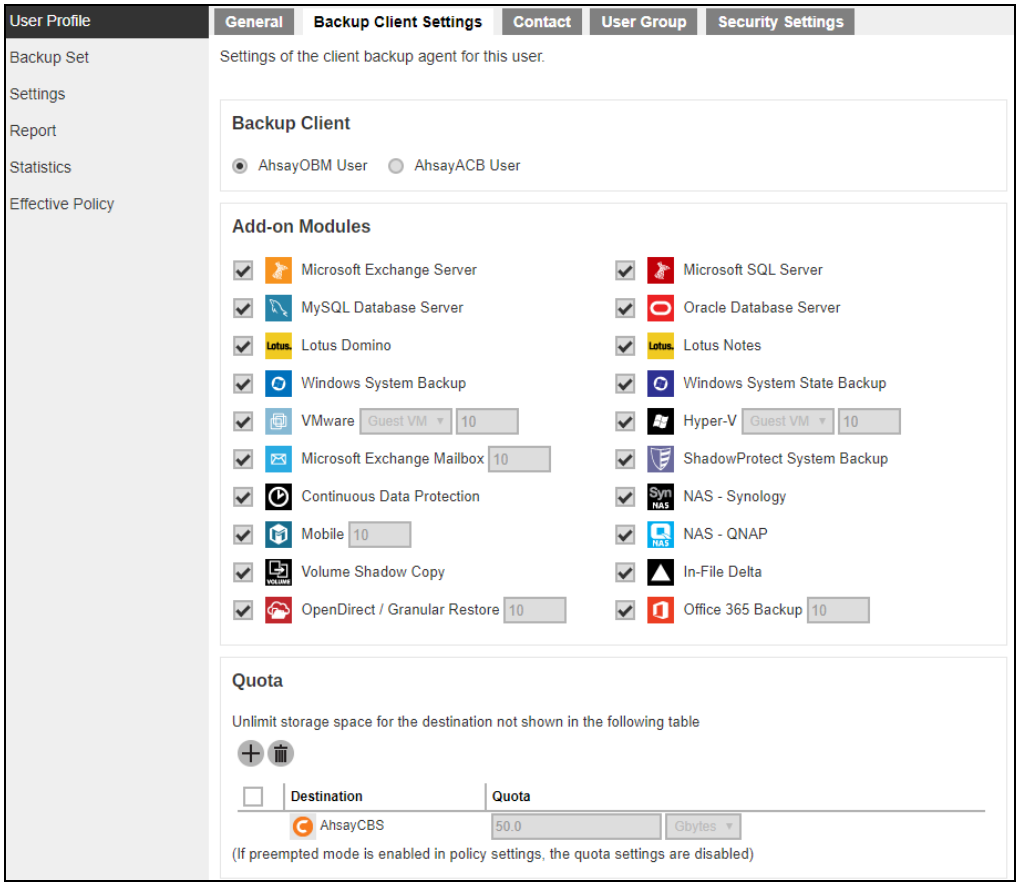
After your trial account has been created, you need to check several things:

- The expiry date of the trial account, which determines when it will be suspended.
- The Language which will be used for sending reports.
- And the Timezone, this is to ensure that your backup schedule will run at the correct time.

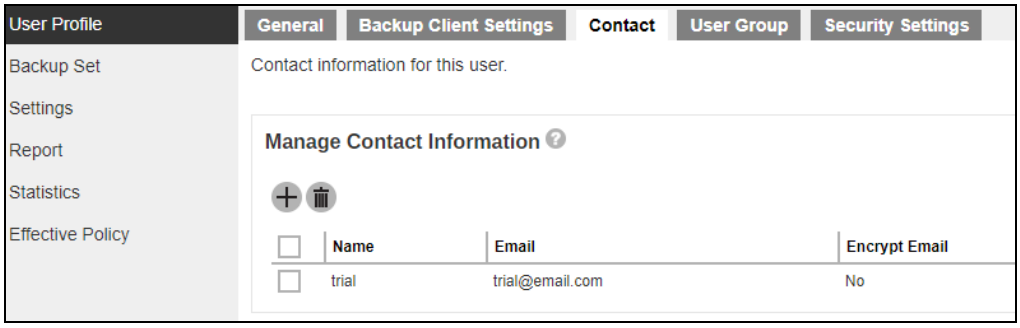
You can check this by logging in to AhsayCBS, go to **Backup / Restore > User > User Profile > General**. For more information, please refer to the AhsayCBS User's Guide.



You also need to check the available add-on modules and quota by going to the **Backup Client Settings** tab.



Lastly, you need to verify if your contact details are correct by going to the **Contact** tab. If you want to add more contact information, you can add it here.



Appendix F: How to Manage Network Drives which are not set in Windows

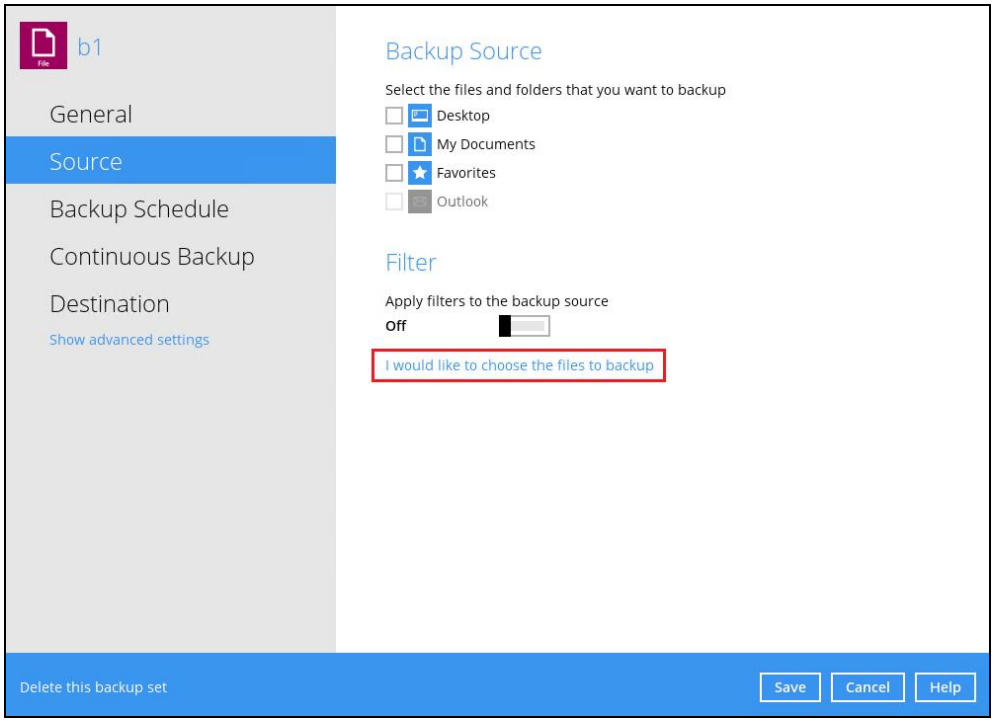
Users have several options in managing network drives that are not set up on Windows, which are the following:

- Select All – selects all the files and folders in the network drive
- Select Only – will only deselect the network drive but the file selection will remain the same.
- Deselect All – deselects all the files and folders in the network drive
- Edit Credential – allows changing the credentials of the network drive even after it has been set upon creation of the backup set.
- Delete – deletes the network drive

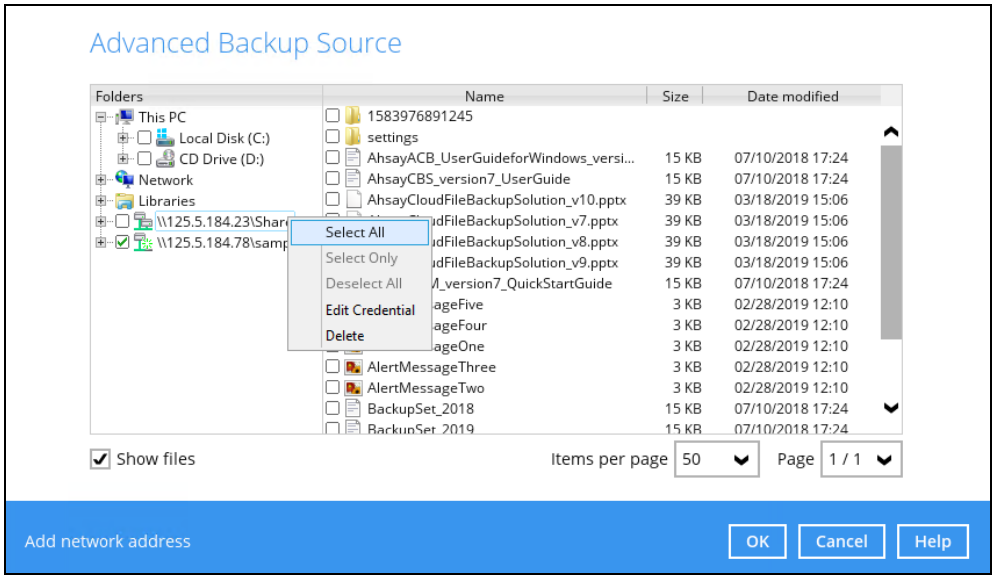
For instructions on how to use the different functions, see instructions below:

Select All

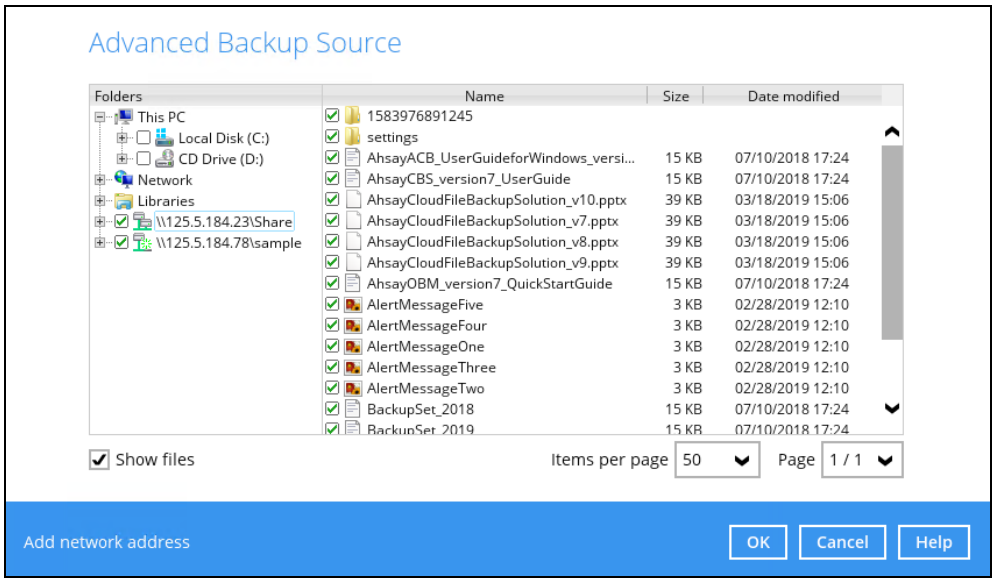
1. Go to Backup Sets, select the backup set. Select Source and click **I would like to choose the files to backup**.



2. Right-click on the network drive and select **Select All**.

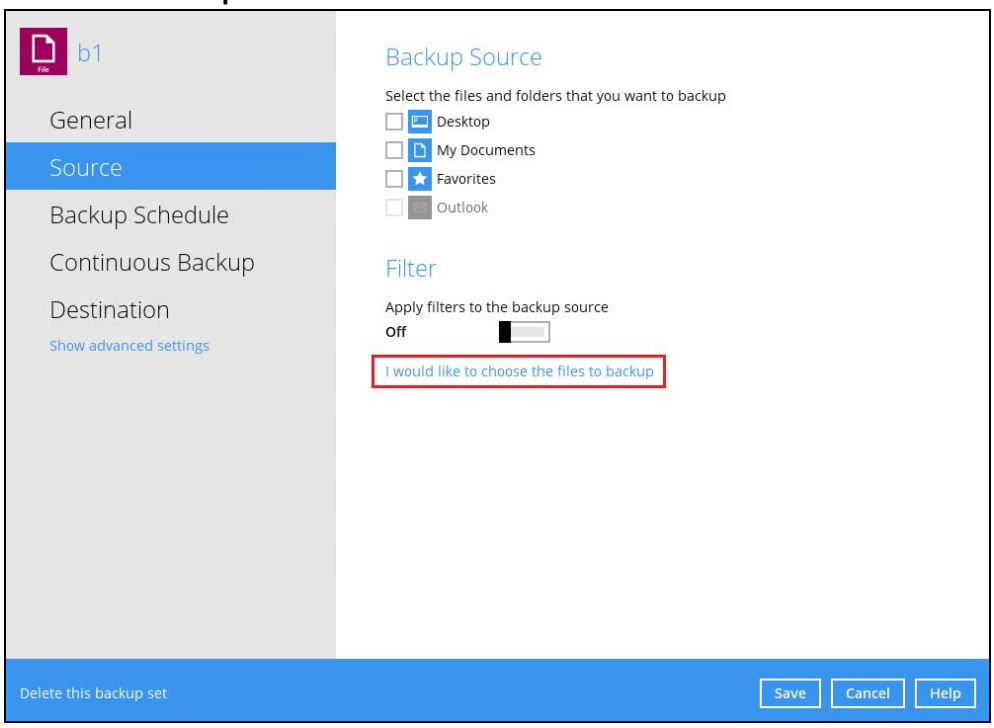


3. All the files and folders in the network drive will now be selected.

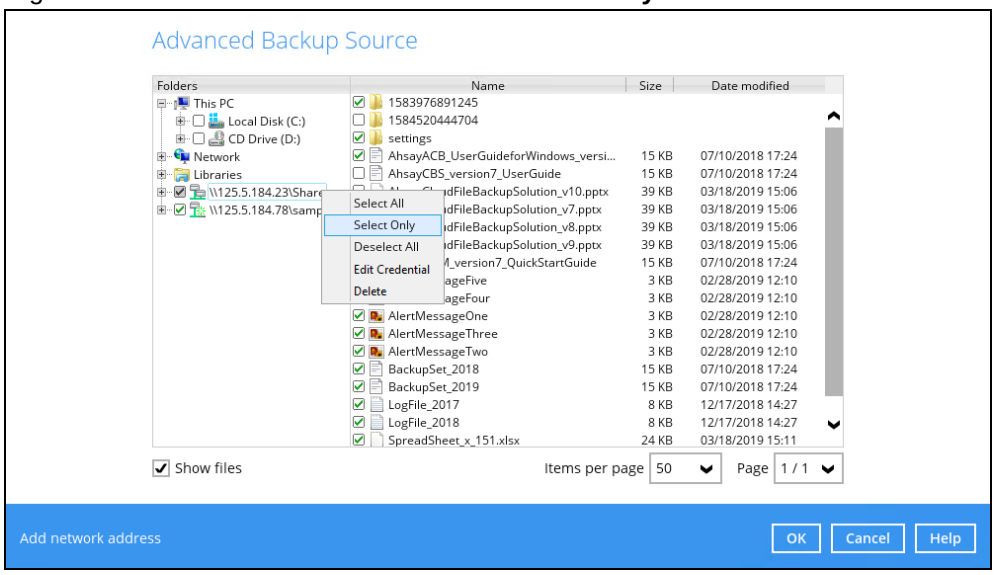


Select Only

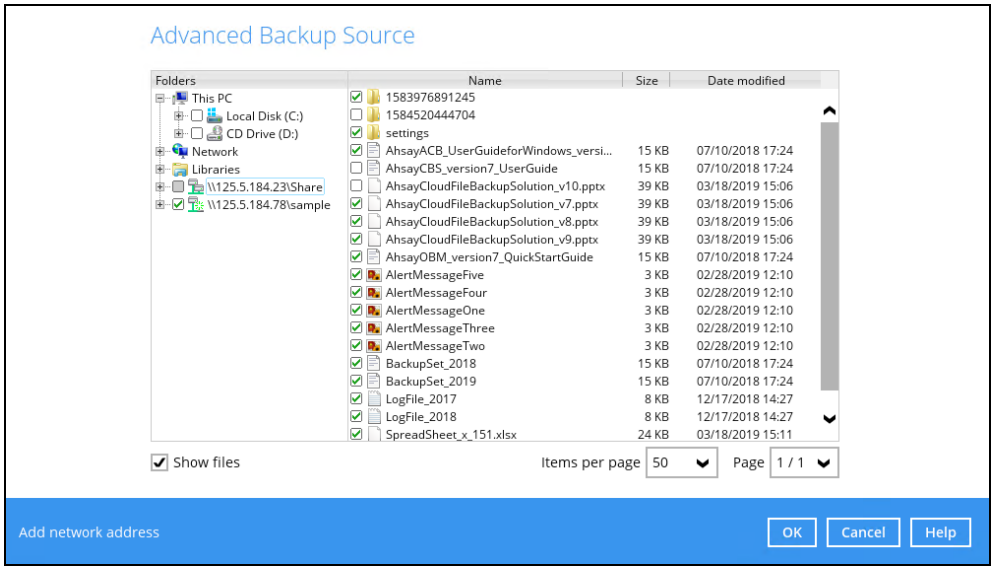
1. Go to Backup Sets, select the backup set. Select Source and click **I would like to choose the files to backup**.



2. Right-click on the network drive and select **Select Only**.

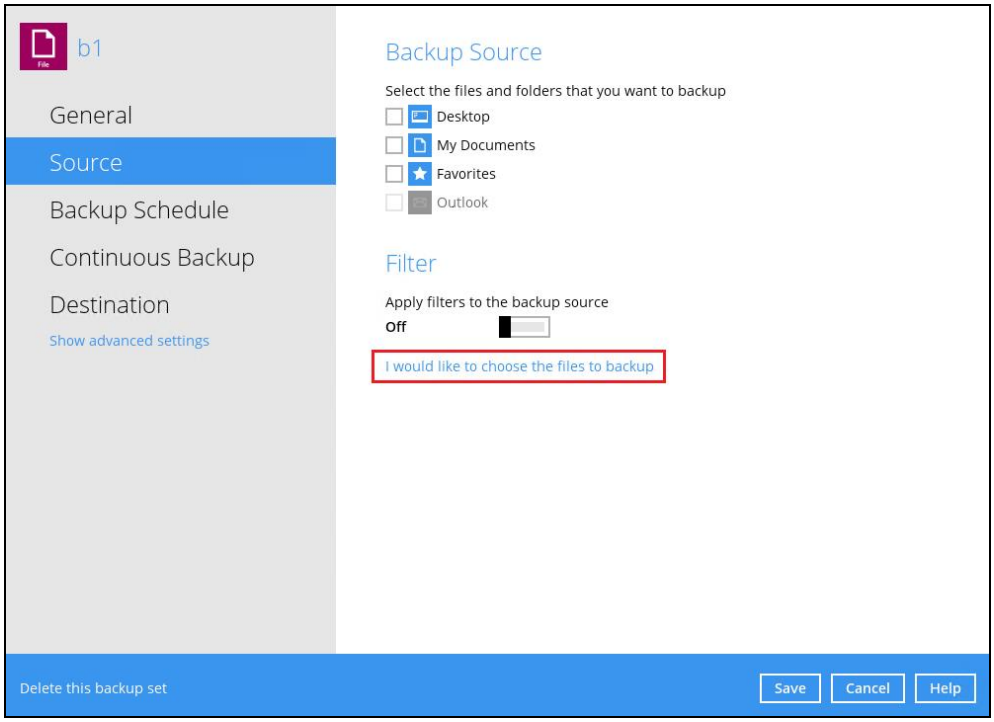


3. The network drive will now be deselected but there will be no change in the file selection.

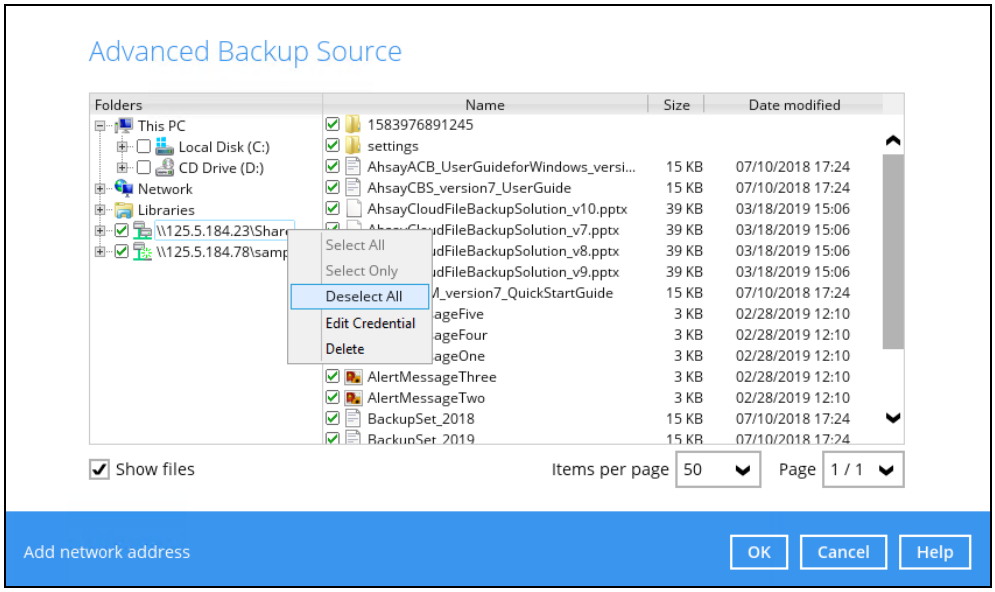


Deselect All

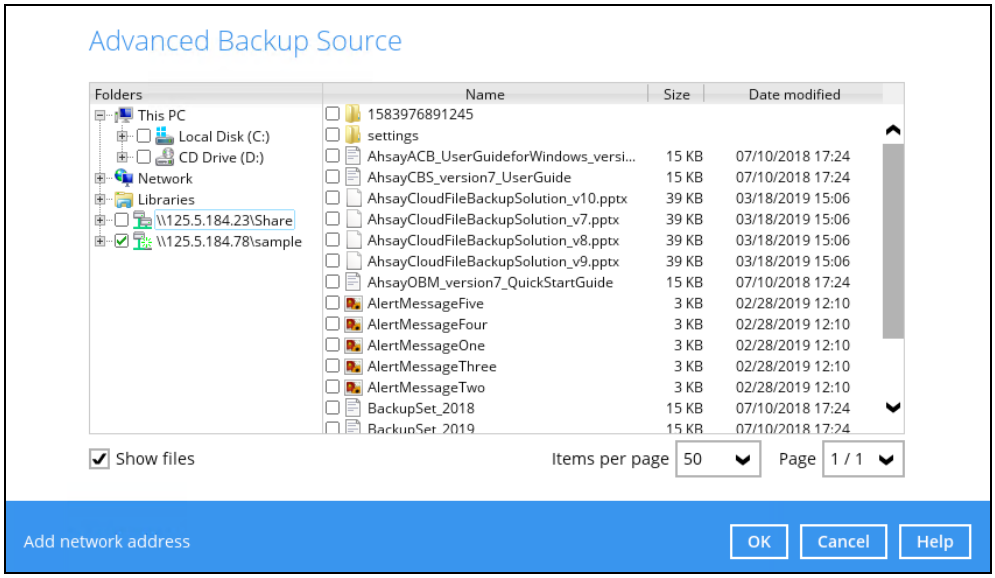
1. Go to Backup Sets, select the backup set. Select Source and click **I would like to choose the files to backup**.



2. Right-click on the network drive and select **Deselect All**.

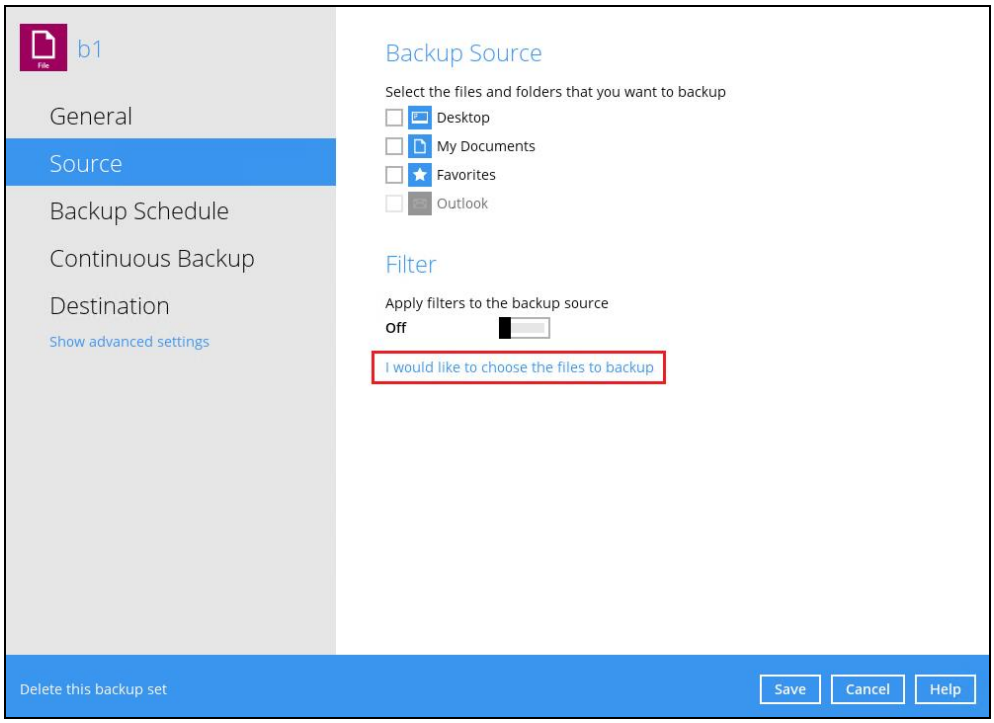


3. All the files and folders in the network drive will now be deselected.

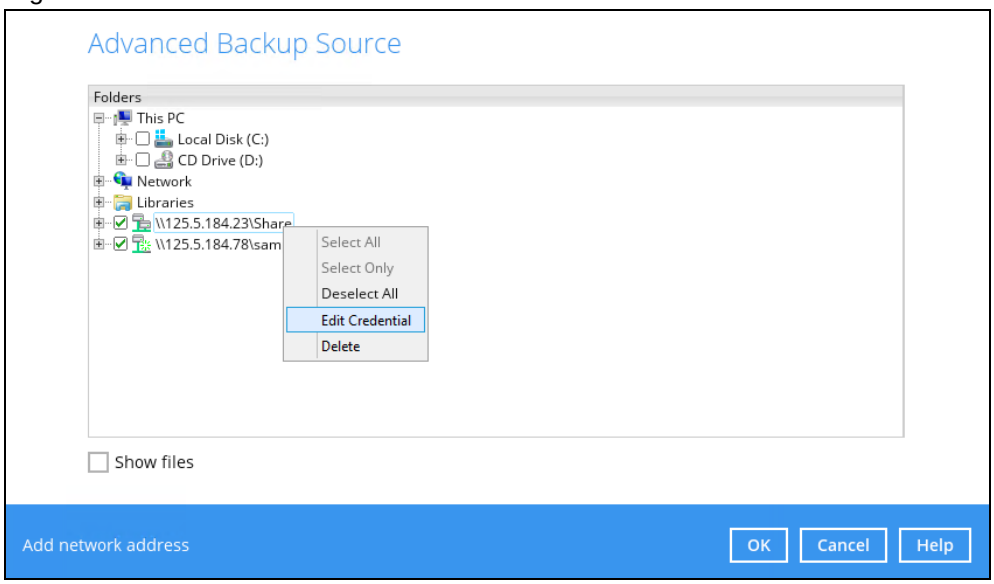


Edit Credential

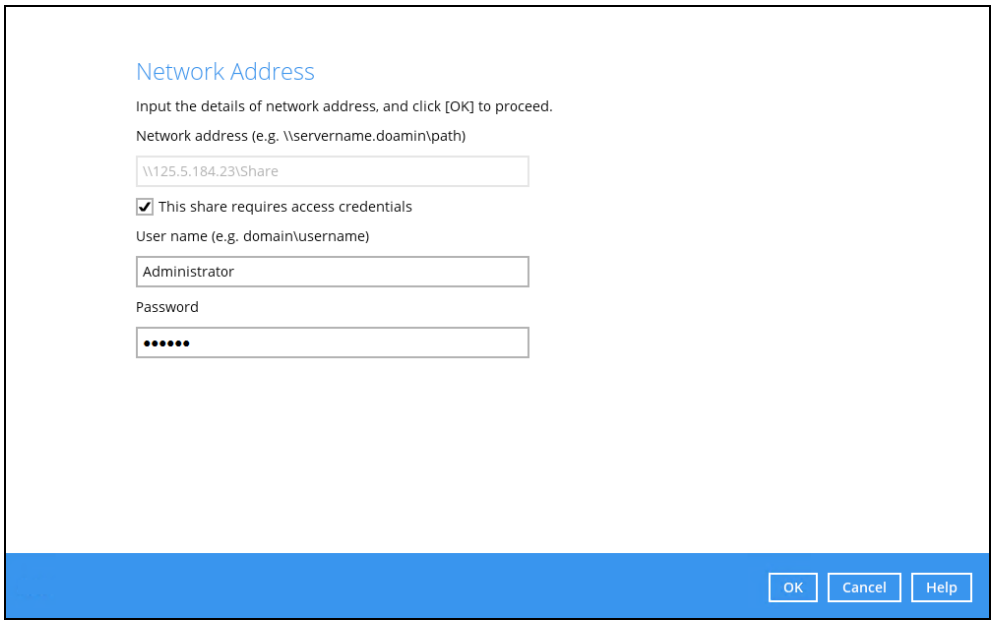
1. Go to Backup Sets, select the backup set. Select Source and click **I would like to choose the files to backup**.



2. Right-click on the network drive and select **Edit Credential**.

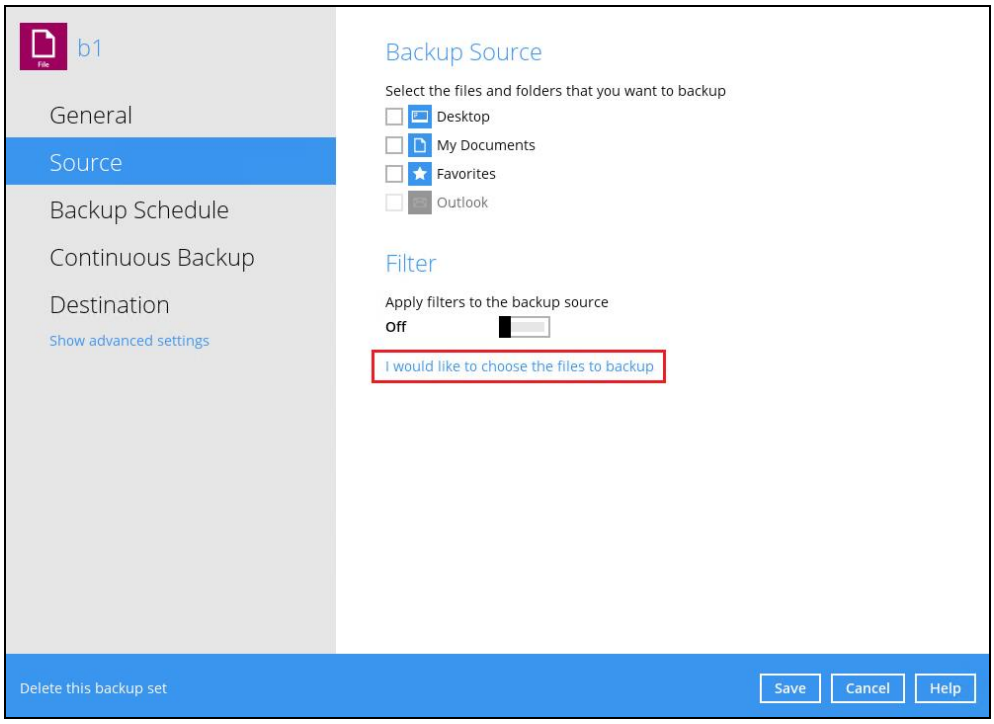


3. The Network Address window will appear, update the User name and/or Password. Click **OK** once done.

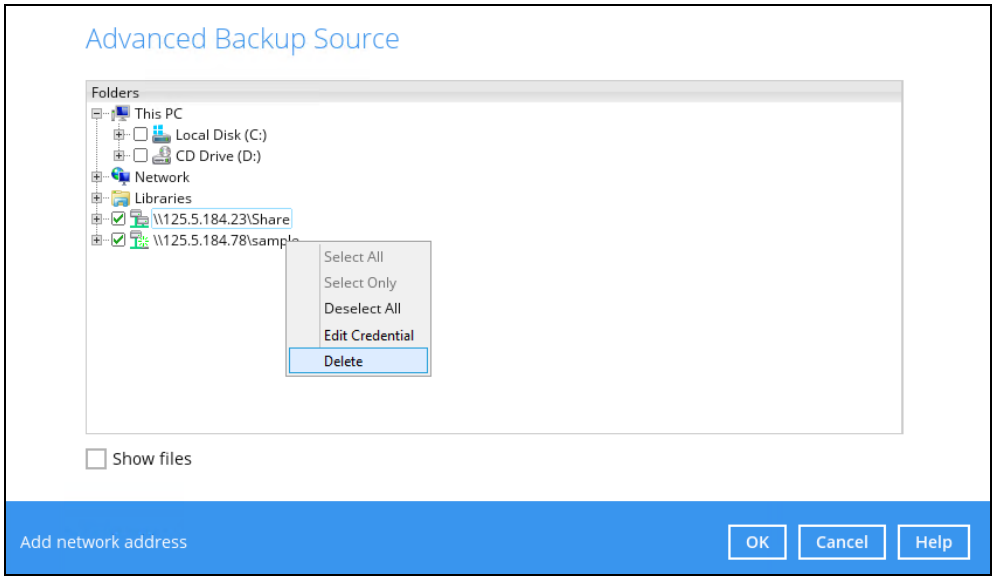
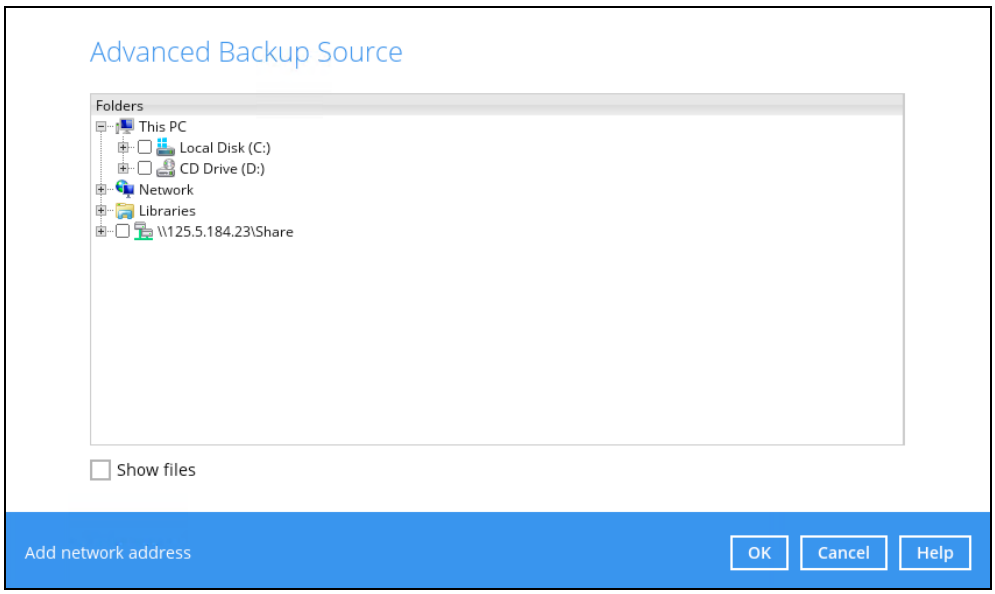


Delete

1. Go to Backup Sets, select the backup set. Select Source and click **I would like to choose the files to backup**.



2. Right-click on the network drive and select **Delete**.



3. The network drive will now be deleted.